Információ- és kiberbiztonság

Szerkesztette
Török Bernát

Fenntartható biztonság és társadalmi környezet tanulmányok V.

LUDOVIKA
EGYETEMI KIADÓ

Információ- és kiberbiztonság

Fenntartható biztonság és társadalmi környezet tanulmányok

V.

Sorozatszerkesztő
Kis Norbert – Koltay András

Információ- és kiberbiztonság

Szerkesztette

Török Bernát

LUDOVIKA
EGYETEMI KIADÓ

Budapest, 2020

Ludovika Egyetemi Kiadó Nonprofit Kft.
Székhely: 1089 Budapest, Orczy út 1.
Kapcsolat: info@ludovika.hu

A kiadásért felel: Koltay András rektor
Felelős szerkesztő: Karácsony Fanni
Olvasószerkesztő: Bíró Csilla, Bujdosó Hajnalka,
Gergely Zsuzsanna, Pokorádi Zsófia, Szarvas Melinda
Tördelőszerkesztő: Tihanyi József

Tartalom

Előszó

Könnyű helyzetben van a szerkesztő, amikor olyan tanulmánygyűjtemény elé kell előszót írnia, amely az egyéni és társadalmi életünk szempontjából egyaránt kulcsfontosságú témákat dolgoz fel. A jelen kötet ilyen írásokat fog össze. Nehezen vitatható, hogy az előttünk álló – nemcsak évek, évtizedek, hanem – korszak egyik legnagyobb stratégiai kihívása a minket körülvevő hömpölygő információáradat kordában tartása – nem abban az értelemben, hogy miként fékezzük azt le, hanem hogy miként garantáljuk biztonságos folyását, illetve hogy mi magunk miként maradjunk a felszín fölött. A kötetben szereplő tanulmányok különféle nézőpontból ugyanarról szólnak, ugyanazt hangsúlyozzák: elsődleges feladattá vált, hogy a mindent átszövő információs hálózatainkra, az egyre összetettebbé váló elektronikus és online tereinkre, valamint a folyton-folyvást fejlődő új technológiákra ne az öncélú technikai haladás termékeiként tekintsünk, hanem életünk kibontakoztatásának szolgálatába állítsuk őket.

Napjaink társadalmát információs társadalomnak szokás nevezni. A kifejezés abban a tekintetben mindenképpen jól ragadja meg a társadalmi-gazdasági folyamatok ismertetőjegyét, hogy egyéni és közösségi életünkben is meghatározó szerepet játszik a rendelkezésre álló információknak az a bősége, amelyet az egyre terjedő digitalizáció termel. Újabb és újabb technológiák és eszközök működésének válik lényegévé a nagyvilág, illetve személyes világunk valamennyi részletének rögzítése digitalizált adat formájában, hogy aztán e rögzített adatokat a maguk funkciója szerint rendszerezzék, felhasználják. „Az adat az új olaj” – szól napjaink egyik mottója, utalva arra, hogy az információ, az adat tekinthető az új technológiai és gazdasági folyamatok legfőbb mozgatójának, legújabb műszaki vívmányaink legértékesebb nyersanyagának.

A minden korábbinál szédületesebb tempóban zajló technológiai fejlődés páratlan lehetőségeket hozott, az emberi élet megszervezésének minden eddiginél tudatosabb és hatékonyabb módszereivel kecsegtet. Mára azonban az is napnál világosabbá vált, hogy nem a Kánaán érkezett el hozzánk, hanem olyan új lehetőségek nyíltak meg, amelyek új kockázatokat is jelentenek, sok esetben ráadásul az előnyökkel már-már vetekedő kockázatokat. Ahhoz, hogy az emberi tudás által életre hívott potenciált biztonságosan a magunk javára tudjuk fordítani, a társadalom egészének odafigyelésére és munkájára van szükség. Korunk egyik legnagyobb kihívása, az információbiztonság megteremtése össztársadalmi feladat – vagy együtt leszünk sikeresek az elérésében, vagy közösen isszuk meg az eredménytelen munka levét.

Ennek figyelembevételével született meg először 2012-ben, majd 2020-ban hazánk biztonsági stratégiája. Az 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról fontos hangsúlyokat és támpontokat ad az információ- és kiberbiztonság témájához is. A *Biztonságos Magyarország egy változékony világban* címet viselő dokumentum már felütésével hangsúlyozza, hogy két dolog biztos a 21. századot tekintve: egyrészt a technológiai forradalom következtében minden eddiginél gyorsabb ütemben állandósult változás, másrészt a bármely korban az emberi lét alapvető igényét jelentő biztonság megteremtésének szüksége. Bár a biztonsági kihívások nagyok, hazánk

kedvező helyzetben veszi fel velük a harcot. A világ legerősebb szövetségi rendszerei, NATO- és EU-tagságunk mind a katonai, mind a más típusú biztonsági kihívások terén olyan erőforrást jelentenek Magyarország számára, amely esélyt és reményt ad a legkedvezőbb válaszok megtalálására. A sorsunk azonban a saját kezünkben van, és biztonságunkat sem várhatjuk másoktól. Különösen igaz ez az információ- és kiberbiztonsági kihívások esetében, amelyek teljes mértékben átszövik közösségi életünket.

A digitalizáció feltartóztathatatlan folyamata életünk minden szegmensét maga alá gyűri: az állam, a társadalmi élet, a gazdaság, az energiaellátás, a klímavédelem, az élelmezésünk és a szórakozásunk is egyre inkább digitális formát ölt. A minket körülvevő tárgyakból, eszközökből egyre több az „Internet of Things" körébe tartozik, ami azt jelenti, hogy a kibertérbe (iskapcsolódva szolgálja jólétünket. Ha viszont életünk egyre jelentősebb része fordul meg az ilyen-olyan internetes platformokon, akkor abból egyenesen következik, hogy biztonságunkat is egyre nagyobb részben ott kell szavatolnunk. Biztonságos körülményeket ott kell kialakítani, ahol jelen vagyunk – ha a mindennapjainkat befolyásoló információk a *virtuális* térből származnak, vagy azon keresztül jutnak el hozzánk, akkor ott kell nagyon is *reális* biztonságot teremtenünk. Az „IoT" betűszót nyugodtan feloldhatjuk úgy is, hogy „Internet of Threats", hiszen a világháló valóban komoly kihívásokkal szembesít minket.

Ezek között az egyik első, hogy mit kezdünk azzal a követhetetlen információbőséggel, amely elérhetővé vált számunkra. Néha már-már azt tapasztalhatjuk, hogy a túlzott információáradat éppúgy elbizonytalaníthat, mint a rendelkezésre álló információk szűkössége. Egy sokszorosára duzzadt információs térben óhatatlanul többszörösére nő a zaj is, ami körülvesz minket: a megbízható(bb)előhelyek mellett ellenőrizetlen források is ontják magukból a megtévesztő vagy egyenesen koholt híreket, és a döntéseinket segítő nagy adathalmazok mellett hamis adatokkal is tele a padlás. Nehéz a tisztánlátás, holott a mind gyorsabb változásokra biztos tudással kellene reagálni.

Magyarországnak az 1139/2013. (III. 21. Korm. határozattal elfogadott Nemzeti Kiberbiztonsági Stratégiája helyesen mutat rá arra, hogy az offline világban hosszú fejlődés alatt kidolgozott alkotmányos értékeinknek ma már az online életünket is meg kell határozniuk. A magyar kibertér szabad, demokratikus, jogállami és biztonságos berendezése éppoly alapvető feladat, mint korábbi életterünk ilyenként való megőrzése. A kibertérben pedig ha lehet, még az eddigieknél is világosabban látszik, hogy a szabadság és biztonság szavatolása nem csupán állami erőfeszítéseket igényel, hanem csakis a kormányzat, a tudományos, a gazdasági és a civil szféra közös felelősségvállaláson alapuló, szoros együttműködésével valósulhat meg. A kiberbiztonság ugyanis nem más, mint a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.

Kulcsfontosságú nemzeti kérdés emellett az is, hogy a biztonságos technológiákból, újabb és újabb vívmányokból a társadalmi és gazdasági élet szereplői minél szélesebb

körben és minél gyorsabban részesüljenek. Enélkül ma már elképzelhetetlen valódi versenyképesség, ezért a hazai piaci szereplőket, kis- és középvállalkozásokat minden eszközzel segíteni kell a legfejlettebb módszerekhez és termékekhez való hozzáférésben.

Ami a jelen kötet szerepét illeti mindebben: az információs és tudásalapú társadalom elemi módon igényli a magas szintű kutatás-fejlesztést és innovációt. Többről van szó, mint az eddig is nyilvánvaló összefüggésről, amely szerint a társadalmi haladás nem képzelhető el a tudományos élet munkásai nélkül. A hihetetlen mértékben felpörgött, változékony világnak már a mindennapok viteléhez szükséges megértése terén is rá vagyunk szorulva a folyamatokat időszerűen és összetetten elemző kutatásokra és az azok eredményét feldolgozó oktatásra, ismeretterjesztésre. A Nemzeti Közszolgálati Egyetemnek pedig különös felelőssége adódik ebben a munkában: a Nemzeti Kiberbiztonsági Stratégia szavai szerint „biztonságunk szempontjából kiemelt figyelmet igényel a katonai, a rendészeti és a közigazgatási felsőoktatás".

A most megjelenő kötet annak egyik bizonyítéka, hogy a Nemzeti Közszolgálati Egyetem tudatában van ennek a felelősségnek, és a magyar felsőoktatás egyik legerősebb információ- és kiberbiztonság-kutatási tevékenységét folytatja, ami szervesen összekapcsolódik azokkal a kutatási projektekkel, amelyek révén összességében az Egyetem páratlan információs társadalmi tudásbázist épít.

A teljesség igénye nélkül kiemelve néhányat a kötetben érintett izgalmas kérdéskörök közül:

Hangsúlyosan foglalkozik a kötet a kiberbiztonság és az innováció kapcsolatával. Szerzőink helyesen mutatnak rá arra a már említett tendenciára, hogy a digitalizációval elburjánzó összekapcsoltadat-alapú rendszerek terjedésével a kapcsolódó fenyegetettség is növekszik, ezért a biztonsági aspektusokkal foglalkozó kibervédelem pontosan ugyanolyan innovatív szemléletet igényel, mint maguk a folyton fejlődő rendszerek. Az innováció kérdésével foglalkozó egyik tanulmányunk ezzel összefüggésben annak az európai paradoxonként emlegetett ellentmondásnak a megértéséhez is közelebb próbálja vinni az olvasót, hogy miért került versenyhátrányba Európa, és ezzel együtt Magyarország a világ innovációs hubokat tömörítő térképének gazdagítása terén, miközben a kontinensnek világhírű hagyományai vannak az oktatásban és kutatásban. Egy másik tanulmány mindemellett bemutatja a kiberbiztonsági kompetenciahálózatok tervezetét, illetve ismerteti, hogy milyen kutatás-fejlesztés-innovációs lehetőségek lesznek a következő évtizedben Európában.

Több írásban tárgyaljuk a kritikus információs infrastruktúrákkal kapcsolatos kihívásokat. Alapvetés, hogy korszerű információtechnológiára épülő információs infrastruktúrák nélkül az információs társadalom működésképtelen. Nemzeti érdek tehát, hogy szavatoljuk biztonságos működésüket az ellenük irányuló ártó szándékokkal szemben. A tanulmányok jól érzékeltetik, hogy óriási feladattal állunk szemben ezen a téren: a hálózatokkal átszőtt globális világ a páratlan lehetőségei mellett – a nyitottságból, a bonyolult technikai rendszerekből, az infokommunikációs rendszerektől való növekvő függésből, illetve az összefonódó és egymással összekapcsolt létfontosságú infrastruktúrákból eredeztethető – rendkívüli sebezhetőséget is hozott.

Nem megy el a kötet szó nélkül az életünket egyre inkább befolyásoló okoseszközök szerepének vizsgálata mellett sem. Ez annál inkább indokolt, mert a mindennapi ember számára a technológiai robbanás egyik legmegragadhatóbb jele és kulturális mozgatója a rendelkezésünkre bocsátott „okos" infokommunikációs eszközök használata. Egyre több hálózatba kapcsolt eszközt használunk, amelyeknek tervezési szinten történő adatvédelme és információbiztonsága kulcskérdés, ha például meg akarunk valamit őrizni azokból a követelményekből, amelyekkel a magánélethez való jogunkat körülbástyáztuk.

Tanulmány járja körül, hogy a kibertér biztonságán fáradozó nemzeti kormányzatok milyen nemzetközi intézményi támogatásra számíthatnak. E támogatás magától értetődően nélkülözhetetlen egy természete szerint globálisan összekapcsolt háló esetében. Az olvasó a kiberbiztonság terén értékes fogalmi tisztázásokat is találhat itt magának, hiszen a nemzetközi együttműködés közös fogalomkészletet és igazodási pontokat igényel.

Nagyon fontos kérdéseket tárgyal az a tanulmány, amely az adatvédelmi jognak a jogfejlődésben mutatkozó szerepét érinti. Miközben figyelmünket elsősorban az új technológiai vívmányok jogi kordában tartásának heroikus munkája köti le, addig a szabályozói lépések összességében nagyon mélyen, de ehhez képest reflektálatlanul alakítják át jogrendszerünket. Akármit is gondoljunk ezekről a folyamatokról érdemben, mindenképp helyes, ha minél tudatosabban tekintünk rájuk.

A kötet külön részben, hat magyar és négy angol nyelvű tanulmánnyal foglalkozik a kibertér egyik speciális elemzést érdemlő, a nemzetközi folyamatokra nagy hatással lévő területével: a kiberdiplomáciával. Szerzőink alapvető fogalmakat tisztáznak, hiszen a kiberdiplomácia viszonylag új terület a nemzetközi kapcsolatok világában, és míg a hatása ma már megkerülhetetlen, addig a megértése, tudományos elemzése terén következetlenségek figyelhetők meg. Zavaró az is, hogy a fogalmat a média is előszeretettel használja, sok esetben komoly pontatlansággal. A kötet vonatkozó írásai helyzetképet adnak a kiberdiplomácia európai és nemzetközi fejleményeiről, illetve kitérnek külgazdasági aspektusaira is.

Összességében a tanulmányok sokféle témát érintve színes és értékes hozzájárulást jelentenek a magyar kibertér információs és biztonsági összefüggéseinek elemzéséhez, és hitelesen jelzik, hogy a Nemzeti Közszolgálati Egyetem erős kutatói potenciállal kívánja és tudja gazdagítani a területen folyó tudományos diskurzust.

Török Bernát

I. Információ- és kiberbiztonság

VÁKÁT OLDAL

1. Innováció a kibervédelemben

VÁKÁT OLDAL

Szakos Judit

Kiberbiztonsági innováció – Az ökoszisztéma szerepe

Bevezetés

Ugyan világunkat globalizáltnak és okosnak tekintjük, ami a lehetőségek végtelen tárházát, ezzel egy optimista jövőképet vetít elő, mégis számtalan olyan problémával állunk szemben, amelyek még megoldásra várnak, vagy éppen most jelennek meg a technológiai fejlődés, a tudás és információalapú gazdaság hatására. Ilyenek a mesterséges intelligencia (MI), a klónozás, a kiberbiztonság vagy a globális felmelegedés által generált egyrészt etikai, illetve jogi, másrészt gyakorlati problémák, ahol az állami vezető szerepvállalását nem lehet megkerülni – nemcsak mint támogatóét és problémamegoldóét, hanem mint vezetőét, felelősségvállalóét is. A különböző negatív prekoncepciókat és az információdeficitet figyelembe véve azonban az állam nem lehet önálló szereplő a folyamat során.

Az egyik kritikus kérdés, a digitalizáció ma áthatja az élet valamennyi területét és az agráriumtól az egészségügyig innovatív, összekapcsolt adatalapú rendszerekkel találkozunk, amelyek folyamatos terjedése töretlen. Ezzel együtt azonban a kapcsolódó fenyegetettség is növekszik, ezért a biztonsági aspektusokkal foglalkozó IT- és kibervédelem ugyanolyan innovatív szemléletmódot igényel, mint maguk a folyton megújuló rendszerek.

Az innováció ökoszisztéma alapú vizsgálata, a kiberbiztonság szempontjából is adekvát megközelítés különös tekintettel arra, hogy a védelmi szféra trendjei jellemzően befolyásolják a piaci irányokat. Ez nem az egyes részterületek kérdéseire fókuszálva segíti a problémamegoldást, hanem egy módszertani segítséget nyújt a szereplők együttműködésére, egymásrautaltságára építkezve.

Az innováció és kiberbiztonság közötti logikai kapcsolat ennek megfelelően két irányból közelíthető meg: egyrészt a fent említett veszélyek és fenyegetések miatt szükséges az alapvető innovációs trendekkel és irányvonalakkal tisztában lenni valamennyi szektorral összefüggésben, elég itt például a meghekkelhető beépített orvosi eszközökre vagy a dolgok internete által átszőtt mindennapokra gondolni. Ugyanígy a tanuló szervezetek, az ember mint leggyengébb láncszem vagy a bürokratikus döntéshozatal lassúsága szempontjából vizsgálva a kérdést, fontos a trendek feltérképezésének időbeli megkésettségét is minél inkább redukálni.

Egy másik aspektusból vizsgálva a kiberbiztonság a 21. század jelentős innovációs potenciállal bíró területe, így az itt dolgozó szakemberek – csakúgy, mint az innovációs rendszer egyéb aktorai – át kell, hogy lássák az innováció és az innovációs folyamat alapvető fogalomkészletét, rendszerét és eszközkészletét. Különösen igaz ez akkor, ha vagy szakpolitika-alkotó vagy hídképző intézmény képviselőjének szerepét veszik fel,

hiszen itt a piaci logika nem feltétlenül kényszeríti őket a horizontális nyitásra. Ezért a könyv ez utóbbi, kapcsolati aspektusra helyezi a hangsúlyt.

Ez a megközelítés azonban nem új keletű. A világ vezető kiberbiztonsággal foglalkozó egyetemeinek és szervezeteinek[1] az utóbbi időben közös kutatási látókörébe került a kiberbiztonsági innováció ökoszisztéma felől történő megközelítése.[2] Álláspontjuk szerint a széles értelemben vett, többszereplős innovációs folyamat képes lehet fokozni, gyorsítani a kiberbiztonság területén megjelenő innovációkat.

Ennek a megközelítésnek a mélyebb vizsgálata pedig közelebb vihet ahhoz az európai paradoxonként emlegetett ellentmondás megértéséhez is, hogy miért nem kerül fel Európa, és ezzel együtt Magyarország sem a világ innovációs *hubokat* tömörítő térképére, miközben a kontinensnek világhírű STEM[3]-hagyományai vannak az oktatás és kutatás terén.

A hatékony innovációmenedzsmenthez ugyanis a különböző szervezeti – formális és informális – együttműködések, intézményi tényezők mellett olyan „puha" tényezőkre is szükség van, mint a humánerőforrás-, az innovációs kultúra fejlesztése vagy a bizalom kérdése. Ez részben az innovációmenedzsment és a vállalkozói ismeretek oktatásba történő beépítésével támogatható, de fontos benne a meritokrácián és együttműködésen alapuló társadalom is.

További fontos, gyakran emlegetett – részben bizalmi, részben kommunikációs – kérdés a technológiai fejlesztésekkel foglalkozó szakemberek és a felzárkózni igyekvő vagy épp leszakadó társadalmi rétegek között mélyülő szakadék kérdése. A technológiai változások mélyebb összefüggéseit, társadalmi kockázatait, adaptációs korlátait is érdemes ismernie azoknak, akik a technológiában keresik a hosszú távú megoldásokat. Az emberi tényező itt is kritikus, mint a kiberbiztonsággal összefüggő valamennyi területen, hangsúlyos a nem technológiai tudás szerepe.

Összességében tehát ez a könyv az innovációmenedzsment olyan adekvát elméleti áttekintését adja, amelyben az állami, vállalkozási és tudástermelési szempontok egyaránt megjelennek, ezzel a jövő kiberbiztonsági szakemberei a megfelelő elméleti tudás birtokában lesznek a kiberbiztonsággal összefüggésben jelentkező innováció és tudástranszfer ökoszisztéma-szintű menedzselésére, bármely szférában helyezkedjenek is el.

Ennek megfelelően az II. fejezet az innováció megértésének alapfogalmait és definíciós kérdéseit foglalja össze kiegészítve a paradigmaváltások alapvető jellemzőivel. Ezt követően a kiberbiztonsági innováció néhány jellemzőjére hoz példákat. A III. fejezet az innovációs folyamat és a modellek fejlődéstörténetét foglalja össze, hogy a IV. fejezetben egyértelmű legyen az ökoszisztéma-alapú megközelítések relevanciája. Végül

[1] Kezdeményező egyetemek: Massachusetts Institute of Technology Innovation Initiative (MITii); The Hebrew University of Jerusalem, Federmann Cyber Security Center (HCSRC).
További kezdeményező szervezetek: Israel's National Cyber Directorate (INCD); UK Department for Digital, Culture, Media & Sport (DCMS); UK Science & Innovation Network.

[2] *Enhancing Cybersecurity – The Role of Innovation Ecosystems* 2019.

[3] *Science, technology, engineering, mathematics,* azaz tudomány, technológia, mérnöki tudományok és matematika.

az V. fejezet az egyes aktorok innovációval összefüggő jellemzőit villantja fel ismét az együttműködések felől megközelítve.

Az innováció alapfogalmai

Schumpeter, a teremtő rombolás és az ipari forradalmak

Az innováció mint újdonság fogalmának meghatározása rendkívül sokrétű, az idők folyamán a témához való közelítés változásával, bővülésével is formálódott. Napjainkban, úgy tűnik, jelentősége ismét felértékelődött: mind vállalkozási és üzleti sikerben játszott szerepe, a globalizációból következő növekvő nemzetközi versenyben a versenyképesség alapjainak lefektetése miatt, mind a tudás-, illetve tanulásalapú gazdaság, társadalom megteremtésével. A fogalom azonban az utóbbi időben olyan kulcsszóként működött, amellyel mindenki igyekezett eladhatóbbá tenni az ötletét, termékét, szolgáltatását – figyelmen kívül hagyva, hogy ténylegesen innovatív volt-e az, vagy sem – így annyira beleivódott a mindennapjainkba, hogy már-már elcsépeltnek tűnhet a használata vagy az arról való tanulás. A valóságban azonban a téma iránti kínálat és kereslet sem elméleti, sem gyakorlati szinten nem csökkent. A témát kutatók és a piac mellett az állam vagy államok közössége is megjelenik a meghatározást kereső aktorok között.

Széles körben ismert és alkalmazott Joseph Schumpeter osztrák közgazdász, szociológus a 20. század első felében végzett munkássága. Megközelítése szerint a gazdasági fejlődés motorja az innováció, hirdette a monopóliumok technológiai fölényét, a vállalkozóban pedig „a kapitalizmus hősét látta, »az intellektus és az akarat kiemelkedő képességeivel megáldott« személyt, akit a győzelem vágya és az alkotás öröme motivál”.[4] Az innováció alapjának az új szereplők által bevezetett *új kombinációkat* tekinti, amelyek ha sikeresen átveszik a vezető szerepet a piacon, az a teljes piaci struktúra átrendezésével járhat, amelyből egyes szereplők nyertesként, míg mások veszteskénti kerülnek ki. Ezért is nevezi ezt a folyamatot *teremtő (alkotó) rombolásnak (creative destruction),* ahol „valami elpusztul, és valami keletkezik”.[5]

A műszaki fejlődés és az innováció fejlődési irányai és dinamikája a hozzájuk kapcsolódó bizonytalansági tényező miatt nehezen jelezhetők előre. Az 1960-as évektől azonban a főáramú közgazdaságtan, emellett pedig – a Schumpeter munkásságára épülő – alternatív közgazdaságtani iskolák is vizsgálni kezdték a területet. Kiemelten fontos ezek közül az evolúciós közgazdaságtan, ami a gazdaságot folyamatosan változónak feltételezi, és a változások ütemének időbeli eltérései miatt ciklikus fejlődést ír le, amelynek a „hátterében a gazdasági növekedés motorjának tekinthető műszaki fejlődés és innováció ciklikussága áll”.[6] Az evolúciós elmélet – amely a biológiai szelekcióhoz hasonló folyamatot feltételez a piacon – a ciklikusság okait és reálgazdasági

[4] Nordhaus–Samuelson 2016.
[5] Bőgel 2008, 344.
[6] Szanyi 2018, 4.

hatásait tanulmányozza.[7] Feltételezi, hogy az újdonságok keresése és megtalálása egy tudatos cselekvés eredménye,[8] a szelekció alapja itt a versengő megoldások közötti piaci visszajelzés, ahol sikeres és sikertelen megoldási alternatívák váltakoznak. Ez a folyamat összességében mind az iparágak és a piacok, mind a nemzetgazdaság folyamatait irányítja.

1. táblázat: A műszaki fejlődéshez kapcsolódó törvényszerűségek fogalomkészlete

Vizsgálati szint	Kapcsolódó fogalmak
vállalati / konkrét termék	műszaki fejlődéspálya *(technological trajectory)*
iparági	műszaki paradigma *(technological paradigm);* technológiai életciklus
nemzetgazdasági	műszaki-gazdasági paradigma *(techno-economic paradigm)*

Forrás: Szanyi 2018, 6. alapján saját szerkesztés

Az új megoldások keresésének azonban különböző útfüggőségei figyelhetők meg: vállalati szinten „a korábbi döntési fázisok eredményei (felhalmozott tőkejavak, műszaki és menedzsmenttudás és gyakorlat) erősen befolyásolják", iparági szinten „a piaci szereplők (versengő vállalatok, fogyasztók) egymással kölcsönhatásban működve együtt hozzák létre az iparágra jellemző technológiai paradigmákat, nemzetgazdasági és világgazdasági szinten pedig műszaki-gazdasági paradigmákat".[9] Itt a műszaki fejlődéshez kapcsolódó fejlődési utat az egyes szinteken az 1. táblázatban összefoglalt fogalomkészlettel lehet leírni: vállalati vagy konkrét termék esetén *műszaki fejlődéspályáról (technological trajectory)* beszélnek, iparági szinten *műszaki paradigmáról (technological paradigm),* míg nemzetgazdasági szinten *műszaki-gazdasági paradigmának (techno-economic paradigm)* nevezik. Utóbbi esetén már az iparágak, piacok és a társadalmi létformák valamennyi elemén látható hatások értelmezendőek. A műszaki paradigma esetén „egy iparágra vonatkozó jellegzetes műszaki és gazdasági (üzleti) problémákra irányuló keresési tevékenység minták összessége", ahol „a szereplők azonos időben hasonló vagy teljesen egyforma ágazatspecifikus problémákra keresnek megoldásokat", „az egyes szereplők rendelkezésére álló erőforrások mennyisége, minősége hasonló, az elérni kívánt ered-

[7] Az alternatív közgazdasági iskoláknál megjelenő felfogások közül itt fontos szerepet kap továbbá „a piaci szereplők döntéseinek korlátozott racionalitása, az információk korlátozott rendelkezésre állása, maximalizálás helyett az elfogadható, kielégítő megoldásokra (és kielégítő profitra) törekvés, a döntésekben hosszabb távon érvényesülő megszokások, rutinok jelenléte, valamint a döntések útfüggősége." Szanyi 2018, 2–4.

[8] Kiemelnénk azonban, hogy a történelem során egy-egy innováció esetén nem elhanyagolható szerepe volt a *véletlennek* is akár azzal, hogy nem a szándékolt, de hasznos eredményt hoztak létre, akár úgy, hogy a felfedezést egy eredeti szándéktól eltérő területen tudták végül alkalmazni, amely nem szándékos felhasználás vezetett végül az elterjedésükhöz.

[9] Szanyi 2018, 5–6.

mény leírása a szereplők között egyforma, és a keresési tevékenységben hasznosított tudás egy része is közös".[10] Az ezt leíró evolúciós folyamatot *technológiai életciklusnak* nevezik.

A műszaki fejlődés irányát több belső és külső tényező is meghatározza. A kutatás és fejlesztés fontos szerepet kap ebben, ahogy az innovációk terjedésében kulcsszerepet játszó szervezeti tanulás. Megjelenik a keresleti (fogyasztó-) oldal is, valamint a piaci egyensúly felbomlása is befolyásolja a piaci viszonyok változását. Utóbbira példa a hirtelen és jelentős árváltozás, a történelem során megtapasztalt nyersanyaghiány vagy tengeri blokádok (helyettesítő termékek kifejlesztése, például műbenzin), a munkásmegmozdulások és sztrájkok a 19. századi Angliában (ipar gépesítése) vagy a kormányzati megrendelések a 20. században (hadiipar, űrkutatás).[11] Ezen fejlesztések jelentős része pedig idővel a mindennapi használatban is elterjedhetett (például internet).

2. táblázat: A technológiai forradalmak kiindulási pontjai

	Az időszak szokásos elnevezése	Központi országok	Az átalakulást kiváltó műszaki újdonság	Megjelenés éve
Első	Az első „ipari forradalom"	Anglia	Arkwright fonalgyára Cromfordban.	1771
Második	A gőzgép és a vasútépítés kora	Nagy-Britannia, majd USA és Nyugat-Európa	A „Rocket" gőzmozdony első útja a Liverpool–Manchester-vasútpályán.	1829
Harmadik	Acél, elektromosság és nehézipar kora	USA és Németország	Pittsburgh-ben megnyílik a Carnegie–Bessemer acélüzem (Pennsylvania).	1875
Negyedik	Petrolkémia, autóipar és a tömegtermelés kora	USA, Németország, majd Nyugat-Európa	Az első T-modell elkészül Detroitban, a Ford-üzemben (Michigan).	1908
Ötödik	Infokommunikációs és telekommunikációs technológiák kora	USA, majd Európa és Ázsia	Bejelentik az Intel mikroprocesszor kifejlesztését Santa Clarában (Kalifornia).	1971

Forrás: Perez 2002; idézi Szanyi 2018, 14.

A műszaki-gazdasági paradigmaváltások vagy közismertebb nevükön technológiai forradalmak az egész gazdaságra hatással vannak azzal, hogy az műszaki kontextus és a termelőeszközök fejlődése (a termelés szervezésének gyakorlatától a vállalatvezetésig) mellett a társadalom egészét befolyásolják. Új, fokozatosan előretörő és dinamikusan fejlődő iparágak jönnek létre, amelyek megváltoztatják a gazdaság szerkezetét, ezzel valamennyi kapcsolódó iparágat forradalmasítanak, így azok képesek újabb és újabb időszakban ösztönözni a gazdaság fejlődését.[12]

[10] Szanyi 2018, 6.
[11] Szanyi 2018, 11.
[12] Szanyi 2018, 14–15.

3. táblázat: A műszaki-gazdasági paradigmák vezető iparágai és új infrastruktúra-elemei

	Kulcstényezők Új technológiák és iparágak	Új infrastruktúrák
1. Az első „ipari forradalom"	Olcsó vízenergia Gépesített pamutipar Kovácsoltvas gépek	Csatornák és országutak
2. A gőzgép és a vasútépítés kora	Olcsó kőszén Gőzgépek Gőzerővel hajtott ipari berendezések Vasérc- és szénbányászat Vasútépítés, vasúti gépgyártás	Vasút Rendszeres postaszolgálat Telegráf Nagy vitorláskikötők
3. Az acél, az elektromosság és a nehézipar kora	Olcsó öntöttvas (Bessemer-technológia) Gőzhajózás Nehézvegyipar Városi közművek és tömegközlekedés Elektromos ipar Konzervgyártás Papíripar, nyomdaipar, sajtótermékek	Világkereskedelem gőzhajózással Szuezi-csatorna Transzkontinentális vasutak Nagy acélszerkezetű objektumok építése Telefon Elektromosenergia-szolgáltatás
4. Petrolkémia, autóipar és a tömegtermelés kora	Olcsó olaj Tömegtermelés az autóiparban Petrolkémia (műanyaggyártás) Belső égésű motorok alkalmazása Elektromos háztartási gépek Mélyhűtött, fagyasztott élelmiszerek	Úthálózat, autópályák, kikötők és repülőterek Üzemanyagtöltő állomások hálózata Általános elektrifikáció Analóg távközlési világhálózatok
5. Infokommunikációs és telekommunikációs technológiák kora	Olcsó mikroelektronikai alkatrészek Számítógépek és szoftverek Telekommunikáció Elektronikus mérő- és érzékelő műszerek Számítógéppel vezérelt gyártás Új anyagok	Digitális távközlési világhálózat (üvegszálas, rádiós és műholdas átviteltechnika) Internet, email, más e-szolgáltatások Diverzifikált energiatermelés Nagy sebességű, kombinált szállítási rendszerek

Forrás: Perez 2002, 14.; idézi Szanyi 2018, 16.

Perez szerint „a technológiai forradalom […] egymáshoz kapcsolódó radikális áttörések csoportja, amely egymással összefüggő technológiák új konstellációját alakítja ki".[13] Az egyes technológiai forradalmakat – szimbolikusan – egy felfedezés, szabadalom időpontjához és helyszínéhez kötik, azonban a valóságban ilyen szigorú megkötés nem lehetséges, nem elszigetelten alakulnak ki, az átmenet fokozatos. Csak a korszakhatárok jellemzése miatt szükséges ezeket a jelentős innovációkat kiemelni a fejlődésüket biztosító innovációs klaszterükből. Fontos megjegyezni, hogy az egyes új paradigmák elemei a megelőző paradigma szétterülési fázisában már megfigyelhetők – emiatt olyan nehéz a 6. paradigma előrejelzése is, hiszen nem egyértelmű, hogy a ma meghatározónak tűnő technológiai változások közül végül melyik fog kiemelkedni.

A paradigmák életciklusa két részre bontható, amelyek szervesen kapcsolódnak egymáshoz. A kialakulás időszakában a vezértermékek és ágazatok jönnek létre. Alapvetően ekkor a tőkepiacokról sok – a szükségesnél több – spekulatív tőke áramlik az iparágakba, a kockázati tőke finanszírozta innovatív vállalatok körül tőzsdei buborékok alakulnak ki, azonban ez döntően fontos, hogy az új iparágak megfelelő finanszírozást kapjanak a mindenkori paradigma megtörésére. A buborékok kipukkanására datálja a szakiroda-

[13] Perez 2009, 8.; idézi Szanyi 2018, 12.

lom a második periódus kezdetét. A szétterjedési szakaszban az új technológiák, kialakult eszközök más iparágakra is hatással lesznek, ott is elterjednek ezzel gazdasági fellendülést okozva. Ekkor a pénzügyi szféra már a reálgazdaság finanszírozását helyezi a fókuszba, a stabil, rendszeres osztalékot jelentő vállalatok finanszírozása kerül előtérbe. Ez a finanszírozási folyamat-trend tört meg a legutóbbi paradigmánál, ahol a globalizált kereskedelem miatt nem lehetett megfelelő szabályozókat kialakítani a finanszírozás reálgazdasághoz való visszatereléséhez.[14]

Az evolúciós közgazdaságtan az egyes paradigmák értelmezése mellett szintén igyekezett a műszaki fejlődés és a gazdasági növekedés közötti kapcsolatot modellezni. Szanyi a két változó hosszú távú együtt mozgását a gazdasági növekedés dinamikáját bemutató Kondratyev-hullámok (K-hullámok) felhasználásán keresztül vezeti le. Tanulmányában bemutatja, hogy a K-hullámok és a műszaki-gazdasági paradigmák ciklusai egymáshoz képest időben eltolva valósulnak meg azzal, hogy az átfedés a 21. században több ok miatt már nem tökéletes,[15] azonban így is demonstrálja a két tényező közötti kölcsönhatást, hogy a hosszú távú gazdasági növekedés motorja a műszaki fejlődés – és ezzel együtt az innováció.

Az irányzat továbbá jövőorientált gazdaságpolitikák alkalmazására ösztönöz, felhívja a figyelmet, hogy a korábbi technológiai paradigmákhoz történő visszatérés nem lehet észszerű cél, a fejlesztések irányát a jelenlegi gazdasági paradigma szétterjedésének támogatására, majd az új – jelenleg még csak találgatás szintjén létező – új paradigmára kell összpontosítani. A technológiai fejlődés következő lépései még ugyan nem láthatók tisztán, azonban számos olyan irány van, ami a következő időszakban kitörési pont lehet. A kutatók között az sem egységesen elfogadott, hogy mely irányok tartoznak még az 5. paradigmához, és melyek jelenik már a 6. paradigma előfutárait.

Mankóként szolgálhat az ipar 4.0 koncepció. A jelenleg meghatározó trendek közül Szanyi a termelés nagy fokú szegmentálódását (kiemelten az egyedi tömegtermelést, *mass customization*), továbbá a komplex termékek növekvő tudástartalmát emeli ki. A következő ciklus egyik potenciális eleme pedig a *Big Data* (adatfelhő) lehet, amely „megfelelő algoritmusok kialakításával sokféle (jó és rossz) célra hasznosítható".[16] Itt az olcsó erőforrásnak az információ tekinthető.[17] Szalavetz 2005-ös munkájában[18] még a nanotechnológia előretörésére számított, amely ma már inkább egy kulcsfontosságú

[14] Szanyi 2018, 18–22.

[15] „Így például a 2000-es évek nagy technológiai és pénzügyi válságai egyelőre nem vezettek a befektetési tevékenység gyökeres átalakulásához, a spekulatív befektetések csak részlegesen folytak át a reálszféra tevékenységének közvetlen finanszírozásába. Egy másik ide kapcsolódó eltérés a gazdaságpolitika és a piaci intézmények korrekciójának elmaradása. A globalizáció folyamatában a piaci szereplők, köztük a pénzintézetek tevékenysége is egyre nehezebben kontrollálható. Ezért a befektetési tevékenység átváltását ösztönző (azt kikényszerítő) szabályozások bevezetése elmaradt a 2000-es években. Ezek a sajátosságok oda vezettek, hogy az 5. műszaki-gazdasági paradigma szétterjedési folyamatai a vártnál lassabban indultak be." Szanyi 2018, 33.

[16] Szanyi 2018, 30.

[17] "Data is the new oil. It's only useful when it's refined". Jessica Greenwood, Global CMO, R/GA.

[18] Szalavetz 2005, 58–75.

alaptechnológiaként *(key enabling technology)* aposztrofálható. 2018-as munkájában azonban megállapítja, „hogy a fejlődés talán soha nem volt még olyan mértékben, olyan látványosan tudomány- és technológiavezérelt, mint napjainkban, amikor három alapvető tendencia csúszik össze, jelenik meg minimális időbeli eltéréssel, gyakorlatilag egymással párhuzamosan. Egyfelől, az *innovációk sűrűsödését* látjuk, főként az ipar 4.0 ernyőfogalmába tartozó technológiai újdonságok körében (kiberfizikai rendszerek, 3D-nyomtatás, kollaboratív robotok, nagy adattudomány, felhőalapú számítástechnika).”[19] Kiemeli továbbá a mesterséges intelligencia és a gépi tanulás fontosságát mint lehetséges új paradigmát:

– „általános célú technológia, vagyis az információtechnológiai iparágon, sőt magán a feldolgozóiparon is messze túlterjeszkedve, az összes ágazatba, a gazdaság és a mindennapi élet összes szegmensébe beépül;
– felerősíti a technológiai konvergencia folyamatait, és felgyorsítja az összes tudományterület fejlődését;
– új, korábban nem létező iparágakat hoz létre, felerősíti a termék-, eljárás-, szervezeti- és marketing-innovációs, valamint a vállalkozási tevékenységeket;
– a schumpeteri teremtő rombolás jegyében megszüntet vagy átalakít létező iparágakat és tevékenységeket;
– megváltoztatja a társadalmi létformákat.”[20]

Az előrejelzések közül kiemelendő a Gartner piackutató vállalat által évente kiadott, feltörekvő technológiákat bemutató kutatása *(Gartner Hype Cycle for Emerging Technologies).* A 2020-as első előrejelzések szerint a következő 5–10 évre több mint 2000 olyan technológiát tart számon a vállalat, ami versenyelőnyt generálhat különböző szektorokban. Erre az időszakra öt fő trendet[21] azonosítottak, amelyet a 4. táblázat[22] foglal össze.

4. táblázat: A Gartner 2020-as előrejelzése az öt fő feltörekvő technológiai trendről

Advanced AI and Analytics	Augmented Humans	Digital Ecosystems	Postclassical Communications and Compute	Sensing and Mobility
Adaptive Machine Learning AI PaaS Explainable AI Generative Adversarial Networks Graph Analytics Transfer Learning Edge Analytics Edge AI	Augmented Intelligence Biochips Biotech – Cultured or Artificial Tissue Emotion AI Immersive Workspaces Personification	Decentralized Autonomous Organization Decentralized Web DigitalOps Synthetic Data Knowledge Graphs	5G Low Earth Orbit Satellites Nanoscale 3D Printing Next-Generation Memory	3D Sensing Camera AR Cloud Autonomous Driving Level 4 and 5 Flying Autonomous Vehicles Light Cargo Delivery Drone

Forrás: Gartner é. n.

[19] Szalavetz 2018, 38–48.
[20] Szalavetz 2018.
[21] *Gartner Hype Cycle for Emerging Technologies.*
[22] Mivel a technológiák egy részének még nincs magyar elnevezése, az egységesség miatt angolul szerepelnek a táblázatban.

Ezek a felsorolt új technológiák már mind az *értékteremtés módját* változtatják meg. A potenciális paradigmaváltó technológiák jelentős része olyan erős társadalmi hatással bír majd, hogy a technikai innovációk mellett elterjedésükhöz társadalmi innovációkra is szükség lesz a leszakadó rétegek csökkentéséhez.

Szintén fontos társadalmi kérdéseket feszeget, hogy a robotok valóban elveszik-e majd az emberek munkáját, vagy hogy várható-e a modern géprombolók[23] megjelenése. Az ezzel kapcsolatos kutatások ugyan egyértelmű adatokkal nem szolgálhatnak, azonban úgy tűnik, hogy optimista várakozásra adhat okot, hogy nem az innovatív vállalkozások foglalkoztatási mutatói romlanak, hanem pont a nem innovatív vállalkozásokban csökken a foglalkoztatás.[24] „Sőt a Világbank kutatóintézetében végzett – tudomásunk szerint legátfogóbb, és módszertanilag megalapozott – nemzetközi (67 országra kiterjedő) vizsgálatának tapasztalatai szerint az innovatív cégek a képzetlen munkavállalókat is nagyobb arányban foglalkoztatják, mint a nem innovatív vállalkozások kedvezően befolyásolják még a kvalifikálatlan munkavállalók munkapiaci integrációját is."[25] Kérdés, hogy közép- és hosszú távon a gyakorlat valóban igazolja-e ezeket a foglalkoztatottsági eredményeket, megvalósulhat-e az inkluzivitáshoz szükséges társadalmi innováció, az azonban biztosnak tűnik, hogy a technológiai fejlődés nem lassul, így a felkészülés és az alkalmazkodás lesz az új stratégiai irány minden szektorban.

Feltalálás, kutatás-fejlesztés és innovációs folyamat

A fenti konstrukciók ugyan az innováció eltérő megjelenési formáit mutatták be, a különböző megközelítések közös metszete minden esetben az újdonságtartalomban gyökerezett. Felmerülhet tehát a kérdés, hogy minden újdonság innováció-e. Hogyan definiálható az innováció, és milyen fogalmaktól szükséges elhatárolni azt a továbbiakban?

Alapvetően innovációnak az az *ötlet* tekinthető, amit a piac is igazol. Fontos elhatárolni az innováció és a műszaki fejlődés fogalompárt, utóbbit „a gazdaság számára exogén folyamatnak tekintjük, amely saját belső törvényszerűségei alapján halad előre, és amely műszaki és tudományos ismereteket generál. Ezek az ismeretek képezik az invenció, találmány alapját. A találmányok a műszaki ismereteket emberi szükségletek kielégítésére teszik alkalmassá."[26]

[23] Gyökere, hogy rövid időn belül az emberi munka fontosságáról a gépekre tevődött át a hangsúly a 19. századi angol textiliparban, így egy érdekvédelmi célú mozgalom szerveződött (luddizmus, Ned Ludd, az 1811–1812. évi nottinghami géprombolás vezetője után). Tevékenységük során a munkásosztály gépek elleni lázadása előbb a bérigények kikényszerítésére törekedett, majd a géprombolás önálló céllá vált.

[24] Nielsen 2006, idézi Makó–Illéssy 2014, 4–20.

[25] Dutz et al. 2011, idézi Makó–Illéssy 2014, 4.

[26] Szanyi 2018, 3.

Az innováció fogalma gyakran keveredik az innovációs folyamat definíciójával is, ami az invenció, innováció és diffúzió (széles körű elterjedés) egymást követő lépéseiből áll. Ez a három egymásra épülő fázis a következőképp határozható meg:

– az *invenció* ideagenerálási folyamat, amely a tanulás különböző formáit is tartalmazza;
– az *innováció* egy még ki nem próbált ötlet gyakorlati megvalósítása s ezáltal kivitelezhetőségének első demonstrációja;
– a *diffúzió* pedig egy innováció széles körű és sokrétű alkalmazása az adott társadalmi-gazdasági rendszerben.[27]

A definíciók ezzel követik Schumpeter megközelítését, aki éles határt húzott az invenció és az innováció szakasza közé, de egyben ki is egészítik Schumpeter tételeit az innováció és a diffúzió közé illesztett szelekciós folyamattal, valamint a diffúzió közben megvalósuló tanuló és fejlesztő folyamattal, itt is hangsúlyozva, hogy az innovációs aktus nem fölérendelt a többi lépéshez képest. Terminológiai meghatározása szerint:

– az *innovációs folyamat* alatt a társadalmi-gazdasági tevékenységek olyan széles körét érti, amely az ideagenerálástól az ötlet első megvalósításán át annak sokoldalú és széles körű gyakorlati alkalmazásáig terjed;
– az *innovációs cselekedetnek/aktusnak* vagy *innovációnak* pedig egy ötlet elsőként történő gyakorlati alkalmazását nevezi.

Jelen könyv az innovációs folyamatra és az azzal kapcsolatos követelményekre, törvényszerűségekre és hálózatokra helyezi a hangsúlyt. Ezzel együtt a továbbiakban, a szakirodalom jelentős részét követve az innovációs folyamat és innováció kifejezéseket – a fentiek tudomásulvétele ellenére – együtt használjuk.

További fogalmi elhatárolás jelenik meg Rekettye munkájában, aki szerint „feltaláláson az új termékekre vagy technológiákra vonatkozó ötletek, módszerek felfedezését, míg az innováció fogalmán a felfedezett új találmányok alkalmazását, az új termékek kifejlesztését és piaci bevezetését értik", így „a feltalálás a tudomány fogalma, az innováció pedig a gazdasági életé".[28] A definícióban használt felfedezés pedig már továbbvisz az innovációval gyakran közösen használt kutatás fogalmához.

A *kutatás és kísérleti fejlesztés* (K+F) a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) által kiadott *Frascati-kézikönyv* 2015-ös kiadásának[29] definíciója szerint az új tudás megteremtése érdekében, szándékosan végzett kutatói, fejlesztői tevékenység összessége. Ez jelenti egyrészt a tudásállomány növelését – beleértve az emberiség, a kultúra és a társadalom ismereteit –, másrészt az ismeretek alkalmazhatóságának kidolgozását is. A kézikönyv a kutatás-fejlesztés öt jellemzőjét különbözteti meg:

1. újdonságtartalma van *(novelty);*
2. kreativitáson alapul *(creativity);*

[27] Kovács 2004, 52–78.
[28] Rekettye 2018.
[29] OECD 2015.

3. magas befektetési kockázat jellemzi *(uncertainty);*
4. szisztematikus tevékenység *(being systematic);* és
5. átruházható és/vagy reprodukálható *(transferable).*

Típusait tekintve megkülönböztetnek alapkutatást, alkalmazott kutatást és kísérleti fejlesztést, amelyeket jogszabályi szinten is definiálnak Magyarországon:[30]

- *Alapkutatás:* elsődlegesen a jelenségek lényegére és a megfigyelhető tényekre vonatkozó tudományos ismeretek bővítését célzó kísérleti, tapasztalati, rendszerező vagy elméleti munka. Ezen belül megkülönböztetnek:
  a. *tiszta alapkutatást,* amely a tudományos ismeretek bővítésére irányuló kutatás, és amelynek nem célja a közvetlen társadalmi vagy gazdasági haszon elérése vagy az eredmények gyakorlati problémák megoldására történő alkalmazása.
  b. *célzott alapkutatást,* amely a tudományos ismeretek bővítésére irányuló olyan kutatás, amelyről valószínűsíthető, hogy a felismert vagy várható, jelenlegi vagy jövőbeli problémák megoldására alapul szolgál.
- *Alkalmazott (vagy ipari) kutatás:* amely új ismeret szerzésére elsődlegesen meghatározott gyakorlati cél érdekében végzett eredeti vizsgálat.
- *Kísérleti (vagy prekompetitív) fejlesztés:* amely a kutatásból és/vagy a gyakorlati tapasztalatokból nyert, már létező tudásra támaszkodó tevékenység, amelynek célja új anyagok, termékek, eljárások, rendszerek, szolgáltatások létrehozása vagy a már meglévők lényeges továbbfejlesztése.

A kutatás-fejlesztés tehát piacra lépés esetén az innováció egyik lehetséges előszobája. Piskóti egy hierarchikus lineáris innovációs modellt vázol fel, amely „az alapkutatások és alkalmazott kutatások által feltárt lehetőségek megvalósításának szervezési feladatait, lépésit mutatja fel".[31] Ez a kapcsolat azonban nem kizárólagos, létezik K+F-tevékenység innovációs törekvés nélkül, és nem minden innováció alapul kutatási eredményeken. Az innovációs folyamat lépéseinek összetettségéről a III. fejezet szól részletesen.

Fontos azonban hangsúlyozni, hogy már Bush érvelésében is kulcsszerepet kap az *alapkutatások* fontossága és az azok arányának növelésére tett javaslat különböző kormányzati támogatásokkal a második világháború utáni Amerikai Egyesült Államokban. Véleménye szerint a kutatás, a vizsgálati tárgy megválasztásának szabadsága központi kérdés az alapkutatások bástyáját jelentő főiskoláknál, egyetemeknél és kutatóhelyeknél, mivel ők a „tudás és megértés kútfői".[32] Az ezzel járó aktív tudásáramlás építhető be aztán a kormányzati, ipari vagy egyéb problémamegoldásba, hiszen ezek szükségesek az új termékek vagy folyamatok kialakításához. Felhívja a figyelmet, hogy ugyan az alapkutatást végzők nem feltétlenül érdekeltek abban, hogy a kutatás hasznosíthatóságával foglalkozzanak, de az ipari fejlesztések stagnálása várható egy alapkutatásokat hanyagoló

[30] 2004. évi CXXXIV. törvény a kutatás-fejlesztésről és a technológiai innovációról 4. §.
[31] Piskóti 2007.
[32] Bush 1944–1945, 234.

periódus után. A kormányzat részéről két fontos pillérben látja az ipari kutatásokhoz való hozzájárulás lehetőségét: az alapkutatások és a tehetséges kutatók támogatásában.

A fenti vita ma sem lehetne aktuálisabb, a tudománypolitika visszatérő motívuma, hogy ki, hogyan és milyen mértékben járuljon hozzá az alapkutatások támogatásához, milyen mértékben szükséges és elégséges az egyetemek kutatási portfóliója. A vállalkozó egyetem és a kutatóegyetem közötti hangsúlyeltolódások, az azokkal járó haszon sok esetben már megközelítés, ideológia kérdése is. Rekettye találóan foglalja össze, hogy manapság „az alapkutatás eredményei egyre gyorsabban befolyásolják a gyakorlatot, és a gyakorlat igényei egyre nagyobb mértékben határozzák meg az alapkutatás irányait".[33] A két terület összefonódása tehát vitathatatlan, gondolva itt akár az egyes szektorokban az egyetemek és a gazdasági társaságok közötti különböző lehetséges együttműködésekre, akár az egyetemi kutatásokból kinövő cégekre, valamint az állam szerepében jelentkező, egyre bővülő feladatkörre. A lehetséges együttműködési formációkat a könyv vonatkozó részei taglalják.

Az innováció fogalma

Ahogy az innovációs folyamat lépéseinél látható volt, a tudásalapú társadalom és gazdaság megteremtéséhez a kutatás-fejlesztés szükséges, de nem elégséges feltétel, azt tágabb kontextusban szükséges vizsgálni. Ugyan bőséges elméleti ismeretanyag áll rendelkezésre, és a gyakorlatnak is egyre nagyobb igénye van a fogalmak tisztázására, egyértelmű és mindenki által egységesen elfogadott definíció az innovációra még mindig nehezen fogalmazható meg. Ebből is következnek az egyes mérési nehézségek, korlátok.[34]

Az egyszerűbb megközelítés felől közelítve az innováció változtatás bevezetését jelenti ahhoz képest, ahogy eddig végeztük a tevékenységet, azért, hogy *a végeredmény jobb legyen*. Ez széles skálán magába foglalhatja egy termék árváltoztatását vagy egy egész piac letarolását, egy régi termék fejlesztését vagy egy meglévő termék új felhasználási lehetőségének felismerését is.[35]

Az Európai Unió *Zöld könyve*[36] szerint „az innováció az újdonságnak a gazdasági és társadalmi szférában megvalósuló sikeres létrehozása, asszimilálása és kihasználása."[37]

Az OECD kutatás-fejlesztés statisztikákat összefoglaló *Frascati-kézikönyvének* 1994-ben kiadott változata az innovációt úgy határozza meg, mint egy ötlet piacképes áruvá vagy szolgáltatássá alakítása új vagy továbbfejlesztett operatív gyártási, forgalmazási vagy új eljárás szociális szolgáltatás nyújtására.[38]

Ugyancsak az OECD az észak-európai innovációs tevékenységről készített összefoglalóját *(Oslo-kézikönyv)* először 1992-ben publikálta ekkor még a termékekre és a gyártási

[33] Rekettye 2018.
[34] Bőgel 2008.
[35] Guzmán-Mares – Castellanos-Villarruel 2017, 135–159.
[36] European Commission 1995.
[37] Bőgel 2008.
[38] OECD 1994.

folyamatra fókuszálva. Az 1997-ben újra kiadott *Oslo-kézikönyvben* már megjelent a szolgáltató szektor szerepe, ezt követően pedig 2005-ben megjelentek a nem technológiai innovációk, mint a marketing- vagy a szervezeti innovációk.[39]

A 2005-ös *Oslo-kézikönyv* definíciója szerint „az innováció új vagy javított termék (áru vagy szolgáltatás), vagy eljárás, új marketingmódszer, vagy új szervezési-szervezeti módszer bevezetése az üzleti gyakorlatba, a munkahelyi szervezetbe vagy a külső kapcsolatokba".[40]

Ezzel szemben az *Oslo-kézikönyv* 2018-as kiadása már a következő definícióval operál: „az innováció új vagy javított termék, vagy eljárás, vagy ezek kombinációja, amely jelentősen különbözik a szereplő korábbi termékeitől, illetve eljárásaitól, és elérhető a vásárlók részére (termék), vagy már használatba vették (eljárás)."[41] Az fogalom egyszerűsítő magyarázata esetén továbbá ideértendő „mindazon tudományos, technológiai, szervezési, pénzügyi és kereskedelmi lépés, amely az innováció megvalósítását ténylegesen szándékolja vagy irányítja".[42] A fogalom újbóli szűkítése azonban kihagyta a marketing- és szervezeti innovációk explicit hangsúlyozását, ezért a továbbiakban a könyvben a kézikönyv 2005-ös definíciója tekintendő irányadónak.

Az innováció típusai

Az innovációk csoportosítása egyrészt az egyes szerzők megközelítésétől, másrészt a vizsgált aspektustól is függ. Rekettye 2018-as munkájában[43] bemutatja, hogy ezek a különböző szerzőknél a folyamatos és diszkontinuus (nem folyamatos, szakadásos),[44] a folyamatos és radikális,[45] az addicionális *(incremental)* és radikális[46] *(breakthrough),* valamint a folyamatos és forradalmi innováció kategóriákra is oszthatóak. Megkülönböztethető továbbá bázisinnováció, fejlesztő innováció és látszatinnováció – ez a megközelítés már a technológiák kisebb mértékű javítását is innovációként ismeri el.[47] A technológiai és a nem technológiai (munkahelyi-szervezeti) innováció elhatárolás is egyre ismertebb.

A folyamatos és diszkontinuus fogalompár esetén a folyamatos innováció már meglévő alapokra építkezik, funkciója azonos, nem igényli a felhasználói szokások változását és a kompatibilitás a régi verzióval továbbra is fennáll. Ez tehát a megismert keretek között és struktúra mellett képes kielégíteni a jövőbeli igényeket. Ezzel szemben a nem folyamatos (diszkontinuus) innováció az egész piacot újradefiniáló forradalmi változás, ami szakít a múlttal, és átlépi a meglévő határokat akár a termék-fogyasztó,

[39] Makó–Illéssy 2014.
[40] OECD 2005.
[41] OECD 2018
[42] OECD 2018.
[43] Rekettye 2018.
[44] Lásd Miller–Morris 1999.
[45] Lásd Cooper 1998, 493–502.
[46] Lásd Johannessen–Olsen–Lumpkin 2001. 20–31.
[47] Lásd Iványi–Hoffer 2010.

akár a termék-más termék vagy termék-adatbázis viszonylatban. A piac újradefiniálása azonban lassabb terjedést eredményezhet, mint a folyamatos innovációk esetén, a kompatibilitás hiánya miatt. Példa lehet a hajlékonylemez *(floppy disk)* és a kompaktlemez (CD) viszonya, a szoftvereknél a verziók vagy programok közötti „olvasási készség", kompatibilitás, de akár az írógép és szövegszerkesztő közötti radikális különbségre is gondolhatunk.[48]

Az inkrementális és a radikális innováció megkülönböztetése esetén az inkrementális az adott piaci szereplő meglévő forrására és tudására épít a fejlesztés során, míg a radikális új tudást, forrásokat kíván bevonni.

A *disruptive* (leváltó vagy bomlasztó, szakító) innováció esetén ugyan a piac meglévő szereplői a terméküket, szolgáltatásukat folyamatosan fejlesztik, azonban nem realizálják, nem veszik figyelembe, hogy a fogyasztói igényekre reflektálva olyan új szereplők lépnek be a szektorba, akik a meglévő struktúrát teljesen átalakítják az új megoldásaikkal.[49]

Városi legenda? Kodak vs. Instagram

Jellemzően a Kodak példáján keresztül szokás bemutatni a nagy szervezetek innovációs képességének hiányát, ez azonban ebben a formában nem fedi maradéktalanul a valóságot. Ugyan más típusú innovációs folyamatok és szervezeti tanulás jellemzi a különböző méretű szervezeteket, de a romboló típusú innovációk ilyen nagy cégeknél is megjelenhetnek.

Például már 1996-ban a Kodak brazíliai, São Pauló-i központjában egy kutatócsoport online képmegosztó lehetőségek kidolgozásával foglalkozott. Az internetre feltöltött fotókban rejlő lehetőséget tehát 14 évvel az Instagram képmegosztó oldal megjelenése előtt felfedezte a cég, azonban szervezeti adottságai miatt végül mégsem volt képes bevezetni ezt az újdonságot,[50] amely később – az anekdotákból már ismert – hanyatlásához is vezetett.

Az *Oslo-kézikönyv* az innovációk következő négy alaptípusát határolja el:

- *termékinnováció:* „olyan áru vagy szolgáltatás bevezetése, amely annak tulajdonságai, rendeltetése vonatkozásában újnak vagy jelentősen megújítottnak, továbbfejlesztettnek tekinthető";
- *eljárásinnováció:* „új vagy jelentősen továbbfejlesztett termelési vagy szállítási módszer megvalósítása. Felöleli a technikában, a berendezésekben és / vagy a szoftverekben bekövetkező jelentős változásokat";
- *marketinginnováció:* „olyan új marketingmódszerek alkalmazása, amelyek jelentős változást hoznak a termék tervezésében, csomagolásában, piaci bevezetésében, reklámozásában vagy az árképzésben";
- *szervezési-szervezeti innováció:* „új szervezési-szervezeti módszerek megvalósítását jelenti a cég üzleti gyakorlatában, a munka szervezésében vagy a külső kapcsolatokban. Innovációs tevékenységnek minősül mindazon tudományos, technológiai,

[48] Miller–Morris 1999, idézi Rekettye 2018.
[49] Bower–Christensen 1995, 43–53.; idézi Rekettye 2018.
[50] Barnett 2017.

szervezési, pénzügyi és kereskedelmi lépés, amely az innováció megvalósítását ténylegesen szándékolja vagy irányítja."[51]

5. táblázat: Az innováció típusai a privát és a közszférában

Privát szektor	Közszféra
termékinnováció	szolgáltatási innováció
folyamatinnováció	folyamatinnováció
szervezeti innováció	szervezeti innováció
marketinginnováció	kommunikációs innováció

Forrás: Makó–Illéssy 2014

Ezt a megközelítést árnyalja, hogy a privát szférában vagy a közszférában megjelenő innováció csoportosításáról van szó. A közszféra innovációs típusai között ugyanis nehezen lehet értelmezni a termék- és marketinginnováció fogalmát, így a közszféra a szolgáltatási és kommunikációs innováció fogalmakkal operál (5. táblázat):

– *szolgáltatási innováció:* „új vagy jelentősen megújított módszerek a szolgáltatás nyújtásában, a felhasználókkal való kapcsolatokban, új vagy megújított logisztikai rendszer a szervezeti ráfordításokban, új vagy megújított támogató tevékenységek (pl. karbantartás, számvitel, adatfeldolgozás), új vagy megújított vezetési rendszer stb.";
– *kommunikációs innováció:* „új vagy jelentősen megújított módszere a közszféra kommunikációjának: a szervezet vagy szolgáltatásának új vagy megújított promóciója, új vagy megújított módszerek a szolgáltatást használók, állampolgárok vagy mások viselkedésének befolyásolására, szolgáltatások első ízben történő bevezetése."[52]

Romboló innováció az IKT-szektorban

Schumpeter innovációs kategóriái is jól azonosíthatók az IKT-szektoron belül:[53]

– új javak vagy a javak új minőségének előállítása, ahol gondolhatunk akár a rendszeresen megjelenő új mobiltelefonok, számítógépek és egyéb IKT-eszközök számára, akár az ezekre készített szoftverek nagyságrendjére is;
– új termelési eljárás / kereskedelmi eljárás bevezetése, ahol visszautalhatunk a korábban már említett új kombinációk fontosságára;
– új piac megnyitása akár földrajzi, akár demográfiai értelemben;
– nyersanyagok vagy félkész áruk új beszerzési forrásának meghódítása;
– új szervezet létrehozása vagy megszüntetése.

A dinamikus-evolúciós közgazdaságtani iskola az infokommunikációs (IKT) szektorban annak intenzív innovációs trendjei miatt jól vizsgálható. A teremtő rombolás megjelenik

[51] Szunyogh 2010, 493–507.
[52] Makó–Illéssy 2014.
[53] Bőgel 2008, 347–348. alapján.

„egyrészt magán a szektoron belül, amikor az új kombinációk (termékek, szolgáltatások, vállalkozások, intézmények) kiszorítják a régieket; másrészt a szektor újdonságai és más szektorok termékei, szolgáltatásai között, amikor egy infokommunikációs termék kiszorít egy egészen másfajta terméket vagy vállalkozást".[54]

Bower és Christensen *romboló* (*disruptive*[55]) *innováció* fogalma tovább árnyalhatja a fogalmat, amely két kategóriára bontja az innovációt. Megkülönböztetnek:[56]

– *Alsó végi rombolást (low-end disruption):* a piac kisebb, gyengébb szereplői azokat a felhasználókat célozzák meg, akik számára a piacvezetők termékei megfizethetetlenek, illetve nincs szükségük minden általuk kínált szolgáltatásra. Idővel, a szolgáltatás fejlődésével ezek a gyengébbként indult szolgáltatók is képessé válnak a piac felső részén található fogyasztók elvárásainak megfelelni megfelelő alternatívát kínálva számukra az esetleges váltásra.
– *Új piaci rombolást (new-market disruption):* azokat célozza, akik számára a piacon lévő termékek nem hozzáférhetők: akár annak tulajdonságai (például ára, bonyolultsága) miatt, vagy mert használatuk csak különleges helyzetekben lehetséges. A nem fogyasztók megcélzása által a versenytársak által nem látott célcsoport igényeit kielégítve tud a belépő cég növekedni és idővel akár komoly versenytárssá válni.

A személyi számítógépek megjelenése

A személyi számítógépek iparában az IBM nagygépei (*mainframe*-ek) szolgálták ki a piac felső végét. Amikor azonban az 1980-as években piackutatók azt jelezték, hogy a tőkeerős cégek igényei mellett az olcsó kisgépekben is potenciális piac nyílik, megszervezték ezek párhuzamos fejlesztését úgynevezett „architekturális innovációként".[57] Ez előbb a piac alsó végét érte el, majd piaci rombolást végzett a nagygépek piacán is, ezzel tehát először az IBM saját részlegei között zajlott a verseny.

Mivel azonban a személyi számítógép egy elérhető tömegcikké vált, új szereplők is megjelentek a piacon. Az 1984-ban kis startupként indult Dell sikerét az üzleti modell innovációjával érte el, amelynek két pillére, hogy csak rendelés után készítették el a gépet, valamint közvetlen online vagy telefonos értékesítést végeztek a viszonteladók kiiktatásával. Mindkét tényező jelentős költségcsökkentést tudott elérni az ügyfelek erős céges kötődése mellett. Mindehhez előfeltétel volt mind a fenti, ipari rombolás (a beszállítói láncok horizontális kiépülése is erre az időre tehető), mind az internet megjelenésének felforgató hatása (például az elsők között kiépült online felhasználói támogatás).[58] A cég 2000-től további jelentős piaci részesedést nyert el versenytársaitól az árak agresszív csökkentésével.[59]

Ebből következik, hogy a gazdasági alkalmazás mellett a társadalmi szempontokat is szükséges figyelembe venni. Makó és Illéssy a szervezeti innovációk kapcsán foglalják

[54] Rekettye 2018.
[55] Míg Schumpeter a *destruction,* addig Bower és Christensen a *disruptive* jelzőt használja munkájában. (Bower–Christensen 1995.)
[56] Bőgel 2008, 348–351.
[57] Bőgel 2008, 352.
[58] Benoit 2005.
[59] Herstatt et al. 2006, 55.

össze, hogy a technológiai innovációk bevezetésének a társadalmi innovációk előfeltételei, a munkahelyi-szervezeti innovációk is alapvető fontosságúak egy-egy újítás bevezetése kapcsán, enélkül a fejlődési lehetőségek elhalasztása is bekövetkezhet. Ezzel felhívják „a figyelmet a technológiai innovációk bevezetését kísérő gyakori mulasztásra, amikor az érintett társadalmi és gazdasági szereplők megfeledkeznek arról, hogy a változások – főleg azok radikális formái – sikerének elengedhetetlen előfeltétele a szervezeti és társadalmi tanulási folyamatok jelentős időigénye".[60] Ugyanígy az infokommunikációs technológiák, a digitalizáció megfelelő felkészülés, tudás nélkül nem képesek automatikusan beváltani a hozzájuk fűzött reményeket.

Technológia: veszélyek és tudatosítás

Bányász foglalja össze részletesen, hogy „az infokommunikációs technológiák elterjedése új típusú fenyegetettségek megjelenését hozta magával",[61] az emberek pedig nincsenek felkészülve rá, hogy olyan ártalmatlannak tűnő platformokon, mint a közösségi média is kiberbűnözés (például *social engineering*) vagy álhírek áldozata lehet valaki.

Ezért is nagyon fontos a tudatosítás, hogy az emberek mint magánszemélyek és mint szervezetekben tevékenykedő aktorok is tisztában legyenek a rájuk leselkedő veszélyekkel. Erre különböző innovatív megoldások születtek, úgymint tudatosító kampányok vagy biztonságtudatosságot erősítő szervezeti képzéseket nyújtó platformok (például a magyar Cyex[62]).

Kiberbiztonsági innováció

Haig Zsolt és Kovács László meghatározása alapján „civil terminológia szerint a cybertér az elektronikus kommunikációs eszközök és rendszerek (számítógép-hálózatok, internet, telefonvonalak, műholdas rendszerek stb.) és a rajtuk található szolgáltatások, információk alkotta virtuális tér vagy világ összefoglaló neve, amit igen gyakran alkalmaznak a virtuális valóság világára is. A cybertér katonai értelmezése azonban kiterjeszti ezt a dimenziót, és nem csak a számítógép-hálózatok működési környezetét érti rajta. Napjainkban a harctéren elektronikai eszközökből (rádiók, radarok, navigációs eszközök, harctéri azonosító berendezések stb.) és számítógépekből olyan hálózatokat hoznak létre, ahol igen nehéz különválasztani egymástól a rendszert alkotó komponenseket."[63]

Ez kiegészíthető azzal, hogy már kevésbé szofisztikált okoseszközök is képesek zavarokat okozni, például amikor egy futóapplikáció adatai vázolták fel egy katonai támaszpont elhelyezkedését.[64] A civil szféra felé közelítve, de még mindig a kritikus állami szektort vizsgálva látható, hogy ma már a (beépíthető) orvostechnológiai eszközök

[60] Makó–Illéssy 2014.
[61] Bányász 2017, 55–74.
[62] *Cyex – Cyber Security Awareness Platform*. Weboldal: https://cyex.io/ (A letöltés dátuma: 2020. 05. 26.)
[63] Haig–Kovács 2008, 62.
[64] Hern 2018.

ugyanúgy meghekkelhetők,[65] mint a számítógépek (a ma már létező kiborgok[66] eszközeiről nem is beszélve), vagy hogy a szenzitív egészségügyi adatok – akár az emberek saját eszközein, akár kormányzati rendszerekben – digitalizáltak, így feltörhetők, ezért látni kell, hogy a technológiai fejlődésre a kiberbiztonságnak is minden aspektusból szükséges reagálnia.

Bár a fogalom elsőre még mindig távolinak tűnhet, olyan további, sok embert érintő közelmúltbeli példákat is ide lehet sorolni, mint az amerikai egészségügyi szervezet (Health and Human Services) elleni támadás 2020 márciusában,[67] a Covid–19 felfutási időszakában, az izraeli vízhálózat elleni támadás 2020 áprilisában[68] vagy pár héttel később egy iráni kikötő megbénítása.[69] Magyarországon ugyanígy elképzelhető lenne a közműhálózatok vagy akár az önvezető 4-es metró elleni fiktív támadás vagy a kormányzati adatbázisok (például a központi címregiszter) ellen elkövetett hekkertámadás.[70] Az ellopható adatmennyiség nagysága nem is tűnik túl abszurdnak, ha összevetjük egy 2020 májusában nyilvánosságra került adatlopással, ahol az EasyJet közel kilencmillió ügyfelének adatai kerültek jogosulatlan kezekbe, több esetekben a személyes mellett bankkártyaadatokkal kiegészülve.[71]

A kiberfenyetéseknek alapvetően négy fajtáját különböztetik meg: a kiberbűnözés, a hacktivizmus és kiberterrorizmus, a kiberkémkedés és a kiberhadviselés.[72]

Porkoláb összefoglalja az amerikai Védelmi Tudományos Tanács törekvéseit, miszerint már abban az időben a következő irányokba terveztek fejlesztéseket a szemléletmód és az együttműködések radikális átalakítására való szándék mellett:

- mesterséges intelligencia és autonóm öntanuló gépek;
- ember és gép közötti együttműködés;
- gépek által támogatott műveletek;
- fejlett ember-gép közös egységek;
- hálózatalapú félautonóm fegyverrendszerek.[73]

Az Európai Unió is kulcstechnológiaként tekint az infokommunikációs technológiára, amely meghatározó szerepet tölt be mind a társadalomban, mind a gazdaságban. Utóbbi esetén ez mintegy 4,8%-os részesedést jelent azzal, hogy az üzleti kutatási beruházások 25%-a szintén idetartozik. Az EU Horizont 2020 K+F programjában is megjelenik minden pillérben (kiváló tudomány; ipari vezető szerep; társadalmi kihívások). A prioritási területek széles köre található itt az intelligens, környezetkí-

[65] Fahey 2020.
[66] Harbisson: *Brain Bar Budapest*.
[67] Shira–Jacobs 2020.
[68] Kovacs 2020.
[69] Warrick–Nakashima 2020.
[70] Lehetséges forgatókönyvekért lásd Kovács–Krasznay 2017, 3–16.; Kovács–Krasznay 2010, 44–56.
[71] Stubbs–Holton 2020.
[72] Krasznay 2012, 142–51.
[73] Porkoláb 2016, 19–28. A jövő várható trendjeiről részletesebben pedig lásd Defense One 2015.

mélő és integrált közlekedéstől az 5G technológián át a robotika és intelligens terek kérdéséig.[74]

A könyv holisztikus és kapcsolatrendszer-alapú megközelítése elengedhetetlen az ezzel a jövőbe mutató szemlélettel való lépéstartáshoz.

Az innováció folyamatának alapmodelljei: Rothwelltől Marinova és Phillimore-ig

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace."[75]

Az innováció folyamatának fejlődése, rendszerré válása Rothwell csoportosítása szerint öt változat vagy generáció megkülönböztetésével írható le.[76] Itt az egyes generációk fokozatosan komplexebbé és integráltabbá válnak, új gyakorlatok épülnek be, fejlődésükkel rávilágítanak az előző generációk korlátaira is. Marinova és Phillimore Rothwell generációit csoportosította és rendezte újra, így a vizsgálat új dimenzióit építette be a csoportosításába (lásd 6. táblázat).[77] Az innovációs folyamat modelljének megértése azonban nem értelmezhető az ezeket mozgató ipari és gazdasági változások megértése nélkül, ezért az egyes generációknál – ahol szükséges – ismertetjük az elméleti előrelépést okozó gazdasági környezetet is.

6. táblázat: Innovációs generációkat összefoglaló főbb modellek

Generáció	Rothwell (1994)	Marinova és Phillimore (2003)
1.	Szükségletteremtő	Feketedoboz-modell
2.	Szükségletkövető	Lineáris modellek
3.	Interaktív *(coupling)* modell	Interaktív *(interactive)* modell
4.	Integrált modell	Rendszermodell
5.	Párhuzamos vagy integrált modell	Evolúciós modell
6.	-	Területi innovációs modell

Forrás: Taferner 2017 alapján saját szűkítés

Jelen fejezet Rothwell, valamint Marinova és Phillimore generációs besorolásának logikáját követi azzal, hogy a közös kategóriákat mindkét szakirodalom alapján (is) a megfelelő mélységben bemutatjuk, amely bemutatás főként, de nem kizárólagosan Taferner[78] összehasonlító logikáját követi.

[74] Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal: Horizont 2020.
[75] Newton Lee, a *Counterterrorism and Cybersecurity: Total Information Awareness* szerzője.
[76] Rothwell 1994.
[77] Marinova–Phillimore 2003.
[78] Taferner 2017, 47–60.

A feketedoboz

A tudomány, a kutatás-fejlesztés és az innováció az 1950-es évekig elhanyagolt vizsgálati terület volt. Solow[79] vizsgálata során arra a felismerésre jutott, hogy a gazdasági fejlődés egyik oka a technológiai változás. Ennek hatására a feketedoboz-elmélet már felismeri, hogy a kutatás-fejlesztésbe befektetett erőforrások (input) új technológiaként jelentkeznek (output). Ekkor azonban még nem tartották fontosnak elemezni, hogy mi történik a „dobozban", milyen folyamattal lesz az inputból output, a cél csupán a szükséges növekedés elérése volt.

Ebben az időben a felismerés mellett a történelmi környezet – a nyugati hatalmak technológiai sikerei – is löketet adtak a K+F-be való befektetés indoklásának és a tudományos szabadság alapjainak lefektetéséhez. Megjelentek az államilag finanszírozott kutatóhelyek mellett a sikeres vállalati K+F-részlegek is.

Az elmélet korlátja ugyanakkor, hogy kihagyja a vizsgálódásból, hogy valójában hogyan működik az innováció, ahogyan figyelmen kívül hagy minden nem kutatás-fejlesztési alapú innovációforrást is. Ezért idővel szükségessé vált „belenézni", hogy mi is zajlik a dobozban,[80] megérteni a tanulás és a technológia létrejöttét, valamint ehhez kapcsolódó ösztönző politikákat kidolgozni.[81]

Lineáris modellek

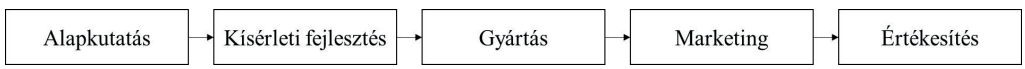
Az 1960–1970-es években indult az a folyamat, amely a kutatás-fejlesztést és ezzel együtt a termékek és folyamatok fejlesztését kívánta stimulálni. Az idetartozó két modell – a Rothwell-féle első és a második generációs innovációs modellek – tehát „az innovációt egy véges, meghatározott szakaszokból álló folyamatként értelmezik, ahol a szakaszok egymásra épülnek, és az egyik szakasz lezárását követően kezdődik a következő szakasz",[82] tehát láncszerű felépítés jellemezte őket. Megállapították, hogy ezen tevékenységek egymást követő sorozata képes elvezetni egy piacképes termékhez.[83]

A szükségletteremtő, technológiavezérelt innovációs modell. A második világháborút követő közel húsz évben[84] úgy tűnt, hogy a tudomány és a technológia, az ipari innováció képes megoldani a társadalmi problémákat a bekövetkezett ipari expanzión és gazdasági növekedésen keresztül. A meglévő szektorok hatékonyabbá, illetve jobb minőségűvé tudtak válni a gépesítés és a technológia által (mezőgazdaság, textilipar), míg a fejlődés

[79] Robert Solow amerikai közgazdász, kutatási területe a gazdasági növekedés elmélete.
[80] Marinova–Phillimore 2003, 44–53.
[81] Bajmócy 2008, 26–46.
[82] Vukoszavlyev–Polereczki–Kovács é. n., 1–11.
[83] Marinova–Phillimore 2003.
[84] Vonatkozó időszak: 1950-es évek – 1960-as évek közepe.

új területek megjelenését is lehetővé tette (számítástechnika, gyógyszeripar). Ez új munkahelyek létrejöttét hozta magával, és egyúttal a kereslet, a hagyományos értelemben vett jólét növekedésével is járt. Közpolitikai oldalról is támogatást kapott a növekedés: az egyetemek kutatási kapacitásainak erősítésén, az adekvát képzéseken, állami laboratóriumokon és egyes ipari K+F-programokon keresztül. A korszak innovációs megközelítése tehát *a több K+F több új termék piacra lépéséhez vezet* logikát tükrözte, az innovációs lánc az alapkutatásokból indult ki.[85] A modell „alapgondolata, hogy az innovációs folyamat valamilyen új kutatási eredményből származik, ezek a kutatási eredmények részben a technológiai fejlődés ösztönző hatásának köszönhetők, ugyanakkor a fejlesztés és az innováció elébe megy a fogyasztói igényeknek, kvázi teljesen kizárja a folyamatból a piaci keresletet”,[86] a marketingszemlélet hiányzik a modellből.

Ezt a szakirodalom *technology-push* innovációs modellként tartja számon (1. ábra). Magyarra ezt lineáris toló, technológiai tolás kifejezésekkel fordították, de *szükségletteremtő vagy technológiavezérelt innovációs modellnek* is nevezik.[87]



1. ábra: Szükségletteremtő vagy technológiavezérelt innovációs modell
Forrás: Piskóti 2007

A szükségletkövető, piacvezérelt innováció. Az 1960-as évek közepétől[88] ugyan a termelés és a növekedés szintje magas maradt, azonban a gyártás hatékonyabbá válása következtében a foglalkoztatás nem tudott tovább növekedni, adott esetben még csökkent is. A piaci verseny kiéleződött, a túlkínálat a valós igényekre reflektáló értékkínálat felé terelte a cégeket. Vállalati oldalról a növekedésre és a diverzifikációra helyezték a hangsúlyt azzal, hogy ugyan még mindig jelentek meg új termékek, a fókuszba a létező technológiák kerültek, a kereslet-kínálat közötti egyensúly kialakulása volt a cél. Ezzel a technológiai változások észszerűsítésére helyezték a hangsúlyt, ahol a piaci részesedés növeléséhez a hatékonyan működő cégek közötti versengés fontos eszközévé vált a marketing, a marketinginnováció. A hangsúly tehát K+F-ről a keresletre helyeződik át. Közpolitikai oldalról szintén a keresletoldal hangsúlyosabbá válása figyelhető meg, az USA-ban például próbálkozások jelentek meg a közbeszerzések – mint az ipari innovációt stimulálni képes eszköz – alkalmazására. A túlzottan keresletre helyezett hangsúly azonban magában foglalja annak a veszélyét, hogy – a K+F elhanyagolása miatt – egy radikális piaci vagy technológiai változáshoz nem lesz képes alkalmazkodni az adott cég.[89]

[85] Rothwell 1994.
[86] Vukoszavlyev–Polereczki– Kovács é. n.
[87] Vukoszavlyev–Polereczki– Kovács é. n.
[88] Vonatkozó időszak: 1960-as évek közepe – korai 1970-es évek.
[89] Rothwell 1994.

A szakirodalom ezt *market-pull* (vagy *need-pull*) modellként ismeri (2. ábra). Magyarul lineáris húzó, piaci húzás modellként vagy *szükségletkövető, piacvezérelt innovációként* emlegetik.[90]

2. ábra: Szükségletkövető innovációs modell [91]
Forrás: Piskóti 2007

Ezt a Rothwell-féle második generációt már sok tekintetben előrébb mutatónak tartják, „mégis a lineáris modellek közös problémája a szükségletkövető modellt is terheli, azaz mindkét modell egy belátható, egyirányú, véges, a részek egymásra épülését feltételező metodikát követ".[92] A kutatások kimutatták, hogy mindkét modell egy extrém, atipikus megjelenési formája volt a technológiai kapacitásnak és a piaci igényeknek,[93] az a kérdés azonban, hogy mi volt előbb, a technológia vagy az arra való igény, az innovációkutatás tyúk-tojás problémájává vált.[94]

Interaktív modellek

Látható, hogy a lineáris modellek túlzottan leegyszerűsítették a tudomány, a technológia és a piac közötti viszonyt, az innovációs folyamat azonban ennél sokkal komplexebb, nemcsak sorozatos lépésekre épül, hanem folyamatos, körkörös interakciókon alapul. A szűk értelemben vett innováció pedig nemcsak a végső termékhez köthető, hanem a folyamat bármely pontján megfigyelhető jelenséggé válik. Egyúttal fontos figyelembe venni, hogy nemcsak zárt, szervezeten belüli interakció, kommunikáció befolyásolja, hanem szervezetek közötti kapcsolatokat is figyelembe kell venni a vizsgálat során. Az interaktív modellek, amelyekbe beletartoznak a Rothwell-féle interaktív és integrált modellek, már ötvözik a szükségletteremtő és szükségletkövető modelleket, azonban még nem képesek megválaszolni azt a kérdést, hogy miért sikeresebb az egyik, míg sikertelenebb egy másik vállalat.[95] A modellek legnagyobb eredménye „az időbeli sorrendiség megkérdőjelezése" és „az innovációs folyamat szereplői közti komplex interakciók megértésének igénye."[96]

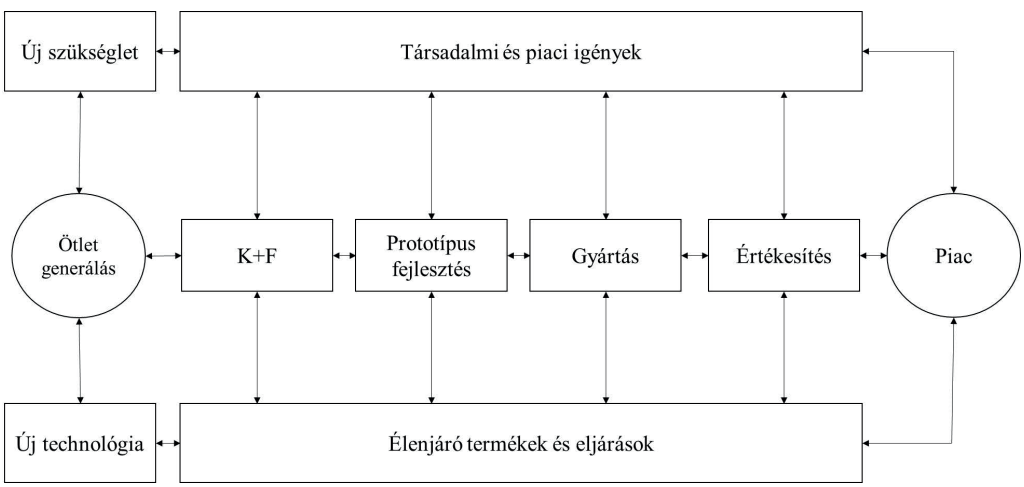
[90] Vukoszavlyev–Polereczki–Kovács é. n.
[91] Az angol nyelvű változat a *sales* szóval fejezi ki egyben azt, amit a magyar szerzők marketing és értékesítés részekre bontanak. Piskóti 2007.
[92] Vukoszavlyev–Polereczki–Kovács é. n.
[93] Rothwell 1994.
[94] Marinova–Phillimore 2003.
[95] Marinova–Phillimore 2003.
[96] Bajmócy 2008.

Az interaktív (coupling) modell

Az 1970-es éveket[97] – két olajválsággal szegélyezve – az infláció, a keresleti telítettség és a strukturális munkanélküliség jellemezte, de egy technológiai újratervezést is magukkal hoztak. Mindez a vállalatok új adaptációs stratégiáját kényszerítette ki. Fontos szemponttá vált a takarékosság, ez magával hozta a sikeres innováció megértésének igényét azért, hogy csökkenteni tudják a sikertelen próbálkozások számát. Ennek hatására nőtt az innovációt tanulmányozó kutatások száma is.[98]

A kutatások eredményeképpen összekapcsolták a két lineáris modellt, és egy visszacsatolásos modellt alkottak, ahol a piac igényeit nemcsak a folyamat elején, hanem annak valamennyi lépésében meghatározónak tekintették, valamint itt deklarálták azt is, hogy az innováció végeredménye a kezdetekben pontosan nem meghatározható. Ez jóval nagyobb rugalmasságot biztosít a folyamatban az első második generációs modellekhez képest, azonban ez a nyitás megfelelő, komplexitásra nyitott szemléletet követelt a projekt koordinátorától is,[99] hiszen ezek az interaktív és kölcsönösen függő, elhatárolható lépések a céget már annak tágabb környezetéhez kötik, és megjelennek a szervezeten belüli tényezők mellett a szervezeten kívüliek is.[100]

A rugalmasságnak azonban még megvannak a korlátjai. Bár a kapcsolási megközelítés visszacsatolási hurkokat tartalmaz, a megközelítés alapvetően még mindig egy lineáris, szekvenciális modell, korlátozott funkcionális integrációval.[101]



3. ábra: Harmadik generáció: interaktív (coupling) innovációs modell

Forrás: Vukoszavlyev–Polereczki–Kovács é. n.

[97] Vonatkozó időszak: korai 1970-es évek – 1980-as évek közepe.
[98] Rothwell 1994.
[99] Vukoszavlyev–Polereczki–Kovács é. n.
[100] Rothwell 1994.
[101] Preez–Louw 2008, 546–558.

Az innováció ezen harmadik generációját *coupling vagy interaktív modellnek* is nevezik (3. ábra[102]), amelynek több gyakorlati megjelenési formáját is ismeri a szakirodalom.

Az integrált modell

Az 1980-as évektől[103] újra gazdasági fellendülés figyelhető meg, kezdetben az alaptevékenységekre és alapvető technológiákra fókuszálva, majd technológiai stratégiát kidolgozva. A termelési stratégiát is megváltoztatta az új típusú IT-alapú termelési eszközök megjelenése. Megjelent a cégek közötti stratégiai partnerség, amelyet gyakran állami ösztönzők támogattak. Ezekben a hálózatokban pedig már nemcsak nagyvállalatok, hanem innovatív kisvállalatok is helyet kaptak.[104]

Az integráció a szervezeten belül és a szervezet határait áttörve is megjelenik már ebben az esetben, így alakítva ki egy többszereplős, esetleg hálózatos innovációs gondolkodást.[105] A gyakorlatban az innováció a szervezet alapvető funkcióival párhuzamosan fut, ahol a hatékonyságra való törekvés következtében megjelentek:

- horizontális stratégiai szövetségek és együttműködő K+F-konzorciumok,
- stratégiai vertikális együttműködések, különösen a beszállítói együttműködésekben,
- a cégen belül nagyobb hangsúly helyeződik az átfogó és párhuzamos integrációra, hogy javulhasson a valós idejű információfeldolgozás.[106]

Ugyan az integrált modell korlátját jelenti, hogy a termék bevezetését már nem veszi figyelembe – hiszen az innovációnak szerves része kellene, hogy legyen a piacra történő bevezetés, adaptáció és folyamatos fejlesztés[107] –, azonban így is nagy előrelépést jelentett a szigorú egymás utáni lépések sorozataként ábrázolt korábbi modellekhez képest.[108]

Rendszermodellek

Az innováció komplexitása már a szervezeti határokat átlépő entitások létrehozását indokolja a hierarchikus mechanizmusok helyett.[109] Ez a modelltípus az innovációt már olyan – dinamikus, ipari, stratégiai és innovációs – rendszerként értelmezi, amely kiemelt hangsúlyt helyez az interakciókra, az összekapcsoltságra és a különböző szinergiákra. Előnye, hogy felismeri, amennyiben egy szervezetnek nincs elég erőforrása saját fejlesztésekre, ezt a hálózatban, más szervezetekkel együttműködve is megteheti,

[102] Vukoszavlyev–Polereczki–Kovács é. n.
[103] Vonatkozó időszak: korai 1980-as évek – korai 1990-és évek.
[104] Rothwell 1994.
[105] Vukoszavlyev–Polereczki–Kovács é. n.
[106] Preez–Louw 2008.
[107] Preez–Louw 2008.
[108] Rothwell 1992, 221–240.
[109] Bajmócy 2008.

így a kis- és középvállalatok is képesek versenyezni a nagyvállalatokkal. Ennek a típusú szervezeti innovációnak az előnye:

- kis cégek is képesek élvonalbeli technológiák használatára a hálózaton belül egymás kölcsönös támogatásával;
- készségek összeadódása és kollektív tanulás, amiből a hálózat minden szereplője profitálhat;
- kulcsemberek mobilitásának lehetősége a hálózat cégei között;
- a készségek (újra)kombinálhatók a gazdasági nehézségek kiküszöbölésére;
- az innovációra fordított idő és pénz csökkenthető;
- a hálózat kisebb innovatív cégek számára is lehetőséget nyújt a szektorba történő belépéshez;
- a hálózat cégei rugalmasan és olcsón tudnak működni, beleértve az általános működési költségeket is.[110]

Ezzel egy időben ezek a hálózatok rugalmasabbak, és könnyebben alkalmazkodnak a változó piaci vagy ügyféloldali körülményekhez, hiszen megfelelő erőforrásaik vannak a technológiai kockázatok és a bizonytalanság kezelésére. A formális tudás mellett már a tacit tudás elsajátítása is lehetséges ebben a rendszerben.

A modell jellemzője továbbá, hogy dinamikusan változik, az egyes szereplők jelenléte nem állandó, azok fejlődésével, változásával maga a rendszer is folyamatosan átalakul. Fontos a bizalom építése is a tagok között, hiszen sok esetben egyszerre van jelen köztük a kooperáció és a verseny.

Fontos kapcsolódó fogalmak: az *innovációs láncok,*[111] amelyek a termelők és a beszállítók, valamint a forgalmazók kapcsolatára utalnak; a *koalíciók,*[112] amelyek a cégek mellett már a közintézmények és a szektorspecifikus kutatóintézetek kapcsolatára is utalnak. A *stratégiai hálózatok vagy szövetségek*[113] pedig hosszú távú együttműködésekre utalnak, amelyeket egyes vállalatok konkrét célra hoztak létre a versenyelőny megszerzésére. Edquist szerint a rendszermodellek kilenc tulajdonságát különböztethetjük meg:[114]

- a modell középpontjában az innováció és a tanulás áll;
- holisztikus és interdiszciplináris megközelítést alkalmaz;
- természetesen megjelenik benne a történelmi perspektíva;
- az egyes rendszerek között különbségek vannak, és nincs optimalitás;
- a kölcsönös függőség *(interdependence)* és a nem lineáris természet fontos eleme;
- magába foglalja a terméktechnológiák mellett a szervezeti innovációkat is;
- az intézmények központi szerepet kapnak benne;
- ugyanakkor jelen van a bizonytalanság és a koncepciók szétterjedése;
- inkább egy tág fogalmi keretet ad, mint szűk elméleti megalapozást.

[110] Marinova–Phillimore 2003.
[111] Marinova–Phillimore 2003.
[112] Marinova–Phillimore 2003.
[113] Marinova–Phillimore 2003.
[114] Edquist 1997.

A rendszermodelleknél már az állam szerepe is explicit módon megjelenik, ahol proaktív közpolitikákkal és a megfelelő szabályozási környezet biztosításával tudja támogatni annak hatékonyságát.

Evolúciós modellek

Taferner Rothwell ötödik generációs (paralel vagy integrált) modelljét párhuzamba állítja Marinova és Phillimore (2003) evolúciós modelljével,[115] így azokat itt együtt mutatjuk be.

A Rothwell-féle modell az 1990-es években megjelent gyors innovációkra való igényre reflektál, és tartalmazza mind a lineáris, mind az interaktív és integrált modellek lényeges jellemzőit, azonban „a tudás által vezérelt gazdaságban integrált módon közelíti meg az innovációt", és „a modellben az innováció gyors és folyamatos implementálásának az alapja az integrált hálózatok és rendszerek intenzív és rugalmas használata".[116]

Ezzel párhuzamosan az evolúciós megközelítés azon a feltevésen alapszik, hogy a neoklasszikus közgazdaságtan nem volt képes kezelni a technológiai innovációk minőségi változását, ezért az elemzők evolúciós hasonlathoz nyúltak ezen modell kidolgozása során. A modell alapelveit már az ipari forradalomról szóló részben is említettük.

Az elméleti kidolgozói a hagyományos darwini értelemben vett biológiai megközelítés mellett merítettek az egyensúlyi termodinamikából, a szervezéselméletből és a közgazdaság nem szokványos (heterodox[117]) megközelítéséből is. A koncepció alapja a történeti és társadalmi kontextus mellett az emberek és szervezetek közötti kapcsolatok, alapvető eleme a bizonytalanság, így elveti a „tökéletes racionalitást" és a „maximalizálás" lehetőségét. A piaci tökéletlenségeket tekinti az innováció alapjának,[118] ebből kiindulva pedig egyenesen odáig jut, hogy a kormányzatnak a piaci kudarcok kezelése helyett az innovatív vállalatok terjedését kellene elősegíteni.[119]

Saviotti[120] a következőképpen foglalja össze az evolúciós modellek jellemzőit:

- *Variációképződés (generation of variety):* az innovációkat a mutációkhoz hasonlítja, amik az új termék-, folyamatváltozatok stb. létrejöttét segítik. Nem minden mutáció sikeres, de amelyik igen, az gyakran felül tud kerekedni a megelőző változaton.
- *Szelekció (selection):* az előző attribútumhoz kapcsolódó fogalom, a különböző változatok közül az „marad életben" (terjed el a piacon), amelyik a leghatékonyabban tud alkalmazkodni a saját piaci körülményeihez.
- *Reprodukció és öröklés (reproduction and inheritance):* az öröklés itt azoknak a termelő vállalatokban zajló mechanizmusoknak a metaforája, amelyek során a minden-

[115] Taferner 2017.

[116] Vukoszavlyev–Polereczki–Kovács é. n.

[117] „A heterodoxia a kor kialakult gyakorlatától, az elfogadott gondolkodási modellektől eltérő megoldásra vagy megoldási kísérletre utal, a nem szokványos intézkedés pedig olyan, amivel korábbi időszakokban éltek, vagy amire kevés gyakorlati példa van." Bod 2013, 9.

[118] Marinova–Phillimore 2003.

[119] Marinova–Phillimore 2003.

[120] Saviotti 1996; idézi Marinova–Phillimore 2003.

napi működésről vagy egy-egy fejlesztésről döntenek, azonban ezt a céges kultúrát nehéz átvinni más cégekbe.
- *Alkalmasság és alkalmazkodóképesség (fitness and adaptation):* a legalkalmasabb túlélése az adott környezetben a közgazdaságtanban is értelmezhető, a sikeresebb megoldások tudnak elterjedni.
- *Populációperspektíva (population perspective):* a változatosság is fontos szempont, így nemcsak az átlagértékeket, hanem a sokaságban megjelenő eltéréseket is érdemes vizsgálni.
- *Elemi interakciók (elementary interactions):* a gazdaságban a versengés és az együttműködés vizsgálata tartozik ide.
- *Külső környezet (external environment):* alapvetően azt a társadalmi-gazdasági környezetet foglalja magában, ahol a technológia fejlesztése történik. Beletartozik a szabályozás (például szellemi tulajdonjogok), a piaci struktúra, a kialakult sztenderdek. A zöldtechnológiák megjelenésével már a természeti környezet is tekinthető idetartozónak.[121]

A modell hátrányát jelenti, hogy míg a múltra és a jelenre magyarázó erővel bír, az előrelátó képessége azonban erősen korlátozott.

Területi innovációs modellek

Németh fogalmazta meg találóan, hogy „miközben az információs és kommunikációs technológiák korában a termelő vállalkozásoknak meg kell felelniük a globális kihívásoknak, ugyanakkor a regionális és helyi igényeket is figyelembe kell venniük, különös tekintettel a vállalati kultúra társadalmi, gazdasági és társadalmi beágyazódására és piaci szerepére".[122]

Ezért a területi innovációs modellek az egyes területek innovációs és technológiai fejlődésének a földrajzi determináltságának koncepcióján alapulnak. Álláspontjuk szerint a terület földrajzi, társadalmi és épített környezete is befolyásolhatja annak innovációs sikerét, ugyanakkor ez adja egyediségét, megismételhetetlenségét is. Az adott térségben kialakított kapcsolatok, az ezek alapjául szolgáló egyszerű kapcsolattartás és bizalom kialakítja a megfelelő környezetet a fejlesztésre és egy kollektív, tacit tudás felhalmozására. Másik megközelítésből vizsgálva az ott élő és dolgozó emberek életminőségét meghatározó tényezők (családalapításhoz kedvező környezet, megfelelő klíma) is befolyásolhatják a terület vonzóerejét. Ugyanakkor a két szempontot figyelembe véve az is egyértelmű, hogy más típusú üzleti környezet tud kialakulni egy kertvárosi környezetben, mint a Szilícium-völgy atmoszférájában.

[121] Bajmócy 2008.
[122] Németh 2006, 6.

Camagni a területi innovációs modellek következő komponenseit emeli ki:
- termelés (például innovatív vállalat);
- az innovációt elősegítő aktív területi kapcsolatok cégek és szervezetek között;
- különböző területi, innovációt ösztönző társadalmi-gazdasági szereplők (magán- és közszféra intézményei egyaránt);
- meghatározott kultúra és képviseleti folyamat;
- dinamikus helyi kollektív tanulási folyamat.[123]

Az együttműködés regionális formája számos hagyományos gazdasági együttműködési formához képest pozitív változást képes indukálni, ilyen például az innovációs potenciál növelése vagy a szinergia az innovációban, így a korábbi versenyszellem ellen ható kooperáció rugalmas, ösztönző rendszerré tud válni.
A területi innovációs modelleknek számos megjelenési formáját ismeri a szakirodalom:
- innovációs miliő;
- ipari körzetek;
- új ipari terek;
- helyi termelési rendszerek;
- regionális innovációs rendszerek;
- tanuló régió.[124]

7. táblázat: Az együttműködések jellemzői eltérő termelési rendszerekben

Együttműködések	Hagyományos tömegtermelésben	Regionális gazdasági integrációban
Célja	Piaci pozíciók javítása	Piaci pozíciók javítása
Eszköze	Versenykorlátozó megállapodások	Innovációs potenciál növelése
Területei	Piac közeli területeken: az árak, termelési volumen vonatkozásában	– A termelési folyamat csaknem minden fázisában – Számos egyéb területen: pl. marketing, szakképzés
Szereplői	Azonos iparág cégei	– Különböző iparágak cégei – Cégek és beszállítók – Cégen belül: menedzserek és munkások
Technológiai alapja	Nincs	Modern rugalmas technológia
Hatásai	– Hatékonysági veszteségek – Innovációs hajlamot elkényelmesítő hatás – Kedvezőtlen rendszerhatások – Versenyszellem csorbulása	– Szinergia az innovációkban – Végtelen rugalmasság hálózati szinten

Forrás: Kocsis–Szabó 1996; idézi Buzás 2007, 54.

A következő alfejezetekben a területi innovációs modellek két tipikus megjelenési formáját mutatjuk be, amelyek alapvetően bírnak a fent ismertetett jegyekkel, azonban a szakirodalom egy-egy jellemző jegyük, hangsúlyuk miatt külön kezeli őket. A regionális innovációs rendszereket a következő, az innovációs rendszerekkel foglalkozó fejezetben mutatjuk be.

[123] Camagni 1991, 121–144.; Marinova–Phillimore 2003.
[124] Részletes ismertetésükért lásd Buzás 2007.

Innovatív klaszterek

Szanyi meghatározása szerint a földrajzi koncentrációra épülő klaszter „olyan regionális szintű kapcsolatokra épülő együttműködési rendszer, amelyben többféle típusú, de tevékenységi kör alapján egymáshoz kapcsolódó szereplő közösen cselekszik azzal a céllal, hogy saját és partnerei, valamint a régió versenyképességét egyidejűleg javítsa. Az együttműködés egyik fontos területe a tudásgenerálás és -megosztás."[125]

A klaszterek négy fő jellemzője:

regionális koncentráció urbanizációs előnyökkel: a pozitív „externális hatások a nagyobb piacokból, a helyben rendelkezésre álló potenciális együttműködő partnerek elérhetőségéből, a nagyobb, speciális igényeket is kielégítő munkaerőpiac létéből és azokból a szolgáltatásokból adódnak, amelyeket az agglomeráció magas színvonalon, hatékonyan és olcsón képes a benne működő vállalkozások számára biztosítani";[126]

- tevékenységi szakosodás ipari körzetek kialakulásával, így lokalizációs előnyök a méretgazdaságosságból fakadóan;
- heterogén összetétel (innovációt hordozó, támogató intézmények), választékgazdaságossági előnyök;
- a verseny és az együttműködés egyidejű jelenléte.[127]

Ez a képződmény olyan tudásátadási és együttműködési lehetőségeket biztosít, amelyek lehetőséget adnak akár a multinacionális vállalatokkal való verseny, akár a velük való együttműködés kereteinek megteremtésére.

Tanuló régiók

A tanuló régiók megjelenése is a tudásalapú gazdaság és társadalom kialakulásához köthető. Az már a korábbiakból is érzékelhető, hogy a térség „gazdasági szerkezete, a társadalmi és politikai kapcsolatok struktúrája, kulturális szerveződése együtt és külön is meghatározzák fejlődése dinamikáját",[128] azonban Florida definíciója szerint mindemellett a „régiók a tudás formálásának és a tanulásnak válnak központjaivá a globális, tudásintenzív tőkés társadalom és gazdaság keretében, mivel maguk alakulnak tanuló régiókká. A tanuló régiók pedig úgy működnek, hogy azok a tudás, a gondolat gyűjtőhelyei és forrásközpontjaiként megfelelő környezetet nyújtanak a tudás, a gondolat és a tanulás tevékenységének folyamatos fejlődéséhez, fejlesztéséhez"[129] különböző hálózatok, partnerségek kialakításával. Céljuk a kis- és középvállalkozások foglalkoztatási és innovációs potenciáljának kihasználása, a helyi gazdasági struktúraváltás, összekapcsolva ezt az oktatási és képzési paletta és annak tartalma korszerűsítésével. Mindezt

[125] Szanyi 2010, 109.
[126] Szanyi 2010, 109–110.
[127] Szanyi 2010, 109–110.
[128] Németh 2006, 3.
[129] Florida 1995, 527–536.; idézi Németh 2006, 3.

a különböző cégek, civil szervezetek, oktatási és egyéb, például kutatás-fejlesztési intézmények, kamarák, önkormányzatok bevonásával.[130]

A régiók funkcióját és szerepét mutatja be Hassink modellje[131] a tanuló régiókról, aki három szintet különböztet meg, így az lehet:

– „térbeli eredménye a makroszintű társadalmi változásoknak;
– mikroszintű egyvelege a vállalkozások tanulásának, az innovációnak és a térbeli kapcsolódásoknak;
– mezoszintű elméleti regionális fejlesztési modell."[132]

Ezekben mind megjelenik az interaktív tanulás, a szervezeti tanulás, az intézményes tanulás, továbbá a tanulva tanulás is, és fontos hangsúly van a tanuláshoz kapcsolódó intézményrendszeren is. A régiófejlesztéssel foglalkozó kutatások is három, nem karakteresen elváló csoportot alkotnak:

– elméleti-strukturális modell;
– az elméleti szereplőorientált modell;
– tevékenységorientált modell.[133]

A modellek átfogó összegzése

Makó és szerzőtársai[134] egy átfogó összegzést adtak a különböző innovációs modellekről, amikor két nagy csoportba rendezték azokat. A tradicionális megközelítés a szűkebb, visszacsatolások nélküli lineáris megközelítésre épít, ahol a tudományos kutatást tekinti az ipari innovációk alapjának. A vizsgálat fókusza a radikális innovációk generálásán van, az inkrementális innovációk, a tacit tudás és az innováció diffúziójának mikéntje itt még másodlagosaknak tekinthető, az explicit és kodifikált tudáson van a hangsúly. A rendszer a tudomány, technológia és innováció *(science, technology, innovation, STI)* hármasára épül. Az állami szerepvállalás szempontjából az irányzat a hagyományos, neoklasszikus közgazdaságtani eszközökhöz nyúl, ahol a piac önszabályozó képessége mellett csak a diszfunkciók (piaci kudarcok) megoldása lehet az állam feladata.

A szerzők Schienstock és Hämäläinen[135] munkája alapján bemutatják ennek az elméletnek a kritikáját is: a szűk megközelítésben értelmezett innovációs folyamat ugyan létezik, de inkább kivételnek, mint a fő szabálynak tekinthető, ugyanis a tudásgenerálás nem egy, a környezetétől elszigetelt folyamat, forrása pedig nem kizárólagosan a K+F. Így

[130] Németh 2006, 7.
[131] Hassink 1999, 93–116.
[132] Németh 2006, 4.
[133] Németh 2006.
[134] Makó–Illéssy–Heidrich 2019, 66–73.
[135] Schienstock–Hämäläinen 2001.

a tisztán tudományalapú innovációt szembeállítják a tevékenységalapú innovációval, ami bárhol és bármikor létrejöhet több szereplő visszacsatolásokon alapuló együttműködése által. A rendszer alapja a „csinálni, használni és interakcióban lenni" *(doing, using and interacting, DUI)* megközelítés. A hangsúly már nemcsak a radikális innovációkon van ennél a megközelítésnél, a társadalmi beágyazottság és a tacit tudás fontos szerephez jut. Az állam szerepe rendszerszinten, a szereplőkkel való interakciókban teljesedik ki.[136]

8. táblázat: Az innováció megközelítésének fejlődése: szűk és átfogó megközelítés

Dimenziók	Szűk megközelítés	Átfogó megközelítés
Innovációs modell	Lineáris	Rekurzív, ismétlődő lépésekből álló
Az innovációk legfontosabb megjelenési formája	Radikális	Inkrementális
	Technológiai	Nem technológiai
A tudás forrása	Tudomány, explicit és egyéni	Praktikum, tacit és kollektív tudás
Az innovációgenerálás módja	Tudomány, technológia és innováció (STI)	Csinálni, használni és interakcióban lenni (DUI)
Fő szektor	Termelés	Nem szektorspecifikus
Közpolitikai megjelenése	Piaci kudarcok felől	Rendszerszinten

Forrás: Makó–Illéssy–Heidrich 2019, 68.

Szervezetek rendszerszintű modellezése

Ahogyan az előző részben bemutattuk, az innovációs rendszereknek számos formáját ismeri a szakirodalom. A korábban ismertetett alapmodellek vagy generációk mellett – ebben a részben – a nem lineáris innovációs elméletek azon modelljei szerepelnek, amelyeknek aktorai mentén történik a vizsgálódás a tanulmány második felében. A fejezetben a nemzeti, a szektorális, a technológiai és a regionális innovációs rendszereket, valamint a Helix modellek különböző formációit mutatjuk be.

Innovációs rendszerek

Az innovációs rendszerek nézőpontjából való vizsgálat előnye, „hogy egy megközelítési módot, nem pedig egy mereven rögzített keretet kínál".[137] Nem vonatkoztat el a technikai, társadalmi, gazdasági rendszertől, amiben az innováció létrejön és elterjed, hanem a folyamatot úgy tekinti, mint ami „szükségszerűen valamilyen társadalmi, intézményi, kulturális közegbe ágyazottan folyik".[138]

[136] Makó–Illéssy–Heidrich 2019.
[137] Vas–Bajmócy 2012, 1248.
[138] Vas–Bajmócy 2012, 1236.

9. táblázat: Az egyes innovációsrendszer-megközelítések legfőbb jellemzői

	Nemzeti	Szektorális	Technológiai	Regionális
Kutatási terület, kutatási cél	Az országok eltérő innovációs (növekedési) képességének magyarázata	A szektorok eltérő innovációs képességének, új szektorok elterjedésének magyarázata	Új technológiák elterjedésének magyarázata	A régiók sikerességének magyarázata
A vizsgálat területi szintje	Ország	A globálistól a lokálisig	A globálistól a lokálisig	Régió, lokális térség
Legfontosabb evolúciós közgazdaságtani alapok	Variáció, szelekció, útfüggőség	Technológiai rendszer, iparágak schumpeteri dinamikája	Technológiai rendszer, technológiai rés *(niche)*	Variáció, szelekció, regionális útfüggőség, iparágak dinamikájának térbelisége
Legfontosabb szakpolitikai következtetések	Korlátozott racionalitás, optimalizálás elvetése, politikaalkotás mint „kísérletek és kudarcok" sorozata, piaci elégedetlenségek helyett rendszerelégedetlenségek	Iparági tudásbázis jellegétől függő beavatkozás, iparági helyzettől függő szakpolitikai mozgástér	Terminológia létrejötte mellett terjedésének elősegítése, elterjedés közbeni interaktív tanulás elősegítése, rezsimváltás irányítása	Differenciált innovációs politika szükségessége, a régió mint a beavatkozás adekvát területi szintje

Forrás: Vas–Bajmócy 2012, 1249.

Az innovációs rendszerek négy megközelítése sem jelent merev határokat, részben átfedő vizsgálati keretet is szolgáltathatnak, célszerűség alapján kombinálhatók, és folyamatosan változnak – ezek adják egyszerre előnyüket és használatuk nehézségét is. Legfontosabb jegyeik összehasonlítását mutatja be a 9. táblázat.

Nemzeti innovációs rendszer

A nemzeti innovációs rendszer – és ennek alrendszerei – befogadó és dinamikus rendszert alkotnak, amelyek a magán- és közszféra szereplőinek hálózataira épülnek. Ez „a köz- és magánszféra mindazon intézményeit jelenti, amelyek tevékenysége és interakciója hozzájárul az új technológiák megjelenéséhez, átvételéhez, módosításához és elterjedéséhez".[139] Fontos, hogy ezek a szereplők és tényezők képesek egyaránt segíteni vagy hátráltatni az innovációs folyamatot.

A megközelítés szűk értelmezése a K+F+I-hez és a tudományos és technológiai szervezetek munkájához való hozzájárulást, így a nemzeti teljesítményt és specializációt vizsgálja, míg a tágabb keret az interakciók közegét befolyásoló tényezőkre (szervezetek, intézmények, kapcsolatok, infrastruktúra) is kiterjed.[140]

Nelson és Rosenberg kiemelték azt a – már többször említett – tényt, hogy az innovációnak sokkal több tényezőre van szüksége, nem csak kutatás-fejlesztésre. Olyan intézményeket hangsúlyoznak itt, mint az oktatás, a képzés és az átképzés, amelyek nemcsak a szakemberkínálatot tudják alakítani, de a munkások hozzáállását is a technikai fejlődéshez. Fontos emellett a munkaerőpiac helyzetére (tárgyalások, elkötelezettség)

[139] Freeman 1987; idézi Vas–Bajmócy 2012, 1238.
[140] Vas–Bajmócy 2012, 1239.

gyakorolt hatása is. A pénzügyi intézmények és a cégek vezetésének módja szintén befolyásolja, hogy a menedzsment milyen technikai lépéseket választ. Ebből következően tehát úgy foglalják össze véleményüket, hogy természetellenes lenne egy nemzeti innovációs rendszert annak gazdasági rendszerétől elválasztva elemezni, vagyis nem lehet innovációs szakpolitikákat felállítani a gazdaság, az oktatás, de akár a nemzetbiztonság figyelmen kívül hagyásával.[141]

A konkrét szervezetek és intézmények megnevezése azonban nehézkes, az egyes empirikus vizsgálatok függvénye. Edquist és Johnson szerint a *szervezetek (organizations / players)* közé sorolhatók:

- a vállalatok,
- az innovációhoz kötődő szolgáltató szektor,
- az egyetemek,
- a kutatóintézetek,
- az oktatási és képző intézmények,
- a politikai, közigazgatási intézmények,
- a finanszírozó szervezetek
- az ügynökségek.[142]

Az ezek közötti *kapcsolatok* formálják a rendszert. Ugyanakkor el kell különítenünk a társadalmilag konstruált[143] *intézményeket (institutions / rules),* amelyek Edquist megközelítése szerint „közös szokások, normák, rutinok, kialakult gyakorlatok, szabályok vagy törvények összessége, amelyek az egyének és csoportjaik, valamint a szervezetek közötti kapcsolatokat és interakciókat szabályozzák".[144] Fontos szerepe van az *infrastrukturális háttértényezőknek* is.

Ez a bizonytalansággal teletűzdelt rendszer egyúttal adaptív szakpolitikákat igényel, igényli, hogy a szakpolitika-alkotók felismerjék azokat a problémás területeket, ahol nem működik elégségesen a rendszer, és ott avatkozzanak be.[145]

A modell gyengesége, hogy a mai globális folyamatokban nem kezelhető minden nemzeti szinten, egyszerre jelenik meg a szubnacionális és a nemzetek feletti kooperáció erősítésére való igény az innováció területén is.

Szektorális innovációs rendszer

A fenti okok miatt kialakultak a nemzeti innovációs rendszer mellett az iparági innovációs minták, és azok térbeli változásának vizsgálatára megalkották a szektorális (iparági) innovációs rendszerek koncepcióját. Malerba meghatározása szerint itt „a szereplők

[141] Nelson 1993, 13.
[142] Edquist 2005; idézi Vas–Bajmócy 2012, 1240.
[143] Vas–Bajmócy 2012, 1240.
[144] Edquist 2005, 182.; idézi Vas–Bajmócy 2012, 1240.
[145] Vas–Bajmócy 2012, 1240–1242.

aktívan részt vesznek egy adott iparág termékeinek kifejlesztésében és gyártásában, az iparági technológia előállításában és felhasználásában".[146] A rendszer elemei:

- a szereplők (egyének és szervezetek);
- a vállalaton belüli és kívüli kapcsolatok;
- a tudás jellege és a tanulási folyamatok;
- az alapvető technológiák, inputok és kapcsolataik;
- a variációképző és a szelekciós folyamat; és
- az intézmények.[147]

A különböző szektorok *különböző iparági innovációs mintákat* formálnak attól függően, hogy

- mekkora a valószínűsége a tudásra fordított erőfeszítés realizálásának;
- mennyire sajátítható ki az így megszerzett tudás a versenytársakkal szemben;
- a tudás kumulatív jellege, vagyis mennyire befolyásolják a korábbi innovációs faktorok az új innovációk megjelenését (technológia-, vállalat-, szektor- vagy térségszinten); valamint
- milyen jellegű tudásról beszélhetünk (általános vagy specifikus, hallgatólagos vagy kodifikált, egyszerű vagy komplex, elkülönült vagy rendszerbe ágyazott).[148]

Ezért a különböző kombinációkkal, technológiai rezsimmel rendelkező szektorok különböző szakpolitikai beavatkozást igényelnek, és valamennyi innovációs rendszernél, így itt is jelen van az a bizonytalansági faktor, az optimális környezet felvázolására való képesség hiánya, amely alapján előre nem számítható ki, hogy mely beavatkozás fog sikerrel járni.

Technológiai innovációs rendszer

A szektorok mellett – de szakirodalmával részben átfedésben – az egyes technológiák megalkotására irányuló innovációs folyamatot befolyásoló tényezők is rendszerbe foglalhatók. Carlsson és Stankiewicz definícióija szerint ez a rendszer „a technológiák megalkotásában, terjedésében és felhasználásában érintett, egymással is kapcsolatban álló szereplők dinamikus hálózata, akiket specifikus intézményi közeg befolyásol".[149]

Irányulhat egy *tudásterületre* (az adott tudás több termékben is megjelenhet), *egy termékre* (az adott termékben több technológia is jelen lehet), továbbá *termékek egy körére* (kiegészítő vagy helyettesítő termékek egy szektoron belül).[150]

[146] MALERBA 2005, 63–82.; idézi VAS–BAJMÓCY 2012, 1242.
[147] VAS–BAJMÓCY 2012, 1242.
[148] VAS–BAJMÓCY 2012, 1242–1243.
[149] CARLSSON–STANKIEWICZ 1991, 93–118.; idézi VAS–BAJMÓCY 2012, 1244.
[150] VAS–BAJMÓCY 2012, 1244.

Ez annyiban tér el a szektorális megközelítéstől, hogy az adott technológia létrehozása és elterjedése is kulcskérdés a sikerhez, így az adott rendszer *fejlődési blokkokká* nőhet ki, ahol a tág értelemben vett vállalkozási készségek és a tudás diffúziója is kulcstényező a sikerhez. A szakpolitikai szerep is utóbbi, elterjedést támogató területen kellene, hogy erősödjön.[151]

Regionális innovációs rendszer

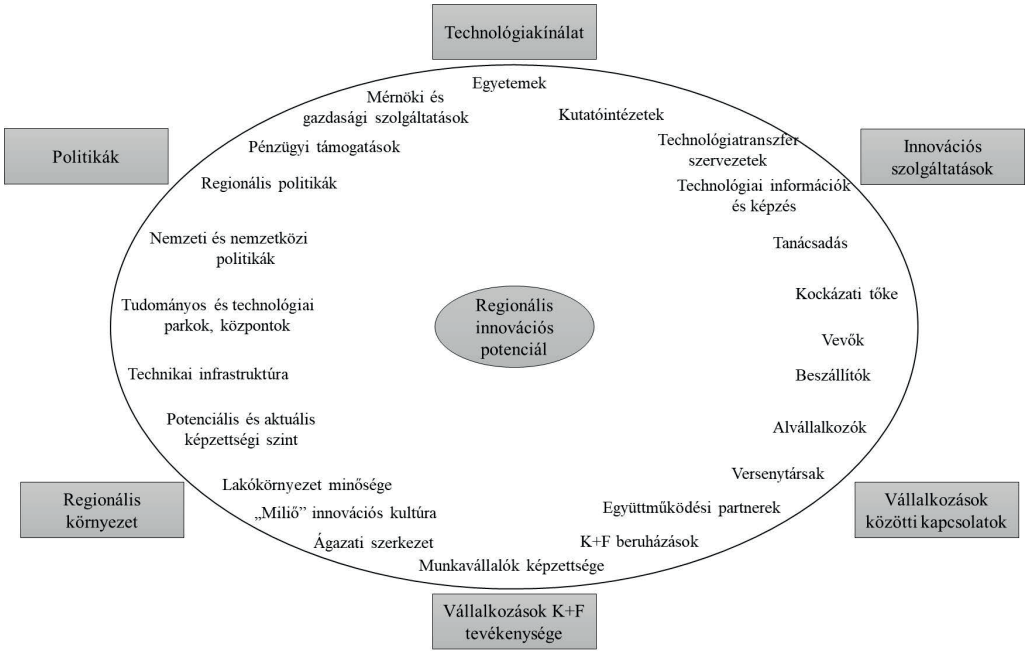
Az innovációs rendszerek utolsó vizsgált alkategóriája a regionális innovációs rendszer, amely területi, szubnacionális szinten járulhat hozzá a területfejlesztési célokhoz, regionális innovációs szakpolitikák kialakításához (*smart specialization,* klaszterek).

A térbeliség ebben az esetben nemcsak egy adott méretet vagy formát jelent, hanem az azáltal determinált tudást és erőforrást is, amelynek egyedisége megkülönbözteti az adott régiót a többi, hasonló formációtól, egyedi karaktereket, másolhatatlanságot (vagy nehéz leképezést) biztosítva ezzel. Ezt biztosítják a régió dinamikusan fejlődő, mégis adott szereplői és hálózatai, valamint a kapcsolataikban megjelenő és elterjedő tudás, amely a földrajzi koncentráció miatt is jobban áramolhat, mint tenné azt nagyobb térbeli közegben.[152]

A szereplők tudásteremtés és -terjedés, valamint a tudáskiaknázás alrendszerekre bonthatók, amelyek az innovációs rendszerben együttműködnek (lásd 4. és 5. ábra[153]).

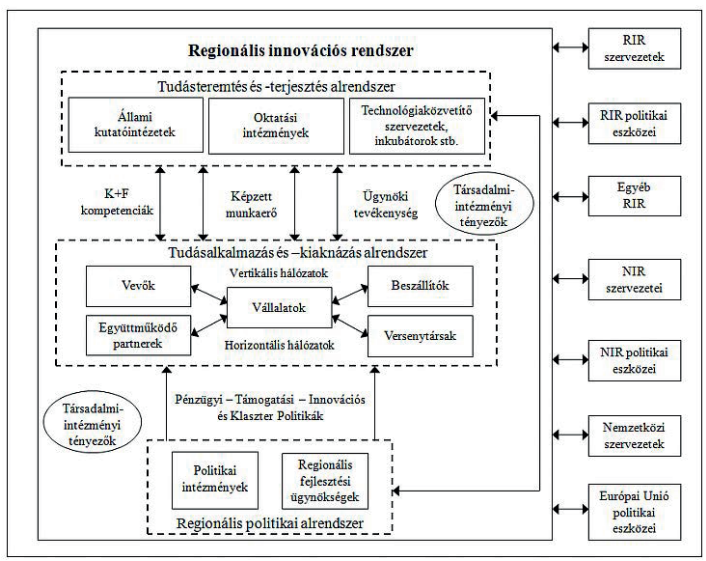
- A tudásteremtés és -terjedés alrendszer részei (főképp közfinanszírozású szervezetek és folyamatok):
  - oktató, képző intézmények;
  - egyetemek, amelyek forrásai a helyi tudásáramlásnak, mivel kimondottan céljuk a tudás megteremtése és terjesztése;[154]
  - állami kutatóintézetek;
  - munkaerőképző szervezetek;
  - technológiatranszfer-szervezetek.
- A tudáskiaknázási alrendszer részei:
  - a vállalati szektor szervezetei;
  - a vállalati szektor tudásmegosztási kapcsolatai.[155]

[151] Vas–Bajmócy 2012, 1245.
[152] Vas–Bajmócy 2012, 1246.
[153] Vas 2017, 18.
[154] Ponds–Oort–Frenken 2010, 233.
[155] Vas–Bajmócy 2012, 1247.



4. ábra: A regionális innovációs rendszer alkotóelemei

Forrás: Buzás 2007, 56.



5. ábra: A regionális innovációs rendszerek felépítése

Forrás: Vas 2017, 18.

Az állam szerepe egy széles skálán mozog, amely függ a politikai-gazdasági hagyományoktól is. Az egyetemek és az ipar, de akár a kis- és középvállalkozások együttműködése az egyetemekkel viszonylag nagy regionális szinten – azt azonban figyelembe kell venni, hogy a tudásáramlás *(knowledge spillover)* nem korlátozódik regionális szintre.[156]

Ezek a tudáshálózatok – a természetes szektorális különbségeikkel – visszavezetnek a regionális innovációs rendszerekhez és a tanuló régió koncepcióhoz, ami képes bevonni a vizsgálódásba a regionális különbségeket is. A hálózat fogalma alatt nemcsak az informális személyes hálózatokat és a formális kutatási együttműködéseket kell érteni, hanem a munkaerő mobilitását is az adott földrajzi területen belül, illetve a köz- és magánszféra között.[157] Ide tartozik továbbá az innovációs infrastruktúra, szakpolitika, helyi kulturális háttér és gazdasági közeg.

Az együttműködés másik előnye, hogy elosztja a szereplők között a költségeket és bizonytalansági faktorokat.[158] Például – a tudásáramlás mellett az egyetemek – akár infrastruktúrát is tudnak biztosítani a kis- és középvállalkozásoknak, hogy azok ezzel is csökkenteni tudják kiadásaikat.

A Helix modellek[159]

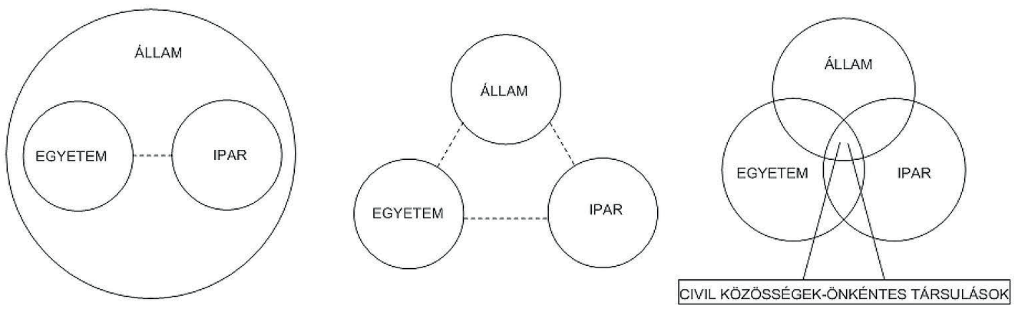
Az inkluzív Triple Helix („hármas spirál") modell az innovációs rendszer egyik tágan értelmezett dimenziója,[160] amely három szereplőt foglal magába: az állam, az egyetemek és az ipar közötti kapcsolatot írja le egy nem lineáris, visszacsatolás-alapú modellben. Ez a tudásteremtés komplex hálózatát mutatja be,[161] hiszen a tudás átadása és átvétele két területen különösen intenzív, így érzékenyebb a tudástranszfer hatékonyságára: az oktatás és az üzleti szféra világában.[162] A modell kiforrott állapotban a tudásalapú gazdaság kialakulását és fejlődését modellezi.

A kapcsolatok típusa alapján három megjelenési formáját ismerjük. A kapcsolatok minősége lehet *statikus modell* gyenge visszajelzésekkel, *laissez-faire,* illetve *kiegyensúlyozott Helix modell* erős visszacsatolásokkal, ahol az interakció erős szintje figyelhető meg.[163] Az elsőben – amely a szovjet blokkban, a latin-amerikai országokban, illetve még egyes európai országokban is létezik – az állam behálózza a másik két szereplőt, és döntő befolyással bír rájuk. A második verzióban a szereplők éles határokkal különülnek el egymástól, szigorúan meghatározott a köztük lévő kapcsolat – például

[156] Ponds–Oort–Frenken 2010, 233
[157] Ponds–Oort–Frenken 2010, 234–235
[158] Callon 1994, 395–424.
[159] Bishimbayeva–Nurasheva–Nurmukhanbetova 2017, 2361–2372.
[160] Inzelt–Bajmócy 2013, 11.
[161] Etzkowitz–Leydesdorff 1995, 14–19.
[162] Szabó 1999, 279.
[163] Choi–Lee 2017, 1465–1478.

Svédországban és az Egyesült Államokban.[164] A harmadik modellben interaktív kapcsolat és klaszterek jelennek meg, ahol az aktorok egymás szerepét is átvéve, egymástól kölcsönös függőségben stimulálják a fejlődést, miközben relatíve egyenlőnek tekinthetők[165] (6. ábra).

Ennek megfelelően az innovációs folyamatot leginkább generáló harmadik formát tekinti át a fejezet. Magyarországon a rendszerváltás óta – ha nem is vegytiszta formában, hanem az átmenet specifikumait figyelembe véve – utóbbi kiépítése figyelhető meg.[166] Ennek kiemelése azért is fontos, mert a szocializmusban jellemző állami befolyás után nehéz rövid idő alatt kiépíteni egy máshol évtizedes hagyományokkal bíró, szerves fejlődéssel kialakult ökoszisztémát, pedig az együttműködés mind a versenyképességet, mind a regionális fejlődést segíteni tudná.[167]



6. ábra: A Triple Helix modell három megjelenési formája

Forrás: Etzkowitz 2008, 12–16.

A modell túllép a lineáris modellek azon elképzelésén, hogy az innovációt elkülönült tevékenységek sorozataként kezelje,[168] azt egy visszacsatolásokkal erősített folyamatnak tekinti. Alapvetően három elemből építkezik: az egyetemek innovációban játszott meghatározó szerepéből, ami során egyenrangúként kezelendők az iparral és a kormányzattal; továbbá jellemzője a kormányzati szabályozás fokozatos háttérbe szorulása és ezzel szemben kölcsönhatások előtérbe kerülése; valamint a szereplők

[164] Klaszterek: „az azonos vagy rokon iparágakba tartozó vállalatok szövetsége annak érdekében, hogy közösen lépjenek fel a piacon, ill. egymás között technológiai és ipari kapcsolatokat létesítsenek és információt cseréljenek.” Szívós 2014, 54.; Kotsis–Nagy 2009, 125.

[165] Etzkowitz 2008, 1–8.

[166] Vesd össze Inzelt 1998, 1–11. „átmenti gazdaság a négyzeten” gondolatmenetével.

[167] Farinha–Ferreira 2013, 1–25.

[168] Kotsis–Nagy 2009, 121.

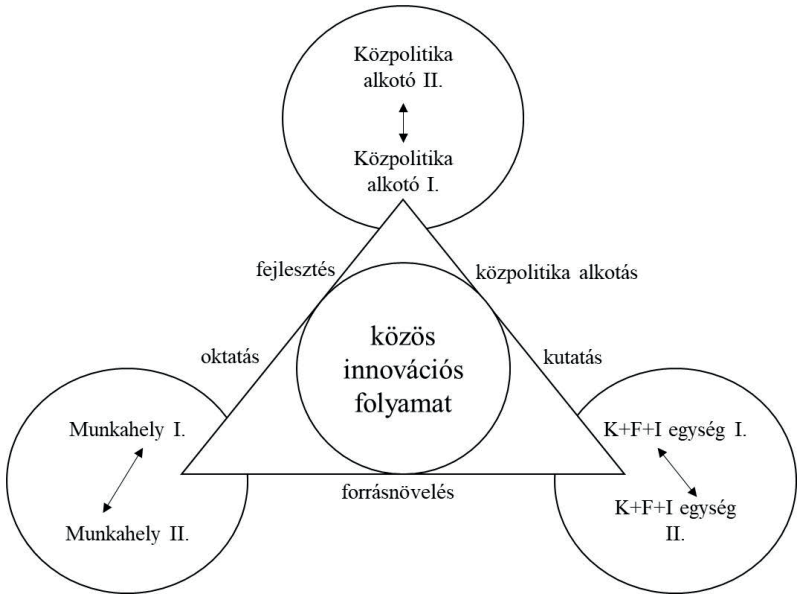
közötti funkcióátvétel.[169] „A három szféra keresztmetszetében hibrid intézményeken (pl. egyetem által alapított inkubátorházakon, spin-off vállalatokon) keresztül valósul meg az interakció. A három szféra fejlődése, koevolúciója a közöttük lévő folyamatos kommunikáció által biztosított."[170]

A modellnek több továbbgondolt, kiterjesztett változata ismert. Ezek közül Ramstad *kiterjesztett Triple Helix* vagy *innovációgeneráló modelljének (innovation generating model)* célja, hogy egy széles körű, rendszerszintű keretet adjon az innováció támogatására összehangolva a hagyományos innovációs politikát a szervezet- és szolgáltatásfejlesztéssel makro-, mezo- és mikroszinten.

Ez a hagyományos nemzeti innovációs rendszer modelltől a következőkben tér el:

- Mivel a tudomány- és technológiai politikába általánosan nem értik bele a társadalmi innovációkat (szervezeti, szolgáltatási, közpolitikai innovációk stb.), ezért a nemzeti innovációs rendszer modellbe sem építik be, ezt a hiányt igyekszik meghaladni az innovációgeneráló modell, és a technológiai mellett a társadalmi innovációkat is bevonja a vizsgálatba, hiszen már a hagyományos neoklasszikus gazdasági növekedési koncepcióknál összefonódó endogén tényezőként jelenik meg a társadalmi és technológiai innováció kölcsönhatása.
- A nemzeti innovációs rendszer modell egyik kritikája, hogy túlságosan a közszférára fókuszál, miközben – az innovációgeneráló modell szerint – a magáncégek az innováció fő mozgatórugói.[171] Utóbbi modell mellérendelt felekként kezeli az egyes szereplőket (ezzel megegyezik a hagyományos Triple Helix modellel), azonban elhatárolva, különböző szerepeik szerint. Megállapítja, hogy az innováció motorját valójában a munkahelyek jelentik, az itteni tudás alakul át új termékké vagy szolgáltatássá.
- Ez a modell nemcsak a szervezetek közötti kapcsolatra helyezi a hangsúlyt, hanem a szervezeten belüli folyamatokat is vizsgálja.
- A makro-, mezo- és mikroszintek közötti csatornák kölcsönös kapcsolatban vannak egymással (nem csak egy top-down csatornára épül az innovációs rendszer).[172, 173]

[169] Dzisah–Etzkowitz 2008, 101–115.; 103.-at idézi Szabó 2012, 4. fejezet.
[170] Vas 2012, 200.
[171] Azonban ez a gondolat sem általánosan elfogadott, teljesen szembemegy például Mazzucato vállalkozóállam-koncepciójával.
[172] Ramstad 2009, 181–197.
[173] Ramstad 2016, 4.



7. ábra: Elise Ramstad kiterjesztett Triple Helix vagy innovációgeneráló modellje

Forrás: Ramstad 2009, 186.

Az innovációgeneráló modell kiegészül egy lehetséges eredmény *(outcome)* résszel, ahol a különböző egységek kapcsán a következőket foglalja össze a szerző:

- Munkahelyek: átfogó fejlődés, jobb megoldások, növekvő innovációs kapacitás és a rendszer jobb megértése, jobb teljesítmény és életminőség-javulás *(quality of working life, QWL).*
- K+F+I-egységek: jobb szakértelem, oktatás, európai, nemzetközi vagy regionális tevékenység, új módszerek és szolgáltatások, publikációk, több K+F+I-tevékenység és finanszírozás.
- Közpolitika-alkotók: javulás a közpolitika, a stratégia és az értékelés terén, jobb szakértelem a munkáról és az innováció infrastrukturális helyzetéről, a pénzügyi eszközökben is javulás és új, nem hivatalos szabályok.
- Társadalom: javuló teljesítmény és életszínvonal (QWL), általános ismeretek és gyakorlatok jönnek létre az innovációs rendszerben és annak tevékenysége során, adatvagyon, Big Data, értékelő rendszerek, kiterjedtebb infrastruktúra és állampolgári közösségi gyűjtés *(civil crowdsourcing).*[174]

A két modell közötti fő eltérés a szerepmeghatározásban található: míg a hagyományos Triple Helix modell az állam, egyetem és ipar kapcsolatából indul ki, addig a kiterjesztett verzió ennél szélesebb körben törekszik vizsgálni az innovációs rendszert.

[174] Ramstad 2009, 186.

10. táblázat: A két modell közötti szerepmeghatározási különbségek

Triple Helix modell	Kiterjesztett Triple Helix / innovációgeneráló modell	Új szereplők a második modellben
állam	közpolitika-alkotók	ipar közeli szereplők (pl. szakszervezetek)
egyetem	K+F+I-egységek	kutatóhelyek
ipar	munkahelyek	közszféra munkahelyei és civil szervezetek

Forrás: Ramstad 2016, 3. alapján saját szerkesztés

A Triple Helix modell további két kiterjesztett változata a Quintuple Helix és a Quadruple Helix modellek.

A civil szféra tudásteremtésben játszott szerepét először a Mode 3 modell emelte ki. [175] A Quadruple Helix modell beemeli a tudásteremtés folyamatába „a médiaalapú és kultúraalapú közösségi teret és a civil társadalom közegét".[176] Itt is megjelenik a kölcsönös függőség és szerepátvétel, mint a hármasspirál-elméletben. „A modell megalkotói a negyedik helix alatt olyan szempontokat is vizsgálat alá vontak, mint a kultúra, az innovációs kultúra, értékek és életmód, a multikulturalizmus, a kreativitás, a média, a művészet és a művészeti egyetemek. A kultúra sokszínűsége és heterogén mivolta elősegíti a kreativitást, és elengedhetetlenné válik az új tudás és az innováció létrehozásában."[177]

A Quintuple Helix modell a társadalom és gazdaság (természeti) környezetét is figyelembe veszi a fenti négy aktor mellett. A modellt – a természeti keret miatt – a globális felmelegedés kutatásához is megfelelő keretnek tartják.[178]

Ezek a modellek már foglalkoznak a fenntartható és inkluzív fejlődéssel, és bevonják a tudásalapú gazdaság, tudásalapú társadalom és tudásalapú demokrácia fogalmakat a tudományos vitába.[179]

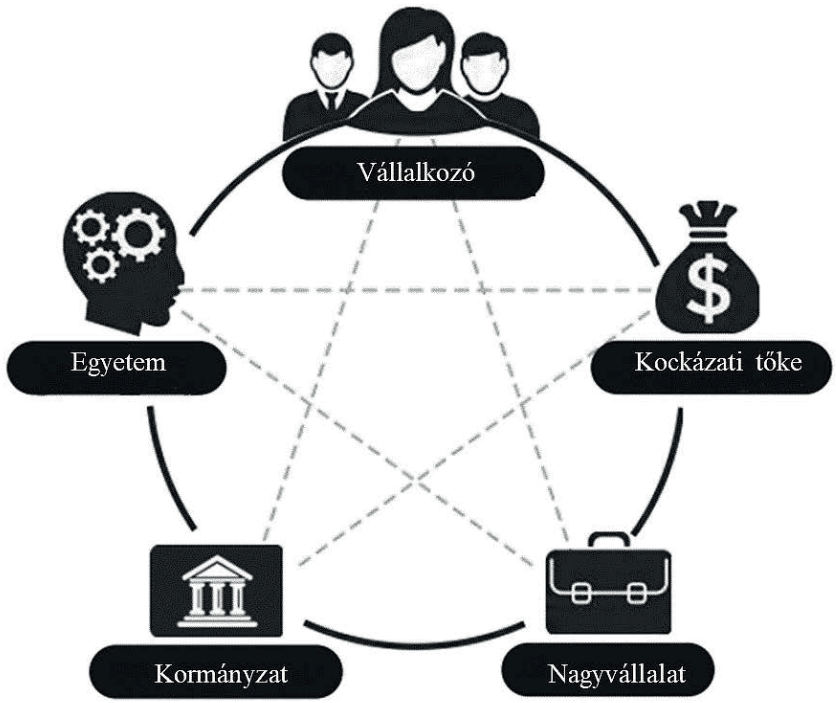
Az ötszereplős MIT-modell

Ezek közel állnak a korábban már hivatkozott kiberbiztonsági innovációs ökoszisztémával foglalkozó találkozón prezentált ötszereplős innovációs ökoszisztémát leíró modellhez, amely a vállalkozók, a kockázati tőke, a nagyvállalatok, a kormányzat és az egyetemek kapcsolataként írja le a hálózatot.

Az együttműködés célja, hogy az ötletekből megoldások szülessenek, amelynek eszközei az akcelerátorok, a tehetséggondozó programok, a tesztelő közegek és a szabadalmi jogokat biztosító közpolitikák kialakítása. Kulcskérdésnek tekintik továbbá az emberi erőforrás kérdését, az infrastruktúra, a kereslet és a kultúra / ösztönzőit az ökoszisztémában.[180]

[175] Carayannis–Campbell 2009, 201–234.; Carayannis–Campbell 2010, 41–69.
[176] Vas 2012, 203.
[177] Vas 2012, 204.; Carayannis–Campbell 2019.
[178] Carayannis–Barth–Campbell 2012, 1–12.
[179] Carayannis–Barth–Campbell 2012.
[180] Murray–Budden 2019, 1–28.

A kutatócsoport ezt a modellt kifejezetten a kiberbiztonság vizsgálatára alkalmazza, azonban egyéb területeken is relevánsnak tekinthető.



8. ábra: Az MIT ötszereplős innovációs ökoszisztémát leíró modellje
Forrás: Morray–Budden 2019, 7. alapján saját fordítás

Az a tény, hogy vezető kutatócsoportok témaspecifikusan is elkezdték vizsgálni a kiberbiztonsági innovációs ökoszisztémát, tovább erősíti a könyv alaptézisét, miszerint a szereplők erős együttműködése lehet a kulcs a kiberbiztonsági innovációk sikeres megszületéséhez és elterjedéséhez.

Az innovációs rendszer szervezeteinek jellemzői

Az előző két fejezetben ismertetett modellek különböző formában és kontextusban igyekeztek leírni az innovációgenerálás, valamint a tudás- és technológiatranszfer legjobb rendszerét. Ebben a fejezetben a hálózatban legjellemzőbb szereplők tevékenységét veszszük górcső alá.

Az állam

A gazdaság állami szerepvállalásának elméleti háttere. Annak megértéséhez, hogy mely potenciális eszközökkel tud az állam beavatkozni az innovációs ökoszisztéma működésébe, szükséges átlátni az állami beavatkozás mélyebb összefüggéseit. Ezért jelen alfejezet az állami szerepvállalás általános közgazdaságtani elméletét foglalja össze, amely a későbbiekben implementálható lesz a kutatás-fejlesztés-innováció témakörére is.

Stigler szerint a közgazdászok skizofrén módon gondolkodnak az államról. Egyrészt kutatják, hogy milyen piaci problémák léteznek, amelyek megoldásához állami beavatkozásra van szükség. Másrészt úgy gondolják, hogy az alapvetően „jóindulatú" *(benevolent)* és demokratikus államok is sok diszfunkcióval bírnak, ami a saját, önös érdekükön alapul.[181] Művében igyekszik újragondolni ezt a fenti elméletet, és három fontos területet emel ki mint figyelembe veendő tényezőket: a külső gazdasági hatásokat (externáliák), a közjavakat és a rossz döntéseket.[182]

A mikroökonómiai megközelítés szerint az államnak különböző feladatai különböztethetők meg, úgymint a szabályok és intézmények formálása, ösztönzők vagy egyéb támogató jellegű intézkedések kidolgozása és használata vagy bizonyos javak és szolgáltatások saját előállítása. Így képes mind a keresletet, mind a kínálatot befolyásolni. Amennyiben ezt privát cégekkel közösen, egymást kiegészítve teszi, vegyes gazdaságról beszélhetünk.[183]

Az állam szerepét sokféleképpen definiálták a történelem során. Coase az állam legfontosabb feladataként a *tranzakciós költségek csökkentését* jelölte meg. A tranzakciós költségeket ő az árrendszer használatának költségével azonosította.[184] A fogalomhoz két fő jelentést lehet társítani: egyrészt a piacokon megjelenő tranzakciós költségeket értik alatta, másrészt a *szabadalmi jogokhoz* köthető a fogalom. Utóbbi esetben látni kell, hogy „amikor a szabadalmi jogok nem teljesek, az egyének mindig a fennálló szabadalmi jogaik fenntartásában és újak létrehozásában érdekeltek", ebből kifolyólag a szabadalmi jogokkal összefüggő tranzakciós költségek úgy definiálhatók, mint a szabadalmi jog létrehozásának és fenntartásának költsége.[185] A neoklasszikus megközelítésben a tranzakciós költségek a tulajdonjogok átadásából eredő költségek, azaz a piaci csere folyamatának költségei.[186]

A gyakorlatban ez azt jelenti, hogy az állam feladata lehet a megfelelő körülmények biztosítása a fentiekhez olyan eszközökkel, mint az egyenlő és olcsó üzleti környezet megteremtése, kikényszeríthető szerződéses viszonyok, megfelelő információ és bizalom mint közjószág.

[181] Stigler 1971, 13.
[182] Stigler 1971, 314–321.
[183] Stiglitz 1999, 4. Itt csak a vegyes gazdaság aspektusaival foglalkozom, és nem teszek említést az olyan extrém esetekről, mint például a laissez faire vagy a szocializmus esetei.
[184] Coase 1988, 3–17.
[185] Allen 2000, 898.
[186] Allen 2000, 901–902.

A piaci kudarcokon alapuló beavatkozások esetén – fő szabály szerint – nem Pareto-optimális a piaci helyzet. Ilyenkor a piac – külső beavatkozás nélkül – nem működik hatékonyan, és nem képes megoldani ezeket a problémáit.[187]

A normatív megközelítés szerint az állam feladata ilyenkor, hogy tompítsa a *piaci kudarcokból* származó negatív hatásokat, és növelje a pozitívokat. Ilyen lehetséges negatív kimenetel például a közjavak esete, a monopólimok, oligopóliumok és természetes monopóliumok, a külső gazdasági hatások (externáliák), az információs aszimmetria vagy tökéletlen információ, a hiányzó vagy nem teljes piacok és az érdemjószágok.

Technológiai óriások monopolhelyzete

A Facebook, Google és Amazon esetén is visszatérő kritika, hogy technológiai monopóliumként működnek. Az első esetében például – a világszerte közel 2,6 milliárd felhasználójával[188] – mind az online hirdetési, tartalomgyártási és hírfogyasztási[189] monopólium összpontosul, amit megfelelő algoritmusokkal és profilozással célzottan tud az egyes felhasználók felé eljuttatni. A verseny hiányát tovább érzékelteti a tény, hogy mind az Instagram képmegosztó, mind a WhatsApp üzenetküldő applikációk a Facebook tulajdonába kerültek. Ez pedig nagy adatmennyiséget, kizárólagosságot és ezzel együtt hatalmat jelenthet. Ezt tompítandó a Facebook 2020-ban felállított egy moderációs kérdésekben döntő, neves nemzetközi szakemberekből álló, a cégtől független felügyelőbizottságot.[190] A kezdeményezés üdvözlendő az elmúlt évek tendenciáit figyelembe véve, ugyanakkor erősíti az állami szupervíziót erodáló tendenciákat.

Stiglitz a munkanélküliséget, az inflációt és az egyensúlyhiányt is piaci kudarcnak tekinti.[191] Munkájában a következő beavatkozásokat különbözteti meg: „a termékek és szolgáltatások előállítása, a szabályozás és ösztönzés a magántermelés esetén, a termékek és szolgáltatások vásárlása […] a jövedelmek újraelosztása."[192] Szintén megemlíti azokat az eszközöket, amelyekkel az állam képes befolyásolni a magáncégek termelését, úgymint ösztönzők és adózás (pozitív és negatív adózás), állami hitelsegítés, alacsony kamatozású hitelek vagy hitelgarancia, illetve a vállalkozások szabályozása.[193]

A legújabb eszközök közé sorolják a közbeszerzések használatát vagy a befektetési adókedvezményeket, ahol – a pozitív diszkriminációért cserébe – a cégek munkahelyeket teremtenek, csökkentik a regionális egyenlőtlenségeket és növelik a kutatás-fejlesztési tevékenységet.[194]

Ugyanakkor az állam sosem lesz képes pontosan felmérni és definiálni azokat a szükségleteket, amelyek a piac tökéletes működéséhez szükségesek. Az állami működés vagy

[187] Bator 1958, 351–379.
[188] Statista: *Facebook Users Worldwide 2020.*
[189] Bene 2017.
[190] *Oversight Board – Independent Judgment. Transparency. Legitimacy.*
[191] Stigler 1971, 9.; Stiglitz 1999.
[192] Stiglitz 1999, 27.
[193] Stiglitz 1999, 30–32.
[194] Szanyi 2009, 64.

beavatkozás diszfunkciói esetén lehet kormányzati kudarcokról beszélni. Ezek – Stiglitz álláspontja szerint – a korlátozottan elérhető információból, a privát cégek válaszreakciói fölötti limitált kontrolllehetőségekből, a bürokrácia fölötti korlátolt kontrollból és magának a politikai folyamatnak a korlátaiból fakadnak.[195]

Az, ahogy a beavatkozást és annak mértékét tekintjük – és hogy mit tekintünk sikernek –, folyamatosan változik. Az egyensúly megtalálása a piaci és kormányzati kudarcok között egyaránt formálódott az elmúlt évtizedben bekövetkezett kurzusváltás hatására, a gazdasági részvétel következtében és a társadalom és a gazdaság gyors változásához köthetően.

Alapvető, visszatérő kérdés, hogy melyik a költségesebb: a beavatkozás vagy a beavatkozástól való távolmaradás, ennek pontos meghatározása azonban nem lehetséges.

Ami azonban megállapítható, hogy a kormányzat bizonyos eszközei a korábbi tapasztalatok alapján hatékonynak bizonyultak: ezek egyrészt a külső gazdasági hatások kezelésére tett lépések, másrészt az információs aszimmetria tompítására tett erőfeszítések. Esetükben az állam olyan célok támogatását is ki tudja harcolni, mint a környezetvédelem, az oktatás vagy a kutatás és fejlesztés. Az ezekhez társuló előnyök a magánszereplőknél csak hosszú távon jelentkeznek, így fontosak az ösztönzők, amelyek képesek a rövid távú profit irányából a hosszú távú befektetés irányába terelni őket, vagy segíteni abban, hogy ne tartsanak a befektetett erőforrásaik elvesztésétől.

Szűkebben a kutatás és fejlesztéshez kötődő piaci kudarcokkal és az azokhoz társuló lehetséges megoldási alternatívákkal a következő alfejezet foglalkozik.

Piaci kudarcok a kutatás és fejlesztés területén

Mint látható volt, a neoklasszikus, *mainstream* közgazdaságtan a piaci kudarcokra alapozó állami szerepvállalást vázol fel az innovációs folyamat kapcsán is.[196]

Ugyanígy előrevetíthető, hogy a kutatás és fejlesztés bír piaci kudarcokhoz köthető tulajdonságokkal – sok esetben például az ebbe történő befektetéshez szükséges ösztönzők hiányoznak. Látható, hogy egyaránt jellemzőek „spillover hatások, pénzügyi korlátok, bizonytalanság, kockázatkerülés és dinamikus externáliák”,[197] továbbá a tudás áramlásának a hiánya,[198] ami arra ösztönözheti a közpolitika-alkotókat, hogy támogató eszközöket fogadjanak el. Ez azt is jelenti, hogy állami beavatkozás nélkül „elégtelen termelés” lenne megfigyelhető a területen.

Mazzucato ennél is tovább megy, és azt mondja, hogy minden világrengető találmány mögött állt (akár rejtett) állami támogatás. Azt állítja, hogy az állami szerepvállalás nemcsak a piaci kudarcok kezelésében *(de-risk)* merül ki, hanem hogy „közvetlenül vezesse az új technológiai lehetőségek és piaci vízió megteremtését”. Itt a *piacteremtő*

[195] Stiglitz 1999, 11.
[196] Az evolúciós közgazdaságtan megközelítéséről részletesen lesz szó az eszközökről szóló fejezetben.
[197] Choi–Lee 2017, 1465.
[198] Nemzeti Innovációs Hivatal 2008, 6.

közpolitika „a változás irányába történő döntéshozatalt" jelenti, „a (köz- vagy magán-) szervezeteknek azt a természetét, hogy képesek üdvözölni a mögöttes bizonytalanságot és a folyamat felfedezését; a küldetésalapú és piacteremtő közpolitikák értékelését; és azt a módot, hogy a kockázatok és az elismerések is egyaránt megoszthatók, így az okos növekedés egyben eredményezhet inkluzív növekedést is."[199]

Széles körben elfogadott, hogy az alapkutatás közjószágnak tekinthető. Ez azt jelenti, hogy se nem kizárható, se nem versengő jószág, így előállítása sokszor nem jó befektetés az egyes cégeknek. Ennek mögöttes oka, hogy a fizetési hajlandóság könnyen potyautas magatartásba csaphat át, mivel ha egy szereplő már fizetett érte, a többi ingyen hozzájuthat (pozitív externáliák), így mindenki arra motivált, hogy alacsonyabb összeget „mondjon" annál, mint amit egyébként hajlandó lenne fizetni a jószágért. Ez azonban csökkenti a kínálatot a valódi kereslethez képest,[200] így végül egyik privát aktor sem lesz érdekelt az alapkutatás „előállításában", ezért az államnak muszáj beavatkoznia akár mint közvetlen előállító, akár mint motiváló különböző ösztönzők használatával.

Callon a következő érveket listázza a kvázi közjószágjelleg és ezzel együtt az állami szerepvállalás mellett:

– a tudományos ismereteknek számos olyan sajátos jellemzője van, amely nem teszi lehetővé a teljes átalakítását árucikké;
– ennek eredményeként a piaci mechanizmusok odavezetnek, hogy a vállalkozások kevesebbet fektetnek be a tudományos kutatásba;
– a piaci kudarc helyreállítása érdekében a kormányoknak ösztönözniük kell a beruházásokat a közvetlen beavatkozásokon és az ösztönző rendszereken keresztül.[201]

Mint látható volt a külső gazdasági hatások léte szintén lassító erővel bír a céges beruházásokra, hiszen minden befektetés profitot tud jelenteni az összes többi szereplőnek is. Figyelembe kell venni továbbá – mint piaci kudarc – a tudás, a piaci és a hálózat *spilloverek,* a nagy mértékű kockázat és az információs aszimmetria tényezőit.[202]

A növekvő termelékenységhez a következő három forrással kell számolni: a tőke növekedése, a humán erőforrás fejlődése (oktatáson és tapasztalaton alapulva) és a technológiai változás. Mivel az oktatás közjószágnak tekinthető, ezt a tényezőt sem szabad figyelmen kívül hagyni.[203]

Kérdéses ugyanakkor, hogy jelen területen a kutatás-fejlesztés támogatásában valóban alacsony érdekeltsége van-e a cégeknek, illetve az államnak az általános közjószág-megközelítés mellett mekkora katonai-védelmi beruházási motivációja van a támogatás során.

[199] Mazzucato 2016.
[200] Stigler 1971.
[201] Callon 1994. 397.
[202] Tétényi 2013, 29.
[203] Stiglitz 1999, 344.

A kutatást, fejlesztést és innovációt támogató beavatkozás

Ahogy látható volt, a piaci kudarcoknál a cégek motivációja a kutatás-fejlesztésbe történő befektetéshez alacsony, mivel nem garantált, hogy az megtérül. Az alfejezet azokat az állami eszközöket foglalja össze, amelyek egyrészt képesek növelni a cégek motivációját, másrészt más módon képesek ösztönözni a társadalmon belüli tudásteremtést.

Először is fontos leszögezni, hogy az állam szerepe azoknak az alapvető körülményeknek a megteremtése, amelyek megfelelő háttért tudnak biztosítani az innováció előállításának és elterjedésének.

Az OECD–Eurostat[204] felmérése szerint egy vállalat innovációs képessége függ:

- az intézményi és innovációs környezettől,
- az innovációs politikától (támogatások és ösztönzők),
- az oktatástól és az állami kutatás-fejlesztéstől,
- más vállalatok innovációs tevékenységétől,
- az ezekkel kölcsönhatásban álló kereslettől.

Ezek a dimenziók szintén azt mutatják, hogy mekkora felelőssége van egy államnak, de egy adott térségnek, régiónak is nemcsak az innovatív ökoszisztéma kialakításában, hanem egy-egy innovációra törekvő vállalat megfelelő körülményeinek biztosításában.

Az egyetemeknek és kutatóintézeteknek fontos szerepe van az alapkutatásban, amelyet egyaránt támogathat állami vagy magánalap. Ezek kiemelten fontosak abban az esetben, amikor nincs közvetlen hatása a kutatásnak az ipari termelésre, így a cégeknek nem éri meg befektetni a terület feltárásába. A direkt ipari hasznosítástól függetlenül azonban ezeknek a felfedezéseknek, kutatásoknak közvetett hasznosulása figyelhető meg, így az állami támogatás biztosítása fontos a területen.[205]

Mindezek mellett – a legtöbb esetben államilag finanszírozott – egyetemek, illetve az oktatási rendszer mint egész több okból is fontos. Ezért lehetséges, hogy mind a finanszírozás, mind a megfelelő oktatási körülmények megteremtése kormányzati feladat. Az oktatási rendszernek alkalmas és használható tudást kell átadnia, és hozzá kell járulnia ahhoz, hogy a diákok megfelelően fejlődjenek. Érthető ez alatt, hogy innovatív, kreatív, kereteken kívül gondolkodó *(think out of the box)* és csapatban dolgozni képes generáció kerüljön ki az iskolapadból. A nyelvtudás is kardinális kérdés, több okból: egyrészt, hogy képesek legyenek elérni mindig a legfrissebb, legadekvátabb tudást és a legújabb kutatási eredményeket a kutatási területükről és a globális piaci helyzetről. Másrészt ez az egyik minimumfeltétele annak, hogy képesek legyenek akár nemzetközi kutatócsoportokhoz csatlakozni, akár nemzetközi piacra bevezetni a cégüket. Korlátokkal, de az oktatásnak a hozzáállás *(mindset)* formálásban is fontos szerepe van. A csapatmunkához is szükséges együttműködési készség, a bizalomra való képesség

[204] Békés 2011, 90–91.

[205] Másik fontos tényező az alapkutatással kapcsolatban, hogy nem várhatunk el úgynevezett kemény eredményeket, követni kell a kutatás általános logikáját és magas színvonalú tudományos munkát elvárni. Tétényi 2013, 31.

(ez fontos például a termék validálásánál), a teljesítmény tisztelete (érdemalapú társadalom) és a versenyszellem szintén formálható képességek. Az egyetemekre fókuszálva egyrészt magas színvonalú tudásátadás zajlik ezekben az intézményekben a kutatásba való bekapcsolódás lehetőségével. Ezzel együtt azonban megjelenik a regionális fejlesztő hatásuk a tudásáramlással az egyetem falin kívül is.[206]

Akár az oktatási rendszeren belül, akár az életen át tartó tanulás támogatásának keretében *(life-long learning)* el kellene helyezni a vállalkozói készségek elsajátítását segítő modult, amely az általános szabályozási, adózási, beszámolási ismereteket és a vállalkozáshoz szükséges praktikus ismereteket és készségeket segítene elsajátítani a résztvevőknek.[207] Ezzel pedig már egy *startup* vagy *spin-off*[208] tevékenységet támogató, vállalkozóbarát kultúra alapjai is létrehozhatók.

Az állami beavatkozás enyhe eszközei közé a tranzakciós és egyéb költségek csökkentését sorolhatjuk. Absztrakt módon megfogalmazva ez segít csökkenteni az információhiányt, a bizonytalanságot és a nem teljes szerződések problémáját. Gyakorlatibb oldalról megközelítve ez az (innovatív) vállalkozás működtetéséhez szükséges alapvető körülmények megteremtését jelenti.

A Világbank összehasonlító elven a következő indikátorokkal méri az egész világon, hogy mennyire egyszerű vállalkozást indítani és működtetni a különböző országokban:[209]

- vállalkozás indítása (folyamat, idő, kiadás, minimumtőke egy korlátolt felelősségű társaság elindításához);
- az építési engedélyek megszerzése (folyamat, idő, egy raktár megépítéséhez szükséges minden követelmény teljesítésének költsége és a minőség-ellenőrzés, valamint a biztonsági mechanizmusok az építési engedélyezési rendszerben);
- az elektromos áram bekötése (folyamat, idő, az elektromos hálózatra való csatlakozás költségei, az áramellátás biztosításának megbízhatósága, az árak átláthatósága);
- a tulajdonjog bejegyzése (folyamat, idő és a tulajdonjog átadásának költsége, a földbejegyzési közigazgatási egység minősége);
- hitelfelvétel (biztosítékok és hitelinformációs rendszerek);
- a kisebbségi befektetők védelme (a kisebbségi részvényesek jogai a kapcsolt felek közötti tranzakciók során és a felelős társaságirányításban);
- adófizetés (kifizetések, idő és összes adó, és a járulék mértéke egy vállalat számára, hogy megfeleljen az összes adózási szabálynak, valamint a bejelentés utáni folyamatoknak);
- határokon átnyúló kereskedés (idő és költség az exporthoz és importhoz);
- szerződések kikényszeríthetősége (kereskedelmi vita és a bírósági folyamatok minőségének megoldásához szükséges idő és költség);

[206] BudapestHUB Work Team 2013, 7.
[207] Lalkaka 2001, 3.
[208] A két fogalom definiálását lásd a vonatkozó fejezetben.
[209] *Doing Business 2018: Reforming to Create Jobs* 2017, 12.

– a fizetésképtelenség megoldása (a kereskedelmi fizetésképtelenség idejére, költségére, eredményére és behajtási arányára, valamint a fizetésképtelenség jogi keretének erősségére vonatkozó információk);
– munkaerőpiaci szabályozás (rugalmasság a foglalkoztatás szabályozásában és a munka minőségének szempontjai).

Ezek az indikátorok nemcsak az egyes cégek indításához és működtetéséhez fontosak, hanem hogy lehetőség legyen akár egy kutatás-fejlesztés intenzív céget kipörgetni *(spin-off)* vagy egy nagyvállalatot arra motiválni, hogy egy nagy hozzáadott értékkel bíró részleget nyisson az adott országban, vagy bármilyen innovatív üzleti forma megjelenjen ott.

A szabadalom, mint egy kutatást ösztönző motivációs eszköz, kizárólagos jogot biztosít a találmányra. Ezzel együtt azonban az intézmény torzítja a piacot, monopóliumot biztosítva az adott vállalatnak egy bizonyos időtávra az adott szabadalom fölött.[210] Ennek ellenére a többség továbbra is kitart amellett, hogy érdemes ezt a lehetőséget biztosítani a cégeknek és alkalmazni a jogintézményt, mert így tudják ösztönözni a cégeket, hogy kutatás-fejlesztésbe fektessenek. Amennyiben – externáliaként – bárki tudná használni az eredményeiket anélkül, hogy hozzájárulna az előállítással járó költségekhez, elmaradnának ezek az áttörések. Nicolaides fogalmazta meg, hogy „a cégek hajlamosabbak több olyan tudást előállítani, amelyet egyszerű szabadalmi védelem alá venni vagy közvetlenül hasznosítani az új termék gyártásában vagy új szolgáltatás nyújtásában".[211]

Az iparhoz kötődő innovációkat – a fenti *spill-over* probléma miatt – nem feltétlenül állítanák elő a különböző kutatás-fejlesztési ösztönzők nélkül, ami a holttehervesztesség minimális szintjét jelenti. Ugyanakkor empirikusan igazolt, hogy a nem direkt kifizetés alapú *ösztönzőknek* van a legnagyobb tőkeáttételi hatása. A fiskális ösztönzők (mint az adókedvezmények) és a nem pénzügyi ösztönzők emelni képesek a vállalkozások kutatás-fejlesztésre fordított kiadásait *(business enterprise expenditure on R & D – BERD).*[212]

A kutatási és kísérleti adókedvezmény szintén lehetővé teszi a cégeknek, hogy azt az adott összeget a kutatásukra fordítsák. Ez pedig – kiszámítható és megbízható adórendszer esetén – lehetővé teszi a hosszú távú tervezést, hogy olyan kutatásokat válasszanak ki a cégek, amelyek hosszú távú sikert biztosítanak, de itt a társadalmi hasznosulás nem jelenik meg a kiválasztási kritériumok között.[213]

A kedvezményes hiteleknek szintén hasonló pozitív hatása van, hiszen az a követelmény, hogy vissza kell fizetni az összeget, arra sarkallja a cégeket, hogy potenciálisan hasznos befektetésekkel éljenek.

Az államnak azonban ennél is több mozgástere van: *közvetlenül megrendelőként* léphet fel, és vásárolhat egy kutatás-fejlesztésben aktív cégtől, például a hadsereg számára, a közbeszerzések során értékelési szempontként tüntetheti a kutatás-fejlesztést,

[210] Stiglitz 1999, 78., 344–347.
[211] Nicolaides 2013, 9.
[212] Tétényi 2013, 31.
[213] Stiglitz 1999, 347–348.

pályázatokat írhat ki (például operatív programok) visszatérítendő és nem visszatérítendő formában, és lehetősége van arra, hogy hitelek segítségével a kockázat egy részét vagy egészét átvállalja a magánszférától (kamattámogatással vagy csökkentett kamatokkal).

Innováció és állam a védelmi iparban

Bonvillian és munkatársai amellett érvelnek, hogy az Amerikai Egyesült Államok vezető szerepe a jelenlegi technológiai és gazdasági paradigmában nem választható szét annak katonai védelmi hatalmától, hiszen a technológia civil és védelmi felhasználása kéz a kézben fejlődött, amiben kiemelkedő szerepe van a védelmi minisztérium kutatásokért felelős részlegének (DARPA).[214] Innen is látható, hogy az állam aktív támogatása a K+F mellett a gazdaságra is élénkítő hatással bír.

Egy dinamikus gazdasági fejlődéshez a fejlődő országoknak is vannak további eszközei, úgymint kutatás-fejlesztési ösztönzők és hatékony támogatások, az egyetemek és a szakképzés és a külföldi fejlesztési befektetések befolyásolása különböző szektorális és területi szempontok szerint, ezzel is támogatva a helyi kis- és középvállalkozásokat.[215]

A már említett, közvetlen finanszírozáson alapuló projektek mint az egyik legerősebb eszköz széles körben kritizáltak, hiszen egyrészt nem egyértelmű, hogy az állam megfelelő tudás birtokában van-e ahhoz, hogy a legjobb kutatás-fejlesztési projekteket válassza ki, és olyan sikertelen befektetéseket is ösztökélhet, amelyeket a piac automatikusan kiszelektálna. Másrészt ez azt jelenti, hogy előfordulhat, hogy nem azokba a projektekbe fektetnek be, ami a piaci kudarcok miatt maradna ki, hanem akár azokba is, amit a piac egyébként is finanszírozna. A probléma az információs kudarcok (nem tökéletes információ) és a két fél különböző motivációjából is ered. A kormányzati kutatás-fejlesztési kiadások és a cégek kutatás-fejlesztési befektetései „úgy viselkednek, mintha helyettesítők vagy a kiegészítők lennének".[216]

Az állami befektetések így kimutatható torzításokat képesek okozni a piacon. Ennek oka lehet:

– nem megfelelő cégek vagy domináns cégek finanszírozása;
– az állami beavatkozás helyettesíti a magánszektor erőfeszítéseit és kockázatvállalását;
– az Európai Unión belül olyan ragadozó politikák, amelyek károsítanak más országokat bérbeadó intézkedések által.[217]

Az Európai Unióval és ennek piacra való hatásaival szintén szükséges számolni: például az állami segélyekre vonatkozó szabályaival. Mivel „a magánszektor kutatási tevékenysége a társadalom számára előnyöket generál, így az EU állami segélyekre vonatkozó szabályozása megengedi bizonyos körülmények fennállása esetén, hogy állami támo-

[214] Bonvillian – Van Atta – Windham 2019.
[215] Csáki 2019, 32.
[216] David–Hall 2000, 1166.
[217] Nicolaides 2013, 5.

gatást kapjon a kutatás-fejlesztés". Alapvetően ez azt jelenti, hogy „minél közelebb van a kutatás a piachoz, annál kevésbé megengedett az állami támogatás".[218]

Végül fontos kiemelni azt a tényezőt, mely az állam innovációt ösztönző szerepe kapcsán kulcsfontosságú, ez pedig a *szabályozás* és a *közpolitika alkotási* tevékenység.

A szabályozási tevékenység egyrészt megjelenik az összes fent említett ösztönző kapcsán. Másrészt a munkaerőpiaci tényezők és más, humánerőforrás-kötődésű jogi döntések is fontosak az innováció terjedése kapcsán.

Azokkal az ipari szakpolitikákkal, amelyek közvetlenül segítenek egy szektort – akár egy másik szektor kárára – ugyanaz a probléma merül fel, mint az állami segélyek kapcsán. A kormányzat itt sem rendelkezik tökéletes információval a piaci mechanizmusokról, így egyszerűen megtörténhet, hogy a közpolitika kritériumrendszere célt téveszt. A fejlődő országoknak azonban – ahogy a fejletteknek is – a tudomány, a technológia és az innovációpolitika megléte nagyon fontos mind a nemzeti innovációs rendszerrel, mind a fejlett technológia és tudás importálásával összefüggésben.[219]

A szabályozással való stabilitás, biztosítás, segítség azonban többfelől is egyértelműen jó iránynak tűnik: minden fenti szereplő számára kiszámítható jogi környezetet teremt. Így lehetőség adódik egyrészt egy megfelelő jogi formát és szabályozást találni a startup cégek számára, másrészt egy észszerű és motiváló környezetet lehetne teremteni a *kockázatitőke-befektetőknek* és *angyalbefektetőknek.* Ezzel egy időben szükséges lenne az úgynevezett spin-off cégek átlátható jogi környezetének megteremtése is, hogy hozzá tudjanak járulni az egyetemek innovációs kapacitásához, és meg tudjanak jelenni a piacon.

Ugyanakkor új cégeket indítani különösen résterületeken vagy speciális piacon jogilag sokszor sebezhető. Ha lehetőséget kapnának arra, hogy az életciklusuk elején egy úgynevezett „védett zónában", minden szükséges segítséget megkapva fejlődjenek, a szükséges infrastruktúrát is megkapva, az segíteni tudná a túlélésüket. Az állam ehhez *üzleti inkubátorok* létrehozásának ösztönzésével tud segíteni. Ezek a szervezetek teljesíthetik azt a követelményt, hogy exponenciális növekedési potenciállal rendelkező innovatív cégeket segítsenek hozzá a növekedéshez és ahhoz, hogy a nemzetközi piacra tudjanak lépni. Ez egyrészt jó a cégnek és az azt támogató inkubátornak, amely – befektetés esetén – részesedést kaphat a cégből, és a méretgazdaságosság miatt a kockázatok is kiegyenlítődnek (megfelelő kiválasztási módszertan mellett). Továbbá jó az államnak, mert a cég érdekeltté válhat abban, hogy az adott országban folytassa a tudásintenzív tevékenységét. Az aszimmetrikus információ veszélyét azonban itt sem szabad elfelejteni.

A vállalkozóállam-koncepció és a K+F+I

Ebben a részben már említettük Mazzucato küldetésorientált közpolitikai szemléletét. Ebben az alfejezetben röviden a kutatás-fejlesztési aspektusokkal egészítjük ki a fenti piacorientáló megközelítésről leírtakat.

[218] Nicolaides 2013, 4., 8.
[219] Szanyi 2009, 65–66.

Mazzucato és Robinson szerint a NASA küldetésorientált programjai a múltban egyrészt a védelempolitikára, másrészt a technológiai fölény megszerzésére irányultak, most azonban már eltolódnak napjaink kihívásai felé,[220] és ezek a küldetésalapú programok egyre szélesebb körben jelennek meg. A 21. század társadalmi, környezeti és gazdasági kihívásaira adandó fenntartható és inkluzív válaszok szintén ezt a megközelítést igénylik. Az átfogó problémák *(wicked problems)* jellemzője, hogy komplexek, rendszerszintűek, átfogók és sürgetők,[221] így az adekvát válasz megtalálása nem halogatható, ugyanakkor nem is egyszerű.

A küldetésalapú közpolitikákhoz, amelyek mind a Holdra jutáshoz, mind a mai klímaválság megoldásához nélkülözhetetlenek, egyszerre feltételezik a különböző aktorok és szektorok innovációját az adott megoldás eléréséhez. Az egyes aktorok szerepét a modellek közötti összefüggésről szóló fejezetben fejtjük ki részletesen, azt azonban szükséges előrevetíteni, hogy az állam szerepe nélkülözhetetlen *(top-down approach),* ezzel együtt nem elvitatva az alulról szervező kezdeményezések fontosságát *(top-down approach).* Utóbbiak egyszerre fontosak a már említett tanulás és tapasztalat becsatornázásához, valamint a visszacsatolások összegyűjtéséhez. „A küldetésalapú közpolitikák nemcsak a támogatások problémákhoz rendelését jelentik, hanem azt is, hogy ezt egy különleges módon teszik."[222] Ezek a küldetések nem csak a piacok hibáinak kiküszöbölését, sokkal inkább a piacteremtő *(co-creating)* és a piacalakító *(market shaping)* közpolitikák kialakítását szolgálják.[223]

A régi és a mai küldetésalapú közpolitikák közötti különbséget a következő táblázat foglalja össze. Ez rámutat, hogy mind a kihívások megváltoztak, mind a bevont szereplők nagysága és köre, valamint a megközelítés módszere.

11. táblázat: A régi és új típusú küldetés alapú közpolitikai alkotás közötti eltérések

Régi típusú küldetésalapú közpolitika	Új típusú küldetésalapú közpolitika
Védelem, atomenergia, repülés	Környezeti és társadalmi kihívások
Az eredmények fő célcsoportján kívüli diffúziónak kicsi a szerepe, vagy tudatosan elkerült.	Az eredmények elterjesztése a fő cél, és ez aktívan támogatott.
A küldetés a technikai eredmények számában van meghatározva, a gazdasági hatás figyelembevétele elhanyagolható.	A küldetés gazdaságilag megvalósítható technológiai megoldások kidolgozása az egyes társadalmi problémák kezelésére.
A célok és az irány egy kis szakértői csoport által meghatározott.	A változás irányát a szereplők széles köre formálja, beleértve a kormányzatot, az ipari szereplőket és a fogyasztókat is.
Központi kormányzati irányítás	Decentralizált irányítás sok szereplő bevonásával
Mivel kisszámú, radikális technológia érintett, a cégek szűk köre vonható be.	A radikális és az inkrementális innovációkat is ösztönzi, ezzel a cégek nagyobb körének bevonását teszi lehetővé.
Önálló projektek, amelyek kevésbé igényelnek átfogó és koherens politikaformálást.	A kiegészítő politikáknak fontos szerepe van a sikerben, és a más szakpolitikákkal való összehangolásnak nagy szerepe van.

Forrás: Kattel–Mazzucato 2018, 804.; Soete–Arundel 1993, 51. átdolgozott változata

[220] Mazzucato–Robinson 2018 166–177.
[221] Kattel–Mazzucato 2018, 787–801.
[222] Kattel–Mazzucato 2018, 803.
[223] Mazzucato 2016, 140–156.

A küldetésalapú megközelítés azt is meghatározza, hogy az egyes innovációs politika hogyan változtassa meg a technológiai, szektorális és nemzeti innovációs rendszert. Ennek a szakpolitikának azonban több feltételnek kell megfelelnie.[224]

Ez a koncepció egybecsenghet a kiberbiztonság mentén történő együttműködéssel, rendszerszintű innovációs menedzsmenttel, illetve orientálhatja az erős állami szerepvállalás irányát.

Az üzleti szféra

Alapvetően három aspektusból lehet a vállalati szektorra tekinteni: az első a kiberbiztonság, IT-biztonság területén érintett cégek, amelyek a mi szempontrendszerünk szerint lehetnek munkaadók, megrendelők-beszállítók vagy együttműködő partnerek. Ugyanakkor a területen alapvetően nem érintett cégeknek is vannak kapcsolódó aspektusai, így ezek egyrészt megrendelőként jelennek meg a piacon, másrészt együttműködő partnerként, amelyek – amennyiben nem figyelnek saját biztonsági rendszerükre – kockázati tényezőként is megjelenhetnek az együttműködő cégeknél, partnereknél is. Ezzel már részben összekapcsolható a harmadik, közpolitika oldaláról vizsgálódó szempont, ahol a kiberhigiéniai ajánlások alanyaiként jelennek meg.[225]

Technológiaelfogadási hajlandóság és a technológia terjedése

Arról már volt szó, hogy a fogyasztók tudatlansága milyen veszélyeket hordozhat (3. keretes írás). A másik fontos, kapcsolódó tényező a technológiaelfogadási hajlandóság, amely bármely innovatív vállalkozás piacra való betöréséhez fontos szempont.

Az idő során sokat fejlődött *technológiaelfogadás-modell* (TAM) és *technológiaelfogadás és -használat egységesített elmélete* (UTAUT)[226] segítségével egyéni szinten vizsgálható, hogy egy adott felhasználó hogyan viszonyul egy új technológiához. Emellett az utóbbi azt is képes felmérni, hogy milyen lépésekkel lehet orientálni azokat az egyéneket, akik kevésbé akarják alkalmazni, illetve elfogadni az új rendszert. A felhasználhatóságot tekintve az UTAUT munkahelyi környezetben is optimálisan alkalmazható.[227]

Egy másik megközelítés, a *Rogers-féle termékelfogadási görbe* egy másik megközelítésből vizsgálja a termékek elfogadásának időbeli lefolyását. Ezek persze ideáltípusok, és a százalékos megoszlás is orientációként szolgál, azonban a terjedés alapelveit jól szemlélteti:

[224] Kattel–Mazzucato 2018, 803–804.

[225] A kiberhigiénia egyszerű, rutinszerű intézkedéseket jelent a számítógépes fenyegetések kockázatának minimalizálása érdekében.
European Union Agency for Network and Information Security (ENISA) (2017): *Review of Cyber Hygiene Practices.* https://doi.org/10.2824/352617.

[226] TAM – technology acceptance model; UTAUT: unified theory of acceptance and use of technology.

[227] A modellek fejlődésének részletes elemzését lásd:
Keszey–Zsukk 2017, 38–47.

– újítók (innovátorok) 2,5% – nagy a kockázatvállalási képességük, rajonganak az új technológiákért, szívesen vesznek részt tesztelésben is, nagy szerepük van a diffúzióban is;
– korai vásárlók (korai elfogadók) 13,5% – tudatosan keresik az újításokat, hogy ezáltal előnyre tegyenek szert, kevésbé árérzékenyek, döntésükkel és tekintélyükkel segítik, orientálják a többi csoportot is;
– korai többség 36% – gyakorlatiasan és racionálisan gondolkodnak, az átlagnál gyorsabban elfogadják az újdonságokat, ha meggyőződtek azok hasznosságáról. A technológia további diffúziójában fontos szerepük van;
– késői többség 36% – alacsony a kockázatvállaló képességük, konzervatívak és szkeptikusak, az új technológiát gyakran külső nyomásra vásárolják meg;
– lemaradók 16% – ragaszkodnak a megszokott dolgokhoz, és új technológiát csak akkor vásárolnak meg, ha a megszokott eszközeik már nem érhetők el.[228]

Egy technológia sikeres elterjedéséhez tehát az egyes cégeknek a második és harmadik társadalmi csoport közötti „szakadékon" kell átjutniuk, különben nem tud elterjedni a piacon a megoldásuk, termékük. Ez a terjedési szakasz gyakorlatilag a következő részben tárgyalt nagy növekedési potenciállal rendelkező kis- és középvállalatok piacon való elterjedésének is egyik kritikus pontja.

Innovatív kis- és középvállalkozási formák

Ez a rész röviden a *startup* és *spin-off* formák bemutatására tesz kísérletet. A *startupok* meghatározását[229] vita övezi. Vannak, akik a valamikor valóban startupként indult, mára sikeresen befutott Skype, NNG vagy Prezi vállalkozásokat is ebbe a kategóriába sorolják, míg mások szigorúbb keretek közé szűkítik ezt a kört. Az *Európai Startup Monitor 2016* definíciója szerint három alapvető vonása van a startup cégeknek:
– tízévesnél fiatalabb vállalkozások;
– kifejezetten innovatív technológiát és / vagy üzleti modellt alkalmaznak; továbbá
– nagy növekedési potenciállal rendelkeznek akár a munkavállalók számát, akár az értékesítést nézve.[230]

Az innovatív jelleg különbözteti meg attól, hogy egyszerűen a *gazella*[231] cég kategóriájába sorolhassuk. A startupok gyakran a digitális gazdaságban, biotechnológiában, fintech

[228] Ruszkai 2014, 68–69.
[229] Már a névhasználatban is sokszínűség figyelhető meg. Csákné Filep et al. 2020 a következő magyar használati formákat gyűjtötte össze: „gyors növekedésű vállalkozások, scaleup vállalkozások, gazellák, új technológiaorientált cégek stb."
[230] Kollmann et al. 2016.
[231] Gazellák a „dinamikus, gyorsan növekvő új kis- és középvállalkozások". Vecsenyi 2017.

és egyéb feltörekvő területeken jelennek meg. Ma már számos finanszírozási forma, ötletverseny és támogató intézmény segíti a hazai induló vállalkozásokat is.[232]

A *spin-offok* vagy kipörgő vállalkozások egy meglévő szervezetből kiváló új egységet jelentenek, amelyek megjelenhetnek egy egyetemi keretekből vagy egy nagyvállalatból kiváló cégként is. Ezek a szervezetek a technológiatranszfer egyik megtestesítői, hiszen gyakran kutatási projektekből, laboratóriumokból kinőtt új tudást kívánnak hasznosítani ebben a formában.[233] Ehhez természetesen szükséges a kiinduló szervezet támogatása és nyitottsága, valamint az ezt lehetővé tevő intézményrendszer is, benne foglalva az ezt lehetővé tevő jogszabályi környezetet.

Egyetemek és képzés

Az egyetemeknek két fontos feladata van a kiberbiztonság szempontjából. Egyrészt az előrejelzések szerint – a jelenleg is égető munkaerőhiány növekedésével – a jelenlegi szakemberállománynak hozzávetőlegesen 145%-kal kellene gyarapodnia, hogy ki tudja elégíteni a keresletet.[234] Folyamatos versengés folyik a különböző szektorok, munkáltatók között a képzett szakemberekért, miközben az egyetemi oktatói utánpótlást is biztosítani kellene.

A munkaadók részéről a pozíciók nagyjából felében elég lenne egy alapszakos diploma is a kiberbiztonsági munkakör betöltéséhez, azonban kifejezetten ilyen irányultságú képzések biztosítása ezen a szinten általában meglehetősen alacsony,[235] Magyarországon pedig a kifejezetten kiberbiztonsági specifikációjú képzéseket bármilyen szinten nehéz direkt szűrni.

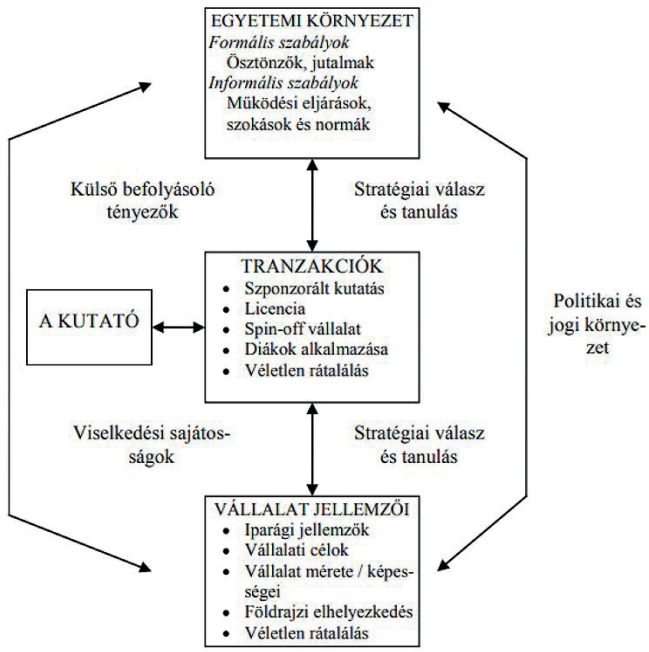
Egyre nagyobb piaca van a hagyományos egyetemi képzések mellett a különböző, nem informatikai háttérrel rendelkező személyek átképzését ígérő oktatási intézményeknek is. Továbbá érdekes kezdeményezés az Egyesült Királyságból, hogy elkezdtek képzést biztosítani HR-szakembereknek egyrészt a munkájukból fakadó érzékeny adatok jobb kezelésére, másrészt az ITC-szakemberek hatékonyabb kiválasztási folyamatához.[236]

Másik irányból megközelítve a kérdést az egyetemek technológia- és tudástranszferben játszott szerepe fontos az ökoszisztéma felőli megközelítéshez. Itt az egyetemek oktató-kutató funkciója mellett megjelenik a harmadik, az úgynevezett vállalkozó egyetem misszió, amely az ipari szereplőkkel való együttműködést ösztönzi. Érdekes és a kiberbiztonság szempontjából releváns elmozdulás az egyetem és az oktatók társadalmi felelősségvállalását, ismeretterjesztő szerepét orientáló felsőoktatási szerepfelfogás.

[232] A startup cég indításának alapjairól lásd Turcsán 2019. Egy konkrét, fiktív kiberbiztonsági startup példáját pedig: Bailetti–Zijdemans 2014, 14–21.
[233] Pavani et al. 2019.
[234] *Global Information Security Workforce Study – Strategies for Building and Growing Strong Cybersecurity Teams.* 2019.
[235] Berzsenyi 2017, 64.
[236] Berzsenyi 2017, 65.

A Novotny által idézett egyetem-ipar kapcsolatait bemutató evolúciós séma a korábbi fejezetek alapján már nem jelent teljes újdonságot. Bemutatja az együttműködés alapjait és lehetséges formációit[237] (9. ábra).

Ez még kiegészíthető az egyetemi tudás- és technológiatranszfer-irodák és üzleti inkubátorok szerepének fontosságával, amelyek a startup és spin-off vállalkozások kipörgését segíthetik.



9. ábra: Az egyetem-ipar kapcsolatok evolúciós sémája

Forrás: Novotny 2009 és Bercovitz–Feldman 2006 alapján

Innovációs intézmények

A technológiatranszfert segítő intézményeknek a következő típusait különböztetik meg:

- hídképző intézmények;
- innovációs ügynökségek;
- technológiai, illetve tudományos parkok;
- technopoliszok;
- inkubációs intézmények;
- egyetemi hasznosító irodák.[238]

[237] Novotny 2009, 79.
[238] Buzás 2007, 63.

Hídképző intézmények

Az aktív hídképző intézmények az alapkutatási eredmények továbbfejlesztését végzik kormányzati támogatással, így a piaci szereplők fel tudják azokat fejlesztésük során használni. Magyarországon a Bay Zoltán Alapítvány végez ilyen kutatáson keresztüli technológia- és tudástranszfer-tevékenységet.[239]

Innovációs ügynökségek

Az innovációs ügynökségek vagy passzív hídképző intézmények már „tisztán információnyújtással, kapcsolatteremtéssel és technológiaközvetítéssel foglalkoznak, saját kutatással nem vesznek részt a technológiaterjedési folyamatokban".[240] Ezek megtalálhatók mind regionális, nemzeti, mind európai uniós szinten.

Európai Uniós innovációs ügynökségek

A *Community Research and Development Information Service* (CORDIS) az Európai Bizottság kutatási eredményeket összefogó, a nyílt tudás elvére épülő szolgáltatása. A felület az uniós forrásból készült kiberbiztonsági és innovációval összefüggő kutatási eredményeket egyaránt elérhetővé teszi a tudásáramlás és növekedés elősegítése érdekében.[241]

Az *European Business and Innovation Centre* (BICs) egy közel 140 akkreditált szervezetet tömörítő szervezet, amelynek célja, hogy innovatív vállalkozók, startupok, valamint kis- és középvállalkozások fejlődését támogassa egy nemzetközi hálózat részeként. Hazai tagjai a Budapesti Vállalkozásfejlesztési Közalapítvány és az Intellexi Kft.[242]

Inkubátorok

Az üzleti inkubátorok a kisvállalkozásokat és a startup cégeket tudják segíteni abban, hogy növelik azok túlélési esélyét, és növekedési lehetőséget biztosítanak számukra. Szerepük a gazdasági növekedésben, az innováció generálásában és a technológiaalapú új cégek felfuttatásában szintén fontos.

A szervezet egyszerre biztosíthat kedvező irodai helyiséget, támogató szolgáltatásokat az általános költségek mérséklésére, professzionális üzleti támogatást, tanácsadást, illetve külső vagy belső kapcsolatrendszert.[243]

[239] Buzás 2007, 63–66.
[240] Buzás 2007, 66.
[241] *About CORDIS.*
[242] *EBN – Innovation Network.*
[243] Bergek–Norrman 2008, 21.

Az egyes szereplőknek eltérő motivációja van egy ilyen támogatási konstrukcióban való részvételre:

– A jelöltek számára a csatlakozás lehetősége növeli a siker esélyét, a hitelességet, segíti a készségek fejlesztését, szinergiát teremt az ügyfél és a cégek között, megkönnyíti a mentorokhoz való hozzáférést, az információkat és a tőkebefektetést.
– A kormányzat számára előnyös, mert az inkubátorok segítenek a piaci kudarcok kezelésében, hozzájárulnak a regionális fejlődéshez, munkahelyeket teremtenek, bevételeket és adót generálnak, továbbá demonstrálják a politikai akaratot a kisvállalkozások támogatására.
– A kutatóintézeteknek és egyetemeknek az üzleti és innovációs központok tudnak segíteni abban, hogy megerősítsék az egyetem-kutatás-ipar kapcsolatokat, a tudás eladhatóságát népszerűsítik, és az intézményi forma lehetőséget ad az egyes karoknak, illetve diákoknak, hogy jobban hasznosítsák a képességeiket.
– A cégek számára az üzleti inkubátorok segítséget tudnak nyújtani abban, hogy lehetőségük legyen innovációkat becsatornázni, menedzseljék ellátási láncukat és a spin-offokat, valamint a társadalmi felelősségvállalással összefüggő tevékenységük ellátásához is hozzá tud járulni a tevékenység.
– A helyi közösség számára növelni tudja az önbecsülést, és megteremti a vállalkozói kultúrát, növeli a helyi bevételeket, mivel a kikerülő cégek többsége helyben folytatja a tevékenységét.
– A nemzetközi közösségnek lehetőséget kínál, hogy kereskedelmi kapcsolatok és technológiaátadás valósuljon meg a klienscégek és az inkubátor között, az üzleti kultúra jobb megértését segíti, továbbá megfelelő terepet biztosít a tapasztalatcserére a szervezeteken és partnereken keresztül.[244]

OXO Cybersecurity Lab

Az egyes üzleti inkubátorok kiválasztási szűrője lehet – egyéb szempontok mellett – hogy az ötlet milyen szektorba illeszkedik, ez a szakterületi lehatárolás azonban hazánkban egyelőre kevésbé elterjedt. Kelet-Közép-Európában elsőként az OXO Cybersecurity Lab csapata fókuszál a kiberbiztonságra, akik szolgáltatási és befektetési konstrukciókat is kínálnak a kiválasztott startupok részére. A specifikáció előnye a tudástranszfer, a kapcsolatrendszer és a mentorok szakismerete, ez azonban nem jelenti az inkubátorprogram kizárólagosságát egy-egy ötletgazda részére.

Technológiai és tudományos parkok

Több megközelítés összefoglalásával Bajmóczy a technológiai parkot olyan innovatív vállalkozások koncentrációjaként definiálja, összegzése szerint ez „egy telephelyalapú kezdeményezés, amely

– ösztönzi a helyi tudásintenzív ipari vagy szolgáltató cégek létrejöttét és növekedését,
– ösztönzi a helyi tudásközpontokkal kialakított formális és informális kapcsolatokat,

[244]Lalkaka 2001, 6.

– olyan környezetet biztosít, amelyben a területileg koncentráltan működő vállalkozások egymással hálózatokat tudnak kialakítani, illetve szinergikus hatásokat generálni, és
– inkubációs funkciókkal rendelkeznek."[245]

Ez a vállalkozások spontán térbeli koncentrációja vagy konkrét gazdaságfejlesztési eszköz eredményeként is létrejöhet. A tudományos park esetén mindez kiegészül egy helyi tudásközponttal (egyetemmel), ami a technológiai parknál nem alapkövetelmény.

Infopark

Budapesten, közvetlenül egyetemek szomszédságában található az 1996-ban alapult *Infopark,* amely Kelet-Közép-Európa első innovációs és technológiai parkja, és az informatikában, a telekommunikációban és a szoftverfejlesztésben érdekelt vállalkozások központja, de itt található az Európai Innovációs és Technológiai Intézet is.

Technopoliszok. A technopoliszok olyan innovációs fejlesztési rendszerek, amelyek a fent bemutatott technológiai park jellegzetességeit magukba foglalják, azonban egy egész városra vagy városrészre is kiterjedhetnek, ahol több technológiai park és inkubátor is helyet kaphat.

Lényegi elemei között megjelennek az *agglomerációs előnyök,* hiszen kritikus tömegben vannak jelen az egyes kulcsiparágak és kutatási kapacitások, ezeken belül megfigyelhető a *kumulatív tanulási folyamat* és megfelelő (specializált) intézményrendszer, hogy a lokalizációs előnyök tudják segíteni az itt megjelenő vállalkozásokat a globális versenyben. *Élénk interakciók* jelennek meg a rendszeren belül, és az *új ötletek* megjelenésére is nagy lehetőség van.[246]

Az utóbbi három, részben átfedő eszközöket alkalmazó, azonban különböző területi és szervezeti lefedettséggel rendelkező intézmények összehasonlítását tartalmazza a 12. táblázat.

12. táblázat: A technopoliszok, technológiai parkok és inkubátorok elhatárolása

	Technológiai inkubátor	Technológiai park	Technopolisz
Technológiai kiterjedés	Központszerű: egy vagy néhány épület	Parkszerű: általában néhány hektárnyi terület	Pólusszerű: egy egész város vagy városrész
Alapvető szereplők	Technológiaalapú kis- és középvállalkozások (kkv-k)	Technológiaalapú nagyvállalatok (főként kutatást és kis szériás termelést végző részlegekkel), valamint kkv-k	Kutatóintézetek, oktatási intézmények, technológiaalapú nagyvállalatok és kkv-k
Inkubációs funkciók	Magas szintű: alapvető cél az induló technológiaalapú kkv-k támogatása	Alapvetően alacsony szintű, DE: – sok esetben egy vagy több inkubátor is helyet kaphat a parkban – a park többnyire kapcsolódik más által koordinált kkv-fejlesztési programokhoz	Alapvetően alacsony szintű, DE: – jellemzően több technológiai park ás inkubátor is része a technopolisznak – a polisz fejlesztési stratégiájában sokszor központi helyet kap a kkv-k fejlesztése

Forrás: Bajmócy 2007, 69.

[245] Bajmócy 2007, 72.
[246] Bajmócy 2007, 77.

Kitekintés

A kiberbiztonság gazdasági és társadalmi szerepe nemzeti, regionális és világszinten is egyre inkább előtérbe kerül, a globális gazdaság egyre nagyobb részét teszi ki a digitalizáció, automatizáció és a dolgok interneteként ismert folyamat, amely a védelmi oldal szerepét is egyre jobban felértékeli. Az innovációk nemcsak az egyes rendszerek kidolgozásában öltenek testet, hanem a biztonság technikai és társadalmi aspektusainak átgondolásában, az közreműködő szervezetek kooperációjának módjában is.

A könyv a kiberbiztonságban lejátszódó innovációs folyamatokat – a legújabb nemzetközi trendeknek megfelelően – a szereplők együttműködése, az ökoszisztéma folyamatai felől közelítette meg. Röviden kitért az egyes szervezetek szerepére is, az intézményeket mint szabadalom- vagy technológiatranszfereket pedig a vonatkozó aktornál említette. Ezzel igyekezett összekötni azokat a képzeletbeli pontokat a felvázolt hálózaton belül, amelyek eredményesebb kiberbiztonsági cégek megjelenéséhez, egyetemi együttműködésekhez és az állam tudatosabb beavatkozásához szükségesek.

A technológiai fejlődés nem áll meg, mindenkinek a saját felelőssége, hogy mennyit tud – szerepétől függően – hasznosítani belőle, és ennek megfelelően hogyan járul hozzá, hogy globálisan képes legyen a régió a változás élére állni. A magyar társadalomról alkotott prekoncepcióink alapján a tudás és a kreativitás megvan hozzá, már csak az a kérdés, hogy képes lesz-e a csapatmunka, a tudásmegosztás vagy épp a meritokratikus rendszerek felállítására egyénileg és szervezeti, intézményi szinten.

Mindazonáltal azt is le kell szögezni, hogy tanulmány átolvasásával ugyan átfogó képet lehet kapni az elméleti keretrendszerről, azonban az innovatív üzleti folyamatoknak, nagy növekedési potenciállal rendelkező kisvállalkozások indításának még számtalan gyakorlati aspektusa van, amelyre terjedelmi korlátok miatt nem volt lehetőség kitérni ebben az anyagban – ismeretük azonban nélkülözhetetlen a sikeres boldoguláshoz. Csak hogy néhány kiragadott példát említsünk: *fundraising, pitch, Business Model Canvas, design thinking.* Ezek elsajátítása azonban szintén fontos aspektus azok számára, akik szeretnék megérteni az innovatív kezdeményezések belső, globálisan azonban nagyon hasonló logikáját.

Irodalomjegyzék

2004. évi CXXXIV. törvény a kutatás-fejlesztésről és a technológiai innovációról

About CORDIS. Weboldal. Elérhető: https://cordis.europa.eu/about/en (A letöltés dátuma: 2020. 05. 26.)

Allen, Douglas W. (2000): Transaction Costs. In Bouckaert, Boudewijn – De Geest, Gerrit eds.: *Encyclopedia of Law & Economics.* Edward Elgar. 893–926.

Bailetti, Tony – Zijdemans, Erik (2014): Cybersecurity Startups: The Importance of Early and Rapid Globalization. *Technology Innovation Management Review,* Vol. 4, No. 11. 14–21.

Bajmócy Zoltán (2007): Technológiai parkok, technopoliszok, inkubációs intézmények és folyamatok. In Buzás Norbert szerk.: *Innovációmenedzsment a gyakorlatban.* Budapest, Akadémiai. 68–89.

Bajmócy Zoltán (2008): A regionális innovációs képesség értelmezése és számbavétele a tanulás-alapú gazdaságban. In Lengyel I. – Lukovics M. szerk.: *Kérdőjelek a régiók gazdasági fejlődésében.* Szeged, JATEPress. 26–46.

Bányász Péter (2017): Kiberbűnözés és közösségi média. *Nemzetbiztonsági Szemle,* 4. évf. 4. sz. 55–74.

Barnett, William P. (2017): Why You Don't Understand Disruption'. *Stanford Graduate School of Business.* Blog. Elérhető: www.gsb.stanford.edu/insights/why-you-dont-understand-disruption. (A letöltés dátuma: 2020. 05. 26.)

Bator, Francis M. (1958): The Anatomy of Market Failure. *The Quarterly Journal of Economics,* Vol. 72, No. 3. 351–379.

Békés Gábor (2011): Nemzeti Innovációs Rendszer. In Pörzse Gábor szerk.: *Kutatásszervezés és innovációmenedzsment az egészség- és élettudományok területén.* Budapest, Semmelweis.

Bene, Marton (2017): Influenced by Peers: Facebook as an Information Source for Young People. *Social Media + Society,* Vol. 3, No. 2. DOI: https://doi.org/10.1177/2056305117716273.

Benoit, Sarazin (2005): *Dell: Market Disruptions That Fostered Its Success. Disruptive Innovation to create a market where you are the standard to follow.* Elérhető: https://marchesenrupture.typepad.com/english/2005/10/dell_market_dis.html. (A letöltés dátuma: 2020. 05. 26.)

Bergek, Anna – Norrman, Charlotte (2008): Incubator Best Practice: A Framework. *Technovation,* Vol. 28, No. 1–2. 20–28.

Berzsenyi Dániel (2017): A kiberbiztonság humán oldala. *Nemzet és Biztonság,* 10. évf. 2. sz. 54–67.

Bishimbayeva, Saule Kozykeyevna – Nurasheva, Kulyanda Kulbosynovna –Nurmukhanbetova, Aigul Adilzhanovna (2017): Models of Innovation Development: Measurement Indicators and Their Interaction (a Case Study of Kazakhstan). *Journal of Advanced Research in Law and Economics,* Vol. 8, No. 30. 2361–2372. DOI: https://doi.org/10.14505/jarle.v8.8(30).06.

Bod Péter Ákos (2013): *Heterodox gazdaságpolitikák Magyarországon.* MTA-doktori értekezés, Budapest.

Bonvillian, William Boone – Van Atta, Richard – Windham, Patrick eds. (2019): *The DARPA Model for Transformative Technologies: Perspectives on the U.S. Defense Advanced Research Projects Agency.* Cambridge, UK, Open Book Publishers.

Bower, Joseph L. – Christensen, Clayton M. (1995): Disruptive Technologies: Catching the Wave. *Harvard Business Review,* No. 1. 43–53.

Bőgel György (2008): A schumpeteri „teremtő rombolás" módjai az infokommunikációs iparban. *Közgazdasági Szemle,* 55. évf. 4. sz. 344–360.

BudapestHUB Work Team (2013): *Runway Budapest 2.0.2.0 – A Startup Credo.* Elérhető: www.nih.gov.hu/runway-2-0-2-0. (A letöltés dátuma: 2014. 04. 16.)

Bush, Vannevar (1944–1945): Science the Endless Frontier. *Transactions of the Kansas Academy of Science,* Vol. 48, No. 3. 231–264.

Buzás Norbert szerk. (2007) *Innovációmenedzsment a gyakorlatban*. Budapest, Akadémiai.

Callon, Michel (1994): Is Science a Public Good? Fifth Mullins Lecture, Virginia Polytechnic Institute, 23 March 1993. *Science, Technology, & Human Values,* Vol. 19, No. 4. 395–424. DOI: https://doi.org/10.1177/016224399401900401

Camagni, R. (1991): Local "Milieu", Uncertainty and Innovation Networks: Towards a New Dynamic Theory of Economic Space. In *Innovation Networks: Spatial Perspectives.* London, Belhaven.121–144.

Carayannis, Elias G. – Campbell, David F. J. (2009): "Mode 3" and "Quadruple Helix": Toward a 21st Century Fractal Innovation Ecosystem. *International Journal of Technology Management,* Vol. 46, No. 3–4. 201–234.

Carayannis, Elias G. – Campbell, David F. J. (2010): Triple Helix, Quadruple Helix and Quintuple Helix and How Do Knowledge, Innovation and the Environment Relate To Each Other? A Proposed Framework for a Trans-Disciplinary Analysis of Sustainable Development and Social Ecology. *International Journal of Social Ecology and Sustainable Development,* Vol. 1, No. 1. 41–69. DOI: https://doi.org/10.4018/jsesd.2010010105

Carayannis, Elias G. – Campbell, David F. J. (2019): *Smart Quintuple Helix Innovation Systems: How Social Ecology and Environmental Protection Are Driving Innovation, Sustainable Development and Economic Growth*. Switzerland, Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-01517-6

Carayannis, Elias G. – Barth, Thorsten D. – Campbell, David F. J. (2012): The Quintuple Helix Innovation Model: Global Warming as a Challenge and Driver for Innovation. *Journal of Innovation and Entrepreneurship,* Vol. 1, No. 1. 1–12. DOI: https://doi.org/10.1186/2192-5372-1-2

Carlsson, Benny – Stankiewicz, Rikard (1991): On the Nature, Function and Composition of Technological Systems. *Journal of Evolutionary Economics,* Vol. 1, No. 2. 93–118.

Choi, Joonhwan – Lee, Jaegul (2017): Repairing the R&D Market Failure: Public R&D Subsidy and the Composition of Private R&D. *Research Policy,* Vol. 46, No. 8. 1465–1478.

Coase, Ronald H. (1988): The Nature of the Firm: Origin. *Journal of Law, Economics, & Organization,* Vol. 4, No. 1. 3–17.

Cooper, Juett R. (1998): A Multidimensional Approach to the Adoption of Innovation. *Management Decision,* Vol. 36, No. 8. 493–502. DOI: https://doi.org/10.1108/00251749810232565

Cyex – Cyber Security Awareness Platform. Weboldal. Elérhető: https://cyex.io/ (A letöltés dátuma: 2020. 05. 26.)

Csáki György szerk. (2019): *A Látható Kéz. A Fejlesztő Állam a Globalizációban.* Budapest, Napvilág.

Csákné Filep Judit – Radácsi László – Timár Gigi (2020): A magyar startup-vállalkozások túlélését és növekedését befolyásoló tényezők. Szakértői interjúk tapasztalatai. *Vezetéstudomány,* 51. évf. 1. sz. 16–31. DOI: https://doi.org/10.14267/VEZTUD.2020.01.02

David, Paul A. – Hall, Bronwyn H. (2000): Heart of Darkness: Modeling Public–Private Funding Interactions inside the R&D Black Box. *Research Policy,* Vol. 29, No. 9. 1165–1183.

Defense One (2015): *Battlefield 2050: How Today's Cutting Edge Technologies Are Shaping the Future of Warfare.* Elérhető: www.defenseone.com/reports/battlefield-2050/123164/ (A letöltés dátuma: 2020. 05. 26.)

Doing Business 2018: Reforming to Create Jobs (2017). Washington, The World Bank. Elérhető: http://documents.worldbank.org/curated/en/803361509607947633/Doing-Business-2018-Reforming-to-Create-Jobs (A letöltés dátuma: 2018. 08. 20.)

Dutz, Mark A. – Kessides, Joannis – O'Connell, Stephen – Willig, Robert D. (2011): *Competition and Innovation-Driven Inclusive Growth.* Policy Research Working Papers. The World Bank. DOI: https://doi.org/10.1596/1813-9450-5852

Dzisah, James – Etzkowitz, Henry (2008): Triple Helix Circulation: The Heart of Innovation and Development. *International Journal of Technology Management & Sustainable Development,* Vol. 7, No. 2. 101–115. DOI: https://doi.org/10.1386/ijtm.7.2.101_1

EBN – Innovation Network. Weboldal. Elérhető: https://ebn.eu/ (A letöltés dátuma: 2020. 05. 26.)

Edquist, Charles (2005): Systems of Innovation: Perspectives and Challenges. In Fagerberg, Jan – Mowery, David C. – Nelson, Richard R. eds.: *The Oxford Handbook of Innovation.* Oxford University Press. DOI: https://doi.org/10.1093/oxfordhb/9780199286805.003.0007

Edquist, Charles ed. (1997): *Systems of Innovation: Technologies, Institutions, and Organizations.* Systems of Innovation: Science, Technology and the International Political Economy Series. London–Washington, Pinter.

Enhancing Cybersecurity – The Role of Innovation Ecosystems (2019). MIT Innovation Initiative. Elérhető: https://innovation.mit.edu/assets/Enhancing-Cybersecurity-The-Role-of-Innovation-Ecosystems.pdf (A letöltés dátuma: 2020. 05. 20.)

Etzkowitz, Henry (2008): *The Triple Helix: University – Industry – Government Innovation in Action.* New York, Routledge Taylor & Francis Group. DOI: https://doi.org/10.4324/9780203929605

Etzkowitz, Henry – Leydesdorff, Loet (1995): The Triple Helix – University-Industry-Government Relations: A Laboratory for Knowledge Based Economic Development. *EASST Review,* Vol. 14, No. 1. 14–19.

European Commission (1995): *Green Paper on Innovation.* Elérhető: https://europa.eu/documents/comm/green_papers/pdf/com95_688_en.pdf. (A letöltés dátuma: 2020. 05. 20.)

European Union Agency for Network and Information Security (ENISA) (2017): *Review of Cyber Hygiene Practices.* DOI: https://doi.org/10.2824/352617

Fahey, Ryan (2020): Hackable Medical Devices. Explore within Healthcare Cyber Threat Landscape. *Infosec Resources.* Elérhető: https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-cyber-threat-landscape/hackable-medical-devices/ (A letöltés dátuma: 2020. 05. 28.)

Farinha, Luis – Ferreira, João J. (2013): Triangulation of the Triple Helix: A Conceptual Framework. *Triple Helix Association, Working Paper.* 1–25. DOI: https://doi.org/10.13140/2.1.4161.1202

Florida, Richard (1995): Toward the Learning Region. *Futures,* Vol. 27, No. 5. 527–536.

Freeman, Christopher (1987): *Technology, Policy, and Economic Performance: Lessons from Japan.* Pinter Pub Ltd.

Gartner (é. n.): *Gartner Hype Cycle for Emerging Technologies*. Elérhető: www.gartner.com/en/webinars/43051/gartner-hype-cycle-for-emerging-technologies (A letöltés dátuma: 2020. 05. 18.)

Global Information Security Workforce Study – Strategies for Building and Growing Strong Cybersecurity Teams (2019). Elérhető: www.isc2.org/Research/2019-Cybersecurity-Workforce-Study# (A letöltés dátuma: 2020. 05. 28.)

Guzmán-Mares, Lucio – Castellanos-Villarruel, Ma Soledad (2017): Innovation of Sustainable Products and Services through Ecodesign Project Management by Applying SINNAPS. In *Technology Innovation, Finance and CRM: Repercussions on Competitiveness.* Universidad de Guadalajara. 135–159.

Haig Zsolt – Kovács László (2008): Fenyegetések a cybertérből. *Nemzet és Biztonság: Biztonságpolitikai Szemle,* 1. évf. 5. sz. 61–70.

Harbisson, Neil: *Becoming Cyborg.* Előadás. Brain Bar Budapest. Elérhető: www.youtube.com/watch?v=d94T5kbr2RU&t=305s (A letöltés dátuma: 2020. 05. 26.)

Hassink, Robert (1999): What Does the Learning Region Mean for Economic Geography. *The Korean Journal of Regional Science,* Vol. 15, No. 1. 93–116.

Hern, Alex (2018): Fitness Tracking App Strava Gives Away Location of Secret US Army Bases. *The Guardian,* 2018. 01. 28. Elérhető: www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (A letöltés dátuma: 2020. 05. 28.)

Herstatt, Cornelius – Stockstrom, Christoph – Tschirky, Hugo – Nagahira, Akio (2006): *Management of Technology and Innovation in Japan*. Berlin – Heidelberg – New York, Springer Science & Business Media.

Inzelt Annamária – Bajmócy Zoltán (2013): Az innovációs rendszer építőkövei. (Bevezetés). In Inzelt Annamária – Bajmócy Zoltán szerk.: *Innovációs rendszerek.* Szeged, JATEPress. 9–18.

Inzelt Annamária (1998): A tudáson alapuló gazdaság. *Vezetéstudomány,* 29. évf. 6. sz. 1–11.

Iványi Attila Szilárd – Hoffer Ilona (2010): *Innováció a vállalkozásfejlesztésben.* Budapest, Aula.

Johannessen, Jon-Arild – Olsen, Bjørn – Lumpkin, G. T. (2001): Innovation as Newness: What Is New, How New, and New to Whom? *European Journal of Innovation Management,* Vol. 4, No. 1. 20–31. DOI: https://doi.org/10.1108/14601060110365547

Kattel, Rainer – Mazzucato, Mariana (2018): Mission-Oriented Innovation Policy and Dynamic Capabilities in the Public Sector. *Industrial & Corporate Change,* Vol. 27, No. 5. 787–801. DOI: https://doi.org/10.1093/icc/dty032

Keszey Tamara – Zsukk János (2017): Az új technológiák fogyasztói elfogadása. A magyar és nemzetközi szakirodalom áttekintése és kritikai értékelése. *Vezetéstudomány,* 48. évf. 10. sz. 38–47. DOI: https://doi.org/10.14267/VEZTUD.2017.10.05

Kocsis Éva – Szabó Katalin (1996): *Technológiai korszakhatáron – rugalmas technológiák – regionális hálózatok.* Budapest, OMFB.

Kollmann, Tobias – Stoeckman, Christoph – Hensellek, Simon – Kensbock, Julia (2016): *European Startup Monitor 2016.* Universität Duisburg-Essen.

Kotsis Ágnes – Nagy Ildikó (2009): Az innováció diffúziója és a Triple Helix modell. *Educatio,* 18. évf. 1. sz. 121–126.

Kovács György (2004): Innováció, technológiai változás, társadalom: újabb elméleti perspektívák. *Szociológiai Szemle,* 3. sz. 52–78.

Kovács László – Krasznay Csaba (2010): Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság: Biztonságpolitikai Szemle,* 3. évf. 1. sz. 44–56.

Kovács László – Krasznay Csaba (2017): Digitális Mohács 2.0. kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság: Biztonságpolitikai Szemle,* 10. évf. 1. sz. 3–16.

Kovacs, Eduard (2020): *Hackers Knew How to Target PLCs in Israel Water Facility Attacks: Sources.* 2020. 04. 30. Elérhető: www.securityweek.com/hackers-knew-how-target-plcs-israel-water-facility-attacks-sources?fbclid=IwAR2TS6-4nsPEAGHS6YXGwVqGPqVd03RMnwUoW1mn53MGbb8ns8ZWDTmvtBY (A letöltés dátuma: 2020. 05. 26.)

Krasznay Csaba (2012): A polgárok védelme egy kiberkonfliktusban. *Hadmérnök,* 7. évf. 4. sz. 142–151.

Lalkaka, Rustam (2001): *Best Practices in Business Incubation: Lessons (yet to Be) Learned.* Presented at the International Conference on Business Centers: Actors for Economic & Social Development, Brussels, 2001. 11. 14.

Makó, Csaba – Illéssy, Miklós – Heidrich, Balázs (2019): When Will Alpha and Omega Collide? In Search of the Theoretical Relevance of EU Innovation Policies. *Vezetéstudomány,* 50. évf. 11. sz. 66–73. DOI: https://doi.org/10.14267/VEZTUD.2019.11.05

Makó Csaba – Illéssy Miklós (2014): A szervezeti innovációk a közszféra szervezeteiben. (A Jó Állam létrehozásának és tartós fenntartásának elhanyagolt dimenziója). *Pro Publico Bono: Magyar Közigazgatás,* 4. sz. 4–20.

Malerba, Franco (2005): Sectoral Systems of Innovation: A Framework for Linking Innovation to the Knowledge Base, Structure and Dynamics of Sectors. *Economics of Innovation and New Technology,* Vol. 14, No. 1–2. 63–82.

Marinova, Dora – Phillimore, John (2003): Models of Innovation. In Shavinina, Larisa V. ed.: *The International Handbook on Innovation*. Oxford, Pergamon. 44–53. DOI: https://doi.org/10.1016/B978-008044198-6/50005-X

Mazzucato, Mariana – Robinson Douglas K. R. (2018): Co-Creating and Directing Innovation Ecosystems? NASA's Changing Approach to Public-Private Partnerships in Low-Earth Orbit. *Technological Forecasting and Social Change,* Vol. 136. 166–177. DOI: https://doi.org/10.1016/j.techfore.2017.03.034

Mazzucato, Mariana (2016): From Market Fixing to Market-Creating: A New Framework for Innovation Policy. *Industry and Innovation,* Vol. 23, No. 2. 140–156. DOI: https://doi.org/10.1080/13662716.2016.1146124

Miller, William L. – Morris, Langdon (1999): *Fourth Generation R&D: Managing Knowledge, Technology, and Innovation.* Wiley.

Murray, Fiona – Budden, Phil (2019): *MIT's Stakeholder Framework for Building & Accelerating Innovation Ecosystems.* Working Paper. MIT's Laboratory for Innovation Science & Policy.1–28.

Nelson, Richard R. ed. (1993): *National Innovation Systems a Comparative Analysis.* New York – Oxford, Oxford University Press.

Németh Balázs (2006): A tanuló régió, mint a regionális fejlesztés eszköze. *Tudásmenedzsment,* 7. évf. 1 sz. 3–14.

Nemzeti Innovációs Hivatal (2008): *A Nemzeti Innovációs Hivatal kutatás-fejlesztési és innovációs (KFI) értékelési feladatainak módszertani vezérfonala (Az EU támogatásával készült EVAL-INNO értékelési standardok alapján).* Elérhető: https://nkfih.gov.hu/hivatalrol/hivatali-kiadvanyok/nemzeti-innovacios-180603-1 (A letöltés dátuma: 2013. 07. 08.)

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal: *Horizont 2020.* Weboldal. Elérhető: www.h2020.gov.hu/ii-ipari-vezeto-szerep/vezeto-szerep-technologiak-teruleten/informacios (A letöltés dátuma: 2020. 06. 30.)

Nicolaides, Phedon (2013): The Economics of Subsidies for R & D: The Intrinsic Difficulty of Determining Optimum Subsidies and Implications for Reform of EU State Aid Rules on R & D. *Bruges European Economic Research Papers,* Vol. 26. 1–19.

Nielsen, Peter (2006): *The Human Side of Innovation Systems – Innovation, Organizations and Competence Building in a Learning Perspective.* Aalborg University Press.

Nordhaus, William D. – Samuelson, Paul A. (2016): *Közgazdaságtan.* [Digitális Kiadás.] Budapest, Akadémiai. DOI: https://doi.org/10.1556/9789630597814

Novotny Ádám (2009): Az elefántcsonttoronytól a tudományos kapitalizmusig: a felsőoktatási intézmények új küldetése. *Periodica Oeconomica,* 2. évf. 5. sz.

OECD (1994): *The Measurement of Scientific and Technical Activities: Standard Practice for Surveys of Research and Experimental Development – Frascati Manual.* Elérhető: www.oecd-ilibrary.org/content/publication/9789264063525-en (A letöltés dátuma: 2020. 05. 26.)

OECD (2015): *Frascati Manual 2015 – Guidelines for Collecting and Reporting Data on Research and Experimental Development.* Elérhető: www.oecd.org/publications/frascati-manual-2015-9789264239012-en.htm (A letöltés dátuma: 2020. 05. 26.)

OECD (2018): *Oslo Manual 2018 – Guidelines for Collecting, Reporting and Using Data on Innovation.* 4th edition. Elérhető: www.oecd.org/science/oslo-manual-2018-9789264304604-en.htm (A letöltés dátuma: 2020. 05. 26.)

OECD and Statistical Office of the European Communities (2005): *Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data.* 3th edition. Elérhető: www.oecd-ilibrary.org/content/publication/9789264013100-en (A letöltés dátuma: 2020. 05. 26.)

Oversight Board – Independent Judgment. Transparency. Legitimacy. Elérhető: www.oversightboard.com/ (A letöltés dátuma: 2020. 05. 26.)

Pavani, Claudia – Oliveira Jr., Moacir De Miranda – Plonsky, Guilherme A. (2019): Cases of University Spin-Offs. In Oliveira Jr., Moacir De Miranda – Riberio Cahen, Fernanda – Borini, Felipe Mendes eds.: *Startups and Innovation Ecosystems in Emerging Markets: A Brazilian Perspective*. Palgrave Macmillan, Cham. 203–223. DOI: https://doi.org/10.1007/978-3-030-10865-6_11

Perez, Carlota (2002): *Technological Revolutions and Financial Capital. The Dynamics of Bubbles and Golden Ages.* Cheltenham, UK, Northampton, MA, USA, Edward Elgar.

Perez, Carlota (2009): *The double bubble at the turn of the Century: Technological roots and structural implications.* CFAP Working Paper. 31. Centre for Financial Analysis & Policy, Cambridge University.

Piskóti István (2007): Az innovációmarketing lehetőségei, gyakorlati megoldásai. *Marketing & Menedzsment,* 41. évf. 4–5. sz. 32–39.

Ponds, Roderik – Oort, Frank – Frenken, Koen (2010): Innovation, Spillovers and University–Industry Collaboration: An Extended Knowledge Production Function Approach. *Journal of Economic Geography,* Vol. 10, No. 2. 231–255.

Porkoláb Imre (2016): Az innováció hatása a hadviselésre. *Hadtudomány,* 26. évf. 1–2. sz. 19–28. DOI: https://doi.org/10.17047/HADTUD.2016.26.1-2.19

Preez, Niek D. du – Louw, Louis (2008): A Framework for Managing the Innovation Process. In *PICMET '08 – 2008 Portland International Conference on Management of Engineering & Technology.* Cape Town, South Africa, IEEE. 546–558. DOI: https://doi.org/10.1109/PICMET.2008.4599663

Ramstad, Elise (2009): Developmental Evaluation Framework for Innovation and Learning Networks: Integration of the Structure, Process and Outcomes. *Journal of Workplace Learning,* Vol. 21, No. 3. 181–197. DOI: https://doi.org/10.1108/13665620910943924

Ramstad, Elise (2016): A Systemic Framework for a Broad-Based Innovation Policy. *EUWIN Newsletter.* 4.

Rekettye Gábor (2018): *Értékteremtés 4.0. Termékek és szolgáltatások vevőorientált tervezése, fejlesztése és menedzselése.* Budapest, Akadémiai. DOI: https://doi.org/10.1556/9789634542230

Rothwell, Roy (1992): Successful Industrial Innovation: Critical Factors for the 1990s. *R&D Management,* Vol. 22, No. 3. 221–240. DOI: https://doi.org/10.1111/j.1467-9310.1992.tb00812.x

Rothwell, Roy (1994): Towards the Fifth-generation Innovation Process. *International Marketing Review,* Vol. 11, No. 1. 7–31. DOI: https://doi.org/10.1108/02651339410057491

Ruszkai Csaba (2014): *Helyi erőforrás és termékpályamenedzsment.* Eszterházy Károly Főiskola. Elérhető: https://regi.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0038_15_ruszkai_hu/ch08s03.html (A letöltés dátuma: 2020. 05. 26.)

Saviotti, Pier P. (1996): *Technological Evolution, Variety and the Economy.* Cheltenham, U.K., Edward Elgar.

Schienstock, Gerd – Hämäläinen, Timo J. (2001): Transformation of the Finnish Innovation System: A Network Approach. *SITRA Reports Series,* No. 7. Helsinki.

Shira, Stein – Jacobs, Jennifer (2020): Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak. *Bloomberg,* 2020. 03. 16. Elérhető: www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response. (A letöltés dátuma: 2020. 05. 26.)

Statista: *Facebook Users Worldwide 2020.* Elérhető: www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (A letöltés dátuma: 2020. 05. 28.)

Stigler, George J. (1971): The Theory of Economic Regulation. *The Bell Journal of Economics and Management Science,* Vol. 2, No. 1. 3–21. DOI: https://doi.org/10.2307/3003160

Stiglitz, Joseph Eugene (1999): *Economics of the Public Sector.* 3th edition. New York, Norton.

Stubbs, Jack – Holton, Kate (2020): Chinese Hackers Suspected of Stealing Details of 9 Million EasyJet Customers. *Reuters,* 2020. 05. 19. Elérhető: https://uk.reuters.com/article/us-easyjet-cyber-idUKKBN22V1JF. (A letöltés dátuma: 2020. 05. 28.)

Szabó Katalin (1999): A tudás globális piaca és a lokális tanulás. *Közgazdasági Szemle,* 46. évf. 3. sz. 278–294.

Szabó Katalin (2012): Hol tartunk? Innovációs trendek a globális gazdaságban. In Hámori B.alázs – Szabó Katalin szerk.: *Innovációs verseny: Esélyek és korlátok.* Budapest, Aula. 101–146. DOI: https://m2.mtmt.hu/api/publication/2348658

Szalavetz Andrea (2005): A nanotechnológia és az új ipari forradalom. *Külgazdaság,* 49. évf. 11–12. sz. 58–75.

Szalavetz Andrea (2018): Néhány gondolat Szanyi Miklós: „Műszaki fejlődés és hosszú távú gazdasági ciklusok" című írása ürügyén. In *Műszaki fejlődés és hosszú távú gazdasági ciklusok.*

Műhelytanulmányok. Budapest, MTA Közgazdaság- és Regionális Tudományi Kutatóközpont, Világgazdasági Intézet. 38–48.

Szanyi Miklós (2009): Tudomány és innováció, avagy mit és hogyan fejlesszen az állam a kis európai országokban? *Külgazdaság,* 53. évf. 5–6. sz. 63–90.

Szanyi Miklós (2010): Innovációs tevékenység a regionális együttműködési hálózatban: innovatív klaszterek? In Kapás Judit szerk.: *Technológiai fejlődés és intézmények.* Competitio Könyvek 10. Debrecen, Debreceni Egyetem Közgazdaság- és Gazdálkodástudományi Kar. 109–122.

Szanyi Miklós (2018): *Műszaki fejlődés és hosszú távú gazdasági ciklusok.* Műhelytanulmányok. Budapest, MTA Közgazdaság- és Regionális Tudományi Kutatóközpont, Világgazdasági Intézet.

Szívós Mihály (2014): A „sokoldalú kutató" és a hiányzó kutatásmenedzser. Érvek a háromszintű kutatásmenedzsment-oktatás mellett. *Vezetéstudomány,* 45. évf. 6. sz. 49–60.

Szunyogh Zsuzsanna (2010): Az innováció mérésének módszertani kérdései. *Statisztikai Szemle,* 88. évf. 5. sz. 493–507.

Taferner, Benjamin (2017): A Next Generation of Innovation Models? An Integration of the Innovation Process Model Big Picture Towards the Different Generations of Models. *Review of Innovation and Competitiveness,* Vol. 3, No. 3. 47–60. DOI: https://doi.org/10.32728/ric.2017.33/4

Tétényi Tamás (2013): *A kutatás, technológiai fejlesztés és innováció erősítése és az információs és kommunikációs technológiák hozzáférhetőségének, használatának és minőségének javítása a korábbi tapasztalatok és értékelési eredmények áttekintése.* Hétfa Elemző Központ. 1–40.

Turcsán Tamás Péter (2019): *Startupbook@me: Az elveszett recept.* Budapest.

Vas Zsófia Boglárka – Bajmócy Zoltán (2012): Innovációs rendszerek 25 éve. Szakirodalmi áttekintés evolúciós közgazdaságtani megközelítésben. *Közgazdasági Szemle,* 59. évf. 11. sz. 1233–1256.

Vas Zsófia Boglárka (2012): Tudásalapú gazdaság és társadalom kiteljesedése: A Triple Helix továbbgondolása – a Quadruple és Quintuple Helix. In Rechnitzer János – Rácz Szilárd szerk.: *Dialógus a regionális tudományról.* Győr, Széchenyi István Egyetem Regionális- és Gazdaságtudományi Doktori Iskola. 198–206.

Vas Zsófia Boglárka (2017): *Innovációs rendszerek a kevésbé fejlett régiókban: tudásintenzív iparágak a Dél-Alföldön.* Szeged, JATEPress.

Vecsenyi János (2017): *Kisvállalkozások indítása és működtetése.* Budapest, Akadémiai. DOI: https://doi.org/10.1556/9789634542254

Vukoszavlyev Szlobodan – Polereczki Zsolt – Kovács Bence (é. n.): *Az innováció fogalmának fejlődése.* Debrecen, Debreceni Egyetem. 1–11.

Warrick, Joby – Nakashima, Ellen (2020): Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility. *Washington Post,* 2020. 05. 18. Elérhető: www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html. (A letöltés dátuma: 2020. 05. 26.)

VÁKÁT OLDAL

Krasznay Csaba

Kiberbiztonsági K+F+I Európában

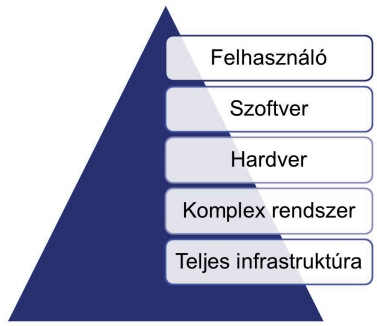
Bevezetés

Ha eddig nem éreztük volna, hogy függünk az információs rendszerektől, a negyedik ipari forradalom változásai egészen biztosan mindenki számára tudatosítani fogják, hogy informatika nélkül nincs modern társadalom. Ha tehát ezek az információs rendszerek nem úgy működnek, ahogy kellene, az jelentős gazdasági-társadalmi hatásokkal járhat, biztonságuk megteremtése ezért alapvető érdek. Az átlagos hírfogyasztó ma már nem nagyon tudja úgy megnyitni kedvenc hírportáljának kezdőoldalát, hogy azon ne lenne híradás valamilyen komoly kiberbiztonsági incidensről. Folyamatosan olvashatunk országok elleni kibertámadásokról, százmilliókat érintő adatszivárgásokról vagy éppen olyan egzotikusnak tűnő információs rendszerek manipulálásáról, mint egy erőművi rendszer ipari irányítástechnikája. Mennyire lehetnek informatikai értelemben biztonságosak az úgynevezett Internet of Things (IoT), azaz dolgok internetét alkotó megoldások? Tágabban értelmezve, megvalósítható-e a dolgok internetére épülő negyedik ipari forradalom olyan eszközökkel, amelyek támadhatók, és megfelelő erőforrásokkal rendelkező entitások sikerrel is támadják majd azokat?

Az információbiztonsági szakértők körében az IoT rövidítés közkeletű feloldása az Internet of Threats, azaz a fenyegetések internete, utalva arra, hogy a szakértői közösségnek komoly aggályai vannak mind az egyes eszközök, mind pedig az ezekből felépülő ökoszisztéma védelmi szintjével kapcsolatban. Továbbmenve, a szakértők viccesen azt is megjegyzik, hogy az IoT betűszóban az S betű jelöli a Security-t, azaz a biztonságot. Az elmúlt évek kibertámadásainak köszönhetően ebben a félelemben ma már a stratégiai védelemmel foglalkozó szakemberek is osztoznak, így egyre több ország nemzeti biztonsági és kiberbiztonsági stratégiája foglalkozik a kibertéri fenyegetésekkel kiemelt nemzetbiztonsági problémaként. A kockázatok enyhítése céljából folyamatosan dolgozzák ki azokat a szabályozókat, amelyek kötelezik az okos-infrastruktúrák építőit és üzemeltetőit bizonyos informatikai védelmi intézkedések megtételére.

Az információs rendszereket érintő fenyegetések

Mérnöki szempontból hajlamosak vagyunk arra koncentrálni, hogy az egyes rendszerelemek biztonságát vizsgáljuk, figyelmen kívül hagyva, hogy az adott rendszerelem egy komplex rendszer részeként működik, amelyet emberek üzemeltetnek. Így bár egyes modulokat lehet, hogy a rendelkezésre álló legátfogóbb információbiztonsági szemlélettel valósítottak meg, a teljes ellátási lánc valamelyik elemének gyengesége alááshatja az egyes részegységek nyújtotta védelmi szint megfelelőségét. Az 1. ábra bemutatja, milyen támadási felületek mutatkoznak egy komplex kiberfizikai rendszer esetén.



1. ábra: Támadási felületek az okos-infrastruktúrákban
Forrás: a szerző szerkesztése

Vizsgáljuk meg az okosközlekedés példáján keresztül, mit jelent az 1. ábrán vázolt támadási felület egy autonóm, önvezető gépjármű szempontjából! A hardver az egyes szenzorokat, beavatkozóegységeket jelenti, amelyek tömegével találhatók meg az autóban. Ezek hálózatokon keresztül juttatnak el adatot a gépjármű központi számítógépéhez, amely az adatokból a szoftver segítségével információt állít elő, és ezzel irányítja a személygépjárművet mint komplex rendszert. Ez a komplex rendszer azonban egy okosközlekedési infrastruktúra esetén folyamatosan kommunikál az őt körülvevő környezettel, így a közlekedésirányító infrastruktúrával és a többi autóval, amelyek a nagyobb rendszert alkotják. Ebben az infrastruktúrában természetesen jelen vannak az emberek is mint sofőrök vagy mint rendszerüzemeltetők.

Ennyire komplex környezetben kiberbiztonsági szempontból hibátlan rendszert megvalósítani szinte lehetetlen. Sokszor már az egyes rendszerelemek is tartalmaznak olyan sebezhetőségeket, amelyeket a megfelelő motivációval és szakértelemmel rendelkező támadó ki tud használni, és ezzel a teljes rendszert nem tervezett működésre tudja bírni. Nincs okunk kételkedni abban, hogy a negyedik ipari forradalom kiberfizikai eszközeit egyre inkább a biztonságos szoftverfejlesztés elveit felhasználva fogják létrehozni, ám ezek számosságuk és hálózati kapcsolatuk miatt könnyebben elérhetők lesznek, így feltételezzük, hogy a bennük felfedezett hibák száma az évek során monoton növekedni fog.

Nem szabad figyelmen kívül hagyni az emberi tényezőt sem! Bányász Péter az ellátási láncok kiberbiztonságáról szóló munkájában a következőket említi az emberi hiszékenységet kihasználó (úgynevezett social engineering) támadásokkal kapcsolatban: „Tegyük fel, a külső támadás lehetetlenné vált, olyan mértékű védelmet valósítottak meg. Ilyen esetben van szerepe a social engineeringnek, hiszen, maradva a hipotetikus példánál, a kikötő takarítószemélyzetéből egy dolgozó megzsarolásával/megtévesztésével a támadók elérhetik, hogy a takarító az informatikai eszközökhöz hozzáférést biztosítson egy pendrive a számítógépbe történő helyezésével, amivel a támadók olyan hátsó kapukat nyithatnak, amellyel átvehetik az irányítást az eszköz felett.”[1] A napvilágra került, kritikus infrastruktúrákat érintő támadások során szinte minden esetben sejthető, hogy szándékos vagy gondatlan emberi tevékenység nélkül a támadás kivitelezése lényegesen nehezebb vagy egyenesen lehetetlen lett volna.

[1] Bányász 2016

A támadási felületek közül nem említettük a hardvert, a komplex rendszert és a teljes infrastruktúrát. Nem véletlenül. Ezek esetében ugyanis hiányoznak azok a megbízható statisztikák, adatforrások, amelyekkel szemléltetni lehet a kitettségüket. A hardverek esetében például tudjuk, hogy számos CPU-tervezési sajátosságuk miatt elméletileg lehetőséget biztosítanak a számítógépen feldolgozott bizalmas adatokhoz való hozzáféréshez (lásd a Spectre- és Meltdown-hibákat), de csak elképzeléseink lehetnek arról, hogy ezek valójában mekkora kockázatot jelentenek. A kínai távközlési gyártók angolszász országokból való távoltartásának szándéka is mutatja, milyen nemzetbiztonsági kihívást érzékelnek a stratégiai védelemért felelős vezetők abban, ha az 5G távközlési rendszerek infrastruktúráját ellenérdekelt országok gyártói szállítják.

A védelem komplexitását tovább fokozza az a tény, hogy az elmúlt 10–15 évben jelentősen átalakultak azok az alaptechnológiák, amelyek információtechnológiai értelemben védelemre szorulnak. Ezek között felsorolhatjuk a kétezres években tömegessé vált közösségi hálózatokat, a hordozható infokommunikációs eszközöket vagy éppen a felhő-számítástechnikát, de a 2010-es évek közepétől kezdve elterjedtek azok az ezekre épülő megoldások is, amelyek új szemléletű, új típusú kibervédelmet igényelnek.

Ezen új disztruptív technológiák alatt elsősorban a mesterséges intelligenciát és robotikát, illetve természetesen a mindenhol jelen levő informatikát, a dolgok internetét lehet érteni. A mesterséges intelligencia különösen fontos, hiszen ez nemcsak olyan kihívásokat jelent az ezt használó alkalmazások védelme szempontjából, amelyeket egyelőre felmérni sem tudunk, hanem lehetőséget ad az új típusú kibervédelem felépítéséhez is. A robotika, illetve az emellett megjelenő okoshálózatok szintén egy korábban nem látott problémát és kihívást okoznak az információbiztonsággal foglalkozó szakemberek számára.

Megfigyelhető, hogy a kibertámadások az utóbbi időben a végfelhasználók és az olyan jól ismert iparágak, mint például a bankszektor, illetve a közszolgálat után egyre inkább a gyártás és az alapvető közművek irányába tevődnek át. Meg lehet figyelni, hogy az olyan speciális rendszerek, amelyek a közműszolgáltatásban vagy a gyártásban üzemelnek, szintén meglehetősen védtelenek a kibertéri fenyegetésekkel szemben. Itt azokra az ICS/SCADA, azaz ipari irányítási rendszerekre kell gondolni, amelyeket a gyártásban, illetve a közműszolgáltatásban használnak, és amelyeket nem egyszer akár évtizedekkel korábban állítottak üzembe, és adott esetben még olyan operációs rendszerek futnak rajtuk, amelyek már régen nem támogatottak. Ugyanakkor gondolni kell arra is, hogy ezek az iparágak éppen átélik a negyedik ipari forradalom generálta fejlődést, és itt is előjönnek azok az új típusú megoldások, amelyekkel a gyártás, illetve a közműszolgáltatás okossá válik. Az okosvárosok (smart city) kivétel nélkül alkalmazzák ezeket a speciális információs rendszereket, sokszor azonban a megfelelő alapfokú védelem nélkül.

Az új technológiák kibervédelmi szabályozása

Belátható, hogy a támadási felületek csökkentése, pusztán a mérnökök eszköztárával csak tyúklépésekben lenne megvalósítható, a veszély viszont reális, ezért azonnali, széles körű cselekvést kíván. Be kell tehát vonni azokat a közpolitikai és diplomáciai eszközöket, amelyek egyrészt a támadók motivációját törik le, másrészt rendszerszinten várnak el

cselekvést a negyedik ipari forradalom szereplőitől. Fogalmi szinten ez azt jelenti, hogy az egyes rendszerelemeket érintő információbiztonság mellett az ennél szélesebb körű kiberbiztonság megvalósítása is kívánatos. A negyedik ipari forradalom és az elmúlt években megjelenő kibertéri fenyegetések miatt tehát új típusú kibervédelmet, új típusú kibervédelmi mentalitást kell megvalósítani, miközben az alapvető információbiztonsági alapelvek változatlanok maradnak.

A kiberbiztonság és az információbiztonság közötti fogalmi különbség egyértelműen megfogalmazott a magyar jogszabályokban. A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról szerint az elektronikus információs rendszer biztonsága „az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos", míg a kiberbiztonság „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez". Hasonló megközelítést mutat a 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról is, amelynek „célja, hogy az Alaptörvény elveivel összhangban, az értékek és érdekek számbavétele, valamint a kibertér biztonsági környezetének elemzése alapján meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is", így tehát közel sem csak a mérnöki feladatokra koncentrál.

Az információbiztonságról a kiberbiztonságra való áttérést mutatja egy másik trend is. E trend nyomán egyre több iparágban jelenik meg valamilyen kibervédelmi szabályozás. A pénzintézeteknél és a kormányzati szektorban régóta léteznek olyan szabályozók és jogszabályok, amelyeknek meg kell felelniük az odatartozóknak, viszont az Európai Unió egy három pillérből álló kiberbiztonsági szabályozással jelentősen kiterjesztette a megfelelőségi kényszert. Ez a három pillér a személyes adatok védelmét, a kritikus információs infrastruktúrák biztonságát és a negyedik ipari forradalom eszközeivel kapcsolatos kockázatcsökkentést hivatott elősegíteni.

Az első pillér az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről. Ez a kiberbiztonsági jogszabály. Ennek legfontosabb üzenete, hogy szükséges az információbiztonság erősítése mind termék-, mind szervezeti szinten, de támogatni kell a kiberbiztonsággal kapcsolatos lépéseket is. Az Európai Unió kiberbiztonsági reformról szóló összefoglalójában a kiberbiztonsági jogszabály, azaz a Cybersecurity Act által lefedett területeket így foglalják össze:

Kiberbiztonsági tanúsítási rendszer: Az Európai Bizottság a 2017 szeptemberi reformcsomagban javaslatot tett az IKT-termékekre, -szolgáltatásokra és -folyamatokra vonat-

kozó uniós tanúsítási rendszerek bevezetésére. A kezdeményezés célja az uniós kiberbiztonsági piac növekedésének elősegítése. E tanúsítási rendszerek szabályok, műszaki követelmények és eljárások formájában valósulnának meg. Szerepük az lenne, hogy csökkentsék a piac széttagoltságát, és felszámolják a szabályozási akadályokat, továbbá hogy segítsék a bizalomépítést is. A rendszereket valamennyi tagállam elismerné, ami megkönnyítené a vállalkozások számára a határokon átnyúló kereskedelmet.

Az uniós kiberbiztonsági ügynökség megerősítése: Az Európai Bizottság javasolta továbbá azt is, hogy a meglévő Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) struktúráját felhasználva jöjjön létre egy erősebb uniós kiberbiztonsági ügynökség. Az új ügynökségnek az lenne a feladata, hogy segítséget nyújtson a tagállamok, az uniós intézmények és a vállalkozások számára a kibertámadások kezelésében.

A kompetenciatámogatástól a csalás elleni küzdelemig: Az Európai Bizottságnak az uniós kiberbiztonság megerősítését célzó javaslata további kezdeményezéseket is tartalmaz:

- a nagy kiterjedésű kibertámadásokra adandó válaszlépéseket meghatározó terv;
- az Európai Kiberbiztonsági Kutatási és Kompetenciaközpont, kiegészülve a hasonló központok tagállami szintű hálózatával;
- hatékonyabb büntetőjogi fellépés a kiberbűnözéssel szemben a készpénz-helyettesítő fizetési eszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló új irányelv révén;
- a globális stabilitás erősítése nemzetközi együttműködés útján.[2]

Fontosak tehát mind az információbiztonsági, mind a kiberbiztonsági szempontú tevékenységek. Az Európai Unió még két olyan pillért, szabályozást alkotott, amelyek komoly hatással vannak a nemzeti jogrendre és a negyedik ipari forradalom szereplőinek is érdemben figyelembe kell ezeket venniük. Ezek egyrészt az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, közkeletű nevén a GDPR), másrészt az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről, azaz az NIS-direktíva. Míg a GDPR célja a személyes adatok védelmének biztosítása akár olyan környezetben is, ahol nagy mennyiségű adat keletkezik, tehát tipikusan egy IoT-rendszerekből álló okoskörnyezetben, addig a NIS-direktíva kijelöli azokat a kritikus információs infrastruktúrákat, amelyek védelme európai szinten kiemelten fontos, így például az olyan digitális infrastruktúra-szolgáltatók, mint az Internet Exchange Point-ok, DNS-szolgáltatók vagy legfelső szintű doménnév-nyilvántartó (TLD).

A három pillért figyelembe véve egyértelműen kirajzolódik az Európai Unió törekvése. Olyan termékek és szolgáltatások kialakítását szeretnék ösztönözni innovációs és regulációs eszközökkel az európai piacon, különösen a kritikus információs infrastruktúrát alkotó kiberfizikai rendszerek esetében, amelyek egyszerre veszik figyelembe

[2] European Council 2020

az adatvédelmi és kiberbiztonsági szempontokat. Tekintettel arra, hogy a negyedik ipari forradalom infrastruktúrája és szolgáltatásai éppen kialakulófélben vannak, az európai okos-infrastruktúrában érintett szereplőknek ezt a politikai szándékot mindenképpen érdemes figyelembe venniük.

Innovációs igények a kiberbiztonságban

A negyedik ipari forradalom szereplői közül a nagyvállalatoknál nagy szabályozói nyomást lehet érzékelni, ezért jellemzően nagyon jól működő információbiztonsági kultúra alakult ki az elmúlt évtizedekben. Ezek a vállalati igények egyértelműek, a legtöbb esetben szabályozásokból erednek, illetve azokban az iparágakban, amelyek sokkal jobban kitettek a kibertámadásoknak, mint a többiek, megvan az eljárásrendje annak, hogy milyen módon építsék be akár a legújabb innovatív megoldásokat is a védelmi rendszerükbe.

A nagyvállalatok mellett azonban számos más érintettje is lehet a kibertámadásoknak, kiemelve közülük elsősorban a kis- és közepes vállalkozásokat, ahol az információbiztonság egy olyan terület, amellyel kevéssé vagy egyáltalán nem foglalkoztak eddig. Az említett szabályozások, főleg a GDPR, e területeken is fontossá válnak, ezért szükséges, hogy elérhető és könnyen használható információbiztonsági megoldások jelenjenek meg. Esetükben a szabályozás ugyan megvan, viszont a megfelelőségi nyomás, azaz konkrétan a hatósági ellenőrzések és az ezekből eredő potenciális büntetések egyáltalán nem jellemzők. Ennek ellenére mindenképpen fontos látni, hogy a kis- és közepes vállalkozások túlnyomó többsége is információs rendszerekkel dolgozik, működésük információs rendszerekre épül, így esetükben is elengedhetetlenül fontos az információbiztonsági kultúra felépítése.

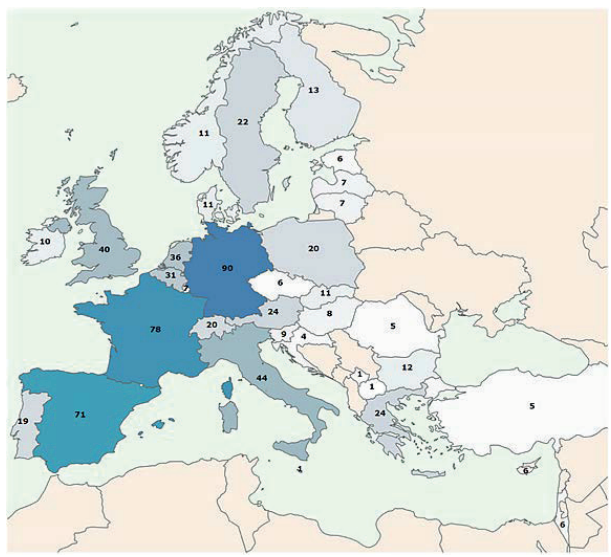
Különös figyelmet kell fordítani a magánszemélyekre is, hiszen jelenleg több mint 4,5 milliárd ember használja az internetet, és a legtöbben olyan eszközökkel kapcsolódnak a világhálóhoz, amelyek információbiztonsági felkészültsége hiányos. A magánszemélyek túlnyomó többsége nem ismeri a kiberhigiénia, azaz a minimálisan elvárt információbiztonsági tevékenységek alapvető fogalmait, így egyrészt potenciálisan saját magukat veszélyeztetik, másrészt pedig ezekkel a nem megfelelően felkészített eszközökkel és elégtelen tudással veszélyt jelentenek a többi internetezőre, az internet teljes struktúrájára.

Elmondható tehát, hogy a negyedik ipari forradalom minden szereplője számára létfontosságú az új típusú kiberbiztonsági kihívásokat kezelni képes termékek és szolgáltatások megalkotása. Számos iparági elemzés mutatja a kiberbiztonsági piac növekedési ütemét. Eltérő számokat látunk, de abban nagyjából minden elemzés egyetért, hogy éves szinten százmilliárd dolláros iparágról beszélünk. A Fortune elemzése szerint 2019-ben 112,01 milliárdos forgalmat bonyolítottak az iparági szereplők, ami éves 12,6%-os növekedési ráta mellett 2027-re 281,74 milliárd dollárra fog nőni. Az európai piac mérete 2019-ben 36,02 milliárd dollár volt.[3]

[3] *Fortune* 2020

Kiberbiztonsági K+F+I Európában és a világban

2018-ban az Európai Unió, készülve a kiberbiztonsági szabályozásainak bevezetésére és a 2021-től induló költségvetés megtervezésére, felmérte a kutatás-fejlesztéssel foglalkozó intézmények számát tagállamaiban, amelyek kimondottan kiberbiztonsággal foglalkoznak.[4] Azt lehetett látni a válaszadásból, hogy míg például Németországban, Franciaországban vagy éppen Spanyolországban meglehetősen sok olyan intézmény van, ahol kiberbiztonsági kutatás-fejlesztés-innovációval foglalkoznak, Kelet-Közép-Európában, így Magyarországon is ezen intézmények száma alacsony, ahogy az a 2. ábrán is megjelenik. Ez azt is jelenti, hogy a globális versenyben, ahol hatalmas országokkal és tudástőkével kell versenyeznie az európai iparnak, nem igazán van meg az az alap, amelyre föl lehet építeni a saját információbiztonsági piacot, illetve tudásbázist.



2. ábra: Európai kiberbiztonsági kutatóközpontok
Forrás: Nai-Fovino et al. 2018

Ez azért lenne fontos, mert a negyedik ipari forradalom robbanásával egyre inkább ki lesz Európa téve azoknak a gyártóknak, amelyek nem európaiak. A hardvereszközöket jellemzően Kínában gyártják, a szoftverek jellemzően amerikai forrásból érkeznek. Éppen ezért az egyes államok által indított kibertámadások előtt gyakorlatilag az európai államok és az európai vállalkozások szinte védtelenül állnak, tekintettel arra, hogy az európai kibervédelem jelenleg nem, vagy nagyon kis számban tud olyan saját gyártású eszközöket használni, amelyek felhasználhatók a külső, akár kiberbűnözésből, akár pedig állami forrásból származó támadások ellen.

[4] Nai-Fovino et al. 2018

Az Európai Unió ezt felismerte, és stratégiai célkitűzése változtatni ezen. Mivel azonban a kutatás-fejlesztéssel foglalkozó intézmények száma meglehetősen alacsony Európában, először is összpontosítani kell az erőfeszítéseket. A felmérés azt is bemutatta, hogy a válaszadók túlnyomó többségében az állami szférából jöttek, tehát valamilyen közintézmény formájában működnek, a magánkézben lévő, piaci alapon működő kutatás-fejlesztéssel foglalkozó intézmények száma lényegesen alacsonyabb, nagyjából harmada a közfinanszírozású intézményeknek, és ennél még alacsonyabb azoknak a PPP-konstrukcióban működő intézményeknek a száma, amelyek mind a magánszféra, mind pedig a köz tudását és tőkéjét felhasználják.

A tervek alapján a következő kutatási érában három pillérre épül a kutatás-fejlesztés-innováció támogatása, ebből az első pillér a kiváló tudomány, a második a globális kihívások és az európai ipar versenyképessége, míg a harmadik pillér az innovatív Európáról fog szólni.[5] Ezt ábrázolja a 3. ábra. A második pillérben *A társadalmat szolgáló polgári biztonság* nevű klaszterben a kiberbiztonság nevesítve szerepel, ez pedig meglehetősen pozitív jövőképet fest azoknak a kutatás-fejlesztés-innovációval foglalkozó intézményeknek és szakembereknek, akik szeretnék az európai kiberbiztonsági ipart megteremteni. Az Európai Bizottság tervei alapján a 2021–2027 közötti szakaszban 100 milliárd euró nagyságrendű összeg áll majd rendelkezésre a kutatás-fejlesztés-innovációra, ezen belül a *Globális kihívások és az európai ipar versenyképessége* pillér 52,7 milliárd euróra számíthat. Tovább bontva, *A társadalmat szolgáló polgári biztonság* klaszterben szerepel a kiberbiztonság, amely a jelenlegi tudásunk szerint körülbelül 2 milliárd euróval fog részesülni ebből a hatalmas összegből.[6]

3. ábra: EU-finanszírozás a kutatás és az innováció területén (2021–2027)
Forrás: Európai Bizottság 2018

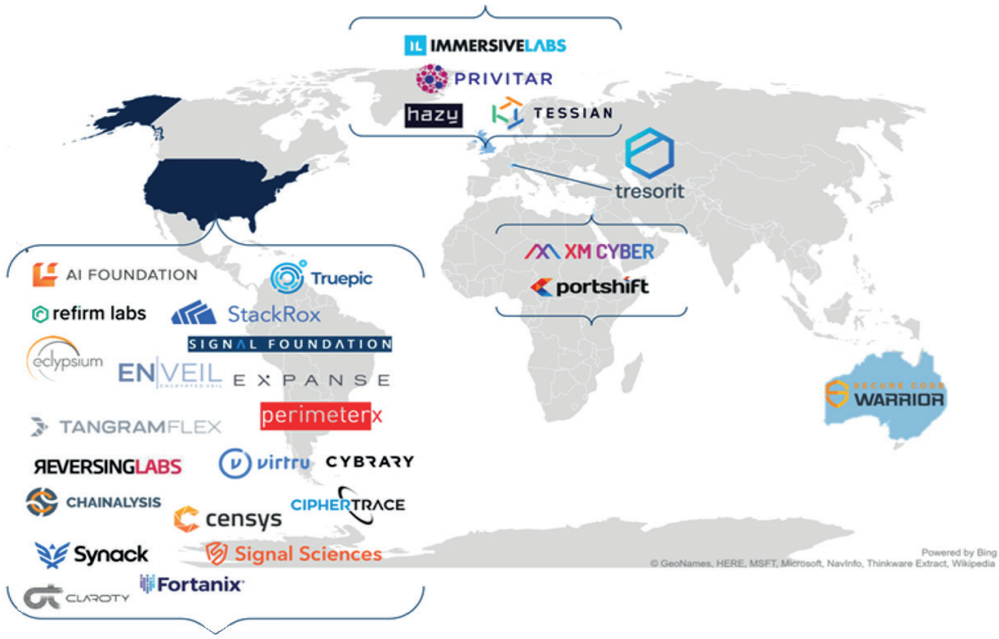
[5] Európai Bizottság 2018
[6] Digital Single Market 2018

Magyarország természetesen aktívan követi az Európai Unió innovációs törekvéseit, és bár a következő időszakra vonatkozó tervek még nem ismertek, a kiberbiztonság biztosan része lesz a magyar kutatás-fejlesztés-innovációs stratégiának. Ezt támasztja alá, hogy a 2020-ban érvényes stratégiai dokumentumok is kivétel nélkül foglalkoznak ezzel a szakterülettel. A 1414/2013. (VII. 4.) Korm. határozat a Nemzeti Kutatás-fejlesztési és Innovációs Stratégia (2013–2020) elfogadásáról már kiemeli, hogy az egyik cél az adaptív innovációs megoldások – elsősorban informatikai és kommunikációs technológiákra alapozott – terjedésének gyorsítása. A részleteket a 1640/2014. (XI. 14.) Korm. határozat a Nemzeti Intelligens Szakosodási Stratégia (S3) elfogadásáról és a Kutatási Infrastruktúrák Európai Stratégiai Fóruma Útitervében szereplő kutatási infrastruktúra nagyprojektekben való magyar részvételről mentén kiadott Nemzeti Intelligens Szakosodási Stratégia (S3) – 2014–2020 segít megérteni. Ebben az IKT-terület céljait az alábbiak szerint fogalmazzák meg: „Az infokommunikációs technológiák széleskörűen fogják át és segítik elő az ágazati prioritásokat, úgy is, mint az egészségiparban a bioinformatika vagy a diagnosztikai képalkotás, a járműiparban az intelligens közlekedési rendszerek, az energetikában a »smart city«. Az ágazati prioritásokhoz nem, vagy nem egyértelműen, vagy akár több ágazathoz is sorolható IKT-megoldások alatt olyan technológiák érthetőek (példálózó jelleggel, nem kizárólagosan), mint: […] információbiztonság, biztonságtechnika." A kiberbiztonság mint fejlesztési terület emiatt az összes releváns kormányzati stratégiából visszaköszön, így a 2020-ban elfogadott Mesterséges Intelligencia Stratégia is kitér erre a szempontra.

Startup-ökoszisztéma a kiberbiztonságban

A forrás tehát kétségtelenül rendelkezésre fog állni ahhoz, hogy az európai kutatás-fejlesztés-innováció a kiberbiztonsági területen fejlődjön. A kérdés az, hogy miként lehet mindezt megtenni. A CB Insight nevű kutatócég 2019-es felmérése alapján ugyanis a kontinentális Európában, tehát az Európai Unió jelenlegi országai között nagyon kevés olyan startup van, amelynek terméke megfelel a globális igényeknek, illetve a piaci potenciálja olyan, hogy ezekkel hosszú távon lehet számolni.[7] A felmérés alapján a legígéretesebb kiberbiztonsági startupok jelen pillanatban az Egyesült Államok területén találhatók, emellett Nagy-Britannia és Izrael a két másik olyan szereplő, akikre érdemes odafigyelni, ahogy azt a 4. ábra is mutatja. Európában egyedül egy svájci bejegyzésű cég, a Trezorit szerepel a listán mint ígéretes startup. A Trezorit egyébként magyarországi alapítású, a termék eredetileg Budapesti Műszaki és Gazdaságtudományi Egyetem hallgatóinak projektjeként indult, de jelen pillanatban ők is az Európai Unió területén kívüli jogi entitásnak számítanak.

[7] CB Insight 2019



4. ábra: 2019 legígéretesebb kiberbiztonsági startupjai
Forrás: CB Insight 2019

A felmérés is mutatja azt az kihívást, hogy a startupnak minősülő piacorientált innováció a kiberbiztonsági szakmában, az Európai Unió területén belül meglehetősen alacsony szinten van, és igen komoly versenyhátránnyal indul a nagy versenytársakhoz képest. Természetesen számos startup létezik, nem is az a probléma, hogy ne lenne meg az innovációs képesség ezeken a területeken, viszont a piacra jutásuk valószínűsége lényegesen alacsonyabb, mint ha ezeket a startupokat az Egyesült Államokban vagy éppen Izraelből indulva jegyeznék be. Meg kell továbbá jegyezni, hogy az ígéretes startupok egy része ettől független európai alapítású, csak a finanszírozás, illetve a piaci környezet miatt elsősorban az Egyesült Államokban indították ezeket útnak, tehát az európai ipar kevésbé fog profitálni ezek sikeréből.

Még aggasztóbb kép, hogyha megnézzük a CB Insight azon elemzését, amely 2014 és 2019 között mutatja be, hogy melyik országokban mekkora beruházások történtek a kiberbiztonsági kutatás-fejlesztés-innovációba. Ebből látszik, hogy a kiberbiztonsági K+F+I-re elköltött összegek túlnyomó többsége, kétharmada az Egyesült Államokban jelent meg, mögötte pedig egy kis ország, Izrael áll, ahol nagyon jól működik a gyakorlatilag az iskolától a piacig tartó kutatás-fejlesztés-innovációs támogatás. Izrael a globális kiberbiztonsági innovációra fordított befektetésekből 6,7%-kal részesül, utánuk következik az Egyesült Királyság 6,5%-os aránnyal, majd Kína jön 5,6%-kal. 14,4%-kal részesül az említetteken kívül minden más ország a világon a beruházásokból, beleérve az Európai Uniót is.

Lehetőségek Kelet-Közép-Európában

Magyarországon, illetve kicsit tágabb értelemben véve a kelet-közép-európai régióban hatalmas innovációs potenciál rejtőzik. Tehetségeket, jó ötleteket a környező országokban, így elsősorban Romániában, Ukrajnában, Lengyelországban, Csehországban, valamint Észtországban is lehet látni. A régió elsőszámú komoly kihívása az, hogy bár a kelet-közép-európai gondolkodásmód nagyon sokban és nagyon jól támogatja a mérnöki gondolkodást, ezek nem konvertálódnak üzleti sikerré. Azt lehet tapasztalni, hogy a nyugati nagyvállalatoknál mérnöki pozícióban számos esetben Kelet-Közép-Európából származó szakembereket alkalmaznak, de a vállalati hierarchiában ritkán jutnak el a régiós szakemberek magasabb, üzleti jellegű pozícióba.

A régióban a tehetséges mérnökök számát tekintve jól állunk. A kérdés csak az, hogy ezeket a tehetségeket hogyan lehet bátorítani. Ennek lehet az egyik alapköve, hogy egy olyan ökoszisztéma épül ki ezekben az országokban, amely már akár középiskolában vagy legkésőbb az egyetemeken segíti a tehetségek fejlesztését, és a mérnöki tudás mellé egy jól meghatározott üzleti, vállalkozásfejlesztési tudást is ad a mérnököknek. Éppen ezért bátorítani kell az iskolai, akár egyetemi szinten történő innovációs képességek fejlesztését. Magyarországon egyébként 2020 szeptembertől indul több egyetemen is olyan innovációs képzés, amely segítheti ezeknek a tehetségeknek a piacra jutását, cégalapítását, illetve segíteni kell azt, hogy a különböző diszciplínákban, különböző tudományterületeken dolgozó szakértők egymással tudjanak dolgozni.[8]

Fontos állami fejlesztéspolitikai lépés lehet, hogy létrejönnek azok az úgynevezett Science Parkok, amelyekben több egyetem együttesen tudja fölépíteni a saját innovációs ökoszisztémáját, beleértve ebbe a kiberbiztonságot is. A Nemzeti Közszolgálati Egyetem például a Semmelweis Egyetem által vezetett Science Park részese, és ezen Science Park fejlesztési, innovációs központjának egyik eleme a kiberbiztonság az orvosi technológiákban, amely potenciálisan piacképes ötleteket tud majd eredményezni.[9]

De természetesen az ökoszisztéma nemcsak az egyetemistáknak segít. Észre kell venni, hogy csakúgy, mint Magyarországon, a környező országokban is számos, úgynevezett Security Operation Center (SOC), azaz biztonsági felügyeleti központ működik, amelyek feladata a globális nagyvállalatok információbiztonsági támogatása. Ezekben számos olyan mérnök dolgozik, akik rálátnak a legfejlettebb, legjobban működő információbiztonsági technológiákra, illetve első kézből tapasztalják meg az aktuális kibertéri problémákat. A startup-ökoszisztéma segíthet abban is, hogy az akár öt-tíz év tapasztalattal rendelkező mérnököknek biztosítson egy olyan közeget, amelyen belül ők a saját ötletüket meg tudják valósítani, és ezt a lehető legjobban a piacra tudják vinni.

További kérdés a finanszírozás rendelkezésre állása. Startupokra rengeteg pénz van, a tőke alapvetően keresi a jó ötleteket. Ez Európában is így van, de nagy aránytalanságokat lehet észrevenni a startup-finanszírozásban. Míg Magyarországon például 1 millió forintot aránylag könnyen lehet szerezni egy startupötletre, ez az összeg

[8] NFKIH 2020
[9] Dobozi 2019

Nyugat-Európában már 10 millió forint, míg az Egyesült Államokban akár 100 millió forintos nagyságrendet is elérheti a bevonható kockázati tőke az izgalmas ötletekhez. Ez a különbség mindenképpen azt eredményezi, hogy az ötleteket inkább az Egyesült Államokban célszerű megvalósítani, nem pedig itt, Kelet-Közép-Európában.

Látható tehát, hogy a régiónkban is vannak kezdeményezések, ezek azonban tőke- és kapcsolatszegényebbek, mint a nyugati és elsősorban az amerikai befektetők kínálatai. Éppen ezért fontos a régiós együttműködés és az, hogy európai szinten is minél jobban megjelenjenek ezek a kelet-közép-európai kezdeményezések. Ezek finanszírozási igénye ugyanis alapvetően alacsonyabb, mint hogyha Nyugaton indítanák el ezeket, viszont éppen ezért szükségesek azok az állami támogatások is, amelyek piacra tudják juttatni a nyugat-európai uniós tagországokban is az itt létrejövő megoldásokat és ötleteket.

Sokat segíthet, ha a kiberbiztonsági jogszabályból egyelőre még hiányzó kutatás-fejlesztés-innovációs területet végre elfogadnák az Európai Unióban. A tervek szerint a Tanács kiberbiztonsági hálózatokat hoz létre, amelyek három szinten épülnének ki. Elsősorban létrejönne valamelyik európai uniós tagországban egy olyan központ, amelynek feladata a kutatás-fejlesztési innovációval kapcsolatos források koordinálása, annak érdekében, hogy a Horizont Európa programban rendelkezésre álló összeget jól költhessék el. Ez az Európai Kiberbiztonsági Ipari Technológiai és Kutatási Központ nevet viseli, és a tanulmány írásának pillanatában tagországi tárgyalás folyik arról, pontosan milyen felhatalmazással működjön. Figyelembe véve, hogy az ENISA-val, az Európai Hálózatbiztonsági Ügynökséggel párhuzamosan kéne ennek működnie, gondoskodni kell arról, hogy ne legyenek olyan átfedések a hatáskörökkel kapcsolatban, amelyek nehezítenék a központ működését. Ennek a központnak a székhelye egyelőre nem ismert, több európai ország is bejelentkezett annak érdekében, hogy a központot vendégül láthassa.

Valószínűsíthető, hogy minden országban létrejön egy nemzeti koordinációs központ, amely felelős lesz azért, hogy az országon belül a forrásokhoz minél többen hozzáférhessenek. Ez pedig a kiberbiztonsági kiválósági központok hálózatán keresztül lesz majd lehetséges. A jelenlegi elképzelések alapján ezek olyan állami kutatás-fejlesztési, innovációs intézmények lesznek, mint például a Nemzeti Közszolgálati Egyetem Kiberbiztonsági Kutatóintézete, amelyek segítik azt, hogy az európai kutatási pénzek el tudjanak jutni a piaci szereplőkhöz, a privát szférához is, és egyben erősítik azt az elképzelést, hogy az egyetemeken és a kutatóintézetekben rendelkezésre álló tudás és a piaci igény találkozhasson. Éppen ezért nagyon fontos, hogy nemzeti szinten még a jogszabály elfogadása és a következő költségvetési időszak megkezdése előtt a kiberbiztonságban érdekelt szereplők egymással együttműködve kialakítsák azt a laza hálózatot, amelyen keresztül az európai kutatási pénzek hozzáférhetővé válnak majd a jövőben.

Összefoglalás

A negyedik ipari forradalom elengedhetetlen előfeltétele a (kiber)biztonságosan működő digitális infrastruktúra létrehozása. Ez azonban nem csupán műszaki feladat: a digitális ökoszisztéma minden szereplőjének, így az államoknak is komoly feladatai és felelősségei vannak a kibertéri fenyegetések kezelésében. Mivel az amerikai és kínai vállalatok jelentős előnyre tettek szert az európai versenytársakkal szemben a modern ipari fejlesztésekben, nem utolsósorban a célzott állami beavatkozásnak köszönhetően, az Európai Unió elemi érdeke olyan környezet létrehozása, amellyel az európai vállalkozások is versenyben tudnak maradni innovatív megoldásaikkal és szolgáltatásaikkal és az európai gazdaságok képesek lehetnek csökkenteni a tengerentúli és ázsiai digitális megoldásoktól való függőségeiket, ezzel pedig az államilag támogatott kibertámadásokkal szembeni kitettségüket is.

Az unió ezt felismerve olyan szabályozások megalkotása mellett döntött, amelyek ösztönzik az okos-infrastruktúrák üzemeltetőit a kiber- és adatvédelem implementálására már a tervezési szakaszban. Magyarország, mint minden EU-s tagország, adaptálta a már létrejött jogszabályokat, és részt vesz az új szabályozások megalkotásában. A már elfogadott joganyag konzervatív módon közelít a negyedik ipari forradalom jelentette kiberbiztonsági kihívásokhoz, azt nem nevesíti, csak közvetve utal arra, hogy a hazai fejlesztők és szolgáltatók sem maradnak ki az uniós tevékenységekből. Figyelembe véve az olyan hazai kormányzati törekvéseket, mint például az okosvárosok létrehozásának szándéka, ez az óvatos megközelítés nem feltétlenül szerencsés, és magában hordozza a kockázatát annak, hogy direkt szabályozási lépések nélkül az újonnan létrejövő okos-infrastruktúrák nem készülnek fel a 2020-as évek kibertérből érkező kihívásaira.

Az előíró szabályozás mellett azonban fontos a támogató szabályokat is megemlíteni, amelyek segítségével az európai kiberbiztonsági innováció olyan eredményeket érhet el, amelyeket a szolgáltatók külön előírás nélkül is célszerűnek tarthatnak bevezetni. A kiberbiztonsági kiválósági központok hálózata olyan keltetője lehet a világszínvonalú ötleteknek, amely érdemi eredményeket érhet el. Ennek az elképzelésnek a pilotolására, kipróbálására az Európai Bizottság 2019-től kezdve négy kiemelt projektet indított el. Ezek a Concordia, a Cyber Security for Europe, az ECHO, illetve a Sparta nevű kezdeményezések, amelyek számos Európai Uniós tagországot egyesítenek és fognak össze, és próbálják kialakítani, hogyan tud majd működni ez a háromszintű felosztás, hogyan valósítható meg az, hogy az európai kutatási pénzek a leghatékonyabban jussanak el az innovációval foglalkozó magán- és közfinanszírozású szereplőkhöz.[10]

A kutatás-fejlesztés-innováció tehát fontos, a lehetőség itt van előttünk, viszont ezzel tudni kell élni, és ehhez a legfontosabb az, hogy a tudatosság meglegyen minden szereplőben. Jelen tanulmány célja az, hogy segítsen felhívni a figyelmet ennek a fontosságára, és minden érintett szereplő figyelemmel követhesse a következő évek fejlesztését, egyben keresse a kapcsolatot azokkal az intézményekkel, amelyek részeivé válnak majd a következő évek információbiztonsági kutatás-fejlesztés-innovációs tevékenységének.

[10] Európai Bizottság 2019

Felhasznált irodalom

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

1414/2013. (VII. 4.) Korm. határozat a Nemzeti Kutatás-fejlesztési és Innovációs Stratégia (2013–2020) elfogadásáról

1640/2014. (XI. 14.) Korm. határozat a Nemzeti Intelligens Szakosodási Stratégia (S3) elfogadásáról és a Kutatási Infrastruktúrák Európai Stratégiai Fóruma Útitervében szereplő kutatási infrastruktúra nagyprojektekben való magyar részvételről

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről

Bányász P. (2016): Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In Csengeri J. – Krajnc Z. szerk.: *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése.* Budapest, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar. 918.

CB Insight (2019): *2019 Cyber Defenders*. CB Insight. Elérhető: www.cbinsights.com/research/report/cyber-defenders-2019/ (a letöltés dátuma: 2020. március 30.)

Digital Single Market (2018): *New Digital Europe Programme brings €9.2 billion investment between 2021–2027.* Elérhető: https://ec.europa.eu/isa2/news/european-commission-has-announced-investment-%E2%82%AC92-billion-align-next-long-term-eubudget-2021_en (a letöltés dátuma: 2020. március 30.)

Dobozi P. (2019): *Bemutatták a Science Park tervezett szakmai tartalmát*. Elérhető: www.uni-nke.hu/hirek/2019/10/24/bemutattak-a-science-park-tervezett-szakmai-tartalmat (a letöltés dátuma: 2020. március 30.)

Európai Bizottság (2018): *EU-finanszírozás a kutatás és az innováció területén (2021–2027).* Elérhető: https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-research-innovation_hu.pdf (a letöltés dátuma: 2020. március 30.)

Európai Bizottság (2019): *Four EU pilot projects launched to prepare the European Cybersecurity Competence Network.* Elérhető: https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network (a letöltés dátuma: 2020. március 30.)

European Council (2020): *Reform of cybersecurity in Europe.* General Secretariat of the Council. Elérhető: www.consilium.europa.eu/en/policies/cyber-security/ (a letöltés dátuma: 2020. március 30.)

EU Tanácsa (2019): *Az EU összefogja és hálózatba szervezi kiberbiztonsági szakértelmét – a Tanács megállapodott a kiberbiztonsági központokkal kapcsolatos álláspontjáról.* Elérhető: www.consilium.europa.eu/hu/press/press-releases/2019/03/13/eu-to-pool-and-network-its-cybersecurity-expertise-council-agrees-its-position-on-cybersecurity-centres/ (a letöltés dátuma: 2020. március 30.)

Fortune (2020): *Cyber security market analysis 2020–2027.* Elérhető: www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165 (a letöltés dátuma: 2020. március 30.)

Graz University of Technology (2018): *Meltdown and Spectre – Vulnerabilities in modern computers leak passwords and sensitive data*. Elérhető: https://meltdownattack.com/ (a letöltés dátuma: 2020. március 30.)

Nai-Fovino, I. – Neisse, R. – ,Lazari, A. – Ruzzante, G. (2018): *European Cybersecurity Centre of Expertise – Cybersecurity Competence Survey*. Luxembourg, Publications Office of the European Union.

NKFIH (2020): *Szeptemberben startol a Hungarian Startup University Program*. Elérhető: https://nkfih.gov.hu/hivatalrol/online-sajto/szeptemberben-startol (a letöltés dátuma: 2020. március 30.)

VÁKÁT OLDAL

2. Kritikus információs infrastruktúrák

VÁKÁT OLDAL

Simon Béla

Kritikus információs infrastruktúrák egyes szabályozási kérdései

Bevezetés

Jelen tanulmány a kritikus infrastruktúrák és a kritikus információs infrastruktúrák üzemeltetői, valamint a rendészeti szervek közti viszony jogi szabályozását vizsgálja. A bűnügyi statisztikai rendszer adataiból nyilvánvalóan levonható a következtetés, hogy a tényállásszerű, büntetendő cselekmények jelentős számban látenciában maradnak a bűnüldöző szervek számára. Nemzetközi gyakorlatok vizsgálatával és összevetésével azokra a kérdésekre keressük a válaszokat, hogy:

- az egyébként pönalizált cselekmények elkövetése esetén az állam büntető hatalmának érvényre juttatása szükséges-e, vagy elegendő a kritikus információs infrastruktúrákat érő jogellenes támadások elhárítása?
- Milyen eszközökkel érheti el az állam, hogy a nem mindig azonos érdekek által vezérelt piaci szereplők megosszák információikat az őket érintő incidensekről?
- Az incidensek tudomásra jutásától mely esetekben indulnak büntetőeljárások?

Korszerű információtechnológiára épülő információs infrastruktúrák nélkül az információs társadalom működésképtelen. De abban az esetben is az, illetve működési zavarokkal küszködhet, ha e rendszereket valamilyen ártó szándékú behatás éri. Ezért amellett, hogy e rendszereket működtetjük, szavatolni kell megbízható működésüket is.[1]

A kritikus infrastruktúrák rugalmas reagálóképességének javítása világszerte az infrastruktúra-szolgáltatók és az állam számára is prioritássá vált. A felmerülő fenyegetések, valamint a kritikus infrastruktúrákkal szembeni szokatlan támadások az elmúlt 15 év során feltárták a hagyományos kockázatértékelés és a kockázatcsökkentési erőfeszítések határait. Néhány veszélyt nem lehet előre jelezni, míg az összes lehetséges kockázat minimális szintre csökkentése nem mindig költséghatékony. Ez a figyelmet az ellenálló képesség fokozásának szükségessége felé irányította annak érdekében, hogy a szolgáltatás folytonosságát potenciálisan befolyásoló események következményeként jelentkező negatív hatásokat minimalizálja.

Az állami szerepvállalás révén – szabályzóin és szervezetein keresztül – egy kritikus infrastruktúrát érintő lehetséges incidenssel összefüggésben tehát intézkedéseket tehetők:

- az incidens előtt,
- az incidens során,
- az incidens lezajlását követően.

[1] Haig Zsolt – Kovács László (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* Budapest, Nemzeti Közszolgálati Egyetem 93.

A büntetőjog eszközrendszere alapvetően követő jellegű, de elhúzódó események esetén az incidensek során is hatékony eszköz lehet, ugyanakkor a jó állam számára a lehetséges veszélyekre történő felkészülés részeként is fontos bevetni a jogkövető magatartás erősítését, az általános és speciális elrettentés[2] funkcióival, amelyeket jelentős részben a rendészeti és bűnüldöző szervek működtetnek.

Az állampolgárok jogosan elvárt igénye, hogy az állami szerepvállalás ne csak a hagyományos offline területeken tartsa fenn a rendet, hanem a kibertérben is, ami az egyes államokat ezen a területen is arra irányítja, hogy együttműködjenek a többi állammal. A nemzetközi kooperáció felé irányultság mellett fontos változás az elmúlt időszakban, hogy eltolódtak az állami szerepvállalás erővonalai és irányai. A különféle szolgáltatások és termékek fejlesztését nem minden esetben a technológia fejlődése teszi lehetővé. Sok esetben nem a piaci verseny motiválja a technológiai kutatásokat, hanem a jogalkotó, szabályozó szervezetek írják elő a célokat, amelyek a technológiai fejlesztéseket meghatározzák.[3] Egyre több olyan szabályozás valósul meg – jellemzően Európából kiindulva – amely az egyén védelmét szolgálja olyan módon, hogy az a vállalkozások profitját csökkenti[4] (például: GDPR, különféle környezetvédelmi szabványok stb).

A hálózatok által átszőtt globális világ sosem volt olyan sebezhető, mint manapság.[5] Ez a sebezhetőség a nyitottságból, a bonyolult technikai rendszerekből, az infokommunikációs rendszerektől való növekvő függésből, illetve az összefonódó és egymással összekapcsolt létfontosságú[6] infrastruktúrákból eredeztethető.[7]

Vajon a jó államnak mennyiben szükséges beavatkoznia jogi normákkal a piaci szereplők (például: kritikus infrastruktúra üzemeltetői) és az ügyfeleik, az egyének közti polgári jogi jogviszonyba? A túlszabályozottság vagy a szabályozatlanság hibájába is eshet a jogalkotó. Előbbi esetén számos hátrány említhető – költséges bürokrácia, a piaci verseny torzulása a piacra lépési küszöbök emelésével (adminisztrációs terhek), improduktív tevékenység –, míg az alulszabályozottság akkor tud negatívan hatni, ha a működés eltér a tervezettől. Ez a kritikus információs infrastruktúrák esetében jellemzően valamilyen incidens következtében valósul meg. Tehát amíg nincs gond, addig

[2] Borbíró Andrea (2009): Prevenció és büntető igazságszolgáltatás In Virág György szerk.*: Kriminológiai tanulmányok 46. kötet.* Budapest, OKRI. 13–37.

[3] Tipikus példája ennek a járművek károsanyag-kibocsátási normáinak fokozatos szigorítása, amelynek a konstruktőrök egyre kevésbé képesek eleget tenni. Ez a politikai igény nemzetközi szinten a gyártókra gyakorol nyomást (bár egyes nézetek szerint a szabályozás éppen a fejlett európai iparágak vezető szerepét kívánja fenntartani).

[4] Bár a költségeiket a vállalkozások jellemzően átterhelik a fogyasztókra, a szabályozások versenyhelyzetet képesek teremteni a piacon, amiből vélhetően a felhasználó profitál.

[5] Haig–Kovács 2012

[6] A nemzetközi terminológia a kritikus infrastruktúra kifejezést használja, míg a hazai jogszabályi terminológiában ugyanez létfontosságú rendszerelemként jelenik meg. Jelen tanulmány szinonimaként kezeli a kifejezéseket.

[7] Bognár Balázs – Bonnyai Tünde – Vámosi Zoltán (2019): *Kritikus infrastruktúrák védelme I.* Budapest, Dialóg Campus Kiadó. 45.

a dereguláció[8] a piaci szereplők számára üdvös, de negatív történések esetén felveti az állam felelősségét.

Ezek a negatív események lehetnek természeti eredetűek, illetve valamilyen emberi tevékenységre visszavezethetők.

Az állam büntető igénye oldaláról szemlélve

Témánk súlypontja az emberi magatartások közül is a szándékosan, csalárd szándékkal vagy súlyos gondatlansággal megvalósuló, kritikus információs infrastruktúrát érő incidensek kezelésén van. Ezen magatartásokat jogszabályaink tiltják. A tilalom megszegőivel szemben az incidensek elszenvedői polgárjogi igényt támaszthatnak, de ennek jogi szabályozása és gyakorlati megvalósulása szintén kívül esik a rendvédelmi és bűnüldöző szervek és jelen tanulmány fókuszán.

A jogellenes magatartások következő lépcsői – a polgári jog eszköztárát követően – a szabálysértések. A csekély súlyú szándékosan vagy gondatlanul elkövetett – tehát az elkövetőnek felróható – és a társadalomra kisebb mértékben veszélyes magatartások között az információs rendszerek[9] elleni jogsértéseket tulajdonképpen két tényállás írja le. A szabálysértésekről szóló 2012. évi II. törvény (Szabs. tv.) 177. § (1) bekezdése a szándékos rongálást ötvenezer forint értéket nem meghaladó esetben büntetni rendeli. Itt azonban – mivel a tényállás megállapításához állagsérelem szükséges – számos elkövetési forma nem jogsértő. Ugyanezen törvény 177/A. §-a közérdekű üzem működésének megzavarása esetén azonban csak az elektronikus hírközlő hálózatok működésének megzavarását pönalizálja. Azon támadások, amelyek nem hírközlő hálózat része ellen irányulnak, hanem valamilyen más információs rendszer ellen, azok a szabálysértési törvény által szankcionálandók. A jogalkalmazók számára azonban nem nyilvánvaló, hogy az elektronikus hírközlő hálózat működésének megzavarása mely esetekben nem valósítja meg a Büntető törvénykönyv (Btk.) 423. § (2) bekezdésébe ütköző Információs rendszer vagy adat megsértése bűntettét, hiszen a Szabs. tv. 2. § (4) bekezdése értelmében nem állapítható meg szabálysértés, ha a tevékenység vagy a mulasztás bűncselekményt valósít meg.

A társadalom magasabb szintű rosszallását kiváltó magatartások lajstromba vételét tehát a Btk.-ban végezték el. Témánk szempontjából a kritikus információs infrastruktúrák elleni informatikai jellegű támadások, tényállásszerű magatartások az alábbi bűncselekményekben ölthetnek testet.[10]

[8] Bővebben: Biedermann Zsuzsánna (2012): Az amerikai pénzügyi szabályozás története. *Pénzügyi Szemle,* 57. évf. 3. sz. 337–354.

[9] Információs rendszer alatt a Btk. 459.§ (1) bekezdés 15. pontja szerinti fogalmat értjük: az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége.

[10] Természetesen e tényállásokkal párhuzamosan számos más, kibertérhez kapcsolódó bűncselekmény is megvalósulhat, de ezek nem a szűken vett kritikus információs infrastruktúrák elleni támadások (tiltott adatszerzés, személyes adattal visszaélés, a nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény – bár ez utóbbi bűncselekmény elkövetését még soha sem regisztrálták).

– *314. § Terrorcselekmény*

2013 és 2020 júniusa között Magyarországon a Belügyminisztérium Bűnügyi Statisztikai Rendszerében összesen 23 terrorcselekményt regisztráltak, de a statisztikai rendszerből nem olvasható ki, hogy mely esetekben volt érintve a kibertér vagy az információs infrastruktúra, az azonban kijelenthető, hogy e cselekmények jellemzően nagyobb sajtóvisszhangot kiváltó bűnesetek, és a médiából megismerhető eseményekkel összefüggésben elenyésző számban érintett ezeknél a kibertér vagy a kritikus infrastruktúra.

– *323. § Közérdekű üzem működésének megzavarása*

1. táblázat: Közérdekű üzem működésének megzavarásának esetszámai 2013 és 2020 között

	2013	2014	2015	2016	2017	2018	2019	2020.1. félév
Esetszámok	73	66	34	40	38	51	30	18

Forrás: a szerző szerkesztése

A kibertér vagy információs infrastruktúra érintettsége egy jelentősen alacsonyabb esetszámot mutatna, azonban az elérhető statisztikaiadat-közlés ez esetben sem alkalmas ilyen szűrők mentén külön válogatni. Megállapításomat arra alapozom, hogy a közérdekű üzemeknek csak egy kis része információs infrastruktúra.

– *423. § Információs rendszer vagy adat megsértése*

2. táblázat: Információs rendszer vagy adat megsértésének esetszámai 2013 és 2020 között

	2013	2014	2015	2016	2017	2018	2019	2020.1. félév
Esetszámok	823	565	520	702	586	564	587	261

Forrás: a szerző szerkesztése

A jelölt regisztrált bűncselekmények esetszámában a kritikus információs infrastruktúrák elleni támadások nem különíthetők el.

– *424. § Információs rendszer védelmét biztosító technikai intézkedés kijátszása*

3. táblázat: Információs rendszer védelmét biztosító technikai intézkedés kijátszásának esetszámai 2013 és 2020 között

2013	2014	2015	2016	2017	2018	2019	2020.1. félév
580	31	15	44	8	9	38	8

Forrás: a szerző szerkesztése

Ezen tényállás csak a 423. §-ban rögzített információs rendszer vagy adat megsértése bűncselekmény előkészületi cselekménye, és mint ilyen még nem éri el azt a szintet, hogy egy kritikus információs infrastruktúra üzemeltetője azt incidensként realizálja.

Ezek tehát azok a mutatók, amelyek a bűnüldöző szervek tudomására jutott informatikai incidenseket is eredményezhető cselekményeket mutatják, de ezeknek csak egy tört része az, amely kritikus információs infrastruktúrákhoz köthető.

Teljesen pontos képet akkor kapnánk, ha minden információs rendszer elleni támadás megjelenne a bűnügyi statisztikában. Ezt számos tényező teszi lehetetlenné:

– bár a cselekmény hivatalból üldözendő, de a nyomozó hatóságoknak nincs lehetőségük minden bűncselekmény detektálására;
– nem volna észszerű és költséghatékony döntés minden információs rendszer üzemeltetőjétől (beleértve a háztartásokat), hogy információs rendszerét ért spam vagy vírustámadási kísérlet esetén minden egyes esetben feljelentéssel éljen,
– a nyomozó hatóságoknak nem áll rendelkezésükre minden egyes ilyen jellegű cselekmény nyomozásához szükséges emberi és technikai erőforrás.

Az üzemeltetői és a bűnüldözői oldal is ellenérdekelt tehát az abszolút igazságszolgáltatással szemben.[11]

A tények oldaláról szemlélve

Az érem másik oldala a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézethez (NKI) tett incidensekről szóló bejelentések száma. Az elektronikus információs rendszerek[12] üzemeltetőinek – így azoknak is, akik lényegében kritikus információs infrastruktúrák – kötelezettségük van arra, hogy az incidenseket bejelentsék [Ibtv. 13. § (3) szerint] a megfelelő eseménykezelő központ felé. Ez a kritikus infrastruktúrák esetében az Nemzetbiztonsági Szakszolgálaton belül működő Nemzeti Kibervédelmi Intézet.

A 2019-es évben az NKI-hez érkezett nemzeti létfontosságú rendszerelemek üzemeltetői, így az alapvető szolgáltatást nyújtó szereplők által tett bejelentések az összes bejelentés 3,78%-át tették ki. Azon bejelentések aránya, amelyek hátterében vélelmezhetően[13] bűncselekmény áll, ezen bejelentések 20%-a.

Joggal merül fel a kérdés, hogy mit láthatnak mindebből a bűnüldöző szervek. Saját felderítésük/észlelésük ezen a téren – éppen az elkövetés helye: a kibertér természeténél fogva – tulajdonképpen nem lehetséges. Így a lehetséges tudomásrajutási formák

[11] Azaz semmilyen bűncselekmény nem maradhat felderítetlen és megtorlás nélküli.

[12] Elektronikus információs rendszer fogalma az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) értelmében tágabb, mint a Btk. meghatározása (az adatokat is magában tartalmazza):
a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;
b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi;
c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

[13] A Nemzeti Kibervédelmi Intézet munkatársainak becslése, amely csak az esetekkel összefüggő büntetőeljárások elrendelésével lenne igazolható vagy cáfolható.

a sértett kritikusinfrastruktúra-üzemeltetők vagy az NKI feljelentései. Ilyen feljelentés – jelentőségénél fogva – tipikusan a Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztályára kellene hogy kerüljön, de ilyen ügyek miatti évente mindössze néhány alkalommal rendelnek el eljárást.

A Nemzeti Kibervédelmi Intézet 2020 első negyedévében vezette be eljárásrendjébe, hogy a közepes és az annál magasabb kockázati besorolású incidensek esetében felhívják a bejelentők figyelmét a rendőrségi feljelentés lehetőségére.

A résztvevők motivációját szemlélve

Azokra a lényeges attitűdbéli különbségekre kívánom felhívni a figyelmet a következőben, amelyek az egyes szereplőknél megjelennek.

A kritikus információs infrastruktúrát üzemeltető piaci szereplők érdeke a folyamatos üzemmenet, a szolgáltatásaik minél magasabb szintű nyújtása, az ügyfél-elégedettség, de legfőbb céljuk a profit.[14] Minden más részleges irány – akár a társadalmi szerepvállalás, akár a jogszabályok betartása, akár a piaci részesedés növelése – mindig ezt a célt kell szolgálja, hiszen rövid vagy hosszú távon, de a piaci szereplők – mint vállalkozások[15] – a profit érdekében léteznek.

Egy profitorientált vállalkozásnak nem áll elsődlegesen érdekében büntetőeljárás kezdeményezése, hisz a büntetőeljárás információkkal történő kiszolgálása (feljelentéstétel, tanúvallomás, adatok kigyűjtése, továbbítása stb.) improduktív tevékenység profit oldalról. Ha az okozott kár megtérülésére nincs reális lehetőség (és a kiberbűncselekmények jelentős része ilyen), akkor ez különösen igaz. Sőt abban az esetben, ha a piaci szereplő a további károsodás lehetőségét megszünteti, akkor alapvetően érdekében áll, hogy ezt titokban tartsa. Egyrészt reputációs veszteséget okoz a sérelem széles körű ismertté válása, másrészt a versenytársak gyengítését eredményezi, ha őket is sújtja ugyanazon modus operandi.

Tény, hogy a piaci szereplők esetében a profitorientáltsággal szemben számos tényező, illetve jogintézmény működik. Ilyenek a vállalati, társadalmi felelősségvállalás (Corporate social responsibility, röviden CSR), illetve a vállalati magatartási kódex intézményei (Corporate code of conduct, röviden CCC),[16] amelyek a morális értékeket hivatottak előtérbe helyezni. Tény, hogy egy multinacionális vállalat egy eltitkolt incidens napvilágra kerülése esetén jelentős reputációs veszteséget szenvedne el, de a KKV-szektort a negatív sajtóvisszhang kevésbé fenyegeti. A kisebb információs infrastruktúrát üzemeltető piaci szereplők kapcsolata a támadó vagy jogsértő személyekkel, szervezetekkel alapvetően semleges.

[14] Fogyasztói igények kielégítésén keresztül.
[15] Közgazdasági értelemben vállalatok.
[16] Ennek is van azonban számos kritikája. Bővebben: www.britannica.com/topic/corporate-code-of-conduct#ref1181142 (a letöltés dátuma: 2020. április 22.)

A létfontosságú rendszerelemet működtető állami szervek/szervezetek esetében a profitorientált működés a legtöbb esetben nem érvényesül.[17] Az állami és piaci szereplőknél azonban fontos megjegyezni, hogy érdekükben áll a kritikus infrastruktúraként történő kijelölésük titokban maradása. A kritikus infrastruktúrákat felügyelő – és jellemzően a végrehajtó hatalom részét képező – intézmények elsődleges célja azon jogi normák betartása és betartatása, amelyeket a jogalkotó és a végrehajtó hatalmi ág felsőbb szervei részükre meghatároznak.

Tény, hogy a hazai hatóságok felismerték, hogy a csupán büntető jellegű fellépés nem célravezető, és az állami felügyelet alatt tartás sokkal inkább a jóhiszemű jogalkalmazást próbálja segíteni az ellenőrzésekkel, a folyamatos kapcsolattartással, a közreműködő és alapvetően támogató hatósági fellépéssel, oktatások, konferenciák szervezésével, incidensek bejelentésének ösztönzésével. A szankcionálás vagy azzal fenyegetés, valamint a partnerként történő támogatás optimális arányának kialakítása a hatóságok számára komoly kihívást jelent. Előbbiek súlyozása a jogszabály címzettjeinek elzárkózásához, titkolózásához vezet, míg az utóbbi túlsúlyba kerülése – figyelemmel a honi jogkövetési kultúrára – a jogszabály és a hatóságok súlytalanságához, devalválódásához vezethet. Minden bizonnyal a lehetséges szankciók skálázása és következetes érvényre juttatása a jogszabály címzettjeit racionális döntésként jogkövetésre kényszerítenék.

A nyomozó hatósági és ügyészi szervek számára az egyes fejlett jogrendszerekben eltérő mértékben, de mindenhol cél a megbomlott jogrend helyreállítása. Az egyes országokban két fontos elv feszül egymásnak: az abszolút igazságszolgáltatás, valamint a felesleges és drága eljárások elkerülése. Mindkettő társadalmi igényekre vezethető vissza: a bűnös kapja meg méltó büntetését, de a bűnüldözés, vádképviselet, igazságszolgáltatás ne legyen költségesebb, mint a megbomlott jogrendhez kapcsolódó káresemény maga. Az abszolút igazságszolgáltatás lehetetlen: mérhetetlenül költséges és az erre fordított költségek határhaszna[18] egy idő után exponenciálisan csökken, majd negatív tartományba kerül. A kérdés csupán az, hogy a jogi normák és a valóság milyen jogsértéseket kénytelenek büntetlenül hagyni.

Van olyan jogrendszer, ahol a közvádra üldözendő cselekmények széles körét pönalizálják és az eljárások hivatalból történő megindítása széles körben érvényesül. Az állampolgárok a jogi normák alapján elvárhatják, hogy minden bejelentett jogsértést a hatóságok az erőforrásaikat nem kímélve felderítsenek, az ügyészség pedig vádat emeljen. A skála másik végén olyan jogi berendezkedést találunk, ahol a jogalkotó kevésbé széles körben állapítja meg a hivatalból üldözendő cselekmények körét, és deklarálja az eljárásökonómiai aspektust, azaz nem fog bagatell ügyekben nyomozást folytatni, és kinyilvánítja, hogy nem szükséges minden erőforrást felhasználni egy kisebb súlyú jogsértésnél.

[17] Ebben az értelemben az állami tulajdonban lévő, de nyereség szerzésére irányuló gazdasági tevékenységet elsődlegesen folytató szereplőket piaci szereplők körébe vonjuk.

[18] Ha Gossen törvényeit össztársadalmi szinten vizsgáljuk, és a hasznosságként a megbomló jogrend helyreállítását értjük.

Az igazságszolgáltatás költséghatékonyságának javítására számos jogintézmény kialakítása valósult meg: az egyszerűsített eljárás, a mediáció, az egyezség. Az is tény, hogy bizonyos súlyosságú vagy bizonyos típusú jogsértő cselekmények deklarált negligálásával a bűnüldöző szerveknek ezen jogsértések drasztikus emelkedésével kellene szembesülniük.

Vajon mi a helyes megoldás? Ha a bűnüldöző szervek és más hatóságok a kibertérben elkövetett jogsértések egy bizonyos körével szemben nem lépnek fel (például hacktivista mozgalom által szervezett DDoS-támadásban történő résztvevővel szemben, aki azt szinte alkalmatlan eszközzel valósítja meg), és ezáltal a további jogsértő magatartások számának emelkedését okozzák. A hatóságok ilyen jellegű viszonyulása azt is eredményezheti, hogy a potenciális sértettek több védelmi intézkedést tesznek a sértetté válásuk megelőzésére. Az állampolgárok és a vállalkozások is több racionális döntést hoznak. Ha az állam gondoskodik javaik/értékeik megóvásáról, akkor erre nem fognak erőforrásokat allokálni, de ha az állami védőháló nem biztosítja a védelmet, akkor szükségesnek látják a fejlesztéseket.[19]

Az nyilvánvaló, hogy egy jogállam sem képes minden detektált tényállásszerű kiberbűncselekményre büntetőeljárást indítani. Ez több okra vezethető vissza:

– sok esetben teljesen értelmetlen eljárást kezdeményezni, mert technikai oldalról látható, hogy nem lehetséges azt eredményesen lefolytatni (például Tor-hálózat kijáratából érkező támadás forrása jellemzően nem deríthető fel, vagy a vírus írójának felkutatása a legtöbb esetben nem lehetséges),
– bagatell súlyú bűncselekmény nyomozása aránytalanul nagy erőforrásokat igényelne (információs rendszerek elleni gyenge támadási kísérlet),
– az eljárás lefolytatása túlságosan nagy erőforrásokat kötne le a nyomozó hatóság részéről (például ha jelzés érkezik egy külföldi hatóságtól/szervezettől, hogy többezer különféle magyarországi IP-címről jelentkeztek be gyermekek szexuális kizsákmányolását tartalmazó képek, videók megosztását is végrehajtó szerverre),
– bizonyos esetekben a törvény aránytalan szigora és a társadalomra való veszélyesség nem koherens (például a legtöbb p2p fájlmegosztó szoftver felhasználója a régi Btk. értelmében a tartalom visszaosztásakor megvalósított a szerzői vagy ahhoz kapcsolódó jogok megsértése bűncselekményt).

Angolszász jogrendszerek megoldásai

Az egyes jogi megoldások közti lényeges különbségeket az alábbi sarokpontok mentén érdemes vizsgálni:

– milyen rendelkezések alapján kerül be egy piaci vagy állami szereplő a kritikus infrastruktúrát üzemeltetők közé? (Itt természetesen a piaci szereplők részvétele hangsúlyosabb a korábban vázolt érdekellentétek okán.)

[19] Emellett a drasztikus rendészeti, bűnüldözői aktivitás ebben a szférában könnyen lehet kontraproduktív – például egy rendkívül gyenge védelmet alkalmazó hatósági vagy kormányzati honlapot deface-elő elkövető elrettentő büntetése okot adhat az elkövető szimpatizánsainak a hasonlóan gyenge védelemmel rendelkező oldalak kompromittálására.

– Az incidensekről történő adatközlés milyen kötelező erejű a címzettek irányába?
– Az állam által üzemeltetett incidensbejelentő rendszerbe érkező incidenseket milyen módon csatornázzák a bűnüldöző szervek felé?
– A bűnüldöző szervek mi alapján döntik el, hogy egyes incidensekkel kapcsolatban bűnügyi nyomozást kezdenek, míg más incidenseknél nem?

Jelen tanulmány kereteit meghaladja egy-egy jogi berendezkedés teljes áttekintése, ezért csak példálózó jelleggel emelünk ki egy példát, amely összehasonlításra érdemes a magyar szabályozással.

A kritikus infrastruktúrák nyilvántartása az Amerikai Egyesült Államokban

A *kritikus infrastruktúra* kifejezés jelentése az USA-ban sokat változott. A Világkereskedelmi Központ (1993) és az Oklahoma City épületének (1995) robbantása, majd 2001. 09. 11. után a korábbi közművekre, utakra és kikötőkre korlátozott jelentése sokkal jobban kiszélesedett.

Ez manapság egy általános kifejezés: az ember alkotta olyan hálózatok és rendszerek összességét jelenti, amelyek a lakosság számára szükséges termékeket és szolgáltatásokat biztosítanak. Általánosságban elmondható, hogy kritikus infrastruktúra az összes olyan rendszer, amely nélkülözhetetlen a társadalom minden szintjének zökkenőmentes működéséhez. Ez a rendszer, amely létfontosságú egy közösség vagy a nemzet számára, ha megszakad, sérül, megsemmisül vagy valamilyen módon nem képes működni, gyengítő hatással lehet a biztonságra, a gazdaságra vagy a nemzeti egészségre, a polgárok és a vállalkozások biztonságára vagy jólétére.[20]

A kritikus infrastruktúrát 3 szintre osztják az Egyesült Államokban:

1. Helyi kritikus infrastruktúra, amelyet speciálisan a helyi viszonyokat ismerő helyi tisztviselők ilyenként jelölnek ki (például egy víztisztító berendezés).
2. Szövetségi kritikus infrastruktúra, amelyet a Belbiztonsági Minisztérium (Department of Homeland Security DHS) tisztviselői a Nemzeti Vagyonbázis regiszterében rögzítenek. A listán országosan hozzávetőlegesen 77 000 nemzeti eszköz található, amelyek kb. 5% -át (csak 1 700) jelölték kritikusnak. Felsorolásuk néha ellentmondásos, mivel a szövetségi, az állami és az önkormányzati tisztviselők, valamint a magánszektor tulajdonosai gyakran nem értenek egyet abban, mit kell felvenni a regiszterbe.
3. Magánkézben lévő kritikus infrastruktúrák, amelyek az Egyesült Államok kritikus infrastruktúrájának 80% -át adják. Mivel sok Nemzeti Vagyonbázisba tartozó eszköz magánszervezetek tulajdonában van, a magánszektort be kell vonni a védelem

[20] Korábbi terminológiában kulcsfontosságú erőforrás (key resources) elnevezést is használták, de jelenleg már a kritikus infrastruktúra kifejezéssel felcserélhető szinonim fogalomként háttérbe szorult.

tervezésébe. Számos dokumentum, köztük a nemzeti stratégia,[21] a belbiztonsági törvény[22] és a HSPD-7,[23] kiemeli az összes partner bevonásának fontosságát a védelmi erőfeszítések koordinálásában. Ezek a dokumentumok világossá teszik, hogy az infrastruktúra védelmét a kormány és a közszféra önállóan nem tudja megvalósítani. Ehelyett együtt kell működniük a magánszektor tulajdonosaival és üzemeltetőivel. A kormány sokféle módon segítheti a kritikus infrastruktúra tulajdonosát és üzemeltetőjét, például:

- időben történő és pontos információk szolgáltatása a lehetséges veszélyekről;
- a tulajdonosok bevonása az eszközök védelmét szolgáló kezdeményezések és politikák kidolgozásába;
- a vállalati vezetők támogatása a biztonsági intézkedések kidolgozásában és végrehajtásában.

4. Ösztönzés nyújtása azon társaságok számára, amelyek vezetői a helyes biztonsági gyakorlatok alkalmazása mellett döntenek. Utóbbi arra utal, hogy az önkéntes vállalás előmozdítását is segíteni szükséges a kötelezés mellett.

A kritikusinfrastruktúra-eszközök mellett az amerikai terminológia használja a kritikus infrastruktúrára vonatkozó információ (Critical Infrastructure Information – CII) fogalmát is, amely alatt olyan adatokat vagy információkat ért, amelyek kritikus infrastruktúrára vonatkoznak és érzékenynek tekinthetők, de nem mindig minősülnek titkosnak. A CII-ra példa a napi működéssel kapcsolatos ismeretek vagy a sebezhetőség és a védelmi tervek leírása. A CII[24] magában foglalhatja az infrastruktúra által generált információkat is, például a betegek egészségügyi nyilvántartásait vagy egy személy banki és pénzügyi nyilvántartásait. A CII bármilyen bizonyíték lehet az infrastruktúrához kapcsolódó jövőbeni fejlesztési tervekkel kapcsolatban, vagy olyan információ, amely leírja annak elhelyezkedésével kapcsolatos releváns geológiai vagy meteorológiai információkat, amelyek rámutathatnak az adott létesítmény potenciális sebezhetőségére (például földrengésre hajlamos terület). A CII általában bármilyen információra utal, amelyet az elkövető felhasználhat az infrastruktúrának vagy annak működési képességének megsemmisítésére, illetve más módon történő károsítására.

A CII védelme fontosságát az USA-ban először a 2002. évi CII-törvény azonosította, amelyet a kongresszus fogadott el. Kiemelték, hogy amikor egy magánszervezet információcserét folytatott a kormányzati tisztviselőkkel, akkor ez az információ nyilvános nyilvántartásokban elérhetővé vált, és a nyilvánosság számára a nyilvánosságra hozatalról

[21] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* Forrás: www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf (A letöltés dátuma: 2020.03.19.)

[22] *Homeland Security Key DHS Laws* Forrás: www.dhs.gov/key-dhs-laws (A letöltés dátuma: 2020.03.19.)

[23] 7-es számú elnöki irányelv*: Homeland Security Presidential Directive 7: Critical infrastructure identification, prioritization, and protection* Forrás: www.cisa.gov/homeland-security-presidential-directive-7 (A letöltés dátuma: 2020.03.18.)

[24] Az olvasó találkozhat a CII rövidítéssel mint Critical Information Infrastructure – de itt nem azt a formáját használjuk.

szóló törvények útján hozzáférhető lett. Sok vállalat nem akarta nyilvánosságra hozni ezt az információt, ezért vonakodtak együtt dolgozni a kormányzati ügynökségekkel és a tisztviselőkkel. Annak érdekében, hogy megvédjék ezt az információt, és ösztönözzék a további együttműködést, a kongresszus új információkategóriát hozott létre, amelyet CII-nek neveztek el. A törvény szerint minden olyan szövetségi tisztviselő, aki tudatosan nyilvánosságra hoz bármilyen CII-t illetéktelen személy számára, büntetendő cselekményt valósít meg. Foglalkoztatási jogviszonyuk megszüntethető, és akár egy év börtönbüntetéssel és pénzbírsággal sújthatók. Az információ más állami vagy helyi tisztviselők számára is kiadható, de csak ha a kritikus infrastruktúrák védelme céljából használják fel. A törvény elfogadta annak biztosítását, hogy csak képzett és felhatalmazott személyek férjenek hozzá, akiknek ismerniük kell az információt, és csak belbiztonsági célokra használhatják fel.[25]

A 2000-es évek során számos rendelkezés született az Egyesült Államokban a kritikus infrastruktúrákkal összefüggésben, de vizsgálatunk szempontjából lényeges, hogy 2010-ben a belbiztonsági miniszter elkészítette a stratégiai nemzeti kockázatértékelést (Secretary of Homeland Security wrote the Strategic National Risk Assessment – SNRA) amely az alábbi fogalmakat használja az információs infrastruktúrák elleni támadásokra:

– adatok elleni kibertámadás: olyan kibertámadás, amely súlyosan veszélyezteti az adatok (a számítógépes rendszerben található információk) integritását vagy elérhetőségét, vagy az adatfeldolgozási folyamatokat, legalább 1 milliárd USD gazdasági veszteséget eredményezve.
– Kibertámadás a fizikai infrastruktúrák ellen: olyan esemény, amelyben a kibertámadást vektorként használják a számítógépen túli hatások elérésére (azaz kinetikai vagy egyéb hatásokra), amelyek halálos kimenetelűek vagy legalább 100 millió USD vagy nagyobb gazdasági veszteséget eredményeznek.[26]

Ezek a meghatározások azért fontosak, mert mutatják, hogy a szövetségi szintű intézmények csak egy meglehetősen nagy hatású támadás esetén aktivizálódnak.

Az Egyesült Államokban a terrortámadások által indított hatékony lépések a későbbi kormányzati ciklusokban is kiemelt szerepet kaptak. Az Obama-adminisztráció időszakában számos intézkedés történt az egyes piaci szereplők közti és az állami szereplőkkel történő információcsere előmozdítása érdekében a kritikus infrastruktúrák kibervédelme okán,[27] amelyekben – szabványok kidolgozásával, a tudományos élet szereplőinek bevonásával – a belbiztonsági titkár, a főügyész, az amerikai nemzeti hírszerzés igazgatója (Office of the Director of National Intelligence), a polgári jogokért és az állampolgári jogokért felelős tisztviselők és számos további aktor együttműködését írták elő.

[25] Pesch-Cronin, Kelley – Marion, Nancy (2017): *Critical Infrastructure Protection*. CRC Press. 8.
[26] *Strategic National Risk Assesment.* Elérhető: www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf (A letöltés dátuma: 2020. 03. 19.)
[27] *Executive Order 13636.* Elérhető: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (A letöltés dátuma: 2020. 03. 20.)

A 2015-ben kiadott 1369. számú végrehajtási rendelet célja a kiberbiztonsággal összefüggő információ áramlásának segítése, és ennek felelőseként a Belbiztonsági Minisztériumot jelölte meg. Létrehozták az információmegosztó és -elemző szervezeteket (Information Sharing and Analysis Organizations ISAOs). A rendeletben Obama a Nemzeti Kiberbiztonsági és Kommunikációs Integrációs Központot (National Cybersecurity and Communications Integration Center NCCIC) jelölte meg a program felelősének a Belbiztonsági Minisztériumon belül. Létrehozták az ISAO szabványügyi szervezetet is, amely együttműködik a kritikus infrastruktúrák összes érdekeltjével az ISAO létrehozására és működtetésére vonatkozó önkéntes szabványok és iránymutatások kidolgozásában.

Az ISAO egy nem kormányzati szervezet, amely tehát 2015. október 1-jén jött létre, és amelyet a San Antonio Texas-i Egyetem (University of Texas at San Antonio UTSA) vezet a logisztikaimenedzsment-intézet (LMI)[28] támogatásával. Küldetésük, hogy javítsák az USA kiberbiztonsági képességét azáltal, hogy meghatározzák a kiberbiztonsági kockázatokkal, eseményekkel és a bevált gyakorlatokkal kapcsolatos fenntartható és hatékony információmegosztás és -elemzés szabványait, irányelveit.

Ebből a szervezeti és feladatmegosztásból érdekes kiemelni tehát a piaci szereplők és a felsőoktatás intézményesített együttműködését, valamint az LMI bevonásának okait, hisz az LMI egy küldetésorientált tanácsadó cég, több mint 50 éves közszolgálati gyakorlattal, amely során nyílt szabványok kidolgozásában, közösségek bevonásában és a versenytársak közötti bizalom kiépítésében szerzett tapasztalatokat. Látható, hogy az USA döntéshozói is olyan szereplőket vontak be a feladatokba, amelyek képesek lehetnek a versenytársakat egy asztalhoz ültetni és együttműködésre bírni a kötelező, előíró szabályrendszerek helyett/mellett.

A bűnüldöző szervek az USA kritikus infrastruktúra védelmét szolgáló intézkedéseiben számos helyen megjelennek. Már a 2003-as 7-es számú nemzetbiztonsági elnöki irányelv is rögzítette: „Az Igazságügyi Minisztérium, beleértve a Szövetségi Nyomozó Irodát, csökkenteni fogja a hazai terrorista fenyegetéseket, valamint kivizsgálja és büntetőeljárások alá vonja a kritikus infrastruktúra és a kulcsfontosságú erőforrások elleni terrorista támadásokat, szabotázsokat vagy zavarokat, azok szabotázsát vagy megszakítását. A főügyésznek és a Belbiztonsági Minisztériumnak ki kell használnia törvényes felhatalmazását és az ehhez kapcsolódó mechanizmusokat kell alkalmaznia az együttműködésre és a koordinációra, ideértve, de nem kizárólag az elnöki irányelv által létrehozott mechanizmusokat."[29]

Az ISAO (Information Sharing and Analysis Organization Standards Organization) 2016-ban kidolgozott egy programot az állami és piaci szereplők együttműködésére vonatkozóan. A dokumentum a súlyponti intézkedéseket természetesen a megelőzésre

[28] Bővebben: www.lmi.org/about-lmi (A letöltés dátuma: 2020. 03. 19.)

[29] *Homeland Security Presidential Directive 7: Critical infrastructure identification, prioritization, and protection.* Elérhető: www.cisa.gov/homeland-security-presidential-directive-7 (A letöltés dátuma: 2020. 03. 18.)

és a felkészülésre helyezi, de témánk szempontjából a rendészeti szervekkel való együttműködést és a bűnüldözést segítő intézkedéseket emeljük ki.
Az ajánlás idevonatkozó elemei:

- szükséges építeni a belső biztonsági szövetség tanácsa (Domestic Security Alliance Council – DSAC)[30] tevékenységére.
- Működtetni kell a fúziós központok nemzeti hálózatát, amelynek tagjai általában államok vagy nagyobb városi területek szintjén létrehozott információk elemzésére, értékelésére, megosztására szolgáló szervezeti egységek, amelyeket állami vagy helyi hatóságok működtetnek, gyakran az FBI támogatásával. Összevonják a résztvevő ügynökségek felderítési eredményeit, hogy átfogóbb fenyegetettségi térképet hozzanak létre helyi és nemzeti szinten. Integrálják az új adatokat a meglévő információkba, értékelik azokat, hogy meghatározzák értéküket, elemezik azokat a kapcsolatok és a trendek szempontjából, és eredményeiket terjesztik az illetékes ügynökségeknek.

Szintén Észak-Amerikából származnak azok a tudományos eredmények, amikor egy kanadai kutatócsoport górcső alá vette a kritikus infrastruktúrák üzemeltetőinek attitűdjét a felügyeleti szervekkel való kapcsolatukra vonatkozóan. Vizsgálták a tudásközösség-koncepció befolyását, amely ösztönzi az információmegosztó rendszerek létrehozását, amelyek célja a szervezeti tanulás, a koordináció és az alkalmazkodóképesség elősegítése alacsony valószínűségű és súlyos következményekkel járó események során. Nem sikerült igazolni, hogy az információcserében részt vevő üzemeltetők sikeresnek ítélték a kapcsolatot. Míg a lefolytatott interjúk résztvevői szinte egyhangúak voltak az információmegosztás támogatásában, tehát fontos mechanizmusoknak nevezték azokat a bizalom építéséhez és a kockázatkezelés közös megközelítésének biztosításához, addig gyakran nem tudták megfogalmazni ezen eszközök konkrét előnyeit. Gyakrabban beszéltek arról, hogy megnyugodtak a közösség részévé válva és a kulcsfontosságú szereplők megismerése révén, és beszélgettek a tájékoztatók értékéről, még akkor is, ha azok általános jellegűek voltak.[31]

Európa és hazánk

A kritikus infrastruktúra védelme a mai kor kihívása, amely a globális terrorizmus terjedésével került a figyelem fókuszába világszerte. A védelem különösen fontos ma, az úgynevezett negyedik generációs vagy aszimmetrikus hadviselés korában, amikor információs hadviselési eszközökkel szinte bármely csoport tudja érvényesíteni az érdekeit, nála jóval nagyobb ellenfelével – tipikusan nemzetállamokkal – szemben. Ezen támadások

[30] A DSAC-program az USA GDP-jének több mint 50%-át adó stratégiai vállalatok és az FBI közti információáramlást segítő belbiztonsági szervezet – bővebben: www.dsac.gov/about (A letöltés dátuma: 2020. 03. 18.)

[31] Quigley, Kevin – Bisset, Ben – Mills, Bryon (2017): *Too Critical to Fail: How Canada Manages Threats to Critical Infrastructure.* Montreal, MQUP. 18.

fő célpontjai lehetnek a kritikus infrastruktúrák, különösen a kritikus információs infrastruktúrák. Kritikus infrastruktúrák segítségével tartja nyilván állampolgárai adatait az állam, ezek igénybevételével működik a közigazgatás (nem csak az e-közigazgatás), és ezek segítségével nyújt az állam (nem csak e-kormányzati) szolgáltatásokat. Ezek védelme tehát jórészt állami feladat, a védelem megszervezése – például követelmények támasztása – pedig kifejezetten az. Már csak azért is, mivel az állam maga is ezekre az infrastruktúrákra támaszkodik. Egy ilyen kritikusinfrastruktúra-elem bármilyen okból történő egyidejű kiesése gyakorlatilag káoszba, anarchiába tudja sodorni az adott nemzetállamot. Ezért a feladatok pontos végrehajtására, a védelem folyamatos fenntartására kell az államnak koncentrálnia.[32]

Az európai közösség számos eszközt és módszertant fejlesztett ki annak érdekében, hogy felmérje a technológiai rendszerek teljesítményét, figyelembe véve azok ágazatok közötti és határokon átnyúló összefüggéseit, és számszerűsítse a kritikus infrastruktúrák megzavarásának társadalmi hatását ezeken a területeken. Az egyik ilyen fontos fejlesztés a földrajzi kockázatok és ellenállóképesség felmérési platformja (Geospatial Risk and Resilience Assessment Platform – GRRASP), amely összekapcsolja a térinformatikai technológiákat és az informatikai eszközöket a kritikus infrastruktúrák elemzésére és szimulálására egy globális, weborientált architektúrában. Lehetővé teszi az információk megosztását, és alapot képez az együttműködési elemzés és az egyesített szimuláció irányába történő jövőbeni fejlesztésekhez. Teljesen nyílt forráskódú technológiákon alapuló rendszer, amelyet az EU tagállamai eszközként használhatnak a kritikus infrastruktúrák kockázatainak és ellenálló képességének elemzésére.

Ez a fejlesztés is jól példázza, hogy a technológia és a közösségi fejlesztések előrehaladott állapotban vannak, de ezekkel párhuzamosan fontos, hogy tagállami szinten is az egyes állami és piaci szereplők közti együttműködést ne ad-hoc módon, hanem a lehetséges veszélyekre felkészülten alakítsák, és felügyeljék a kritikus infrastruktúrákat.

Uniós szinten is számos fórumon megjelenik, hogy a kiberbiztonság prioritást élvez. Az Európai Parlament és a Tanács 2018. évben adta ki az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról[33] szóló rendeleti javaslatát, amely orvosolható hiányosságként nevesítette az alábbiakat:

- Nem kielégítő együttműködés a kiberbiztonság kínálati és keresleti szegmensei között.
- Ipari kapacitásépítést célzó, hatékony, tagállamok közötti együttműködési mechanizmus hiánya.
- Elégtelen együttműködés a kutatói és az ipari közösségek között és ezeken belül.
- Elégtelen együttműködés a polgári és a katonai kiberbiztonsági kutatói és innovációs közösségek között.

[32] Sík Zoltán Nándor (2011): *A kritikus információs infrastruktúra védelme és a közigazgatás. Vezetéstudomány – Budapest Management Review,* 42. évf. 3. sz. 42–47.

[33] Elérhető: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2018:0630:FIN:HU:PDF (A letöltés dátuma: 2020. 03. 04.)

- A kritikus infrastruktúrák védelmének fő prioritásai az Európai Unióban:[34]
- A kritikus infrastruktúrák hibrid fenyegetésektől való védelmére szolgáló eszközök, indikátorok azonosítása;
- módszerek és eszközök a kritikus infrastruktúrákat érintő belső fenyegetések kezelésére, például belső ellenőrzések és figyelemfelkeltés az érintett hatóságokkal együttműködésben;
- A kritikus infrastruktúrákat érintő új kihívások és a felmerülő fenyegetések (például drónok stb);
- Egyéb kritikus infrastruktúrákat érintő fejlesztések:
  - kockázatértékelési módszerek területén,
  - transznacionális együttműködés területén,
  - polgári együttműködés területén,
  - nemzetközi szervezetekkel való együttműködés területén.

A Horizon 2020 programban[35] ezen a területen a támogatott projektek elvárt hatásai:[36]

- rövid távon a sebezhetőség, a technológiák és a kockázati forgatókönyvek elemzése; lehetséges forgatókönyvek;
- középtávon az eszközök, innovatív megközelítések; biztonsági kockázatkezelési tervek; tesztkörnyezetek kialakítása a kritikus infrastruktúrák teljesítményének mérésére, ha kiber- és fizikai biztonsági intézkedésekkel vannak felszerelve;
- hosszú távú elvárt hatásként nevezték meg a konvergenciát a biztonsági és védelmi előírásokkal és a biztonságos/átjárható interfészekkel; hozzájárulás a szabályozási kezdeményezésekhez.

Látható tehát, hogy közösségi szinten is kiemelt szerepet kap a kiberbiztonság és a kritikus információs infrastruktúrák védelme, illetve azok keresztmetszetei. Azt azonban a NIS-irányelv is létrejöttének indokaként nevesíti, hogy az alapvető szolgáltatásokat nyújtó szereplőkre és a digitális szolgáltatókra vonatkozó egységes követelmények hiánya miatt nem lehetséges uniós szinten átfogó és hatékony együttműködési mechanizmust létrehozni.[37] Éppen ez az irányelv egyik célja, hogy ezen szereplők között meghatározott követelmények által uniós szintű és hatékony együttműködési mechanizmus alakuljon ki.

A NIS-irányelv azonban deklarálja, hogy nem sértheti a tagállamok számára biztosított azon lehetőséget, hogy megtegyék az alapvető biztonsági érdekeik védelméhez, a közrend és a közbiztonság megóvásához, valamint a bűncselekmények kivizsgálásának, felderítésének és a büntetőeljárások lefolytatásának lehetővé tételéhez szükséges intézkedéseket – azaz az irányelv ezeket a jogokat és kötelezettségeket nem szabályozza, nem korlátozza.

[34] Morentin, David Rios előadása 2019. március 13-án Brüsszelben a 'H2020 Secure Societies 2019 Info Day and Brokerage Event' rendezvényen. Elérhető: https://prod5.assets-cdn.io/event/3765/assets/8447002065-d961561682.pdf (A letöltés dátuma: 2020. 03. 06.)

[35] Bővebben: www.h2020.gov.hu/horizont2020-program (A letöltés dátuma: 2020. 03. 06.)

[36] Morentin 2019.

[37] Az Európai Parlament és a Tanács (EU) 2016/1148 Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről – 5. pont.

A tagállamon belüli együttműködés jó példája Magyarországon a Választási Informatikai Biztonsági Műveleti Központ (NVI SOC), amely eseti jelleggel, de jól példázza a begyakorolt, kipróbált együttműködési csatornák felhasználását, amikor az NKI és azon belül a nemzeti CSIRT, valamint az EU-tagállamok CSIRT- (Computer Security Incident Response Team) egységei, az informatikai szolgáltatók, illetve a bűnüldöző szervek képesek operatív módon azonnali és összehangolt intézkedésekre.
A honi szabályozás témánk szempontjából fontos sarokkövei:

– az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.);
– az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet;
– az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Korm. rendelet;
– az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet.

Ezek csak a rendészeti szervekkel történő együttműködési kötelezettséget írják elő, de ennek nem konkrét célja a büntetőjogi felelősségre vonás. További részletszabályok nincsenek, amelyek azt céloznák, hogy akár a bűncselekménynek minősülő további cselekmények megszakítása, más bűncselekmények elkövetésének megelőzése vagy az elkövetők kézre kerítése érdekében mely szerveknek, milyen feladataik lennének. Így a kialakult gyakorlat szerint a bűnüldöző szervek csak eseti jelleggel szereznek tudomást az incidensek mögötti bűncselekményekről, és nem vesznek részt a postmortem analízisekben sem.

Annak számos oka van, hogy a nyomozó hatóságok csak kevés esetben indíthatnak eljárást az informatikai incidensekkel összefüggésben. A sértetti attitűd[38] is fontos e körben. Jól példázza ezt az is, hogy például a WannaCry zsarolóvírus-kampánnyal összefüggésben mindösszesen egyetlen büntetőeljárás indult Magyarországon.

A tudomásra jutás hiányán túl meg kell említenünk, hogy a rendészeti szervek büntetőeljáráshoz kötött intézkedései viszonylag lassúak. Még egy nyomozás elrendelése nélkül végrehajtott intézkedés is sokkal lassabb, mint az ipari szereplők együttműködésén alapuló intézkedések. Ha egy kritikus információs infrastruktúrát informatikai támadás ér – például egy kártékony kód vagy DDOS-támadás formájában –, akkor a támadott infrastruktúra azonnali és hatékony segítséget kaphat a Nemzeti Kibervédelmi Intézettől.

[38] A korábban említett bizalmatlanság az állami szervek irányába, versenytársakkal való kooperáció hiánya, az eredménnyel nem kecsegtető nyomozásokkal kapcsolatos ráfordítások elkerülése stb.

Magyarországon jelenleg nincs külön jogszabályi rendelkezés vagy eljárási rend arra vonatkozóan, hogy az elektronikus információs rendszerek biztonságát felügyelő Nemzeti Kibervédelmi Intézet,[39] illetve a magyar CSIRT-ek[40] milyen formában kötelesek együttműködni a bűnüldöző hatósággal. Best practice-ként említhető, hogy a BM OKF kialakított olyan együttműködést az NNI-vel, amely alapján minden incidenst, amelyről a kijelölő hatóságon vagy az érintett szolgáltatón keresztül értesülnek és amelynél bűncselekmény gyanúja fennáll, írásban jeleznek a Nemzeti Nyomozó Iroda (NNI) Kiberbűnözés Elleni Főosztálya felé, amely hivatalból vizsgálatot indít. (Az információáramlás természetesen nem egyirányú, hiszen a nemzeti CSIRT-et eseti jelleggel, egyes incidensek kapcsán az NNI is megkeresi a büntetőeljárások szempontjából releváns adatok megszerzése érdekében.)

Általános szabály, hogy bűncselekmény gyanúja esetén minden hatóságnak és hivatalos személynek a büntetőeljárási törvény szerinti alapvető kötelezettsége (376. §) a feljelentést megtenni. Ez azt eredményezi, hogy a NIS-érintettségű hatóságok és a CSIRT állománya mint hivatalos személy szintén kötelezett arra, hogy a tudomására jutó incidenssel kapcsolatosan bűncselekmény gyanújának felmerülése esetén a nyomozó hatóságok felé azt haladéktalanul jelezze. Tekintettel arra, hogy az Ibtv.[41] szerint a NIS hatálya alá tartozó szervezetek[42] vezetői haladéktalanul kell jelentsék a szervezetüket ért biztonsági eseményeket, a folyamat önálló szabályozottság nélkül is azt kellene eredményezze, hogy az illetékes bűnüldözési hatóság tájékoztatása megtörténik.[43] A jog által rögzített szabályok azonban a gyakorlatban eltérő módon érvényesülnek, és jelentős mértékben függnek a kötelezettek jogkövető magatartásától. Elenyésző ugyanis azon feljelentések száma, amelyek a nyomozó hatóságokhoz érkeznek.

Következtetések

A kibertér biztonságát szavatolni szándékozó állam számára az az optimális, ha minden azt sértő vagy fenyegető incidensről azonnal értesül. Számos ok van, ami ezt gátolja, de ezeket a gátakat szükséges szisztematikusan lebontani. Ehhez meg kell nyerni a piaci szereplők bizalmát.

[39] Bővebben: www.katasztrofavedelem.hu/109/kritikus-infrastruktrk-vdelmvel-sszefgg-hatsgi-feladatok-jogszablyok, valamint https://nki.gov.hu/hatosag/tartalom/vonatkozo-jogszabalyok/ (A letöltések dátuma: 2020. 03. 06.)

[40] Computer Security Incident Response Team – azaz (számítógép-biztonsági incidenskezelő csoport, amelyből Magyarországon 3 létezik. Bővebben: www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Hungary (A letöltés dátuma: 2020. 03. 06.)

[41] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

[42] Egy részük kritikus információs infrastruktúrát üzemeltető. Bővebben: https://nki.gov.hu/hatosag/tartalom/hataskor-ekertv/ (A letöltés dátuma: 2020. 03. 06.)

[43] Bonnyai Tünde (2020) Nemzeti Kibervédelmi Intézet nemzetközi összekötőjével folytatott interjú során elhangzottak.

A rendészeti, bűnüldöző szerveknek, nyomozó hatóságoknak, a jog érvényre juttatására akár erőszak alkalmazásával is felhatalmazott szerveknek egyértelmű szabályok mentén kell működniük. A büntetőjogi normák meglehetősen alacsonyan húzzák meg a kibertérrel összefüggő bűncselekmények határát:

– a jogsértések valójában nem tudnak szabálysértési alakzatot felvenni. A legcsekélyebb tényállásszerű magatartás azonnal bűncselekmény (például nincs különbség aközött, hogy egy rendkívül gyenge védelemmel ellátott, adatokat nem tartalmazó, információs rendszerbe lép be az elkövető, vagy egy értékes adatokat tartalmazó, komoly védelmet győz le a jogosulatlan belépés érdekében);
– A jogalkotó a védendő területet már nagyon távoli veszélyeztetés esetén is büntető törvénykönyvi tényállás segítségével védi. Nem csupán az információs rendszerek elleni támadás konkrét előkészülete, hanem absztrakt előkészülete, egy lehetséges elkövető információs rendszerekbe történő jogosulatlan belépését megkönnyítő ismeretekkel való ellátása is bűncselekmény az információs rendszer védelmét biztosító technikai intézkedés kijátszása tényállás által;[44]
– Az információs rendszer vagy adat megsértése (Btk. 423. §) a terrorcselekmény (Btk. 314. §) tényállása alkalmazásában személy elleni erőszakos, közveszélyt okozó vagy fegyverrel kapcsolatos bűncselekménynek minősül az emberöléssel azonos módon. Ha valaki tehát az információs rendszer vagy adat megsértése bűncselekményét[45] például egy nemzetközi szervezet működését megzavarva követi el,[46] akkor tíz évtől húsz évig terjedő vagy életfogytig tartó szabadságvesztéssel büntetendő. Ha valaki például az ezt könnyítő feltételeket biztosítja, vagy ezen tevékenység elkövetésével fenyeget, akkor két évtől nyolc évig terjedő szabadságvesztéssel büntetendő.

A jogalkotó határozott rosszallását fejezi ki a kibertér elemei és ezen belül a kritikus információs infrastruktúrák megzavaróival szemben. A fenyegetés azonban önmagában hatástalan, ha (szinte) senki sem akarja/tudja felkutatni az elkövetőket.

A jelenlegi helyzetben a jogalkotó bízik a jogalkalmazók józan értékítéletében, és nem indítanak (a törvény passzusait szó szerint betartva) naponta százával feljelentéseket az informatikai incidensekkel kapcsolatban a rendőrséghez, hisz az nem szolgálná a közjót, de az sem helyes, ha a jelek azt mutatják, hogy a kibertérben a bűn – például a kritikus információs infrastruktúrák támadását megkísérelve – üldözés nélkül terjedhet.[47]

[44] A büntető törvénykönyv jellemzően a konkrét bűncselekmény elkövetésére vonatkozó előkészületet is csak súlyosabb bűncselekmények esetén rendeli büntetni, például népirtás, emberülés, terrorcselekmény. Itt azonban már az absztrakt előkészület is büntetendő.

[45] Ami lehet egy munkavállaló általi hálózati meghajtó jogosulatlan megtekintése, vagy egy hekkelést Youtube-videók segítségével elsajátító fiatal szárnypróbálgatása, amikor 5USD-os wifijammert fabrikál.

[46] Ha az előbb említett munkavállaló letörli például a hálózati tartalmat munkáltatója szerveréről, ami történetesen például a Nemzetközi Sakkszövetség, vagy az említett tinédzser éppen a Türk Nyelvű Államok Együttműködési Tanácsa vagy a Nemzetközi Migrációs Szervezet wifihálózatát teszi elérhetetlenné.

[47] A szerző ahhoz hasonlatosan érzi magát, mintha senki sem ellenőrizné a közutakon a sebességkorlátozások betartását.

A jó állam a legmagasabb szintű közjó elérése érdekében az erőforrásait logikusan, költséghatékonyan kell hogy felhasználja. Ha rendelkezésre állnak az erőforrások a bűnüldöző szervek részéről,[48] akkor lehetséges és szükséges irány az emberi erőforrások továbbképzése, a technikai erőforrások[49] fejlesztése annak érdekében, hogy a Nemzeti Kiberbiztonsági Stratégiában[50] meghatározott alábbi vállalás teljesüljön:

„Magyarország a kibertér védelemével összefüggő feladatok ellátását felelősséggel vállalja és a magyar kiberteret, mint a gazdasági és társadalmi élet meghatározó pillérét szabad, biztonságos és innovatív környezetté kívánja alakítani."

Felhasznált irodalom

Bognár Balázs – Bonnyai Tünde – Vámosi Zoltán (2019): *Kritikus infrastruktúrák védelme I.* Budapest, Dialóg Campus Kiadó.

Borbíró Andrea (2009): Prevenció és büntető igazságszolgáltatás In Virág György szerk.: *Kriminológiai Tanulmányok.* 46. kötet. Budapest, OKRI. 13–37.

Bonnyai Tünde (2020): Nemzeti Kibervédelmi Intézet nemzetközi összekötőjével folytatott interjú.

Haig Zsolt – Kovács László (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* Budapest, Nemzeti Közszolgálati Egyetem.

Morentin, David Rios előadása 2019. március 13-án Brüsszelben a 'H2020 Secure Societies 2019 Info Day and Brokerage Event' rendezvényen. Elérhető: https://prod5.assets-cdn.io/event/3765/assets/8447002065-d961561682.pdf (A letöltés dátuma: 2020. 03. 06.)

Pesch-Cronin, Kelley – Marion, Nancy (2017): *Critical Infrastructure Protection*. CRC Press.

Quigley, Kevin – Bisset, Ben – Mills, Bryon (2017): *Too Critical to Fail: How Canada Manages Threats to Critical Infrastructure.* Montreal, MQUP.

Sík Zoltán Nándor (2011): *A kritikus információs infrastruktúra védelme és a közigazgatás. Vezetéstudomány – Budapest Management Review,* 42. évf. 3. sz. 42–47.

Jogszabályok

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

7-es számú elnöki irányelv: Homeland Security Presidential Directive 7: Critical infrastructure identification, prioritization, and protection. Elérhető: www.cisa.gov/homeland-security-presidential-directive-7 (A letöltés dátuma: 2020. 03. 18.)

Az Európai Parlament És A Tanács (EU) 2016/1148 Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről – 5. pont

Executive Order 13636. Elérheő: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (A letöltés dátuma: 2020. 03. 20.)

Homeland Security Key DHS Laws. Elérhető: www.dhs.gov/key-dhs-laws (A letöltés dátuma: 2020. 03. 19.)

[48] Az elmúlt évek bűnügyi statisztikája csökkenő tendenciát mutat, miközben a rendőrség bűnügyi állományában a fluktuáció nem olyan magas, mint a közrendvédelmi területen.

[49] A digitális bizonyítékok felkutatásához, rögzítéséhez, elemzéséhez szükséges hardverek és szoftverek.

[50] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

Strategic National Risk Assesment. Elérhető: www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf (A letöltés dátuma: 2020. 03. 19.)
The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. Elérhető: www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf (A letöltés dátuma: 2020. 03. 19.)

Krasznay Csaba

Okoseszközök a kritikus információs infrastruktúrákban

Kivonat

A 2020-as évek kezdetén a negyedik ipari forradalom zajlik éppen, és talán észre sem vesszük, hogy a digitális technológia átalakítja a mindennapi életünket. A hétköznapi ember ezeket a változásokat leginkább úgy érzékelheti, hogy okostelefont, okosórát, okos villanykörtét használ, miközben a háttérben az ipar, a termelés, a közművek, általánosságban az egész gazdaság is egyre jobban függ ezektől a hálózatba kötött eszközöktől, amelyeket összefoglaló néven a „dolgok internetének", azaz Internet of Things-nek (IoT) nevezünk. Jelen tanulmány célja bemutatni, hogyan hat a negyedik ipari forradalom a közműszolgáltatásra, és ezen belül azt is érzékeltetni, hogy milyen kibertéri veszélyeket fog jelenteni a következő években ez az átalakulás.

Bevezetés

A negyedik ipari forradalom a szemünk előtt zajlik. Ezt a fogalmat sokan Klaus Schwab nevéhez kötik, aki így foglalta össze a forradalmi változásokat: „Mint ahogy az első ipari forradalom gőzzel működtetett gyárai, a másodiknál a tömeggyártás tudományának alkalmazása, továbbá a harmadik ipari forradalom során a digitalizáció elkezdése, addig a negyedik ipari forradalom olyan technológiái, mint a mesterséges intelligencia, a genomszerkesztés, a kiterjesztett valóság, a robotika és a 3D nyomtatás, gyorsan megváltoztatják azokat a folyamatokat és módszereket, ahogy az emberiség az értékeket létrehozza, cseréli és elosztja. Ahogy az az előző forradalmak során is történt, ez a változás is mélyen átalakítja az intézményeket, iparágakat és a magánszemélyeket is. Ennél is fontosabb azt észrevenni, hogy ezt a forradalmat az emberek ma meghozott döntései vezérlik. A világ 50–100 év múlva nagymértékben függ majd attól, hogy hogyan gondolkodunk ma ezekről a befektetésekről, és hogyan vezetjük be ezeket az erőteljes új technológiákat."[1]

Nagy Judit tanulmányában részletesen áttekintette a negyedik ipari forradalomra vonatkozó fogalmakat, és így szintetizálta az egyes szerzők véleményét: „A negyedik ipari forradalom alapja a digitalizáció, és az adat, a számítógép csupán eszköz. Az internet és a technológia fejlődése megteremti az emberek, gépek és vállalatok folyamatos összeköttetésben lévő hálózatát, és az értékteremtő folyamatok adatainak folyamatos megosztásával elérhetővé válik a versenyképes, a vevő számára teljesen testreszabott termék előállítása. A versenyelőny forrása tehát nem csupán az összehangolt vagy éppen teljesen új alapokra helyezett termelés (pl. additív termelés) lesz, hanem a termékek digitális szolgáltatásokkal való körbeágyazása, valamint, hogy melyik vállalat hogyan válogatja ki a keletkező adatokból a releváns információt a döntéshozatal támogatásához."[2]

[1] Schwab 2018
[2] Nagy 2019

A negyedik ipari forradalom egyik leglátványosabb jele a mindennapi ember számára azonban az, hogy otthonaink okossá válnak, olyan informatikai eszközöket kezdünk el használni, amelyeknek 10 évvel ezelőtt még nyomuk sem volt. Az első iPhone-t mint az okoseszközök egyik legjellegzetesebb példáját 2007. január 9-én jelentették be, majd terjedt el villámgyorsan a fogyasztók között, és alakította át a mobiltávközlést, de például az okos-fitneszkarkötők, az okosizzók, az okosautók, az okoshűtőszekrények mind-mind a 2010-es évek innovációi.

Ez az évtized kitermelt számos olyan okoseszközt is, amelyeknek a létjogosultságát sem feltétlenül értik azok, akik nem ebben a világban nőttek fel. Példaként lehetne kiemelni az okosvizespalackot, amelynek célja nem más, mint hogy ezt az eszközt összekötve az okostelefonnal és a fitneszkarkötővel jelezze, hogy nem ittunk eleget, és figyelmeztessen minket az ivás fontosságára. Mivel a vízfogyasztás alapvető biológiai szükséglete az embernek, felmerül a kérdés, vajon mi indokolja egy ilyen eszköz létrehozását? Különös tekintettel arra, hogy nemcsak egy megoldás van jelen, hanem számos gyártó dobott piacra olyan terméket, amely ezt az igényt fedi le, ami azt is jelenti, hogy a fogyasztóknak feltehetőleg ténylegesen szükségük van ilyen eszközökre.[3]

A hálózati társadalmak

A választ a generációs különbségekben kell keresni. Jelen pillanatban 6 különböző generáció él egymás mellett, és ezek különböző módon alkalmazkodtak a technológiához, különböző módon élték meg az elmúlt 100 év technológiai vívmányait.[4]

- Az első, ahogy az amerikai terminológiában hívják, az *építők generációja* (1946 előtt születettek), amelynek tagjai a második világháború után újjáépítették a világot, és kialakították azt a fogyasztói társadalmat, amelyet ma is ismerünk. A számítógépek ennek a generációnak köszönhetők.
- Utánuk következtek a *Baby Boomerek* (1946 és 1964 között születettek), akiket Magyarországon a Ratkó-gyerekeknek ismerünk. Az ő életükben változott át a gazdaság és az ipar számítógépesítetté, az ő idejük alatt jelent meg az első hálózatba kötött eszköz, a ma ismert internet elődje. Az ő idejükre tehető a harmadik ipari forradalom.
- Az *X generáció* (1965–1979 közöttiek), más néven a digitális bevándorlók világa hozta el az otthoni számítógépek korszakát, illetve az internetet olyan formában, ahogy azt ma ismerjük. Mivel fiatalkorukban érte őket a kétpólusú világrend összeomlása, a globalizáció megjelenése, egyrészt érdeklődésből, másrészt munkahelyi kényszerből is elkezdték használni az informatikai eszközöket, amelyeket sokkal könnyebben tanultak meg, mint az előttük levő generációk.
- Az *Y generáció,* az 1980 és 1994 közöttiek generációja az, amely már ösztönszinten használta az informatikai vívmányokat. Az ő idejükben jelent meg például a Google

[3] Bondor 2020
[4] Howe–Strauss 2007

vagy a Facebook, vált tömegessé a mobiltelefonok használata. Ők azok, akik fiatalkorukban tapasztalták meg először a kibertér árnyoldalait.
– Utánuk következett a *Z generáció,* az 1995 és 2009 között születetteké, akiket már digitális bennszülötteknek lehet nevezni. Életükben a kezdetektől jelen van az internet és a különböző digitális technológiák használata, így ők, a következő évtizedek dolgozói azok, akik a negyedik ipari forradalomhoz a legjobban tudnak alkalmazkodni.
– Végül az *Alfa generáció* tagjairól kell megemlékezni, a 2010 után született gyerekekről, akiknek a digitális életük már születésük előtt 6–8 hónappal elkezdődött, amikor édesanyjuk a közösségi hálózaton bejelentette, hogy a gyerek majd egyszer meg fog születni. Ők azok, akik már a tévé képernyőjét is megpróbálják úgy húzkodni, mint az okostelefonokét, hiszen azt látták, hogy az reagál arra, amit ők tesznek, és ők azok, akiknek az életükhöz elválaszthatatlanul hozzátartoznak a digitális eszközök.

Látható tehát, hogy ahogy a generációkban haladunk előre, úgy a digitális technológiákhoz való hozzáállás is jelentős mértékben megváltozik, ami kikényszeríti azt, hogy a szolgáltatók is alkalmazkodjanak ügyfeleikhez. Ennek a következménye, hogy kialakult az úgynevezett hálózati társadalom, amelyet Manuel Castells, a fogalom megalkotója a következőképp fogalmazott meg: „egy olyan társadalom, amelynek társadalmi struktúráját a mikroelektronikai alapú információs és kommunikációs technológiák által táplált hálózatok alkotják."[5]

Azt, hogy hálózati társadalomban élünk, mi sem mutatja jobban, mint hogy jelenleg a világon körülbelül 7,8 milliárd ember él, 55%-uk városokban, s 5,2 milliárd ember használ mobiltelefont. Az emberek 67%-a tehát mobileszköz-használó. 4,5 milliárd ember, a teljes népesség 59%-a aktív internetfelhasználó, és 3,8 milliárd ember, a népesség 49%-a aktív a közösségi hálózatokon. Elmondható tehát, hogy a fizikai mellett a digitális létünk is kialakult, ami óhatatlanul hatással van nemcsak a mindennapi életünkre, hanem a munkahelyi tevékenységeinkre, és ezen keresztül a gazdaságunkra is.

Nem véletlen, hogy a digitáliseszköz-használók a hagyományos értelemben vett okoseszközök használata mellett egyre inkább felokosítják a környezetüket is, azaz kialakulnak az okosotthonok, amelyek száma körülbelül 150 millióra tehető jelenleg világszerte. Ez a szám azonban hónapról hónapra növekszik, egyre többen döntenek úgy, hogy az otthonaikat is különböző okoseszközökkel látják el, ezzel növelve a dolgok internetének méretét. Az okosotthonok létrehozása körülbelül 70 milliárd dolláros iparág.[6]

De természetesen az okosotthonok mellett az okosotthont kiszolgáló infrastruktúra megteremtése is fontos feladat. Az okosotthonok egyik legfontosabb építőköve az okosasszisztens, amelyből a legismertebbek közé tartozik az Amazon Echo, az Apple HomePod vagy a Google Home megoldása. Ezek olyan eszközök, amelyek az okosotthon középpontjaként a felhasználótól kapott szóbeli parancs vagy előre beállított feladat

[5] Castells 2004
[6] Kemp 2020

alapján irányítják, hogy mit csináljon az okosotthon, koordinálva a különböző okosotthon-felszereléseket. Az okoseszközök száma egyébként robbanásszerűen növekszik. 2017 és 2030 között a jóslatok szerint 27 milliárd eszközről várhatóan 125 milliárd eszközre fog növekedni a számuk.[7]

Feltehetőleg azonban ezek az adatok ma már el is avultak, hiszen napról napra újabb és újabb forradalmi megoldások jelennek meg. Az olyan társadalmat megrázó események, mint például a koronavírus-fertőzés például elősegítik az okoseszközök számának a növekedését, hiszen akár a gyógyászatban, akár a fertőzöttek követésében is elengedhetetlenül fontosak az embereket szolgáló és információkat szolgáltató eszközök. Így nem meglepő, hogy Kínában a koronavírus-járvány legyűrésében vitathatatlanul fontos szerepet játszottak a különböző okoseszközök is, illetve hogy iparági elemzők az okosasszisztensek számának jelentős növekedését várják a járvány „mellékhatásaként".[8] Mindez európai szemmel komoly adatvédelemi és az információbiztonsági kérdéseket vet fel, tekintettel arra, hogy az ilyen megoldások óhatatlanul sértik a személyek magánszféráját.

Az IoT információbiztonsági kihívásai

Az információbiztonság szempontjából tehát a kihívás adott. Egyre több hálózatba kapcsolt eszközt, egyre több okoseszközt látunk, amelyeknek tervezési szinten történő adatvédelme és információbiztonsága finoman szólva megkérdőjelezhető. Hiszen gondoljunk csak bele abba, hogy ma már egy egyszerű kábel is sok esetben tartalmaz néhány mikroprocesszort, amelyekről nem feltétlenül tudjuk, konkrétan mit csinálnak, milyen adatokat forgalmaznak, hogyan hatnak működési környezetükre. Vagy gondoljunk egy modern önvezető autóra, amelynek működéséhez különböző beágyazott informatikai eszközök hálózatba kapcsolása szükséges, ezek irányítása pedig szoftveren keresztül történik. Ráadásul várhatóan nemsokára megjelennek majd az egymással, illetve a különböző forgalomirányító eszközökkel is kommunikáló önvezető autók, így egyértelmű, hogy egy hálózatba kapcsolt teljes ökoszisztémáról beszélünk, amelynek ha bármelyik eleme is sérülékeny, az mindenképpen hatással lesz a teljes ökoszisztémára is.

Azt, hogy milyen fenyegetést jelentenek a hálózatba kapcsolt eszközök, a legjobban a Mirai botnet mutatja be, amely 2016-ban pusztított végig a világon. Működési mechanizmusát tekintve úgy működött, hogy különböző hálózatra kapcsolt okoseszközöket fertőzött meg, tipikusan IP-kamerákat, illetve sérülékeny routereket. A megfertőzött eszközök folyamatosan szkennelték az internetet, újabb és újabb gyenge eszközöket keresve találták meg azokat a réseket, sebezhetőségeket és tervezési hibákat, mint például a beépített gyenge jelszavakat, amelyeket kihasználva fel tudták telepíteni saját magukat ezekre az eszközökre, majd a távolról jövő utasításokat elfogadva hajtottak végre olyan kibertámadásokat, amelyek hatással voltak olyan globális digitális szolgáltatásokra is,

[7] IHS 2017
[8] Shein 2020

mint például a legnépszerűbb videóstreaming-szolgáltatás. Ez mutatja, mi történhet, hogyha tömegesen tud uralma alá hajtani valaki ilyen hálózatba kapcsolt okoseszközöket.[9]

További figyelmeztető jel a 2017-ben a Wikileaksen megjelenő Vault 7 nevű szivárogtatás, amely az amerikai Central Intelligence Agency (CIA) kibertevékenységébe adott bepillantást, és mutatta meg, hogy ez a hírszerző szervezet is aktívan keresi a sebezhetőségeket olyan okoseszközökben, mint például az okostelefonok, okostelevíziók vagy éppen az önvezető autók. El lehet tehát mondani, hogy mind a kiberbűnözésnek, mind pedig az államilag támogatott kiberkémkedésnek és kiberhadviselésnek célpontjai lehetnek az okoseszközök. A probléma pedig az, hogy ez hatással van a hétköznapi ember okosotthonain túl a létfontosságú rendszerekre is.[10]

Okosvárosok biztonsága

Bár a hétköznapokban kevésbé látszódik, az okosotthonok mellett kialakulóban vannak az okosvárosok is. Az okosvárosok, hasonlóan az okosotthonokhoz, okoseszközök hálózatba kapcsolását valósítják meg. Céljuk azonban nem az, hogy fel tudjuk húzni a redőnyünket szóban kimondott paranccsal, hanem az olyan közművek irányítása, mint például a villamos energetikai ellátás, a gázellátás, az egészségügy, a közbiztonság, az épületvezérlés. Sallai Gyula így foglalja össze az okosváros koncepcióját, amely létrejöttének elsődleges kiváltója a túlzott urbanizáció miatt lassan élhetetlenné váló települések fenntarthatóságának biztosítása: „Az okosváros-koncepció lényege a »smartintegráció«, egy olyan platform, amelyen a különféle területek megoldásai egymást erősítő rendszerré állnak össze, és a város erőforrásait hatékonyan, koordináltan használják fel. Ennek érdekében a város életének minden releváns információját gyűjtik, elemzik, és egy közösen használt tudásbázist hoznak létre, amelynek bázisán adatvezérelt komplex megoldások valósíthatók meg. Egy város akkor nevezhető igazán okosnak, ha az IKT-megoldások segítségével a fizikai infrastruktúrák hatékony használatát és az életminőség javítását:

– a különféle erőforrások és szolgáltatások együttes, integrált kezelésével,
– adatvezérelve, adaptívan, a körülmények tényszerű változására reagálva,
– környezettudatosan, fenntarthatóan, energiatakarékosan,
– az érintett közösség aktív részvételével, érdekeltjeinek bevonásával,
– gazdaságilag önfenntartó módon éri el.”[11]

A szerző 6 + 1 különböző kulcsterületet azonosít, amelyek az okosváros létrehozásához feltétlenül szükségesek. Ezek az okosváros-igazgatás, az okosvárosi környezet, az okosközlekedés, az okosenergetika, az okoséletvitel, az okos-infokommunikációs infrastruktúra és az okosváros kiberbiztonsága mint horizontális kulcsterület. Jelen tanulmány három kulcsterület, az okosközlekedés, az okosenergetika és az okosvárosi környezet

[9] Bederna et al. 2019
[10] Wikileaks 2017
[11] Sallai 2018

példáján keresztül mutatja be, hogy az okosváros kiberbiztonsága miért kiemelkedően fontos. Az okosvárosi környezet körében jelenik meg az okosvízkezelés, azaz a vízi közművek is. Az okos vízi közművek megjelenése azt jelenti, hogy a víz kitermelése, tisztítása, célba juttatása, illetve szétosztása is egyre inkább „okossá válik", ezzel új, korábban nem látott lehetőséget, egyben biztonsági kihívást hozva a víziközmű-szolgáltatóknak.[12]

Az okosvárosok esetében biztonsági szempontból több különböző, egymással párhuzamosan versengő aspektust kell figyelembe venni. Egy közlekedési példával lehetne mindezt a legjobban illusztrálni. Gondoljunk bele abba, mi történik, ha egy önvezető autóban valamilyen sebezhetőség jelenik meg, amelyet azonnal frissíteni kell, hiszen ha egy Miraihoz hasonló kártékony kód tudna elterjedni az okosközlekedés ökoszisztémájában, akkor az autóvezetés gyakorlatilag lehetetlenné válna. Az autókban azonban, hasonlóan bármilyen más létfontosságú rendszerhez, három különböző szempont tartandó szem előtt: az üzembiztonság, a kiberbiztonság, illetve az adatvédelem.

Kiberbiztonsági szempontból a probléma tehát az, hogy egy súlyos informatikai sebezhetőség jelenik meg az önvezető autókban, és hogyha egy olyan féregtípusú kártékony kód jelenik meg ezekben, amely automatikusan tud a hálózaton keresztül terjedni, akkor a fertőzés perceken belül globális mértékben szét tud terjedni a sebezhető gépjárművekben. Ez adott esetben több tízmillió autót is érinthet, éppen ezért az informatikában megszokott módon azonnal frissíteni kell az ezeken futó szoftvert. Itt azonban szóba kerülnek az üzembiztonsági kérdések is, hiszen egy informatikai eszközben egy új hibajavítás előre nem látható gondokat okozhat. Éppen ezért nem lehet menet közben frissíteni ezeket a gépjárműveket, meg kell várni, amíg leállnak. Az önvezető autókban ez egy egyszerű állapotinformáció, amely interneten lekérdezhető, meg kell tehát néznünk, hogy áll-e az autó. Csakhogy itt előjönnek azok az adatvédelmi kérdések, amelyek korábban nem jelentettek problémát, hiszen hogyha a helyi adatokból és a szenzorokból kiderül, hogy mozgásban van az autó, az azt jelenti, hogy a gyártó figyelheti is az autó konkrét közlekedési helyzetét, ami adatvédelmi szempontból problémás lehet. Azaz, a kiberbiztonság hatással van az üzembiztonságra, az üzembiztonság hatással van az adatvédelemre, és mindhárom szempontot egyenlő mértékben kell figyelembe venni az új típusú okosváros-megoldásoknál.

Természetesen az önvezető okosautók tömeges elterjedése még nem napjaink kihívása, de észre kell venni, hogy a technológia az ablakon kopogtat. A Society of Automotive Engineers (SAE) 2014-ben adott közre egy tanulmányt, amelynek címe *J3016, Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems* volt. Ebben írták le az autonóm autók különböző szintjeivel kapcsolatos követelményeket, s összesen hat szintet határoztak meg, amelyeket Mester Gyula így foglalt össze:

0. szint: a hagyományos autó teljes mértékben emberi irányítás alatt áll, nincs automatizáltság, a vezetési környezetet az ember figyeli.

[12] Sallai 2018

1. szint: az autó teljes mértékben emberi irányítás alatt áll, autóvezetés támogatása kormányzás vagy fékezés/gyorsulás esetében, a vezetési környezetet az ember figyeli.
2. szint: az autó teljes mértékben emberi irányítás alatt áll, részleges automatizáltság, az autóvezetést támogató rendszer a kormányzási és a fékezési/gyorsítási műveleteket egyszerre átveheti, a vezetési környezetet az ember figyeli.
3. szint: feltételes automatizáltság, az autót teljes mértékben ember irányítja, az autóvezetést támogató rendszer a kormányzási és fékezési/gyorsítási műveleteket egyszerre átveheti, a vezetési környezetet az automata rendszer figyeli.
4. szint: magas szintű automatizáltság, az automata autóvezető-rendszer irányítja az összes dinamikus vezetési műveletet, a vezetési környezetet az automata rendszer figyeli.
5. szint: teljes automatizáltság, az automata autóvezető-rendszer folyamatosan irányítja az összes dinamikus vezetési műveletet, a vezetési környezetet az automata rendszer figyeli, az autó ember nélkül is közlekedhet.[13]

2020-ban a legtöbb új autó az 1. szinten meghatározott automatizálási fokon van, de kereskedelmi forgalomban már kaphatók a 2. szintet elérő gépjárművek is. A Tesla Autopilot megoldása például erre a szintre sorolható. Az első 3. szintet is elérő gépjárművet az Audi jelentette be, A8L-modelljét tekinti a követelmények teljesítőjének. A Gartner elemzőcég Hype Cycle for Emerging Technologies, 2019 jóslata szerint a 4. szint két éven belül, az 5. szint 2–5 év múlva várható.[14] Az okosvárosok autókkal kommunikáló intelligens vezérlési rendszerei pedig egyelőre csak tesztpályákon léteznek. Kijelenthető tehát, hogy ha figyelembe vesszük a gépjárművek életciklusát és az átlagos városfejlesztési sebességet, a vázolt kiberbiztonsági kihívások inkább a 2030-as, semmint a 2020-as évek problémáját fogják jelenteni.

Általánosságban is kijelenthető, hogy az okosváros kiépítése ugyan elkezdődött, de általánossá válására még jó pár évet várni kell. Hiányzik ugyanis néhány olyan infrastrukturális építőkő, amelyek nélkül a milliónyi okoseszköz kommunikációja és az általuk szolgáltatott adatok feldolgozása, majd ezek alapján a (fél)automata döntések nem valósíthatók meg. A „hiányzik" ebben az esetben nem azt jelenti, hogy a technológia nem létezik, hanem azt, hogy még nem terjedt el, nem áll tömegesen a városok szolgálatában. Példa erre az ötödik generációs mobiltávközlés, az 5G-hálózat, amelynek technológiája, szabványai ismertek, de a frekvenciaengedélyek kiosztására Magyarországon 2019-ben, az első kereskedelmi szolgáltatás elindítására 2020-ban került sor. A szükséges városi lefedettség kiépítése pedig éveket vesz majd igénybe, amelyet a lakossági ellenállás is hátráltat, amelynek az olyan összeesküvés-elméletek lehetnek az alapjai, mint hogy az 5G-hálózatok terjesztenék a koronavírust.

De az adatfeldolgozás területén is számos akadályozó tényezőt lehet azonosítani, amelyek megint csak nem műszaki jellegűek. Az okosváros-megoldások lényege, hogy

[13] Mester 2018
[14] Panetta 2019

a szenzoradatokból felépített nagyadat-adatbázisok (Big Data) szolgálnak alapul a mesterséges intelligencia által segített döntéshozatalban. A legtöbb városi önkormányzat azonban nem áll azon az érettségi fokon, hogy képes legyen a mesterséges intelligenciát felhasználni a döntéshozatalban. Jellemzően a szakapparátus és a politikai vezetés is a Baby Boomer vagy az X generáció tagjai kezében van, akik a jelenleg zajló negyedik ipari forradalom vívmányait nehezebben fogadják be. Legalább még egy évtized kell, amikorra megjelenik az Y és a Z generáció a magas szintű döntéshozatalban, és általánossá válik az adatalapú, mesterséges intelligencia által támogatott várostervezés és önkormányzati működés.

Mindeközben az okosvárosokat ellátó közműszolgáltatók elkezdték az átállást az okos-infrastruktúrákra, de ez sem gyors folyamat. Az ipari irányítórendszerek életciklusa évtizedekben mérhető, így nem ritka, hogy 20–30 éves informatikai megoldások támogatják a létfontosságú rendszerelemek működését. Ez alapesetben nem okoz problémát, hiszen mindhárom vizsgált területen (villamos energetika, víz, közlekedés) az üzembiztonság jelenleg a legfontosabb, és ezt gond nélkül meg tudják valósítani ezek a rendszerek. Hatékonysági okokból viszont ezeket folyamatosan hálózatba kötik, így kiberbiztonsági szempontból védhetetlenné válnak. Nem ritkák az olyan SCADA/ICS-rendszerek, amelyeken Windows XP vagy még régebbi, már évek óta nem támogatott operációs rendszer fut, így ha ezek bármilyen módon hálózatra kerülnek, védelmük teljesen esélytelen a kibertéri veszélyekkel szemben. Ezeket tehát cserélni kell, a gyártói kínálatban pedig ma már az okosmegoldások dominálnak, érthető módon a dolgok internetének halmazába tartozó megoldásokat szeretnének a közműszolgáltatóknak értékesíteni. Ezek üzembiztonsági szempontból megfelelők, a kiberbiztonságot is jobban megvalósítják, mint régebbi társaik, ám egyrészt az adatvédelem továbbra sem szempont, illetve még évekig egy hálózatban fognak működni a hagyományos SCADA/ICS-megoldásokkal, így az üzemeltetőknek egy hibrid infrastruktúra védelmére kell felkészülniük. Tekintettel arra, hogy az ipari irányítórendszerek üzemeltetése jellemzően villamosmérnöki feladat üzembiztonsági fókusszal, itt is meg kell jelennie azoknak a mérnököknek, akik szélesebb látókörrel, kiberbiztonsági szemléletmóddal is rendelkeznek. Ezen szemléletmódváltás és az új üzemmérnök-generáció megjelenése is éveket fog igénybe venni, így a létfontosságú közművi információs rendszerek még jó darabig alacsonyabb védelmi szinten fognak működni, mint ahogy azt a kibertéri veszélyek indokolttá tennék.

Kiberbiztonság az okos vízi közműveknél

Ma már tehát egyetlen ipari irányítástechnikai rendszerrel foglalkozó mérnök számára sem lehet kérdés, hogy az üzemeltett infrastruktúra esetén nemcsak az üzembiztonság, hanem az információbiztonság, tágabban véve a kiberbiztonság is olyan szempont, amelyet figyelembe kell venni. Nehéz viszont felmérni, hogy valójában mekkora a fenyegetettség az olyan kritikus infrastruktúrák esetén, mint amilyen például a vízi közművek. A következőkben azokat a kihívásokat ismertetjük, amelyek mind a klasszikus SCADA/

ICS-rendszerekre, mind pedig az új típusú okos-infrastruktúrákra vonatkoznak, kiemelve mind a biztonságpolitikai, mind pedig a műszaki kihívásokat.

Orbók az okosvárosok biztonsági kihívásait így foglalja össze: „A kibertér biztonsági kockázatainak befolyása a fizikai világra jelentősen megnövekszik, így közvetlenül hatással lesznek majd a személyes biztonságunk és a közösség biztonságának minden területére, függőségünk és a kiszolgáltatottságunk jelentősen megnő."[15] Ennek a kiszolgáltatottságnak a mértékét azonban egyelőre csak sejtjük, a bizonyosságot a következő évtizedek fogják elhozni. Az amerikai U. S. Department of Homeland Security *The Future of Smart Cities: Cyber-Physical Infrastructure Risk* című tanulmánya azonban megpróbálja előrejelezni, mi vár a legfontosabb közművek üzemeltetőire a digitális átalakulás folyományaként. A kiadvány a közlekedés, az energiaellátás és a vízi közművek területén mutatja be, hogy milyen kockázatokkal fognak szembesülni ezek az alapvető infrastruktúrák.

A vízi közművek területén az okosvízkezelésben két példát hoz a tanulmány a kibertámadásra. Az egyik lehetőség, hogy kibertámadás éri a vízkezelő központot, és ezen keresztül olyan hatást érnek el a támadók, amely hathat a közegészségügyre. A másik példa, hogy az információs rendszereken keresztül a támadó tönkreteszi a vízbázist, és ezzel okoz környezeti katasztrófát. A következő ilyen példa az okosvízelosztásnál jelentkezik. Az első, hogy egy rosszindulatú támadó távolról behatol a rendszerbe, és lekapcsolja az érzékelő szenzorokat, így szennyezett víz kerül a háztartásokba, a másik példa pedig, hogy a támadó rendkívüli időjárási helyzetben teszi lehetetlenné a felgyűlt csapadékvíz elvezetését. Az okosvíztárolásnál a példatámadások úgy szólnak, hogy egy rosszindulatú támadó távolról manipulálja a víztárolók berendezéseit, ezzel áradást okoz, illetve egy rosszindulatú támadó az internetről behatolva zavarja meg a biztonsági berendezéseket, ezzel fedve el a potenciális vészhelyzetet.[16]

Mindhárom példa nagyon jól mutatja, milyen problémákat tud okozni az okoseszköz a vízi közművekben. De ha stratégiai szinten vizsgáljuk a közeljövőt, célszerű kitérni az államilag szervezett kibertámadásokra is. Ezen kihívások közül is érdemes figyelembe venni azt, hogy a negyedik ipari forradalommal párhuzamosan számos olyan, korábban nem látott lehetőség nyílik a nagy befolyással rendelkező, elsősorban gyártó államok számára a kibertéri befolyásolásra, amelyekre sem a vízi közműveknél, sem általában a kritikus infrastruktúrák esetében nem vagyunk felkészülve. Gondoljunk itt például az ötödik generációs mobilhálózatok kérdéskörére: a kínai gyártókkal szembeni kérdések és kétségek elsősorban azért merülnek föl, mert az okosvárosok, így az okosközművek kommunikációját ezeken az ötödik generációs mobilhálózatokon keresztül lehet a legideálisabban megoldani, márpedig ha egy államnak lehetősége van az állam területén belül működő gyártókon keresztül hatni az okosváros-infrastruktúrákra, akkor nyilvánvalóan ez egy előre nem látott nemzetbiztonsági kihívást jelenthet majd.

[15] Orbók 2018

[16] Office of Cyber and Infrastructure Analysis 2015

Emellett a gyártók is okozhatnak nem várt kiberbiztonsági problémákat. Példaképp lehet említeni azt, hogy a korábban említett okosasszisztensek mindegyikéről kiderült, hogy a gyártó nem az információbiztonság és az adatvédelem alapvető eljárásai szerint jár el, hiszen az okosasszisztenseknek mondott parancsok több gyártó esetében is embernél landoltak. Állítólagos minőségbiztosítási okokból ugyanis a gyártók munkatársai hallgatták végig azt, mi minden történik a háztartásokon belül, így a gyártók korábbi állításaival szemben, miszerint csak a mesterséges intelligencia dolgozza föl a hangot, ez bizonyítottan többeknél nem teljesült. Gondoljunk csak bele, milyen kihívást jelenthet, hogy ha az okosvárost felépítő alap-infrastruktúrákban is ilyen tervezési hibák vannak, akár szándékosan, akár nem szándékosan, amelyek révén a gyártó is hathat az okos-infrastruktúra működésére! Gondoljuk csak végig, milyen kockázatot jelentene az, ha az okosvárost építő infrastruktúra-elemek mögött egy rosszindulatú országot vagy egy rosszindulatú gyártót kellene sejtetni!

Kiberbiztonság az okos-villamosenergetikában

Az energiatermelés, -átvitel, -elosztás és -fogyasztás forradalmi változása mutatja meg talán legjobban az okoseszközök helyét ebben a közműszektorban. A világ energiafelhasználása kétségtelenül évről évre egyre nagyobb, miközben az energiatermelés módszereinek mindenképpen változniuk kell, hiszen a klímaváltozás kikényszeríti a szénhidrogén-alapú energiatermelés visszaszorítását. Mindez elősegíti a kisebb, megújuló energiatermelők előretörését, mint például a szélerőművek, napenergiafarmok megépítését. Ezek azonban, jellegüknél fogva, akkor termelnek, amikor fúj a szél és süt a nap. Sajnálatos módon Európa középső részén a téli időszakban, amikor a legnagyobb energiafogyasztás történik, jellemzően nem süt a nap és szélcsend van, így a nem megújuló forrásokra épülő erőművek még addig működésben maradnak, ameddig a nagy volumenű energiatárolás meg nem valósul. A „régi” és az „új” megoldásoknak tehát együtt kell működniük, egyszerre kell a létrehozott energiát úgy irányítani, hogy néhány, jól tervezhetően működő alaperőmű és sok tízezer, környezeti hatásoktól függő kis energiatermelő megbízhatóan 230 V és 50 Hz feszültséget adjon a háztartási aljzatokban. Ez összehangolt informatika nélkül nem lenne lehetséges.

Mindeközben a felhasználói oldal energiafogyasztása is változik. Ma már nem a nagyfogyasztású hűtőszekrény kiszámítható, egész napos fogyasztása a meghatározó, hanem az éjszakára töltőre tett okoseszközöké, amelyek közé a legnagyobb fogyasztók, mint az elektromos autók is oda értendők. Az okoseszközök hatását jól lehet mérni azzal, hogy a koronavírus miatti otthoni munkavégzés és távolléti oktatás alatt az energiafogyasztás szerkezete érdemben változott meg. A MAVIR adatai alapján az Energiaklub kimutatta, hogy jelentősen kevesebb energiát fogyasztottak a kijárási korlátozás első két hetében Magyarországon (6000–6200 MW helyett 5700–5800 MW-ot), illetve az is kimutatható, hogy a korábban reggel 8 óra körül jelentkező első napi terhelési csúcsok dél körülre tolódtak el, és többször meghaladták a korábban rendre magasabb, este 7 óra

körül mutatkozó második napi terhelési csúcsokat.[17] Mindeközben 2020. április 16-án termelési csúcsot sikerült elérni a napenergia-termelés terén, aznap 942,8 MW-ot sikerült elérni, amelyből a háztartási kiserőművek akár 30–40%-kal is részesülhettek, hiszen ezek együttes teljesítménye 460,77 MW volt ebben az időszakban a közlés szerint.[18]

A változó termelés és fogyasztás kezelésének a megoldása az okoshálózatokban, azaz smart gridekben rejlik. Definíció szerint „a smart grid (SG) elképzelés kiindulópontja az, hogy az intelligens, oda-vissza vezérelt és ellenőrzött fogyasztás decentralizált erőművi mikrorendszereket képes integrálni. A smart grid technikával a jelenlegi hálózati túlterheltség, a nagy hálózati veszteség és az erőművek rugalmatlansága részben orvosolható, növelhető továbbá az energiahatékonyság, illetve a megújulók integrációja [lehetővé válik]. […] A harmadik lépésben kezdődik el a valódi smart grid kiépítése, miközben a már megszokott rendszer öregszik. A hatásfokok romlanak, a veszteségek emelkednek. Az új struktúrában már lehetőség lesz kisebb erőművi termelők lokális hálózatra kapcsolására. Fontos kiemelni, hogy a smart grid, amely lényegét tekintve egy irányítási technika, a hagyományos hálózatra építve képzelhető el, és nem izolációs célként".[19]

Az okoseszközök megjelenésének első példája a háztartási villamos energetikában az okosmérő, azaz a smart metering. Ez Haddad Richárd összefoglalója szerint azt jelenti, hogy „[a]z okos mérési rendszerek lehetőséget adnak arra, hogy a szolgáltatók és a hálózatüzemeltetők a végfogyasztókra lebontva képesek egyedi adatszolgáltatásra. Ennek az egyik legfontosabb előnye, hogy a fogyasztók az elfogyasztott energiával, valamint a hálózatban lévő energia költségével arányosan fizetik meg a felhasznált energiát. Mint ismeretes, a különböző napszakokban más és más energiaforrások (különböző költségen termelő egységek) érhetők el. Az okos mérési rendszerek transzparenssé tudják tenni a felhasználás és a költség mértékét".[20] A smart metering eszközei valójában hálózatra kapcsolt informatikai megoldások, azaz a dolgok internetének részei. Elsődleges funkciójuk, hogy a fogyasztási adatokat elküldjék a szolgáltatóknak. Azonban logikus lépés lenne, hogy ne csak a szolgáltató, hanem a fogyasztó is percre pontosan értesüljön az aktuális fogyasztásáról, hiszen ezen adatok alapján ő is optimalizálni tudja otthona energiafelhasználását. Ha tehát a smart metering megoldása felkerül az otthoni vezetéknélküli hálózatra, és az adatokat az okosasszisztens számára is rendelkezésre bocsájtja, az az előre meghatározott fogyasztási szabályok alapján tudja ki- és bekapcsolni az okosotthon eszközeit. További lépés lenne, ha ezek az adatok az otthont segítő mesterséges intelligencia számára is elérhetővé válnak, így a szabályokon túlmenően még rugalmasabb, jobb döntéseket tud hozni az okosotthon, jelentős energiamegtakarítást lehetővé téve. Ez az úgynevezett „edge AI", azaz határon, az otthonban történő mesterséges intelligencia is 2–5 éven belül valósággá válik a Gartner már idézett elemzése szerint. Az okosközmű és az okosotthon tehát összeér, a kiberbiztonság és főleg az adatvédelem

[17] Zsolt 2020
[18] MAVIR 2020
[19] Baranya–Csernus 2018
[20] Haddad 2018

elkerülhetetlenné válik a szolgáltatói oldalon, hiszen ha nem terveznek megfelelően, nemcsak saját létfontosságú rendszereik, de felhasználóik is veszélybe kerülhetnek.

A U. S. Department of Homeland Security okosváros-biztonsággal foglalkozó tanulmányában jól nyomon követhető, mely pontok lehetnek sérülékenyek az okos-villamosenergetikában. Az első ilyen felület az okoserőművek körében fedezhető fel. A kutatók három példát említenek. Az első szerint a támadó hozzáférést szerez a SCADA/ICS-rendszerhez azok nem megfelelő hálózati szegmentációja miatt. A második példát az élet számos esetben igazolta, és a későbbiekben vissza fogunk rá térni. Eszerint a támadó jogosulatlan hozzáférést szerez az erőmű hagyományos IT-rendszereihez. A harmadik példa pedig a már említett „régi" és „új" rendszerek nem megfelelő együttműködése, ami komoly rendelkezésre állási és sértetlenségi hiányosságokhoz vezethet. Az okoselosztás és -átvitel a smart grid problémakörét mutatja be. A két példa szerint egy rosszindulatú támadó kompromittálja az átviteli rendszert, ezzel megfosztva a felhasználókat az áramellátástól, azaz klasszikus rendelkezésre állás problémát okoz. A másik forgatókönyv szerint egy rosszindulatú támadó manipulálja az energiaárakat mutató adatokat, emiatt a rendszer inkonzisztens módon irányítja a megtermelt energiát, felhíva ezzel a figyelmet arra, hogy az energiatermelésben nem néhány szereplő van csak, mint korábban, hanem a háztartások tömegei is eladnak áramot az országos hálózatba az általuk megtermelt, de nem felhasznált napenergia segítségével. A kutatók az okosmérőhelyek, azaz a smart metering támadásaival is foglalkoztak. Elképzelésük szerint a mérőhelyek elleni támadással a háztartások áram nélkül maradnak, illetve sikeres támadás esetén a támadó be tud jutni akár a háztartások belső informatikai hálózatába.

Az okosközlekedés kiberbiztonsági szempontjai

Az okosközlekedés kialakítása talán a legégetőbb a három mintaként kiválasztott terület közül. A nagyvárosok közlekedése ugyanis már ma is a legtöbb helyen élhetetlen helyzetet teremt, a városi légszennyezés elsődleges forrásaként a városlakók mentális egészsége mellett fizikai jólétüket is veszélyezteti. Az önvezető autók mellett számos más innovatív megoldás is segíti az okosközlekedés kialakítását, például az autómegosztó szolgáltatások, vagy éppen a közlekedési viszonyokat másodperces pontossággal figyelő navigációs applikációk. Ezt az ökoszisztémát együttesen Intelligens Közlekedési Rendszernek (Intelligent Transport System – ITS) nevezik. Kialakításának fontosságát mi sem jelzi jobban, mint hogy az Európai Unió külön irányelvben szorgalmazta ennek létrehozását már 2010-ben. Ez az Európai Parlament és a Tanács 2010/40/EU irányelve (2010. július 7.) az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről.

Bódi Antal összefoglalója szerint „[a]z intelligens közlekedési rendszerek nagyvárosi alkalmazásának operatív célja a várost érintő hazai, adott esetben nemzetközi tranzitforgalom, a nagyvárosi agglomerációs forgalom és a városon belüli forgalom egyenletesebb, kevesebb zavarral járó és kontrollált, ezáltal biztonságosabb és kevesebb környezeti ter-

heléssel járó lebonyolítása. Ezzel párhuzamos távlati, stratégiai célja pedig a közlekedők környezetkímélőbb közlekedési módok használatára való ösztönzése, az új közlekedési formákra való váltás kedvező feltételeinek megteremtésével, illetve ezen közlekedési módok szolgáltatási színvonalának emelésével".[21] Jelenleg talán ez a legösszetettebb ökoszisztéma, kiberbiztonsági szempontból viszont talán kevésbé van szem előtt, mint a másik két ágazat.

Ettől függetlenül természetesen a U. S. Department of Homeland Security okosváros-biztonsággal foglalkozó tanulmánya itt is megemlít néhány példát, amelyeket célszerű komolyan venni. A kiadvány rögtön az autonóm közlekedés veszélyeivel kezd, megemlítve, hogy az informatikai vezérelt járműveket kibertámadás útján el is lehet téríteni, illetve ha egy kártékony kód tönkreteszi az autonóm jármű szenzorait, akkor az irányíthatatlanná válik, működése nem biztosítható tovább. Az intelligens közlekedésirányító rendszerek esetében elképzelhető, hogy egy rosszindulatú támadó egy természeti katasztrófa idején úgy befolyásolja az eszközöket, hogy azok ne működjenek megfelelően, ezzel csapdába ejtve az embereket, illetve lehetséges, hogy a támadó manipulálja a rendszer adatait, ezzel aláásva a hosszú távú biztonságot és megbízhatóságot. A gépjárművek közötti úgynevezett vehicle-to-vehicle (V2V) és a gépjárművek és működésüket segítő infrastruktúra-elemek közötti, azaz vehicle-to-infrastructure (V2I) kommunikáció esetén a példák szerint előfordulhat, hogy egy rosszindulatú támadó manipulálja a V2V- és V2I-jeleket, illetve nem elképzelhetetlen, hogy egy kiberbűnöző megzsarolja a gépjármű-tulajdonosokat vagy -gyártókat például azzal, hogy zsarolóvírussal fertőzi meg ezeket az eszközöket.

A SCADA/ICS-közműrendszerek fenyegetettsége

A jövő kihívásait a múlt eseményeivel lehet a legjobban szemléltetni. A közművek ipari irányítási rendszerei elleni kibertámadások ugyanis nem újkeletűek. 2009-ben szerzőtársammal, Dr. Kovács Lászlóval tartottam több előadást *Digitális Mohács* címmel, amelyben egy elképzelt, összehangolt kibertámadás forgatókönyvét mutattuk be Magyarország ellen. Ez az előadás folyóiratcikk formájában is megjelent, és a következő mondattal zárult: „Gyakran elhangzó vélemény jelen tanulmány szerzőitől is: nem az a kérdés, hogy egy ilyen támadássorozat bekövetkezik-e, hanem az, hogy mikor fog bekövetkezni."[22] Az egyik ilyen előadás után egy vízi közműnél dolgozó, információbiztonsággal foglalkozó kolléga jött oda hozzánk, és csak ennyit mondott: „Ez nem az a téma, amelyet a nyilvánosság előtt kéne kibeszélni, ne adjunk ötleteket az ellenfeleinknek." Eltelt több mint 10 év, megjelent a *Digitális Mohács 2.0,* az élet pedig folyamatosan igazolta vissza mindazt, amit az eredeti cikkünkben feszegettünk. Szerzőtársam pedig azóta dandártábornoki minőségben a Magyar Honvédség Parancsnokságának kibervédelmi szemlélője, beosztásából adódóan hivatalból azzal foglalkozik, hogyan védekezhetünk

[21] Bódi 2019
[22] Kovács–Krasznay 2010

az országunkat a kibertérből érő katonai csapások ellen, illetve a NATO keretein belül hogyan tudunk hozzájárulni a kibertéri műveletek kivitelezéséhez. Célszerűnek tűnik tehát, hogy minél nagyobb nyilvánosság előtt beszéljünk arról, mi is történt az elmúlt 10 évben, melyek azok az okok, amelyek miatt a létfontosságú rendszerek védelme során a szakmának oda kell figyelnie a kiberbiztonságra.

A történet nem sokkal a *Digitális Mohács* cikkünk megírása után kezdődött. Pontosabban akkor került nyilvánosságra, hiszen a Stuxnet nevű kártékony kódról beszélünk, amely izraeli-amerikai közös katonai műveletként évekkel korábban indult, célja pedig az volt, hogy megakadályozza vagy legalábbis hátráltassa Irán nukleáris ambícióit.[23] A Stuxnet nevű kártékony kód működése, a részletekbe nem belemenve, azt a célt szolgálta, hogy az iráni urándúsító centrifugákat különböző, az optimálistól jelentősen eltérő fordulatszámon hajtva azokat a lehető leghamarabb tönkre tegye, így lehetetlenné téve a fegyvertisztaságú urán létrehozását. A kód azt a Windows operációs rendszert fertőzte meg, amelyen az ipari vezérlő szoftver futott, ezen keresztül közvetlenül a PLC-ket irányította, miközben az operátorok által figyelt képernyőn látszólag a megfelelő adatok jelentek meg, tehát elfedte a valódi üzemi adatokat a szoftverben. Mivel az üzemeltetők a szemüknek, azaz a meghamisított adatoknak hittek, sokáig nem értették, mi okozhatja a leállásokat. A művelet amerikai–izraeli szempontból totális siker volt, Irán feladta nukleáris fegyverkezési programját anélkül, hogy emberek haltak volna meg (legalábbis nyílt háborúban, a titkos műveletek áldozatairól még sejtésünk sem lehet).

A SCADA/ICS-rendszereket használó mérnökök számára a Stuxnet volt az első olyan szemnyitogató támadás, amelynél a korábban alaptézisként szolgáló elveket felül kellett vizsgálni. Először is a támadás közvetlenül hatott a vezérlésre, a humán-gép interfész (Human-Machine Interface – HMI) nem mutatott eltérést, így megdőlt a rendszer megbízhatóságába vetett hit. Másodszor a rendszer nem volt elérhető az internet felől, egy szigorúan védett katonai objektumba tudtak kártékony kódot bejuttatni, amely autonóm módon éveken keresztül működött. Harmadszor kiderült, hogy van az az anyagi és emberi erőforrás, amellyel egy ennyire speciális rendszert is kompromittálni lehet. Ami pedig talán a legtragikusabb felismerés volt, hogy az üzembiztonság erőteljesen függ az informatikai biztonságtól, tágabb értelemben véve a kiberbiztonságtól, holott erre az ipari környezetben sem az üzemeltetők, sem pedig az üzemeltetett rendszerek nem voltak felkészülve.

Természetesen a kiberfizikai rendszerek biztonságának kérdése nem újkeletű, a 2010-es években viszont számos olyan incidens történt, amelyek eredményeképp a termelésirányító rendszerekkel foglalkozó mérnökök eljutottak oda, hogy kénytelenek a kiberbiztonsági kérdésekkel is foglalkozni. Az OT (operational technology) és az IT (information technology) olyan szoros szinergiát alakított ki, annyira elválaszthatatlanok egymástól, hogy a szakterületek együttműködése elkerülhetetlen. Különös tekintettel arra, hogy a negyedik ipari forradalom hatásaként a közművek területén is sorra jelennek meg azok az okosmegoldások, -szenzorok, hálózatba kapcsolt ipari okoseszközök (Industrial

[23] Kovács–Sipos 2010

Internet of Things – IIoT), amelyek kiberbiztonsági hatásai egyelőre felmérhetetlenek. A tudományos közösség aktívan foglalkozik a témával, a Google Scholar tudományos keresőbe beírva a „cyber attack water" keresőszót például 54 000 potenciálisan érdekes cikket találhatunk, a gyakorlat azonban egyáltalán nem érte utol a tudósok elméleti eszmefuttatásait.

Kibertámadások a közművek ellen

De ki és miért támadna közműveket a kibertérből? Mi az indok, amiért országok vállalják, hogy súlyosan megsértik a nemzetközi humanitárius jog azon pontját, amely a civil objektumok védelméről szól? Hiszen az informatikai rendszereken keresztül történő beavatkozások olyan hatásokkal járhatnak, amelyek a akár a vízbázist, a biztonságos vízellátást vagy éppen a villamosenergia-ellátást veszélyeztetik, amelyek nélkül a modern társadalom működésképtelen. Számos olyan esettanulmány létezik, amelyek bemutatják a kritikus infrastruktúrák kitettségét. Két példán keresztül szeretném bemutatni azokat az okokat, amelyek miatt a vizes szakma képviselői sem aludhatnak nyugodtan. Az első eset még 2013-ban történt, amikor iráni hackerek jutottak be egy New York melletti gát vezérlőrendszerébe.[24] Az eset nem kavart túl nagy vihart a közvéleményben, holott egy nagyobb, komplexebb képbe illik bele. A már említett Stuxnet mellett számos olyan, kiberteret érintő esemény történt, amely az amerikai-iráni relációt terhelte. Iráni részről a Twitter-fiókok feltörésétől kezdve, amelyeken propagandát terjesztettek, a kifinomult, kőolajtermelést érintő kibertámadásokig (Shamoon, szaúdi célpontok ellen) különböző intenzitású, de saját stratégiai céljukat szolgáló műveleteket láthattunk, amelyeket hatékonyan, jó hatásfokkal hajtottak végre, de érezhetően egy bizonyos komplexitást már nem tudtak átlépni. Az amerikaiak eközben 2019-ben képesek voltak iráni katonai célpontokat semlegesíteni pusztán kiberműveletekkel, illetve olyan iráni katonai vezető célzott likvidálására is sor került, aki a kiberbiztonsági terület felelős vezetője volt.

Ennek az adok-kapoknak a sorába illeszkedett ennek a bizonyos gátnak, a Bowman Damnek a számítógépes rendszerébe történő behatolás. A híradások mellett a különböző szakkonferenciák előadásaiból lehet rekonstruálni, mi is történt valójában. A banálisan egyszerű probléma az volt, hogy ez a gát egy viszonylag jelentéktelen közmű volt, amelyet természetesen nem őriztek 24 órában, hanem interneten keresztül tudtak belépni a vezérlő számítógépre, ha erre szükség volt. Az iráni támadó véletlenül, egy egyszerű Google-kereséssel talált rá a számítógépre, amelynek belépési felhasználóneve és jelszava az admin/admin volt. Bár a manipulációra nem nagyon volt lehetőség, az iráni propaganda mégis hatalmas győzelemként tudta eladni ezt a hacket a hazai közönségnek. A támadó haszna ebben az esetben tehát a propagandagyőzelem volt, illetve egy újabb figyelmeztető jelet sikerült küldeni az amerikai kormányzatnak arról, hogy a kritikus infrastruktúráik közel sem sérthetetlenek.

[24] Francescani 2016

A második eset ennél lényegesen komolyabb és figyelmeztetőbb. Az érintett országok Oroszország és Ukrajna, az időpont 2018. A Krím-félsziget annektálása és Kelet-Ukrajna elszakadási törekvéseinek támogatás miatt ekkor már negyedik éve folyt a sem nem béke, sem nem háború a két ország között. Oroszország az USA és Kína mellett az az ország, amelynek kiberképességei messze a többi ország fölé emelkednek. A híradások szerint az ország keleti felében, Dnyipropetrovszk megyében lévő Auliban működő klórdesztillációs állomást érte a támadás a hálózati rendszeren keresztül. A támadás hátterében a VPNFilter nevű kártékony kód állt.[25] A támadást az ukrán biztonsági szervek meghiúsították. A VPNFilter többfunkciós támadó kód, amely otthoni és kisvállalati routereket fertőz, amelyeket gyakran használnak közművek adatátviteli rendszereiben. Funkciói az adatgyűjtés, amely segít megérteni, hogyan működik az adott kritikus infrastruktúra, a beavatkozás, amelynek segítségével bizonyos hálózati elemek elérhetetlenné válnak, illetve feltehetően a router teljes törlése, amely után az adott hálózati szegmens működésképtelenné válik.[26]

Bár nincsenek arra bizonyítékok, hogy a klórdesztillációs állomás támadásával tömegkatasztrófát akartak volna előidézni, az bizonyosnak látszik, hogy a kártékony kód segítségével az orosz fél törekedett az ukrán kritikus infrastruktúrák működésének teljes feltérképezésére, ahogy azt egyébként tette más országokban is. Legalábbis a brit és az amerikai kormányzatok közzététele alapján orosz felderítő tevékenységet fedeztek fel az országok villamosenergia-rendszereiben. Az is biztos, hogy 2015-ben és 2016-ban komolyabb áramkimaradások történtek Ukrajnában, köszönhetően orosz eredetű kibertámadásoknak. A 2015-ös BlackEnergy támadás után például 230 000 ember maradt áramellátás nélkül decemberben.[27] A 2015-ös esemény különösen szofisztikált támadás volt. 2015. december 23-án, tehát karácsony előtti nap, kora délután indult az akció, a nyugat-ukrajnai, tehát az orosz-ukrán konfliktusban az Oroszország szempontjából ellenérdekelt területen. A Kyivoblenergo nevű áramszolgáltatónál az ügyeletes üzemmérnökök azt tapasztalták, hogy az alállomási távkezelésért felelős számítógépes rendszerbe valaki távolról belépett, és megpróbálta lekapcsolni a lakossági áramellátást biztosító alállomásokat. Végül összesen 30 darab, 110 kV-os és 35 kV-os alállomást sikerült kiiktatni.[28] Mi a támadó motivációja? Nyilvánvalóan a nyomásgyakorlás, a biztonságérzet csökkentése oly módon, hogy ne lehessen egyértelműen kijelenteni, háborús cselekmény történt.

A katonai tevékenységeknek tehát velejárójuk a kibertéri műveletek összessége. Nem véletlen, hogy a NATO 2016-ban a kiberteret a negyedik műveleti térnek ismerte el, jelezve, hogy a föld, a víz és a levegő mellett itt is számítani kell mind védelmi, mind támadó képességfejlesztésre. A már most is komoly képességekkel rendelkező országok pedig nem félnek felhasználni a kiberteret saját céljaik elérésének támogatásához. Bár a sajtó elsősorban Kína és Oroszország tevékenységével foglalkozik, egyre többet enged

[25] Bolcsó 2018
[26] Symantec 2018
[27] Lipovsky–Cherepanov
[28] Pongrácz 2019

láttatni az Egyesült Államok is saját képességeiből, de például Nagy-Britannia is saját kiberműveleteit emelte ki az ISIS terrorszervezet visszaszorításával kapcsolatban. A jövő pedig még több kihívást tartogat. Gondoljunk itt csak arra, hogy a már említett IIoT elterjedésének alapfeltétele az 5G-s kommunikációs hálózatok kiépítése, márpedig aki kontrollálja az átviteli hálózatot, az kontrollálja többek között az „okos" közműveket is. A kínai Huawei körüli polémiát és az amerikai aktivitást ezen a területen érdemes tehát ebben a kontextusban is vizsgálni. Nem is beszélve arról, hogy a kiberbűnözői csoportok is egyre jobban vizsgálják, hogyan lehet az alapvető infrastruktúrákat sikeresen támadni.

Az ICS/SCADA-rendszerek biztonsága

A probléma nagyságát jól illusztrálja a BlackCell Kft. nemrég publikált tanulmánya, amely *ICS/OT snapshot 2019* címmel jelent meg, és részletesen áttekinti, milyen állapotban vannak a magyarországi ipari infrastruktúrák kibervédelmi szempontból.[29] A tanulmány írói a shodan.io szolgáltatás, az „ipari rendszerek Google-ja" segítségével keresték meg azokat az interneten elérhető ICS/SCADA-rendszereket, amelyek Magyarországon vannak. Összesen 2013 ilyen rendszert találtak. A feltárt eszközök között megtalálhatók PLC-k és egyéb kontrollerek, HMI-eszközök és webes felületek, különböző kiegészítő modulok, webes menedzsment- és monitoringeszközök, ipari switchek, átalakítók, illetve egyéb eszközök, amelyek felhasználása köthető valamilyen ipari vagy más, vezérléstechnikai (például épületvezérlési) tevékenységhez. Ezek közül számos eszköz tűnt sebezhetőnek elavult firmware, gyenge kriptográfia vagy akár nem megfelelő hitelesítés miatt. A vízellátással és energiával kapcsolatos protokollokat többször is említi a tanulmány. Egyrészt a DNP3-protokollt nevesíti, amely szabványos kommunikációs eljárást használó eszközök közül tizenkettőt találtak az interneten a kutatók, mindegyiket Budapesten, másrészt felsorol néhány gyártót, mint például a Saia-Burgess Controls (SBS) nevű céget, amelynek 134 termékét találták meg, kivétel nélkül sebezhető firmware-t futtatva, illetve a Siemens S7 családot, amelyből 75 darabot találtak az interneten. A napelemek vezérlésére használt Fronius-megoldásból is jutott 82 hazai telepítés a kibertéri érdeklődők számára. Nem maradt ki a közlekedési szektor sem: az elektromos gépjárművek töltésében használt Etrel-megoldásból 6 volt elérhető Magyarországon a nyílt hálózat felől. A shodan.io egyébként több mint 6000 találatot ad ki a „water", 3000 találatot az „energy" szóra keresve.

Természetesen mindez nem jelenti azt, hogy az ipari rendszerek triviálisan törhetők lennének. Eleve érdemes észrevenni, hogy a példaképp hozott támadások jellemzően olyan rendszereket értek, amelyek informatikai szempontból könnyen hozzáférhetők, tehát a HMI-gépek, amelyek jellemzően valamilyen, többnyire elavult, nem frissített Windows operációs rendszert futtatnak, vagy pedig a hálózat olyan elemei, amelyek Linux-alapúak. A célrendszerek, a PLC-k és azok speciális protokolljai egyelőre olyan nehezen áttörhető akadályt jelentenek, amelyet csak felkészült, megfelelő emberi és anyagi erőforrással

[29] Kocsis 2019

rendelkező titkosszolgálatok és hadseregek tudnak megugrani. Természetesen ez nem azt jelenti, hogy ne lenne példa ilyen támadásokra, hiszen a Stuxnet után folyamatosan jelentek meg hírek olyan kártékony kódokról, amelyek „beszélnek SCADA-ul". A 2016-os ukrán áramkimaradást okozó Industroyer nevű kártékony kód például az IEC 60870-5-101, IEC 60870-5-104, IEC 61850 és az OLE for Process Control Data Access (OPC DA) protokollok mindegyikén tudott kommunikálni.[30]

A kiberbiztonsági szakértő szemében tehát az HMI és az oda vezető hálózat a legkritikusabb. Egy olyan infrastruktúra, amely szélsőséges esetben nem más, mint egy információbiztonsági szempontból rosszul megírt szoftver, amely egy frissítés nélküli, elavult operációs rendszeren fut, látszólag szeparáltan, légréssel védve, de valójában az internetről elérhető módon, egy olyan tagolatlan hálózatban, ahol minden eszköz egy szegmensben van, amelyhez ráadásul az üzemeltetés miatt harmadik felek is hozzáférnek távolról. A HMI után következő infrastruktúra-elemek, a szenzorokkal, PLC-kkel pedig egy olyan világot tár fel, ahol nagyon sok esetben esély sem mutatkozik az információbiztonsági alapelvek teljesítésére, hiszen egy víruskereséssel vagy akár csak egy logüzenet legenerálásával sem lehet veszélyeztetni az üzembiztonságot, hiszen minden, ami információbiztonság, akár milliszekundumos késleltetést is jelenthet, ami sokszor nem megengedhető.

A támadási eljárások megértéséhez a DragonFly 2.0 elnevezésű kampányt hozom példának, amely energetikai szereplőket támadott, gyaníthatóan orosz háttérrel.[31] Az alábbi lépések pontosan bemutatják, mi mindent kell tennie a támadónak a sikeres betöréshez. A hét felsorolt lépés egyébként a kiberbiztonsági szakterületen gyakran használt Cyber Kill Chain nevű modellt is ismerteti, gyakorlatilag minden támadás ezt követi, egyben jelzi, milyen sok lehetősége van egy potenciális áldozatnak a védelem kialakítására.

1. szakasz: felderítés. Ekkor történik az áldozat feltérképezése. A konkrét esetben például a támadók letöltöttek egy kis fényképet az egyik áldozat nyilvánosan elérhető HR-oldaláról. A kinagyított kép egy nagy felbontású fotó volt, amely a vezérlőrendszerek berendezéseinek modelljeit és az állapotinformációkat jelenítette meg a háttérben.

2. szakasz: fegyverkészítés. Ez a konkrét támadó kód kialakítását jelenti. Példánkban a támadók egy speciális e-mail-mellékletet állítottak össze, így használták ki a Microsoft Office legális funkcióit. Ezzel a módszerrel dokumentumokat tudtak letölteni egy távoli kiszolgálóról az SMB- (Server Message Block) protokoll használatával. Az ismert támadások nagyjából felében a dokumentumokat folyamatirányítással, ICS-sel vagy kritikus infrastruktúrával kapcsolatos kereskedelmi kiadványokban és információs webhelyeken helyezték el. Ezen lépéssel tudták felderíteni a potenciális áldozatok körét és az általuk használt informatikai megoldásokat.

3. szakasz: kézbesítés. Ebben a fázisban történik a konkrét támadó kód célzott eljuttatása. Célzott adathalász e-mailekben általános szerződési megállapodásnak tűnő témát használtak (a „SZERZŐDÉS & Bizalmas" tárgysorral), amely egy általános PDF-do-

[30] Lipovsky–Cherepanov 2016
[31] Symantec 2016

kumentumot tartalmazott, amelynek neve document.pdf volt. A dokumentum rövidített URL-t tartalmazott, amelyre kattintva a felhasználók egy olyan webhelyre érkeztek, amely e-mail-címet és jelszót kért a felhasználótól. Az e-mail-üzenetek ipari vezérlőberendezésekre és protokollokra való hivatkozásokat tartalmaztak. Bizonyos esetekben az e-mailek olyan rosszindulatú Microsoft Word-mellékleteket használtak, amelyek valódinak önéletrajzoknak tűntek az ipari irányítórendszerrel foglalkozó munkatársak számára, valamint meghívókat és szabályzatokat tartalmazó dokumentumokat is küldtek, rávéve a felhasználót arra, hogy megnyissák a mellékletet.

4. szakasz: kihasználás: Ilyenkor történik a rosszindulatú kód futtatása. A célpont fertőzésére a támadók rosszindulatú.docx fájlokat használtak, amelyekben a kártékony kód a felhasználói hitelesítő adatok rögzítésére szolgált. Amikor egy felhasználó megkísérelte hitelesíteni magát a hálózatban, a támadó által üzemeltetett külső szerver megkapta a jelszó lenyomatát (hash).

5. szakasz: telepítés. A támadó ekkor veti meg a lábát hosszabb távra a számítógépen. A támadók a kompromittált hitelesítő adatokat használtak az áldozatok hálózatainak eléréséhez, de csak ott, ahol nem használták a kétlépcsős hitelesítést. A hozzáférés fenntartása érdekében a támadók helyi adminisztrátori fiókokat hoztak létre a célponthálózatban, és rosszindulatú fájlokat helyeztek el a feltört gépeken.

6. szakasz: irányítás és vezérlés. Ekkor történik a kommunikáció, a feladatok kiadása a kompromittált hálózaton. A támadók távoli elérést lehetővé tevő szoftvereket, úgynevezett remote shelleket telepítettek a nyilvánosan elérhető e-mail- és webszervereken.

7. szakasz: célokkal kapcsolatos tevékenységek. Miután a támadók a kiszemelt célhálózatban voltak, kiemelt jogosultságot szereztek és használták fel az áldozat domainvezérlőjének kompromittálásával, általában RDP-protokollon keresztül. A támadók többször is hozzáfértek olyan munkaállomásokhoz és szerverekhez a vállalati hálózaton, amelyek az energiatermelő létesítmények vezérlőrendszereiből származó adatokat tartalmaztak. A támadók hozzáfértek az ICS/SCADA-rendszerekhez kapcsolódó fájlokhoz is.

Ha pedig sikerül eljutni erre a szintre, akkor már bármi történhet. 2018-ban az NCC Group nevű kiberbiztonsági cég egyik ügyfele megbízásából hajtott végre tesztet egy energetikai ipari irányítási környezetben. A cél az volt, hogy kipróbálják, mekkora károkat okozna a NotPetya kiberfegyver, ha bejutna egy ilyen infrastruktúrába. Az ICS Cybersecurity Blog így foglalta össze a teszt eredményét: „A módosított malware-t egy mérnöki hálózatban engedték szabadon és semmilyen jogosultságot nem kapott a hálózaton található eszközökön. Első körben a módosított malware három, az EternalBlue sérülékenység ellen nem patch-elt számítógépet talált. A malware-be kódolt exploit-ot használva a NotPetya mindhárom sérülékeny számítógépen kernel szintű jogosultságot szerzett, majd ezzel a jogosultsággal megfertőzte ezeket a számítógépeket. Tíz percen belül az első három számítógépről szerzett felhasználónevekkel és jelszavakkal a teljes mérnöki hálózatot átfésülte további megfertőzhető eszközöket keresve. Két további perccel később a malware átvette az uralmat a teljes tartomány felett. A módosított NotPetya nagyjából 45 perc alatt 107 számítógép felett szerzett irányítást, mielőtt az NCC Group

ügyfele aktiválta volna a beépített leállító és eltávolító funkciót." Mindez jól illusztrálja, miért fontos a mérnöki hálózat kiemelt védelme. A módosított kártékony kód egyáltalán nem érintette a SCADA/ICS-hálózatot, pusztán a HMI-gépeket pusztította volna el, ha a hatásmechanizmus az eredeti.

A kiberbiztonság európai szabályozása

A megfelelően biztonságos okos-infrastruktúra kiépítése tehát nemcsak a közműszolgáltató érdeke, hanem nemzetbiztonsági kihívás is. Különösen, ha figyelembe vesszük, hogy egyes közművek, mint például a villamos energetika esetében, a komplex hálózatok európai szinten értelmezhetők. Nem csoda, hogy az Európai Unió 2013-ban kelt kiberbiztonsági stratégiájában célul tűzte ki az európai létfontosságú rendszerek egységesen magas kiberbiztonsági szintjének elérését. A közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az *Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér* című dokumentum az alábbi célokat fogalmazza meg:
„A Bizottság:

- az európai kritikus infrastruktúrák hálózat- és információbiztonsági sebezhetőségeinek azonosítása és ellenálló rendszerek kifejlesztésének ösztönzése érdekében folytatja tevékenységeit, amelyeket a Közös Kutatóközpont a tagállamok hatóságaival és a kritikus infrastruktúrák tulajdonosaival és üzemeltetőivel szoros együttműködésben lát el.
- 2013 elején a botnetek és rosszindulatú programok elleni küzdelemmel kapcsolatos uniós finanszírozású kísérleti projektet indít el a tagállamok, a magánszektorbeli szervezetek, például az internetszolgáltatók és a nemzetközi partnerek közötti koordináció és együttműködés keretének megteremtése érdekében.

A Bizottság az alábbiakra kéri az ENISA-t:

- A tagállamok támogatása az erős nemzeti képességek kialakításában a kibertámadásokkal szembeni ellenálló képesség területén, főleg az ipari vezérlőrendszerek, a szállítás és az energiaipari infrastruktúra biztonságával és ellenálló képességével kapcsolatos ismeretek összegyűjtése révén.
- Az ipari vezérlőrendszerekre szakosodott uniós hálózatbiztonsági incidenskezelő csoportok (SCIRT) megvalósíthatóságának vizsgálata 2013-ban.
- A tagállamok és az uniós intézmények további támogatása rendszeres páneurópai kiberbiztonsági gyakorlatok megrendezésével, amelyek az Unió nemzetközi kiberbiztonsági gyakorlatokban való részvételének működési alapjául is fognak szolgálni.

A Bizottság az alábbiakra kéri az Európai Parlamentet és a Tanácsot:

- Az uniós közös, magas szintű hálózat- és információbiztonságra (NIS) vonatkozó irányelvjavaslat minél hamarabbi elfogadása, amely a nemzeti képességekkel és fel-

készültséggel, az uniós szintű együttműködéssel, a kockázatkezelési gyakorlatok elterjedésével és a NIS-sel kapcsolatos információk megosztásával foglalkozik.

A Bizottság az alábbiakra kéri az ágazatot:
- Vezető szerep vállalása a magas szintű kiberbiztonságba való beruházásban és bevált gyakorlatok, valamint ágazati szintű és a hatóságokkal való információmegosztás kidolgozása abból a célból, hogy biztosítsa az eszközök és egyének hatékony és megbízható védelmét, főleg az állami és a magánszektor partnerségei, például az EP3R és a Digitális élet iránti bizalom"

A stratégia eredményeképp egy három lábon álló európai kiberbiztonsági szabályozás alakult ki, amelynek elemei a következők:
- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről, azaz a NIS Direktíva,
- a GDPR-ként ismert Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
- Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről, azaz a Kiberbiztonsági Jogszabály.

A 2013-ban kiadott stratégiát 2017-ben vizsgálták felül, a *Közös közlemény az Európai Parlamentnek és a Tanácsnak Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése* című anyagban. Ekképpen értékelték az Európai Unió előrehaladását:

„A kibertámadásokkal szembeni uniós ellenálló képességhez elengedhetetlen, hogy az irányelvet valamennyi tagállam 2018 májusáig teljes körűen végrehajtsa. A folyamatot a tagállamok kollektív munkája támogatja, ami 2017 őszére iránymutatást fog eredményezni az összehangoltabb végrehajtás támogatására, különösen az alapvető szolgáltatások üzemeltetői tekintetében. A Bizottság közleményt fog kiadni az említett kiberbiztonsági csomag részeként, hogy azzal támogassa a tagállamok erőfeszítéseit, az irányelv végrehajtására vonatkozó bevált gyakorlatokat a tagállamoknak átadva és útmutatással szolgálva arról, hogy az irányelvnek miként kellene a gyakorlatban működnie. […] Erősíteni kell a bizalmat a közszféra és magánszféra közötti partnerségek iránt, hogy meg lehessen alapozni a több ágazat közötti szélesebb körű együttműködést és információcserét. Az információcsere és -elemző központok szerepe különösen fontos abban, hogy kiépítsék a szükséges bizalmat a közszféra és a magánszféra közötti információcsere iránt. Történtek bizonyos első lépések egyes kritikus ágazatok tekintetében, mint például a repülés terén az Európai Repülési Kiberbiztonsági Központ, illetve az energetikában

az információcserei és -elemző központok létrehozásával. A Bizottság teljes mértékben hozzájárul ehhez a megközelítéshez az ENISA által nyújtott támogatás révén, jóllehet fel kell gyorsítani a folyamatot, különösen a kiberbiztonsági irányelvben azonosított alapvető szolgáltatásokat végző ágazatok tekintetében."

A hét évvel ezelőtti stratégiában foglalt, kritikus információs infrastruktúra védelemével kapcsolatos elvárások tehát lassabban teljesülnek, mint az kívánatos lenne. Elsősorban a NIS Direktíva felgyorsítása lenne célszerű, amelyet Tikos Anita így foglal össze: „Az irányelv célja, hogy megteremtse a gyors és hatékony európai szintű kiberbiztonsági együttműködés és (incidenskezelés és -elemzés szintű) reagálóképesség alapjait, amely remélhetőleg hatékonyan alkalmazható lesz valamennyi lényeges biztonsági esemény és kockázat kezelésére. Annak érdekében, hogy egy ilyen hatékony és gyors együttműködési mechanizmus létrehozható legyen, a legkiemelkedőbb szektorokban meg kell teremteni a hálózati és információs rendszerek biztonsága általános védelmének alapjait Unió-szerte. Ezért az irányelv ezen szektorokra vonatkozóan megfogalmazza a legfontosabb védelmi szempontokat és minimumelvárásokat, valamint az EU-s együttműködési mechanizmusok megfelelő működéséhez szükséges nemzeti szakosított szervezeteket és azok minimumfeladatait, -képességeit."[32] Az irányelv hatálya egyébként kétfajta szolgáltatóra terjed ki, az alapvető szolgáltatókra, ahova a vízi közművek is tartoznak, és a digitális szolgáltatást nyújtó szolgáltatókra, mint például az online piacterek.

Az okosvárosok kiberbiztonsági szabályozása direkt módon nem következik egyébként a NIS Direktívából, indirekt módon viszont egyértelmű, hogy hosszú távon kikerülhetetlen lesz az okos-infrastruktúra és az európai követelmény összehangolása. A pontos meghatározás szerint a NIS-irányelv alá tartozik minden olyan szolgáltató, aki „A 98/83/EK tanácsi irányelv (17) 2. cikke 1. pontjának a) alpontjában meghatározott emberi fogyasztásra szánt víz szolgáltatói és elosztói, kivéve azokat az elosztókat, amelyek esetében az emberi fogyasztásra szánt víz elosztása csupán egy részét teszi ki az egyéb, alapvető szolgáltatásoknak nem tekinthető közszolgáltatások és áruk elosztására irányuló általános tevékenységüknek". Ezen szolgáltatók kijelölése a nemzeti hatóságok feladata. Viszont ahogy ezek a szolgáltatók áttérnek az okos-infrastruktúra használatára, a kiberbiztonsági szempontok figyelembevétele elkerülhetetlenné válik.

További lehetőséget biztosít a Kiberbiztonsági Jogszabályban megfogalmazott *Európai kiberbiztonsági tanúsítási keretrendszer* létrehozása is. Eszerint az Európai Unióban csak olyan informatikai termékek hozhatók forgalomba, amelyek teljesítik az alapvető információbiztonsági eljárásokat. Tóth Tamás összefoglalója szerint: „Az igényeknek megfelelően kialakított stratégiai cél, hogy létrejöjjön az egységes európai IKT-biztonsági tanúsítási keretrendszer, amely megszünteti a tagállami és ágazati eljárások általi széttagoltságot, az elfogadott kiberbiztonsági tanúsítási szakpolitikai javaslat alapján biztosítottá válik. Az új keretrendszer a lehető legharmonikusabban fog illeszkedni a nemzetközi szabványokhoz, bizonyos nemzeti érdekeket is figyelembe véve annak érdekében, hogy csökkenjenek a kereskedelmi akadályok. Az uniós kiberbiztonsági

[32] Tikos 2019

tanúsítási keretrendszer alapvető célja igazolni, hogy a meghatározott kiberbiztonsági kritériumoknak maximálisan megfelelnek az e keretrendszer részeként elfogadott nemzeti tanúsítási eljárások során tanúsított IKT-termékek, -szolgáltatások és -folyamatok. Ez a tevékenység javítja az IKT-termékek és -szolgáltatások biztonságosságát a biztonsági paraméterekről szóló kielégítő tájékoztatást, ezáltal növelve a fogyasztók termékekbe és szolgáltatásokba vetett bizalmát."[33] Bár ez az előírás sem mondja ki explicit módon azt, hogy az okoseszközöket és konkrétan az okosvárosokat alkotó dolgok internetét biztonsági tanúsításnak kell alávetni, a szakpolitikai érdek egyértelmű, az évtized második felétől az a cél, hogy a kiberbiztonság egész Európában egységesen, az okosotthonoktól kezdve az okosvárosokig magasabb legyen.

Védelmi lehetőségek

Mint a Dragonfly támadásnál felsorolt lépésekből látszik, ICS/SCADA-protokollok nem sérültek, a támadás mégis komolyan hozzájárult ahhoz, hogy a támadók fel tudták térképezni az amerikai és más országok energiarendszereit. Ezt a kockázatot természetesen a magyar jogszabályalkotók sem hagyhatták figyelmen kívül, ráadásul az európai direktívákat is honosítani kellett, így az elmúlt években több olyan szabályozást is elfogadtak, amelyek hol finomabban, hol keményebben presszionálják a létfontosságú rendszerek üzemeltetőit a kiberbiztonság megvalósítására. Magyarországon a 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről felsorolja, hogy melyek a kiemelten védendő infrastruktúra-elemek, a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, illetve annak végrehajtási rendelete, a 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről pedig részletesen leírja, hogyan is kell ezen kijelölt létfontosságú információs rendszerek és rendszerelemek információbiztonságát megvalósítani.

A jogszabályalkotók természetesen nem közműszakemberek, így a gyakorlatban ezen követelmények teljesülése kérdéses. A humán és anyagi erőforrásokban szűkölködő közműszektoroknak valószínűleg a kiberbiztonság a legutolsó problémájuk. Mégis érdemes felkészülni erre a kihívásra is, hiszen, mint láthattuk, ez nem a jövő kihívása, ez a jelen fenyegetése. Éppen ezért a felkészülést érdemes az iparági ajánlások szerint elkezdeni. Az amerikai víziközmű-szolgáltatók kiberbiztonsági szervezete, a WaterISAC ajánlása például jó kiindulási alapot jelent. A szöveg 15 pontban szedi össze a javasolt intézkedéseket.[34]

- Legyen egyértelmű leltár az információs rendszerekről.
- Mérjük fel a kockázatokat.
- Minimalizáljuk vezérlőrendszerek kitettségét.

[33] Tóth 2019
[34] WaterISAC 2019

- Kényszerítsünk ki felhasználóihozzáférés-kontrollt.
- Legyen védelem a nem jogosult fizikai hozzáféréssel szemben.
- Telepítsünk független kiberfizikai biztonsági rendszereket.
- Legyen folyamatunk a sebezhetőségek kezelésére.
- Alakítsuk ki a kiberbiztonság kultúráját.
- Legyenek kiberbiztonsági szabályaink és folyamataink és ezeket tartsuk is be.
- Alakítsunk ki fenyegetésészlelési és monitorozási folyamatot.
- Legyen tervünk az incidensek, vészhelyzetek és katasztrófák kezelésére.
- Számoljunk a belső fenyegetéssel.
- Biztosítsuk az ellátási láncunkat.
- Foglalkozzunk az összes okosmegoldás biztonsági kérdésével.
- Vegyünk részt az információmegosztásban, tartsunk kapcsolatot ezekkel a szervezetekkel.

Ez utóbbi ponthoz kapcsolódóan a magyarországi közművek számára kijelölt kibervédelmi hatóság az Országos Katasztrófavédelmi Főigazgatóság, az incidenskezeléssel pedig a Nemzeti Kibervédelmi Intézet foglalkozik. Személy szerint viszont a 8. pontot, a kultúra kialakítását tartom a legfontosabbnak. Nemcsak a jogszabályi követelmények miatt, hanem a józan előrelátás érdekében is célszerű, ha a közműszolgáltatónál van információbiztonsági felelős. A jogszabály alapján képzésüket egyébként a Nemzeti Közszolgálati Egyetem látja el.

Összefoglalás

2019 nyarán a Tripwire magazin megkérdezett néhány kiberbiztonsági szakértőt, hogy véleményük szerint hogyan fog alakulni a SCADA/ICS-rendszerek biztonsága a következő 5–10 évben. Az összes megszólaló kivétel nélkül kiemelte a digitális transzformációt, az IIoT előretörését, a hálózatosodást, illetve azokat a kibertéri veszélyeket, amelyeket elsősorban állami szereplők felől kell várni. Patrick Miller, az Archer Energy Solutions szakértője így foglalta össze mindezt: „Más szavakkal: a folyamat adatokat generál, majd ezek az adatok elhagyják a folyamatot vezérlő hálózatot, és bárhová/mindenhová eljutnak (pl. felhő, köd, tó, helyi adatközpont, távoli adatközpont), elemzésre kerülnek, újból felhasználhatók lesznek és a végén visszajutnak a folyamatba. Mindez olyan új kockázatokat vet fel a folyamatok azon adataira és az ezekhez kapcsolódó rendszerekre nézve, melyek a vezérlő/folyamathálózatokon kívül kerülnek, amelyet most kezdünk csak megérteni.”[35]

Biztosak lehetünk azonban abban, hogy a megelőzés minden körülmények között olcsóbb, mint hogyha utólag kellene a biztonságot beleépíteni az okosváros-infrastruktúrákba. Ehhez viszont szemléletváltásra van szükség! Először is, a legfontosabb a tudatosság, azaz az okoseszközök beszerzésénél legyünk tisztában a kiberbiztonság kiemelt

[35] Pettit 2019

szerepével, és az anyagi megfontolások mellett mindenképpen tervezzünk az információbiztonsággal is. Második fontos szempont a szabályozás megléte. Az NIS Direktíva fontos kötelezettséget ró az alapvető szolgáltatások üzemeltetőire. Eszerint fontos, hogy olyan belső szabályozás is létrejöjjön a vízi közmű és más közműszolgáltatóknál, amely tervez a tanulmányban említett kibertéri veszélyekkel. A harmadik lépés pedig a műszaki védelem megvalósítása, hiszen egyre több olyan szolgáltatás, illetve termék érhető el, amelyek ezekben a speciális közműszolgáltatói szektorokban is tudják emelni a kiberbiztonsági szintet.

Irodalomjegyzék

Baranya G. – Csernus I. szerk. (2018): *A fenntartható fejlődés és az állam feladatai.* Budapest, Dialóg Campus.

Bederna Zs. – Váczi D. – Pollner P. – Szádeczky T. (2019): Támadás hálózatba szervezve. In Auer Á. – Joó T. eds.: *Hálózatok a közszolgálatban.* Budapest, Dialóg Campus. 223–247.

Bódi A. – Marosi D. (2019): A komplex ITS ökoszisztéma alapjai. *Acta Periodica.* 17. kötet. 48–70.

Bolcsó D. (2018): *Orosz kibertámadást hiúsított meg Ukrajna*. Elérhető: https://index.hu/tech/2018/07/11/orosz_kibertamadast_hiusitott_meg_ukrajna/ (a letöltés dátuma: 2020. április 22.)

Bondor, M. (2020): *The best smart water bottles of 2020*. Elérhető: www.mbreviews.com/best-smart-water-bottle/ (a letöltés dátuma: 2020. április 14.)

Castells, M. (2004): Informationalism, Networks, and the Network Society: a Theoretical Blueprint. In *The Network Society: A Cross-cultural Perspective*. Cheltenham, Edward Elgar. 3–45.

Francescani, C. (2016): *U. S. Infrastructure Can Be Hacked With Google, Simple Passwords*. Elérhető: www.nbcnews.com/news/us-news/u-s-infrastructure-can-be-hacked-google-simple-passwords-n548661 (a letöltés dátuma: 2020. április 14.)

Haddad, R. (2019): Okoseszközök a kritikus információs infrastruktúrákban, villamosenergetikai fókusszal. In Deák V. szerk.: *Kritikus információs infrastruktúrák védelme – Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyszámára – 2019.* Budapest: Nemzeti Közszolgálati Egyetem. 72–113.

Howe, N. – Strauss, W. (2007): The next 20 years: how customer and workforce attitudes will evolve. *Harvard Business Review,* Vol. 85, No. 7–8. 41–52.

ICRC. (2020): *Rule 9. Definition of Civilian Objects.* Elérhető: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule9 (a letöltés dátuma: 2020. április 14.)

IHS Markit (2017): *The Internet of Things: a movement, not a market*. Elérhető: https://cdn.ihs.com/www/pdf/IoT_ebook.pdf (a letöltés dátuma: 2020. április 14.)

Kemp, S. (2020): *Digital 2020: 3.8 Billion People Use Social Media*. Elérhető: https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media (a letöltés dátuma: 2020. április 14.)

Kocsis T. (2019): *ICS/OT snapshot 2019.* Budapest, Black Cell Magyarország Kft.

Kovács L. – Krasznay Cs. (2010): Digitális Mohács – Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* No. 1. 44–56.

Kovács L. – Sipos M. (2010): *A Stuxnet és ami mögötte van: tények és a cyberháború hajnala*. *Hadmérnök,* V./4. 163–172.

Lipovsky, R. – Cherepanov, A. (2016): *BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry.* Elérhető: www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/ (a letöltés dátuma: 2020. április 14.)

Lipovsky, R. – Cherepanov, A. (2016): *Industroyer: Biggest threat to industrial control systems since Stuxnet*. Elérhető: www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (a letöltés dátuma: 2020. április 14.)

MAVIR (2020): *Újabb rekordok születhetnek a folyamatos napos időben*. Elérhető: http://mavir.hu/web/mavir/kozlemenyek/-/asset_publisher/FPi3DcWJuTiD/content/ujabb-rekordok-szulethetnek-a-folyamatos-napos-idoben (a letöltés dátuma: 2020. április 14.)

Mester Gy. (2018): *Önvezető robot autók újdonságai és biztonsági kérdései*. XII. Innováció és fenntartható felszíni közlekedés konferencia. XII. IFFK 2018. Budapest. Elérhető: www.researchgate.net/publication/334599495_Onvezeto_robot_autok_ujdonsagai_es_biztonsagi_kerdesei (a letöltés dátuma: 2020. április 14.)

Nagy J. (2019): Az Ipar 4.0 fogalma és kritikus kérdései – vállalati interjúk alapján. *Vezetéstudomány,* L. évf. 1. sz. DOI: 10.14267/VEZTUD.2019.01.02

Office of Cyber and Infrastructure Analysis (2015): *The Future of Smart Cities: Cyber-Physical Infrastructure Risk*. Elérhető: www.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf (a letöltés dátuma: 2020. április 14.)

Orbók Á. (2018): Az okos város kiberbiztonsága. In Sallai Gy. szerk.: *Az okos város (Smart City).* Budapest, Dialóg Campus. 187–202.

Panetta, K. (2019): *5 Trends Appear on the Gartner Hype Cycle for Emerging Technologies, 2019*. Elérhető: www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019/ (a letöltés dátuma: 2020. április 14.)

Pettit, J. (2019): *Ask the Experts: What Will Have the Greatest Impact on ICS Security in the Next 5–10 Years?* Elérhető: www.tripwire.com/state-of-security/ics-security/greatest-impact-ics-security/ (a letöltés dátuma: 2020. április 14.)

Pongrácz P. (2019): Kibertámadások villamosenergetikai környezetben. In Deák V. szerk.: *Kritikus információs infrastruktúrák védelme – Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyszámára.* Budapest, Nemzeti Közszolgálati Egyetem. 113–138.

Sallai Gy. (2018): Az okos város koncepciója. In Sallai Gy. szerk.: *Az okos város (Smart City)*. Budapest, Dialóg Campus. 13–34.

Schwab, K. (2018): *The Fourth Industrial Revolution*. Elérhető: www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734 (a letöltés dátuma: 2020. április 14.)

Shein, E. (2020): *COVID-19 pandemic impact pushing smart home voice control devices to predicted 30% growth*. Elérhető: www.techrepublic.com/article/covid-19-pandemic-impact-pushing-smart-home-voice-control-devices-to-predicted-30-growth/ (a letöltés dátuma: 2020. április 14.)

Symantec. (2017): *Dragonfly: Western energy sector targeted by sophisticated attack group.* Elérhető: www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks (a letöltés dátuma: 2020. április 14.)

Symantec. (2018): *VPNFilter: New Router Malware with Destructive Capabilities.* Elérhető: www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware (a letöltés dátuma: 2020. április 14.)

Tikos A. (2019): A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései. In Deák V. szerk.: *Kritikus információs infrastruktúrák védelme – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest, Nemzeti Közszolgálati Egyetem. 11–39.

Tóth T. (2019): Az Európai Unió tervezett kiberbiztonsági tanúsítási keretrendszerének bemutatása. *Szakmai Szemle,* XVII. évf. 1. sz. 97–115.

Zsolt M. (2020): *Karácsony és szilveszter körül szoktunk így fogyasztani.* Elérhető: https://energiabox.blog.hu/2020/04/02/karacsony_es_szilveszter_korul_szoktunk_igy_fogyasztani (a letöltés dátuma: 2020. április 14.)

WaterISAC. (2019): *15 Cybersecurity Fundamentals for Water and Wastewater Utilities.* Elérhető: www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf (a letöltés dátuma: 2020. április 14.)

WikiLeaks (2017): Vault 7: CIA Hacking Tools Revealed. Elérhető: https://wikileaks.org/ciav7p1/? (a letöltés dátuma: 2020. április 14.)

VÁKÁT OLDAL

Csaba Krasznay – Miklós Danyek

Protecting the National Electricity System in the Cyberspace – A Case Study[1]

Introduction

Electricity is "the most critical" essential infrastructure. Without reliable services, our economy and society cannot be operated. Nowadays, these kinds of infrastructures are intensively attacked from the cyberspace since information technology has become an inherent element of electricity production and transmission. Most of the special systems were designed with safety but not from a cybersecurity point of view; therefore, as these SCADA/ICS systems became interconnected, their built-in vulnerabilities were exposed to highly qualified attackers who had sufficient knowledge and who were state-sponsored. Moreover, due to the changing nature of electricity consumption and the need of environmentally friendly electricity production, the whole industry started a paradigm shift, that holds a currently unpredictable threat for the next decade.

As a result, the protection of these critical information infrastructures is in the focus of both legislators, diplomacy and military leaders. According to Healey and Jenkins, a cyberattack against electric grid falls into the "Destabilizing Presence" category that might invoke a straight answer from a country.[2] The European Union expressed the need for a joint diplomatic response to malicious cyber activities under the Cyber Diplomacy Toolbox, as the Council "expressed concerns about the increased ability and willingness of State and non-State actors to pursue their objectives by undertaking malicious cyber activities", by defining that *"cyber-attacks constituting a threat to Member States include those affecting information systems relating to, inter alia: [...] services necessary for the maintenance of essential social and/or economic activities, in particular in the sectors of: energy (electricity, oil and gas)".* According to the Cyber Diplomacy Toolbox, *"the Council stressed that clearly signalling the likely consequences of a joint Union diplomatic response to such malicious cyber activities influences the behaviour of potential aggressors in cyberspace, thereby reinforcing the security of the Union and its Member States."*[3]

The Directive on security of network and information systems (NIS Directive) identifies the key type of entities related to the electricity system as essential services, in its Annex II:

[1] We thank Levente Buttyán, Péter Görgey, Gábor Illés, Tünde Bonnyai, Zsolt Csaba Szabó-Nyakas, Zsolt Baranya and Péter Pongrácz, members of the SeConSys initiative who participated in the joint work, for their support.

[2] Healey–Jenkins 2019.

[3] Council of the EU 2019.

– Electricity undertakings as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council (1), which carry out the function of 'supply' as defined in point (19) of Article 2 of that Directive
– Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC
– Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC (NISD 2016)

In practice, these declarations and legal texts could not reach their goals without the extensive cooperation of responsible national players as were identified in the NIS Directive, the responsible national authorities, local SCADA/ICS and cybersecurity developers and service providers. In Hungary, the Security for Control Systems (SeConSys) initiative was established in 2018 to support the cooperation of these actors and facilitate the implementation of the NIS Directive, meanwhile increase the competitiveness of Hungarian developers on the European market by providing leading cybersecurity technologies for the electricity sector. Among others, the National Cyber Security Center, which is responsible for the National Single Point of Contact (SPOC) and also acts as the national CSIRT, as well as the sectoral authority – responsible for designation of critical infrastructures in electricity subsector – are also part of this cooperation as it can be seen on Figure 1. There are two working groups in SeConSys, one is responsible for regulatory questions, the other deals with technical challenges, both are aiming to provide an acceptable and feasible cybersecurity framework for the national electricity system in compliance with the NIS Directive.[4]

Figure 1: Members of the Security for Control Systems (SeConSys)
Source: Compiled by the authors.

[4] SeConSys 2019.

Cyberattacks in the electricity sector

As the first step, we identified those cyber incidents that affected the electricity system. This list can serve as a basis for the key stakeholders to have an overall view on the threat landscape.

- U.S. Navy – San Diego utility providers, San Diego, USA, 1999: In November 1999, during a U.S. Navy military exercise near San Diego Bay, a naval radar generated an EMI (electromagnetic interference) effect that caused disturbance in connection with the remotely controlled equipment used in the ICS systems of the San Diego County waterworks and San Diego gas and electric companies. Affected substations had to be restored for manual control.[5]
- Blaster worm, USA, Canada, 2003: Some sources say the Northeast blackout of 2003 was due to the Blaster worm attack. Although post-incident analyses indicate that ICS/SCADA systems at the affected providers were not running on Windows, some monitoring systems did. Blaster made these useless, which prevented electrical engineers in charge to detect and prevent large-scale malfunctions in time. Approximately 55 million consumers were left without electricity for longer or shorter periods (from 4 hours to two weeks).[6]
- Havex/Dragonfly, Europe, USA, 2014: This campaign was launched against ICS systems and ICS developers/users in Europe and North America. It was designed to steal information from targeted critical infrastructures (primarily in the energy sector) and their suppliers. Since the purpose of the attacks was to gather information, the impacts of these incidents on physical world and processes are unknown.[7]
- Calpine, USA, 2014: Attackers compromised some elements of Calpine's SCADA system that controls wind farms and switched it to manually controlled mode. Calpine is a major player in the U.S. electricity sector. The ICS/SCADA incident had no direct impact on the electricity system.[8]
- Malware attack on Asian nuclear power plants, Japan, South Korea, 2014: Malware attack was carried out on some systems used in the control room of Japanese (Monju) and South Korean (Korea Hydro and Nuclear Power Plant) nuclear power plants. Impacts are unknown.[9]
- Ukrainian power suppliers, Western Ukraine, 2015: Attackers compromised the ICS systems of 4 Western Ukraine power suppliers, caused significant malfunctions at several substations, then wiped the discs of SCADA systems and made many RTUs unusable with malicious firmware updates. As a last step, attackers used DDoS attacks against those websites and call centres used for reporting errors of the affected power providers. Service recovery was significantly accelerated by the low level of automation at the affected power suppliers, so they were able to quickly

[5] Repository of Industrial Security Incidents 2015.
[6] Moyer 2011.
[7] Symantec Security Response 2014.
[8] Burke 2015.
[9] Paganini 2014.

switch to manual control. About 225,000 consumers left without service and 135 MW was missed from the system. The full replacement of RTUs involved in the incident took months (in some cases 4–6 months).[10]

- Israeli utility authority, Israel, 2016: A serious cyberattack has hit several systems of Israeli public utility regulator. Details of the incident are not known.[11]
- Malware attacks on German nuclear power plant, Germany, 2016: Malware was found in nuclear power plant systems of Gundremmingen. Systems responsible for controlling the power plant were not affected by the incident. That was a non-targeted malware attack, the incident had no direct impact on the power plant's basic functions.[12]
- Industroyer/CrashOverride, Ukraine, Kiev district, December 2016: The attack on the Ukrainian system controller Ukrenergo is the fourth known attack on ICS systems and the second in which autonomous, ICS-targeting malware was used by the attackers (first was Stuxnet). According to some analysts, the attackers' aim was not to cause a simple malfunction, but they planned that, after the blackout, when Ukrenergo specialists were working on service restoration, DoS attacks would eliminate the rest of the defence, and then the unprotected substation equipment could have suffered fatal damage due to overload, which could have caused months of, half-yearly, year-long power outages. According to the analysis, this did not happen in the end because attackers made an error in developing computer codes used for the DoS attack.[13]
- NotPetya, Ukraine, Chernobyl, June 2017: NotPetya ransomware (other sources name it as a cryptowiper malware) attack, that exploited the EternalBlue vulnerability stopped the operation of a radiation measurement system used in the vicinity of Chernobyl nuclear power plant. The operation of the affected system had to be manually controlled. The system of the power plant was not affected.[14]
- Irish electricity system controllers, Ireland, Northern Ireland, August 2017: Irish system controller EirGrid and its Northern Ireland subsidiary, SONI were attacked by unknown perpetrators, with an estimated two months of intercepting network traffic of the two electrical system controllers. The incident had no known impact on the electricity system.[15]
- Attacks on the U.S. electricity system, U.S., July 2018: U.S. Department of Homeland Security (DHS) held a public webinar on Russian cyberattacks on critical infrastructure in the United States. One of the novelties of the presentation was that attackers often attacked various targeted critical infrastructures through their suppliers, com-

[10] Lee et al. 2016.
[11] Staff 2016.
[12] Paganini 2016.
[13] Slowik 2019.
[14] Griffin 2017.
[15] McMahon 2017.

promising their systems and often products. These incidents had no known impacts on the electricity system.[16]
- Ransomware attack on the Johannesburg electric company, South Africa, July 2019: Ransomware infected the Johannesburg power supply systems, and though the company's ICS systems were not affected by the incident, some customers who paid in advance for electricity, suffered longer power outages.[17]
- DoS attack on equipment used for communication between the control centre and the substations, USA, September 2019: Exploiting the vulnerabilities of one internet connected device (a firewall) of an electricity company called sPower in the west of the United States, the remote control of power plant substations became unavailable. The outage of communication caused a temporary degradation of control functions, but there is no information about malfunction or power outages that have occurred to consumers.[18]
- Malware attack on Indian nuclear power plant systems, India, October 2019: Suspected malware attack at Kudankulam nuclear power plant in India. The malware, known as Dtrack, is believed to be linked to the North Korean state-sponsored Lazarus group. According to operator and responsible Indian authority, the incident had no impact on the power plant's control systems.[19]

Cybersecurity challenges of present and future electricity systems

Present electricity systems

By taking an integrated approach within the SeConSys initiative, exploring electrical and cybersecurity aspects together, we identified the following key challenges of today's electricity systems:
- *Electricity storage problem:* Storage is not economically feasible neither in large quantities nor in the long run (and will not be available in the foreseeable future), thus a steady state of produced and consumed quantities must be maintained. This requires monitoring of the system through an extensive data collection, communication and data processing network. Information technologies are already available but adapting them in a secure way is a major challenge.
- *Electricity outage:* If electricity service is lost in a given area (country), infrastructures it serves will only be able to function until their own uninterruptible power supplies (UPS) are performing. These vary from sector to sector, ranging from a few hours to a few days. Served infrastructures include almost every elements of civilization (including but not limited to): short- and long-term public and private

[16] U.S. Department of Homeland Security 2018.
[17] Rumney 2019.
[18] Sobczak 2019.
[19] Dragos, Inc. 2019.

transport, gas, water, sewage, health, banking, education, police, fire service, justice, public administration, productive and consumer activities, communication (wired and wireless), etc.

– *Spatial extension, distributed nature:* Protection relay, automation, control technology and data communication devices form a network and form nationwide systems with a more extensive attack surface. These systems can even cross borders in the case of continental system-saving automation. On the area of electricity, TCP/IP based communication systems are widespread and only such devices are used in reconstructions or as newly integrated elements. These communication protocols were designed to provide unified and manufacturer-independent connectivity, resulting that cybersecurity was not a primary concern and thus have potential for cybersecurity development (e.g. IEC 60870-5-(101)104, IEC 61850, MODBUS TCP/IP, etc.).
– *Time factor:* This is critical especially for protection relays. Only cyber defence solutions can be considered that do not or only marginally (and definitively!) increase the 10 ms magnitude of protection time for the fast short-circuit elimination and preserve the sustainability of the selective protection time steps. Increased protection operating time can cause significant damage (e.g. € 1.2M per 400/132 kV transformer) to the affected equipment of the electricity system, moreover, the failure of them could lead to a widespread malfunction.
– *Diversity of system components:* Due to the diversity of manufacturers, models, operating modes and age, the cybersecurity level of system components cannot be unified. In many cases, 30- and 40-years old devices operate smoothly in the power grid, including the power transmission and auxiliary sides. Such devices should be declared as black boxes and their cyber protection should be managed accordingly. Many manufacturers produce excellent protection relays, control and SCADA equipment, but their cybersecurity readiness is highly scattered, rather weighted toward the weaker.
– *Energy Management System (EMS) and SCADA:* These systems are operating in control centres. They provide power system stability work with a significant amount of real-time data (status and fault indication, measurement) by describing the current operational status of the monitored system. Their reliability is always essential. Stuxnet warned that the reliability of status and error signals, as well as measurements is indispensable in the power system. This real-time data can come from multiple independent data sources (substations or power plant RTUs). Their credibility should be continuously monitored by elaborated methods (e.g. load flow calculations) and by methods to be developed in the future thus increasing the reliability of real-time data entering the EMS and SCADA systems. A special case might be an attack when data provided by multiple RTUs are falsified. In order to prevent significant consumer deprivation in space and time, the credibility test should also recognise such attacks.

– *Remote Terminal Units (RTU):* EMS and SCADA systems are primarily served with data by RTUs in substations and power plants. These data are provided by near-to-technology or field-level devices (Intelligent Electronic Devices or IEDs as called in IEC 61850 standard). IEDs and RTUs are equipped with special hardware and software that have a varying level of cybersecurity depending on the manufacturer, rather weighted toward the weaker. Local attack against the substation/power plant system can result in local or large-scale power grid outages depending on the strategic role of the attacked object in the system. In the event of a physical attack on a substation or power plant – that is an actual intrusion – the data acquisition network and other substations or power plants become vulnerable because the attackers have physical access to the communication network.
– *Data and Communication Systems:* Due to the spatial extent mentioned above, bridging significant distances (100 meters – n * 100 km) is required during data transmission. For longer distances, wired communication (e.g. Optical Ground Wire or OPGW in transmission line) is essential. In case of spatially distributed areas, when wired communication cannot be built up economically, wireless solutions (e.g. GSM, LTE, ZigBee, LoRa) are also widely used, especially on urban areas and renewable production sites. Wireless technology can be attacked easier due to its scattering principle. In many cases, data lines are not separated (e.g. owned by an energy provider), but they are leased lines provided by larger communications companies (e.g. MPLS system), like in other sectors (e.g. banking, internet and cable TV). Attacks on these can also make the power system vulnerable.
– *High priority of AC or DC UPS:* Continuous power supply and increased protection of ICS devices and systems in case of a cyberattack is a prerequisite for the smooth operation of the power grid and recovery after a malfunction. Although the uninterruptible power supply is generally not considered the part of ICS, in case of the 2015 cyberattack in Kiev, attackers, among others, reconfigured the UPS that supplied the SCADA and caused a downtime of it. For this reason, SeConSys considers UPS a part of ICS. The issue of power supply is closely related to the attack. On the one hand, remote monitoring of the UPS is integrated under ICS/SCADA systems, so the latter can be attacked through it. On the other hand, continuous availability of UPS that also operates as high-voltage switchgear is essential for the rapid elimination of short circuits in the high-voltage grid. A serious risk occurs when a UPS supplier requests an open internet connection for remote device management. Unfortunately, this is a common request from suppliers that must be controlled with strict security policy.
– *Complex and resource-intensive testing requirements:* These tasks occur in case of first maintenance and modification of protection relays, control systems, data communications, auxiliary supplies and systems. For existing systems, the primary consideration is the operational security of the high-voltage network and system components. Any modification (e.g. patch installation) to the operating system can only be made after thorough and detailed preliminary testing, which must be designed and

implemented according to a strict protocol. In case of installation of a new system component, cybersecurity related questions must be considered at the design stage and new system components must be assembled and tested from that perspective. In both cases, it is necessary either to design a test system (simulation surface) with a high degree of accuracy of the existing system or to separate a distinct part of the operating system for testing. Devices and systems to be tested, operated or patched, involve many in-house and outside professionals from many disciplines. Therefore, it is important from the security point of view to strictly manage their local and remote privileges, moreover monitor their activity continuously and, if necessary, send an alert to the responsible team.

– *Complex attack:* Threats that were listed so far are risks in themselves. At the same time, a coordinated attack against several interconnected elements of the electric grid could result in a significantly more severe malfunction (e.g. disabling UPS and simultaneously blocking an operation controller communication system that is essential for recovery). In this context, it is worthwhile for electric grid system operators to consider the amount of data that is published about their systems in order to make life more difficult for potential attackers.

Transforming electricity systems

As we discussed in the previous section, an electricity network is already vulnerable in the present condition of technology with the current degree of digitalisation, while this vulnerability is boosted in both quantity and quality because of the fundamental transformation of the electricity network that has already begun. The main elements of this digitalisation, which are also relevant from a cybersecurity perspective, are the following. This was examined with the integrated approach adopted by the SeConSys initiative from both electricity and cybersecurity aspects:

– Conversion of the traditional centralised network model to a decentralised one.
– The emergence of the industrial and domestic, decentralised – usually renewable – electricity generation and storage. The ratio of them is growing exponentially at present.
– In addition to the well-planned electricity generation, the emergence of seasonal, day and weather-dependent electricity generation is also increasing both in the industrial and residential sectors.
– Instead of earlier well-planned quantities and directions of energy flows, the formation of stochastic energy flows with network effects has evolved (changing primary disposition, protection relay, automation, control technology and plant management).
– In addition to the production of electricity by “turbine + generator” rotary machines, which have significant inertia, the importance of non-rotating photovoltaic electricity generation is increasing; therefore, the sum inertia of the electricity system is decreasing. This process reduces the resistance of the power system to very fast (10 μs – 1 sec) transient disturbances.

– The spread of smart grids, microgrids.
– The emergence and spread of IoT and IIoT.
– The spread of e-mobility.
– Transformation of a passive consumer role into an active producer and storage role.

Without exceptions, this incomplete list of changes has significant ICT implications. *Changes that are a paradigm shift because of their quantity and quality, will greatly increase the vulnerability of the electricity system due to their exposure to ICT.* Moreover, as an additional risk, public and private investors, who are typically non-cyber security and energy professionals, become participants of the electricity system and its data communication network. This increases the responsibility of legislator and sectoral authorities. Figure 2 illustrates the cybersecurity challenges of power systems and the scope of SeConSys.

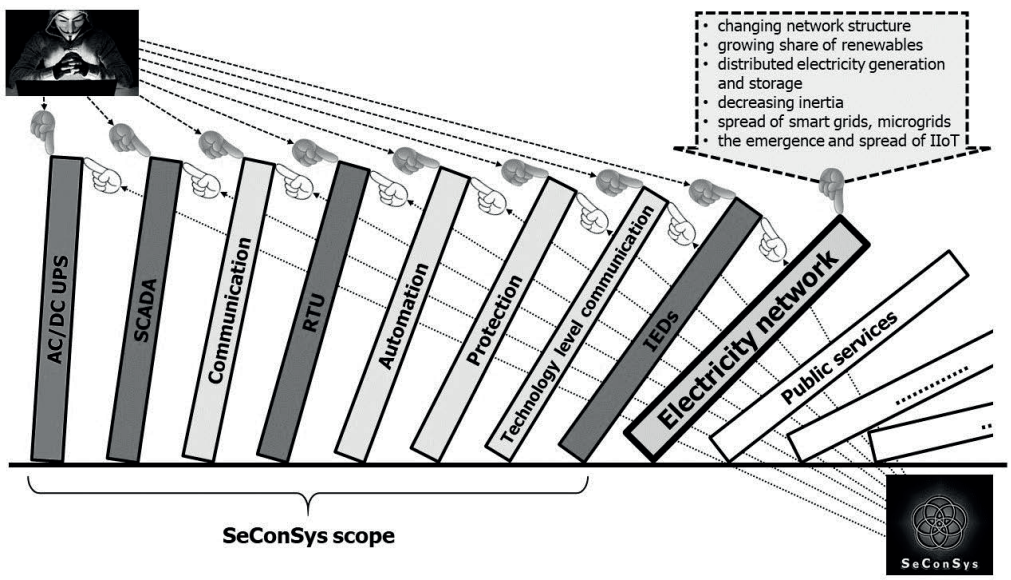


Figure 2: Challenges of power systems and the scope of SeConSys
Source: Compiled by the authors.

The SeConSys initiative can be a good framework for integrated management of the outlined complex and rapidly changing electrical and cyber security challenges.

Applicable security measures and related challenges

Within the technical working group of the SeConSys initiative, our initial activity was the structuring of the cybersecurity problem domain as it relates to and is perceived by the stakeholders of the Hungarian electricity system. The goal of this structuring is to help stakeholders focus their cyber defence activities, identify where they need to put

more effort, and understand the challenges related to the application of various existing security technologies and methodologies within their specific ICS/SCADA environment. In addition, we also aimed at identifying those areas where the application of security technologies and methodologies needs legislative support that provides an appropriate legal framework and incentives for the stakeholders.

At the highest level of our structuring, we followed the well-known *Prevention – Detection – Reaction* triad, and we also added a category for some general aspects of cybersecurity that spans across all three elements of the triad. Naturally, one would like to prevent cyberattacks on critical systems in the first place, and in the *Prevention* category, we identified those security technologies and methodologies that can help stakeholders achieve this primary goal. However, as we all know, some cyberattacks cannot be prevented, or would be too expensive to prevent entirely, and for those attacks, the next best thing one should do is to detect them as fast and accurately as possible. In the *Detection* category, we identified the tools and methods that stakeholders can use to achieve this secondary goal. Detection alone is not enough, as one also needs to react to a detected attack in order to minimise its harmful impact both in the short term and in the long run. *Reaction* category contains those technologies and methodologies that can help stakeholders achieve this third goal. In the rest of this section, we elaborate on each of these categories in more detail, and we also summarise the recommendations that were made for the regulation working group, and will serve as a basis for future regulations.

General aspects

Prevention and detection of, and reaction to cyberattacks can benefit from a thorough understanding of both the threat landscape, which a critical system is operating in, and the risks it is faced with. In addition, to address the risks, systems should have some fundamental baselines for preventive, detection and reaction measures covering technical, organisational, and personnel aspects as well. Lastly, increasing general security awareness, as well as special security trainings to different employee groups is indispensable for effective and efficient prevention, detection and reaction activities.

The main challenges in this category include reluctance to share incident related information for better threat intelligence and awareness at national or even higher level; fundamental differences in the risk assessment mindset of the often separated safety and security communities, while critical systems clearly have to address risks related to both safety/reliability and security/trustworthiness; proliferation of legacy equipment in existing critical systems that do not support even baseline security mechanisms; and the still frequently encountered negligence of cybersecurity in ICS/SCADA domain that stems from myths such as an air gapped system or from simple ignorance of reality both in terms of attacker capabilities and system weaknesses.

Prevention

Vulnerability assessment aims at finding weak points in the security posture of an organisation before attackers do so. An important part of this activity is *penetration testing,* a.k.a. ethical hacking. Testing methods can never guarantee completeness, yet, penetration testing is considered useful in IT environments, and should also be used in ICS/SCADA systems. The main challenge, however, is that unlike in IT environments, penetration testing in ICS/SCADA systems cannot usually be carried out on the operational system, because any side effect of the testing may have undesirable consequences, including making critical services unavailable or even resulting in physical damage of control equipment. So, organisations may need to establish special testing environments with equipment and configurations identical or very similar to those of the real system.

Configuration and patch management involves acquiring, testing and installing updates to firmware and software running on computers and control equipment, as well as keeping track of their configuration settings. One challenge of patching in ICS/SCADA systems is that updates need thorough testing and their deployment may follow pre-defined maintenance cycles, which usually introduce significant delays that leave systems vulnerable for extended periods of time. Another important challenge is that ICS/SCADA systems contain many legacy equipment, which may have reached their end-of-life and have no available updates.

Identity and access management is another essential preventive activity that involves the definition of authentication policies, the implementation of authentication procedures, as well as the definition and the enforcement of access control rules. Proper identity and access management helps to prevent unauthorised access to services and equipment both from outside and from inside the system; the latter being indispensable to counter insider threats and lateral movement of attackers within the system after gaining initial access. However, authenticating and access control may not be supported on legacy equipment and it may be difficult to integrate equipment originating from different vendors into a unified identity and access management system.

Perimeter defence and intrusion prevention try to control the boundary between the ICS/SCADA system and the world outside of it and typically uses traffic filtering at different levels to prevent harmful traffic from reaching internal parts of the system. Perimeter defence technology includes packet filtering firewalls, application layer proxies, and in some environments, data diodes that guarantee one-way communication across (sub)system perimeters. The biggest challenge here is to clearly define the perimeter of the system. For instance, firewalls placed between networks can be easily bypassed by remote VPN connections or by connecting computing devices, such as maintenance equipment, directly to internal networks. Also, data storage devices can be connected to internal equipment without any firewall "seeing" them and filtering their potentially malicious content. Another important challenge is that erroneous filtering configurations may lead to loss of important traffic, which may have negative effects on critical services provided by the system.

Protecting data with cryptographic mechanisms can prevent unauthorised access to sensitive information. In ICS/SCADA systems, such sensitive information may include login credentials, process data, configuration settings, control logic and network logs. The challenges of using cryptography in such environments include the lack of tool support in legacy equipment, the difficulty of cryptographic key management, and the potentially long lifetime of field equipment, which means that currently acceptable cryptographic algorithms will likely become obsolete still within the active lifetime of the equipment.

Detection

Fast and accurate detection of attacks requires situational awareness, which means that the operator of the system is aware of what is currently happening in its system in all conceivable situations. This is typically implemented by collecting information about important events in the system, analysing collected events, detecting anomalies and storing event information for retrospective analysis. Situational awareness is a prerequisite for intrusion detection and effective handling of incidents.

Intrusion detection systems (IDS) provide a second line of defence: when attackers succeed in defeating perimeter defence measures, an IDS can still identify the activities of the attacker. IDS systems can be signature based, which detect known adversarial patterns in network traffic or event logs, or anomaly based, which detect deviations from known good behavioural patterns of the system. While in IT systems anomaly detection is difficult because it is hard to characterise all legitimate behavioural patterns, ICS/SCADA systems have much more regular and predictable behaviour, so anomaly detection in such systems makes a lot of sense. The effectiveness of IDS systems heavily depends on the amount and quality of data that they operate on; collecting relevant data for intrusion detection can be challenging in ICS/SCADA systems.

Log collection, management and analysis deal with the detection of suspicious system behaviour retrospectively. Logs can be analysed periodically or in an on-demand manner during incident handling. In any case, it is important to collect logs, and log collection must be configured appropriately before incidents occur. As there are many places in large systems where logs can be collected, and it is useful to correlate logs originating from different sources, it makes sense to collect and manage logs in a centralised manner using a SIEM (Security Incident and Event Management) system, which may be a part of the Security Operations Center (SOC) operated by the organisation. The primary challenge of log collection in ICS/SCADA systems is that legacy equipment may not support logging at all, or they may only support logging of events that are not so useful for security analysis purposes. Another challenge is the transfer of logs from field equipment to the centralised SIEM, which may generate traffic overhead and interfere with control operations.

Malware is a relevant risk for any system that involves programmable equipment, and ICS/SCADA systems are not exceptions, as they increasingly contain programmable devices. In addition, a malware infected device may be under the full control of an

attacker and exhibit arbitrary behaviour. *Malware detection* is the process of identifying a malicious code in files, on storage devices and incoming network messages. Anti-virus products perform malware detection by scanning potential carriers for known malware patterns (signatures), by emulating the execution of suspicious programs, or by opening suspicious files in a sandbox and spotting anomalous behaviour that they produce. However, anti-virus products used in IT systems may not be directly applicable in ICS/SCADA systems, because they may silently quarantine suspicions files, which can cause problems in case of false positive detections. In addition, anti-virus products need up-to-date signature databases; therefore, they are frequently updated with potentially large amount of information, which is difficult to implement in an ICS/SCADA environment.

Reaction

One cannot hope for preventing and detecting all attacks with 100% precision, so it is important to be prepared for security incidents in order to handle them effectively. *Incident response* is a process, which aims at minimising disruption to operations, prevention of future incidents of the same kind, and, in certain cases, supporting law enforcement by forensically sound evidence collection and management. The biggest challenge of incident response in ICS/SCADA systems is that cyber security incidents may have physical consequences and incident response processes must take this into account. Also, recovery procedures may require stopping and restarting physical processes which may be non-trivial, time consuming, and they may require careful scheduling. Data collection for incident analysis may also be challenging due to legacy equipment and proprietary protocols.

Conclusions

Currently, in Hungary, there are three strategies (national security, cybersecurity and energy), three laws (CI, cybersecurity and energy) and many government decrees that reflect to the cybersecurity of electrical system, but none of them requires explicitly and on a feasible way those countermeasures that were proposed in our paper. During our problem domain analysis, we identified areas where legislative support is needed to create incentives for stakeholders for investing in appropriate cyber security measures and speeds up the replacement of obsolete devices. Moreover, there are many technical questions that are obvious in an IT environment but needs further R&D&I to implement them in an OT environment.

Legislation should require stakeholders to perform cyber security risk assessment regularly and to report cyber security incidents to an appropriate authority and the national CSIRT. In addition, legislation should also require regular penetration testing of critical systems by properly qualified ethical hacking teams without the risk of outages. Organisations must also have an incident management policy and plan, and preferably a local CSIRT that can take at least the initial steps in case of an incident. Regular cyber

security awareness trainings should also be made mandatory. Furthermore, legislation should encourage stakeholders for proper perimeter defence, malware detection, log collection and sharing of incident related information as a minimum set of measures, keeping in mind the specialties of ICS/SCADA, RTU, IED, protection relay and UPS systems. All of these requirements are mandatory only for those companies, who are under the CIP and NIS Directive, but the scope should be widened as many "not so critical" information infrastructures are not under the legislative umbrella.

References

Burke, G. (2015): *AP Investigation: US power grid vulnerable to foreign hacks.* Source: https://apnews.com/c8d531ec05e0403a90e9d3ec0b8f83c2 (Accessed: 08.05.2020.)

Council of the EU (2019): *Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States.* Source: http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf (Accessed: 05.06.2020.)

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Dragos, Inc. (2019): *Assessment of Reported Malware Infection at Nuclear Facility.* Source: https://dragos.com/blog/industry-news/assessment-of-reported-malware-infection-at-nuclear-facility/ (Accessed: 08.05.2020.)

Griffin, A. (2017): *'Petya' cyber attack: Chernobyl's radiation monitoring system hit by worldwide hack.* Source: www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html (Accessed: 08.05.2020.)

Healey, J. – Jenkins, N. (2019): Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing. In Minárik, T. – Alatalu, S. – Biondi, S. – Signoretti, M. – Tolga, I. – Visky, G. eds.: *11th International Conference on Cyber Conflict: Silent Battle.* Tallinn, NATO CCD COE Publications. 123–142.

Lee, R. M. – Assante, M. J. – Conway, T. (2016): *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Washington, D.C., Electricity Information Sharing and Analysis Center.

McMahon, C. (2017): *Exclusive: EirGrid targeted by 'state sponsored' hackers leaving networks exposed to 'devious attack'.* Source: www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html (Accessed: 08.05.2020.)

Moyer, M. (2011): *Expert: A Virus Caused the Blackout of 2003. Will the Next One Be Intentional?* Source: https://blogs.scientificamerican.com/observations/expert-a-virus-caused-the-blackout-of-2003-will-the-next-one-be-intentional/ (Accessed: 08.05.2020.)

Paganini, P. (2014): *Malware based attack hit Japanese Monju Nuclear Power Plant.* Source: http://securityaffairs.co/wordpress/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html (Accessed: 08.05.2020.)

Paganini, P. (2016): *Virus discovered at the Gundremmingen nuclear plant in Germany.* Source: https://securityaffairs.co/wordpress/46708/security/virus-gundremmingen-nuclear-plant.html (Accessed: 08.05.2020.)

Repository of Industrial Security Incidents (2015): *Salt River Project Hack.* Source: www.risidata.com/Database/Detail/salt-river-project-hack (Accessed: 08.05.2020.)

Rumney, E. (2019): *Johannesburg power body hit by ransomware attack.* Source: www.reuters.com/article/us-safrica-city-power/johannesburg-power-body-hit-by-ransomware-attack-idUSKCN1UK15N (Accessed: 08.05.2020.)

SeConSys – Security for Control Systems (2019): *Introduction.* Source: http://seconsys.eu/ (Accessed: 08.05.2020.)

Slowik, J. (2019): *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack.* Source: www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf (Accessed: 08.05.2020.)

Sobczak, B. (2019): *Report reveals play-by-play of first U.S. grid cyberattack.* Source: www.eenews.net/stories/1061111289 (Accessed: 08.05.2020.)

Staff, T. (2016): *Steinitz: Israel's Electric Authority hit by 'severe' cyber-attack.* Source: www.timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/ (Accessed: 08.05.2020.)

Symantec Security Response (2014): *Dragonfly: Cyberespionage Attacks Against Energy Suppliers.* Mountain View, CA, Symantec Corporation.

U.S. Department of Homeland Security (2018): *Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.* Source: www.us-cert.gov/ncas/alerts/TA18-074A (Accessed: 08.05.2020.)

VÁKÁT OLDAL

3. Egyes intézményi kérdések

VÁKÁT OLDAL

Gyaraki Réka

A nemzetközi intézmények szerepe a kiberbiztonságban

Bevezetés

A kiberbiztonság a digitális világ szélesedésével egyre kiemelkedőbb jelentőségű. Bár a biztonság szubjektív fogalom, ennek ellenére fontosnak tartom, hogy a nemzetközi szervezetek bemutatása és feladataik ismertetése és megértetése előtt a témához szükséges alapfogalmakat tisztázzuk, hiszen függetlenül a nemzetközi, nemzeti szinttől, az együttműködés megteremtésének egyik feltétele a közös fogalomhasználat.

A biztonság fogalma szubjektív, hiszen az egyes helyzetekben az embereknek különböző a biztonságérzete. A biztonság fogalmát a *Rendészettudományi szaklexikon* hosszasan fejtegeti, én mégis az alábbi meghatározást emelem ki: „A biztonság többtényezős, komplex fogalom, amely az állam és a társadalom érdekeinek, értékeinek, az ország területének és lakosságának külső és belső veszélyektől, fenyegetésektől mentes állapotát fejezi ki. (A létezés és a működés káros befolyásoló hatásaitól és a veszélytényezőktől kellően mentesített, védett állapot.)”[1]

A biztonságérzet szubjektivitása a kibertérben még inkább érzékelhető, hiszen az informatikai eszközök egyre szélesebb körű elterjedése, így a kommunikáció, az elektronikus ügyintézés, az elektronikus kereskedelem, a helymeghatározás, a fizikai aktivitás mérése, a közösségi média, videók és fényképek készítése, használata stb. egyre népszerűbb és egyre természetesebb. Az alkalmazásokhoz vagy egy-egy telekommunikációs eszköz szükséges, vagy – épp kényelmi funkcióik legteljesebb kihasználásához – személyes adatok, így név, születési adatok, e-mail-cím, biometrikus adatok stb. megadása szükséges, amelyek további felhasználásáról a felhasználók csak nagyon ritka esetben döntenek.

Az információs rendszerek terjedése, az általuk nyújtott szolgáltatások kiszélesedésének köszönhetően az állami, a vállalati és pénzügyi szektor, a magánszemélyek részéről függőség alakult ki ezen rendszerek, szolgáltatások és eszközök felé. Ezt a függőséget és aktivitást használják ki azok, akik a kibertéren keresztül támadásokat és bűncselekményeket követnek el.

A kiberbiztonság és veszélyei

A kiberbiztonságot a kibertérből érkező fenyegetések, támadások, az azon keresztül megvalósított bűncselekmények veszélyeztetik.

A Magyar Honvédség utasításának értelmező rendelkezése szerint a kiberbiztonság az az állapot, amelyben a kibertérre vonatkozóan az eszközök, politikák, irányelvek,

[1] Boda 2019, 66.

kockázatmenedzsment-megközelítések, műveletek, tréningek, bevált gyakorlatok, biztonsági megbízhatóságot szavatoló eljárások és technológiák érvényesülnek.[2]

Az ITU (Nemzetközi Távközlési Egyesület) T-X 1205. számú dokumentumában találhatunk egy meghatározást a kiberbiztonság fogalmára: „A kiberbiztonság az eszközök, a politikák, a biztonsági koncepciók, a biztonsági garanciák, az iránymutatások, a kockázatkezelési megközelítések, a cselekvések, a képzés, a legjobb gyakorlatok, a biztosítékok és technológiák gyűjteményét jelenti, amelyek a kiberkörnyezet, a szervezet és a felhasználói eszközök védelmére használhatók. A szervezet és a felhasználói eszközök közé tartoznak a számítástechnikai eszközök, a személyzet, az infrastruktúra, az alkalmazások, a szolgáltatások, a telekommunikációs rendszerek, valamint a továbbított és/vagy tárolt információk összessége a kiberkörnyezetben. A kiberbiztonság célja a szervezet és a felhasználók eszközei biztonsági tulajdonságainak elérése és fenntartása a kiberkörnyezetben meglévő biztonsági kockázatokkal szemben."[3]

Az Európai Unió kiberbiztonsági stratégiája[4] pedig a következőképpen definiálja a fogalmat: „A kiberbiztonság azokat a biztosítékokat és intézkedéseket jelenti, amelyek segítségével mind a polgári, mind a katonai területeken egyaránt megvédhető a virtuális tér azoktól a fenyegetésektől, amelyek azok összefüggő hálózataival és információs infrastruktúráival kapcsolatosak, vagy amelyek károsíthatják ezeket."

A kiberbiztonsági és biztonsági nemzetközi stratégiák a kiberbiztonságra vonatkozó fogalmi meghatározásukkal utat mutattak Magyarország nemzeti kiberbiztonsága fő irányainak kidolgozására, így született meg 2013-ban a Magyarország Nemzeti Kiberbiztonsági Stratégiája.[5] A kormányhatározat a kiberbiztonság fogalmát az alábbiak szerint definiálta: „A kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez."

A kibertér és jellemzői

A kibertér elsődleges ismérve, hogy olyan határok nélküli tér, aminek köszönhetően az információk, kommunikációk szabadon áramlanak, sokszor ellenőrzés nélkül, vagy épp ellenőrzés mellett, és ami fölötti felügyelet megvalósítása feladatonként és együttműködve lehetséges csak.

Az Amerikai Egyesült Államok Védelmi Minisztériuma a kibertér fogalmát a következőképpen határozta meg: „az információs környezetben az egymással kölcsönös függőségben lévő információs infrastruktúrák hálózata és a bennük lévő adatok által létre-

[2] 60/2013. (IX. 30.) HM utasítás.
[3] *ITU-T X.1205...* 2008, 8.
[4] *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér* 2013.
[5] 1139/2013. (III. 21.) Korm. határozat.

hozott globális tartomány, amely magában foglalja az internetet, a távközlési hálózatokat, a számítógépes rendszereket, valamint a beépített feldolgozó és vezérlő elemeket."[6]

A kibertér Magyar Honvédségen belüli értelmezése eltérő. A HM utasítás fogalmi meghatározás szerint a kibertér az elektromágneses spektrum használatával meghatározható, dinamikusan változó tartomány, amely az összekapcsolt hálózatok, eszközök és kiegészítő fizikai infrastruktúrák közötti adatok kezelésére szolgál.

Munk Sándor a kibertér értelmezésének és elemzésének tanulmányozása során a kibertér alábbi jellemzőit emeli ki:

– a kibertér egy sajátos (képzeletbeli, virtuális) környezet;
– a kibertér egy tartomány;
– a kibertér egy hálózat.[7]

Ugyanakkor a 2013-as magyarországi nemzeti kiberbiztonsági stratégiában használt megfogalmazás szerint a „kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti".[8]

Jelen tanulmány nemcsak a kiberbiztonság nemzetközi intézményeinek bemutatására fog korlátozódni, hanem minden olyan intézményre, amely a kibertérrel összefüggő jogellenes cselekmények felszámolását, megelőzését, felderítését hivatott szabályozni. Mivel nem kizárólag az intézmények foglalkoznak a kibervédelem elleni küzdelemmel, hanem kutatóközpontok és egyetemek is, ezért ezekről szintén említést fogok tenni.

A kiberbűncselekmények megelőzésére, felszámolására, a kiberbiztonság megteremtésére tett lépések nemcsak nemzetközi szinten érdemelnek említést, hanem nemzeti szinten is, így az utolsó fejezetben hazai intézményekkel, szervezetekkel is fogunk foglalkozni.

Az információs támadások közvetlen és közvetett formában valósulhat meg.

A *közvetlen információs támadás* – más néven belső vagy behatoló jellegű támadás – során a támadó fél egyrészt a különböző információbiztonsági rendszabályokat kikerülve bejut a kommunikációs rendszerekbe és a számítógéphálózatokba, hozzáfér különböző adatbázisokhoz stb., és számára hasznosítható információkhoz jut. Másrészt zavaró jelekkel, megtévesztő információkkal, rosszindulatú szoftverek bejutásával, bejuttatásával tönkreteszi, módosítja, törli stb. a szemben álló fél számára fontos információkat.

A *közvetett információs támadás* – más néven külső vagy szenzoralapú támadás – során a támadó fél hozzáférhetővé teszi a szemben álló fél számára a saját félrevezető információit, ezáltal megtéveszti annak felderítő rendszereit, és így befolyásolja a helyzetértékelést.[9]

[6] Paráda 2018.
[7] Munk 2018.
[8] 1139/2013. (III. 21.) Korm. határozat.
[9] Haig–Kovács 2008, 65.

Kiberfenyegetésnek, azaz a kibertérből vagy a kibertér felhasználásával elkövetett jogellenes cselekménynek, fenyegetésnek tekinthetjük

- a kiberbűnözést;
- a kiberkémkedést,
- a hacktivizmust;
- a kiberterrorizmust;
- a kiberhadviselést.[10]

Kiberbiztonsági stratégiák

A kiberbiztonság megteremtésének tárgyalásához mindenképpen szükséges azokról az alapvető, a kibertérben biztonságot teremtő dokumentumokról is beszélni, amelyek a kibertérrel összefüggő területek biztonságának és védelmének alapját adják.

Az Európai Unió 2003-ban megalkotta az első biztonsági stratégiáját *Biztonságos Európa egy jobb világban*[11] címmel, amelyben többek között az alábbi területekről érkező fenyegetéseket sorolja fel: a tömegpusztító fegyverekről, a szervezett bűnözésről, a terrorizmusról és a számítógépes biztonságról, így közvetetten a kiberbiztonságról határoz meg feladatokat.

Ezt követően öt évet kellett várni a következő stratégia megalkotására (2008), amely a kiberbiztonságot már fő kihívásként azonosította, hiszen a korábbi, 2003-as stratégiában nevesített kihívások tekintetében érezhető, hogy azok továbbra is globális problémát jelentenek.

„A modern gazdaságok nagymértékben függnek a létfontosságú infrastruktúrától, ideértve a közlekedési, kommunikációs és energiaellátási infrastruktúrát, de az internetet is. Az internetalapú bűncselekményekkel a 2006-ban elfogadott, a biztonságos európai információs társadalomra irányuló stratégia foglalkozik. A tagállamok kormány- vagy magántulajdonban lévő IT-rendszerei ellen elkövetett támadások következményeként azonban ez új dimenzióként jelenik meg mint esetleges új gazdasági, politikai és katonai fegyver."[12]

2009-ben az Európai Unió Bizottságának közleménye a kritikus informatikai infrastruktúrák védelméről *Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: A felkészültség, a védelem és az ellenálló képesség fokozása* címmel kiadta az EU első olyan dokumentumát, amely a hálózatok elleni támadásokkal foglalkozik. Ez tartalmazza a tudatosítást és a jövőben egyre inkább a szervezetek feladatává vált kibervédelmi gyakorlatok alapötletét. Továbbá a közlemény meghosszabbította az ENISA (Európai Hálózat- és Információbiztonsági Ügynökség) megbízatási idejét.[13]

[10] Berki 2016.

[11] *Európai biztonsági stratégia – Biztonságos Európa egy jobb világban* 2009.

[12] *Jelentés az európai biztonsági stratégia végrehajtásáról…* 2008.

[13] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről… (2009).

A következő biztonsági stratégia csak hosszú idő múlva született, ez volt *Az európai digitális menetrend (DAE)* 2010-ben, a Lisszaboni Stratégia nyomán. A DAE egyike az Európai Bizottság által elfogadott Európa 2020 stratégia hét kiemelt kezdeményezésének.[14] Célkitűzései között szerepel továbbá, hogy a tisztességes, nyílt és biztonságos digitális környezet biztosítása érdekében a Bizottság ezt követően az alábbi három pillérre építi a digitális egységes piaci stratégiát: Európa-szerte a digitális termékekhez és szolgáltatásokhoz való jobb hozzáférés biztosítása a fogyasztók és a vállalkozások számára; a digitális hálózatok és szolgáltatások fellendülését elősegítő feltételek megteremtése; valamint a digitális gazdaság növekedési potenciáljának maximalizálása.[15]

2012-ben az Európai Parlament határozatot fogadott el a *Kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: A globális kiberbiztonság felé* címmel, amely javaslatokat fogalmazott meg többek között a nemzeti kiberbiztonsági stratégiára.[16] Ezen kívül megfogalmazta az alábbiakat: „mivel a – kibertámadásokat, de más típusú internetes bűncselekményeket is magukban foglaló – kiberbűncselekmények vonatkozásában elérhető bűnüldözési adatok a különböző európai országokban a bűncselekmények számának erőteljes növekedésére utalnak; azonban mind a bűnüldöző szervek, mind a számítástechnikai szükséghelyzeteket kezelő csoportok (CERT) közössége továbbra is csak elvétve bocsát rendelkezésre a kibertámadásokra vonatkozó, statisztikailag reprezentatív adatokat, amelyeket a jövőben megfelelőbben kell összesíteni, ami Unió-szerte lehetővé fogja tenni a bűnüldöző szervek részéről a határozottabb válaszlépéseket, és több információt fog szolgáltatni az egyre növekvő kiberfenyegetésekre adott jogalkotási válaszlépésekhez."[17]

2016-ban a *Közös jövőkép, közös fellépés: Erősebb Európa – Globális stratégia az Európai Unió közös kül- és biztonságpolitikájára vonatkozóan*[18] címmel megjelent az újabb biztonsági stratégia, amely már használta és kiemelten is foglalkozott a kibertér fogalmával és annak biztonságával.

Az Európai Unió kiberbiztonsági stratégiája

Az Európai Unió első kiberbiztonsági stratégiájának kiadására 2013-ban került sor *Az Európai Unió kiberbiztonsági stratégiája – Nyílt, biztonságos és megbízható kibertér* címmel. A stratégiába lefektették a kiberbiztonsági alapelveket, így:

– az Európai Unió alapértékei ugyanolyan mértékben vonatkoznak a digitális világra, mint a fizikai világra;

[14] *Az európai digitális menetrend* 2010.
[15] *Az európai digitális menetrend* 2010.
[16] *Jelentés „A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: A globális kiberbiztonság felé" című dokumentumról* 2011.
[17] *Jelentés „A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: A globális kiberbiztonság felé" című dokumentumról* 2011.
[18] *Közös jövőkép, közös fellépés: Erősebb Európa – Globális stratégia az Európai Unió közös kül- és biztonságpolitikájára vonatkozóan* 2016.

– ugyanazok a törvények és normák vonatkoznak a kibertérre, mint amelyek mindennapjaink más területein is érvényesek;
– az alapvető jogok, a szólásszabadság, a személyes adatok és a magánélet védelme;
– mindenki számára biztosított hozzáférés;
– demokratikus és hatékony, számos érdekelt fél bevonásával történő irányítás;
– közös felelősségünk: a biztonság.

A stratégiában *öt stratégiai prioritásba* foglalták össze a jövőképet, amelyek a fent kiemelt kihívásokra adnak választ:
– kibertámadásokkal szembeni ellenálló képesség elérése;
– a számítástechnikai bűnözés drasztikus csökkentése;
– kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (KBVP) tekintetében;
– kiberbiztonsági ipari és technológiai erőforrások kifejlesztése;
– összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, és az EU alapértékeinek támogatása.[19]

A felsorolt dokumentumok tanulmányozása során megismerhettük a közös, az Európai Unió kiberbiztonsági stratégiájának megalkotásához vezető szabályozásokat, alapelveket és a következő fejezetekben bemutatott szervezeteket, feladataikat és a működésükhöz szükséges jogszabályi felhatalmazásokat.

Kovács László rámutatott arra, hogy a nemzetközi együttműködés egyik alapfeltétele, hogy az országok olyan kiberbiztonsági irányelvekkel, valamint azokat végrehajtani is képes szervezeti rendszerrel rendelkezzenek, amelyeket átfogó stratégiákban is rögzítettek. Ugyanakkor egy átfogó terminológiai egységesítés is üdvös lenne, ahogy az ENISA is rámutatott a 2012-ben kiadott ajánlásgyűjteményében.[20]

Magyarország Nemzeti Kiberbiztonsági Stratégiája

A magyar kormány a 139/2013. (III. 21.) Korm. határozattal fogadta el Magyarország Nemzeti Kiberbiztonsági Stratégiáját, amely az Alaptörvény elveivel összhangban, az értékek és érdekek számbavétele, valamint a kibertér biztonsági környezetének elemzése alapján meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is. A stratégia célja a szabad és biztonságos kibertér kialakítása és a nemzeti szuverenitás védelme a 21. század meghatározóvá vált új közege, a kibertér létrejöttének következtében megváltozott nemzeti és nemzetközi környezetben.[21] A hazai kiberbiztonsági stratégia előzményének

[19] *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér* 2013.
[20] Kovács 2018, 37.
[21] 1139/2013. (III. 21.) Korm. határozat 1. pont.

tekinthető a 2012-es *Magyarország Nemzeti Biztonsági Stratégiája,*[22] amely szintén utal a kibertérből érkező fenyegetésekre és veszélyekre, és amely feladatokat fogalmaz meg.

A kiberbiztonsági stratégia a fogalmak meghatározása (például a kibertér) mellett feladatokat és célokat fogalmaz meg, valamint hangsúlyozza a biztonságos kibertér megteremtésében az együttműködés fontosságát, kiemelten többek között a 3. és 4. fejezetben ismertetett szervezetekkel, hivatalokkal.

Az Európai Unió kiberbiztonsággal foglalkozó és a számítógépes bűnözés ellen fellépő szervezetei

A folyamatosan változó és egyre sűrűsödő biztonsági kihívásokkal terhelt nemzetközi környezetben az EU biztonságfelfogása és az ezzel kapcsolatban megfogalmazott elvi és elméleti hangsúlyok is folyamatosan eltolódnak.[23]

A kiberbűncselekmények számának évről évre történő növekedése és az elkövetők által okozott gazdasági, erkölcsi károk, és nem utolsó sorban az államok és állampolgárok biztonságának veszélye miatt az Európai Unió folyamatos lépéseket tesz annak érdekében, hogy megfelelően fel tudja venni a harcot ennek a folyamatosan fejlődő bűncselekménynek a megakadályozása és megelőzése érdekében.

Az Európai Unió 1993-ban a maastrichti szerződéssel hozta létre az EU II. pilléreként a közös kül- és biztonságpolitika dimenzióját az unió közös értékeinek, alapvető érdekeinek, függetlenségének megőrzése miatt az ENSZ Alapokmányával, a Helsinki Záróokmány alapelveivel és a Párizsi Charta céljaival összhangban.[24]

A kibertámadások és a kiberbűncselekmények elleni védekezés fontosabb feladatai közül az EU II. pillérében a kiberbiztonsággal kapcsolatos szabályozás kapott helyet, míg az EU III. pilléréhez, az igazságügyi együttműködéshez tartoznak a számítógépes bűncselekmények.

Ahogy az előző fejezetben is láthatjuk, szinte valamennyi dokumentumban, rendeletben a három fogalmat – a kibervédelmet és kiberbiztonságot, valamint a kiberbűnözést (amelyet leginkább számítógépes bűncselekményként említenek – egymás mellett alkalmazzák, hiszen ezek ténylegesen sem választhatók el egymástól.

Ezt támasztja többek között alá a Bizottság (EU) 2017/1584 számú ajánlása, amely szerint „uniós szinten a kiberbiztonsági válsághelyzetek kezelésében részt vevő legfontosabb szereplők közé tartoznak a kiberbiztonsági irányelv által újonnan létrehozott struktúrák és mechanizmusok, így a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) hálózata, továbbá a következő ügynökségek, hivatalok, szervezetek:

– az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA),
– a Bűnüldözési Együttműködés Európai Uniós Ügynökségén belül működő Számítástechnikai Bűnözés Elleni Európai Központ (Europol/EC3),

[22] 1035/2012. (II. 21.) Korm. határozat.
[23] Molnár 2019.
[24] Várnay–Papp 2005, 845.

– az Európai Unió Helyzetelemző Központja (INTCEN),
– az Európai Unió Katonai Törzsének Hírszerzési Osztálya (EUMS INT) és Helyzetelemző Központja (SITROOM), amelyek együtt alkotják az egységes információelemzési kapacitást (SIAC),
– a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport (az INTCEN-en belül),
– az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportja (CERT-EU) és
– az Európai Bizottság Veszélyhelyzet-reagálási Koordinációs Központja".[25]

A Bizottság ajánlásában nem szereplő, de az EU kiberterének, kiberbiztonságának megteremtésében szerepet játszó további szervezetek, azok dokumentumai is bemutatásra kerülnek.

Az Európai Unió *lisszaboni szerződése* értelmében – amely megszüntette a hárompilléres szerkezetet[26] – „az Európai Parlament és a Tanács rendes jogalkotási eljárás keretében elfogadott irányelvekben szabályozási minimumokat állapíthat meg a bűncselekményi tényállások és a büntetési tételek meghatározására vonatkozóan az olyan különösen súlyos bűncselekmények esetében, amelyek jellegüknél vagy hatásuknál fogva több államra kiterjedő vonatkozásúak, illetve amelyek esetében különösen szükséges, hogy az ellenük folytatott küzdelem közös alapokon nyugodjék.

Ezek a bűncselekményi területek a következők: terrorizmus, emberkereskedelem és a nők és gyermekek szexuális kizsákmányolása, tiltott kábítószer-kereskedelem, tiltott fegyverkereskedelem, pénzmosás, korrupció, pénz és egyéb fizetőeszközök hamisítása, számítógépes bűnözés és szervezett bűnözés."[27]

A fentiek fényében az Európai Unió nemcsak irányelveket, ajánlásokat fogalmaz meg folyamatosan a kiberbűncselekményekkel, a kiberbiztonsággal és a kibervédelemmel összefüggő változásokra reagálva, hanem az Európai Unió tagállamainak, kereskedelmének, gazdaságának, az állampolgárainak biztonsága, tájékoztatása érdekében igazságszolgáltatással és kiberbiztonsággal kapcsolatos szerveket is létrehozott.

Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér című uniós stratégiáról szóló, 2013-ban közzétett közlemény[28] rögzítette a kiberbiztonság megteremtésének, a kibertámadások és jogellenes cselekmények visszaszorításának és egy biztonságos kibertér megteremtésének fontosságát. Ezek miatt célként fogalmazta meg:

– az információs rendszerek kibertámadásokkal szembeni ellenálló képességének megteremtését;
– a kiberbűnözés drasztikus visszaszorítását;

[25] A Bizottság (EU) 2017/1584 ajánlása.
[26] Urszán 2011.
[27] Lisszaboni szerződés… 2017, 69/b cikk.
[28] *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér* 2013.

– a kibervédelmi politika kidolgozását és a közös biztonság- és védelempolitikát érintő képességek fejlesztését;
– a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtését;
– az Európai Unió által képviselt, a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozását, valamint az alapvető uniós értékek terjesztését.[29]

Az Európai Bizottság és a kiberbiztonsági válsághelyzet

A tanulmány célja a kiberbiztonsággal foglalkozó szervezetek bemutatása, ugyanakkor semmiképpen nem mehetünk el, ahogy lentebb is látjuk, azon szervezetek mellett, amelyek nagyban hozzájárulnak az Európai Unió (kiber)biztonságának megteremtéséhez. Éppen ezért a következőkben minden olyan unió szervezet bemutatására törekszem, amelyek ha mással nem is, de ajánlásokkal, rendeletekkel, utasításokkal hozzájárultak és hozzájárulnak ahhoz, hogy a kibertérrel összefüggő jogellenes cselekmények megelőzésében, az érintett szervezetek működésében és a feladataik meghatározásában megteremtse a megfelelő jogszabályi és szabályozási környezetet.

Az *Európai Bizottság* (a továbbiakban röviden: Bizottság) az EU politikailag függetlenséget élvező végrehajtó szerve. Kizárólagos hatáskörébe tartozik az új uniós jogszabályjavaslatok kidolgozása, és ez az intézmény felelős az Európai Parlament és az Európai Unió Tanácsa által hozott döntések végrehajtásáért. Székhelye Brüsszel, és 1957-ben alapították.

A Bizottság javaslatai többek között arra irányulnak, hogy hogyan védelmezzék az Európai Unió és az uniós polgárok érdekeit olyan kérdésekkel kapcsolatban, amelyeket nem lehet hatékonyan kezelni tagállami szinten. Szakmailag megfelelően előkészítettek, mivel kidolgozásuk során a Bizottság szakértőkkel és a lakossággal is konzultál.[30]

A Bizottság ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról című 2017-es dokumentum kifejezetten egy kiberbiztonsági válsághelyzetre történő reagálásra összpontosít.

Az ajánlás alapelveket fogalmaz meg, amelyek szükségesek az Európai Unió kiberbiztonsági célkitűzéseinek és a felelősségi körök meghatározásához.

– *Arányosság elve:* az eseményekre való reagálás terén a tagállamok közötti együttműködés alapját a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) kiberbiztonsági irányelvvel (NIS-irányelv) létrehozott hálózata biztosítja. A nemzeti CSIRT-ek önkéntesen együttműködnek és napi szinten információt cserélnek az egy vagy több tagállamot érintő kiberbiztonsági eseményekkel kapcsolatban.
– *Szubszidiaritás elve:* elsődlegesen a tagállamok felelőssége a kiberbiztonsági válsághelyzetre való reagálás, de fontos szerep jut a Bizottságnak, az Európai Külügyi Szolgálatnak és más olyan intézménynek, szervnek is, amely meg van határozva az integrált válságelhárítási intézkedésekben, de megtalálható az uniós jogban is.

[29] Bodó–Zámbó 2018.
[30] *Az Európai Bizottság* 2020.

– *Komplementaritás elve:* a tervezet figyelembe veszi a már meglévő uniós szintű válságkezelési mechanizmusokat – az integrált válságelhárítási intézkedéseket, az ARGUS-t és az EKSZ válságelhárítási mechanizmusát –, amelybe beépítik a NIS-irányelv struktúráit és mechanizmusait, a CSIRT-hálózatot, valamint az Európai Unió Hálózat- és Információbiztonsági Ügynökségét (ENISA), az Europol Számítástechnikai Bűnözés Elleni Európai Központját (EC3), az Európai Unió Helyzetelemző Központját (EU INTCEN), az Európai Unió Katonai Törzsének Hírszerzési Osztályát (EUMSINT) és az azon belül működő helyzetelemző szolgálatot (SITROOM), amelyek az egységes információelemzési kapacitás (SIAC) keretében működnek együtt a hibrid fenyegetésekkel foglalkozó EU információs és elemzőcsoporttal, valamint az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportjával (CERT-EU). Ennek keretében a tervezetnek biztosítania kell, hogy az említettek a kölcsönhatásuk és az együttműködésük során kiegészítsék egymást és minimalizálják az átfedéseket.
– *Az információk bizalmas kezelésének elve:* minden információcserének meg kell felelnie a biztonságra és a személyes adatok védelmére vonatkozó szabályoknak (lásd később a FIRST bemutatásánál), valamint a TLP-protokollnak. A minősített adatok cseréjéhez az alkalmazott minősítési rendszertől függetlenül a rendelkezésre álló akkreditált eszközöket kell alkalmazni[31]. A személyes adatok feldolgozása tekintetében a tervezet tiszteletben tartja az alkalmazandó jogszabályokat, így különösen az általános adatvédelmi rendeletet (GDPR), az elektronikus hírközlési adatvédelmi irányelvet, valamint az egyéneknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról szóló rendeletet.

Ez a dokumentum elemzi az ARGUS koordinációs rendszert, ami egy, az Európai Bizottság által 2005-ben létrehozott válságkezelési koordinációs rendszer, amely súlyos, több ágazatot érintő válsághelyzet esetén különleges koordinációs eljárást biztosít. A rendszert az azonos nevű sürgősségi riasztórendszer támogatja. Az ARGUS-on belül két szakaszt különítettek el: az első szakasz a súlyos, több ágazatot érintő válsághelyzethez kapcsolódik, míg a másik szakasz a válságkezelési koordinációs bizottságnak a Bizottság elnöke vagy egy felelős biztosa hatáskörében történő összehívását vonja maga után.[32]

A válságkezelési koordinációs bizottság a főtitkárhelyettes elnökletével értékeli a helyzetet, mérlegeli a lehetőségeket, és az intézkedéseket lehetővé tevő határozatokat hoz a Bizottság hatáskörébe tartozó uniós eszközökkel és mechanizmusokkal kapcsolatban, és gondoskodik a határozatok végrehajtásáról.[33]

[31] CIMS: Classified Information Management System – minősített adatok kezelésére szolgáló rendszer.
[32] *Bizottsági rendelkezések az „ARGUS" általános sürgősségi riasztórendszerről* 2005.
[33] A Bizottság 2006/25/EK határozata.

Az Európai Unió Tanácsa

Az Európai Unió Tanácsát (a továbbiakban röviden: Tanács) 1958-ban alapították Európai Gazdasági Közösség Tanácsa néven. Ez az EU-tagállamok kormányainak képviseletét ellátó intézmény, amely uniós jogszabályokat fogad el, és összehangolja az uniós szakpolitikákat. A Tanácsban a tagállamok miniszterei üléseznek, akik felhatalmazással bírnak arra, hogy a kormányuk nevében kötelezettségeket vállaljanak.

Az Európai Unió Tanácsának elnöki feladatait az uniós országok 6 havonta, rotációs rendszerben látják el.

Az Európai Unió Tanácsának összetétele. Az Európai Unió Tanácsának nincsenek állandó tagjai. A Tanács 10 különböző formációban ülésezik a megvitatásra kerülő szakpolitikai terület függvényében. Az egyes tagállamokat az adott formációnak megfelelően a kérdéses szakpolitikai területért felelős miniszterek képviselik az ülésen.

Az Európai Unió Tanácsa és a kiberbiztonság. Az EU egészére kiterjedő, informatikai elemeket érintő válsághelyzet esetén a reagálás uniós szintű politikai koordinációját a politikai szintű integrált válságelhárítási intézkedések (IPCR) segítségével a Tanács végzi.[34]

A Tanács 2019. május 17-én létrehozott egy olyan jogszabályi keretet – *Cyberdiplomacy Toolbox* néven –, amely lehetővé teszi az EU számára, hogy célzott, korlátozó intézkedéseket vezessen be az olyan kibertámadásoktól való elrettentés és az azokra való reagálás érdekében, amelyek külső fenyegetést képeznek az EU vagy annak tagállamai számára, beleértve a harmadik államok vagy nemzetközi szervezetek ellen irányuló kibertámadásokat is, amennyiben ilyen korlátozó intézkedéseket szükséges bevezetni a közös kül- és biztonságpolitika (KKBP) céljainak elérése érdekében.

Ezen új szankciós rendszer hatálya alá olyan kibertámadások tartoznak, amelyek jelentős hatást gyakorolnak és:

- amelyek az Európai Unión kívülről erednek, vagy amelyeket az Unión kívül követnek el; vagy
- amelyek az EU-n kívüli infrastruktúrát alkalmaznak; vagy
- amelyeket az unión kívül letelepedett vagy tevékenységüket az EU-n kívül végző személyek vagy szervezetek követnek el, vagy
- amelyeket a tevékenységüket az Európai Unión kívül végző személyek vagy szervezetek támogatásával követnek el.

Az olyan megkísérelt kibertámadások, amelyek potenciálisan jelentős hatással bírnak, szintén e szankciós rendszer hatálya alá tartoznak.

[34] A Bizottság (EU) 2017/1584 ajánlása.

Európai Unió Tanácsa és a kiberbűncselekmények

Az Európai Unióban egyre több kiberbűncselekménnyel és kibertámadással kell szembesülni, amelyek mind a tagállamoknak, mind pedig a közösségnek komoly anyagi károkat okoznak. Ezek a jogellenes cselekmények több szektorra is veszélyt jelentenek, ahol a Tanács ajánlások és rendeletek révén törekszik a kiberbiztonság megteremtésére. Ilyen jogszabályi háttér többek között a kritikus infrastruktúrákra vonatkozó *(Zöld könyv),* a gyermekek védelmére megalkotott *Biztonságos Internet Program* és a 2005 februárjában elfogadott, az információs rendszerek elleni támadásról szóló *kerethatározat,*[35] amelyben a korábban használatos számítógépes rendszer fogalma helyett már az információs rendszer *(information system)* fogalma jelenik meg. Az egyes fogalmak összevetésekor megfigyelhető, hogy annak ellenére, hogy a megjelölés különbözik (információs rendszer – számítógépes rendszer), a fogalmak tartalma gyakorlatilag megegyezik.
A kerethatározat az *üldözendő magatartásokat* a következőképpen csoportosítja:

- információs rendszerekhez való jogsértő hozzáférés;
- rendszerbe való jogsértő beavatkozás;
- adatokba való jogsértő beavatkozás.

A kerethatározatot 2013-ban felváltotta az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv.[36] Az *új irányelv* különös figyelmet fordít az úgynevezett botnetekre és a személyazonossághoz kapcsolódó bűncselekményekre, valamint súlyosabb szankciókat helyez kilátásba arra az esetre, ha az informatikai bűncselekményt bűnszervezetben követik el. Ezenfelül előírja, hogy a büntetőeljárás során figyelembe kell venni azt a körülményt, ha a bűncselekményt az elkövető alkalmazotti minőségben követi el.

Az Európai Tanács

Az Európai Tanács adja az Európai Uniónak a fejlődéséhez szükséges ösztönzést, és meghatározza annak általános politikai irányait és prioritásait.

A közös biztonság- és védelempolitika megvalósításának egyik legfontosabb szereplője az állam- és kormányfőket tömörítő Európai Tanács *(European Council),* amely a lisszaboni szerződéssel az EU formális intézménye lett, és állandó elnök vezeti. Az Európai Tanács egyik legfontosabb feladata, hogy politikai prioritásokat és iránymutatásokat fogalmazzon meg az EU előtt álló biztonság- és védelempolitikai kihívások kapcsán, és válságok esetén is. Az ülések után kiadott következtetések politikai súlya elsősorban abból fakad, hogy a lehető legmagasabb szinten fejezi ki a tagállamok politikai akaratát, így lehetőséget nyújt a kihívások és a kül- és biztonságpolitikai prioritások közös, uniós szintű rendezésére.[37]

[35] A Tanács 2005/222 IB kerethatározata az információs rendszer elleni támadásokról.
[36] Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról.
[37] Molnár 2019.

Az Európai Tanács nem lát el jogalkotási feladatokat.

Az Európai Tanács a tagállamok állam-, illetve kormányfőiből, valamint saját elnökéből és a Bizottság elnökéből áll. Munkájában részt vesz az Európai Unió külügyi és biztonságpolitikai főképviselője.

Az Európai Tanács elnökének összehívására, félévente kétszer ülésezik. Amikor a napirend úgy kívánja, tagjai úgy határozhatnak, hogy munkájukat tagonként egy miniszter, illetve a Bizottság elnökének esetében egy biztos segítse. Ha a helyzet úgy kívánja, az elnök az Európai Tanácsot rendkívüli ülésre hívja össze.

Ha a szerződések eltérően nem rendelkeznek, az Európai Tanács konszenzussal dönt.

Az Európai Tanács minősített többséggel, két és fél éves időtartamra választja meg elnökét; az elnök megbízatása egy alkalommal megújítható. Akadályoztatás vagy súlyos hivatali mulasztás esetén az Európai Tanács az elnök megbízatását ugyanilyen eljárással megszüntetheti.

Az Európai Tanács elnöke

- elnököl az Európai Tanács ülésein, és lendületet ad munkájának;
- a Bizottság elnökével együttműködve és az Általános Ügyek Tanácsában folytatott munka alapján gondoskodik az Európai Tanács munkájának előkészítéséről és folyamatosságáról;
- erőfeszítéseket tesz az Európai Tanácson belüli kohézió és konszenzus megteremtésére;
- az Európai Tanács minden ülését követően jelentést nyújt be az Európai Parlamentnek.

Az Európai Tanács elnöke – a saját szintjén és e minőségében, valamint az Európai Unió külügyi és biztonságpolitikai főképviselője hatáskörének sérelme nélkül – ellátja az EU külső képviseletét a közös kül- és biztonságpolitikához tartozó ügyekben. Az Európai Tanács elnöke semmilyen nemzeti tisztséget nem tölthet be.[38]

Az Európai Tanács megbízásából készült 1994-ben az információs társadalommal[39] szemben tanúsított alábbi elvárásokat (célkitűzéseket) fogalmazta meg:

- az informatikai eszközöket szabványosítani kell;
- ha nem szabványosak az eszközök, elveszik a lényeg, az információáramlás;
- azért kell szabványosítani, mert az üzleti élet, a versenyszféra ellenérdekelt;
- a monopolhelyzetek megszüntetése, különös tekintettel a telekommunikációra;
- a jog hosszú ideig elfogadta a monopolhelyzetet, mert a beruházás e területeken nagyon sokba kerül, de most már nem fogadják el ezt az érvelést;
- a szellemi alkotások megfelelő szintű védelme;
- a szerzői jogban ez teljesen új terület, amelyre (a zene-, kép-, filmletöltésekre) még – sem akkor, sem ma – nincs megfelelő szabályozás, védelem;
- a magánszféra védelme, mivel ez van kitéve a legnagyobb veszélynek. Felismerték, hogy a mai világban a magánszférát egyetlen eszközzel lehet védeni, és ez a jog.

[38] Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata (2008).

[39] Komanovics 2007.

A magánszemélyt technikai eszközzel már nem lehet az állammal szemben megvédeni;
– az adatbiztonság szabályainak kidolgozása. (A vírusok elleni védelemmel összefüggésben az Európai Tanács megállapította, hogy olyan rendszert nem lehet építeni, amibe nem lehet belenyúlni, de olyat igen, ahol ez nem marad észrevétlen.)

Európai Unió Belső Biztonsági Állandó Bizottsága (COSI)

Az Európai Unió Belső Biztonsági Állandó Bizottsága (COSI) meghatározta a stratégiai célokat a számítógépes bűnözés területén. Az Állandó Biztonság célja a belső biztonság területén, hogy megkönnyítse a tagállamok közötti operatív tevékenységek koordinálását. A belső biztonsággal kapcsolatban ez az operatív együttműködéssel kapcsolatos rendőrségi és vámügyi együttműködést, a külső határok védelmét és a büntetőügyekben folytatott igazságügyi együttműködést érinti. A COSI operatív szerepére tekintettel Magyarországot a Belügyminisztérium képviseli.
A 2014–2017 közötti időszakban a COSI elsősorban
– a nagy károkozással járó, online és bankkártyás fizetéssel összefüggő, továbbá
– az áldozatok részére komoly hátránnyal járó – például a gyerekek sérelmére elkövetett – számítógépes bűncselekmények, valamint
– a kritikus infrastruktúrát és a számítógépes rendszereket érintő informatikai bűncselekmények tekintetében kíván hatékony lépéseket tenni a kialakítandó védekezés érdekében.[40]

A stratégia kitér a lehetséges informatikai rendszer sebezhetőségeinek beazonosítási problematikájára is. Az informatikai támadásokat okozó bűnözést illetően is definiálták a problémákat, így például:
– kevés információ a bűnözői hálózatokról;
– a kockázatokhoz kapcsolódó tudatosság hiánya;
– jogi akadályok fennállta az információcserében;
– az elégtelen bűnfelderítői együttműködés;
– az állam jogalkalmazó és igazságszolgáltató szerveinek elégtelen felkészültsége;
– az incidensek azonosításának és besorolásának országonként eltérő formája;
– a civil szféra alacsony szintű bevonása;
– az Európai Unión kívüli cselekmények jelentős hatása;
– az alacsony mértékű felderítés;
– a bűnelkövetői elfogások alacsony száma.[41]

[40] *SOCTA…* 2017.
[41] *Az Európai Unió Belső Biztonsági Állandó Bizottsága (COSI) által meghatározott stratégiai célok a kiber-bűnözés ellen harc terén a 2014–2017 közötti időszak tekintetében* 2013.

A COSI a 2018–2021-es időszakra vonatkozóan továbbra is prioritásként kezeli a szervezett bűnözés és a kiberbűnözés kérdését, amikor is kiemeli, hogy a kibertámadások 400 milliárd euró kárt okoznak évente, és három további területre kíván a jelzett időszakban összpontosítani:[42]

– fellépés az informatikai rendszerek elleni támadásokkal szemben;
– a készpénz-helyettesítő fizetési eszközökkel való visszaélések felszámolása;
– a gyermekek online biztonságának fokozása, többek között a gyermekbántalmazást ábrázoló tartalmak előállítása és terjesztése elleni küzdelem révén.

Európai Parlament

Az Európai Parlament (a továbbiakban röviden: Parlament) az Európai Unió jogalkotó intézménye, amelyet ötévente választanak meg az uniós polgárok. Székhelye Strasbourg, Brüsszel és Luxemburg.

A Parlament jogalkotási, felügyeleti és költségvetési hatáskörrel rendelkezik, jelenleg 705 képviselője van, amely helyekből a tagállamok népességük arányában részesülnek, de egyik tagállamnak sem lehet 6-nál kevesebb és 96-nál több mandátuma. A képviselők politikai nézetük alapján és nem tagállamuk szerint alkotnak frakciókat.

A Parlament munkája két fő szakaszra bontható:

Jogszabályok előkészítése, amit bizottságok révén gyakorol. Az Európai Parlamenten belül 20 bizottság és 2 albizottság működik. Mindegyikük egy adott szakpolitikai területtel foglalkozik. A bizottságok górcső alá veszik a jogszabályjavaslatokat, amelyeket a képviselőcsoportok is megvitatnak. A képviselők és a képviselőcsoportok módosításokat terjeszthetnek elő, illetve a jogszabályjavaslat elutasítását is kezdeményezhetik.

A jogszabályjavaslatok elfogadása plenáris üléseken zajlik. Az összes európai parlamenti képviselő megjelenik az ülésteremben azért, hogy részt vegyen a jogszabályjavaslat és az előterjesztett módosítások sorsát eldöntő zárószavazáson. A plenáris üléseknek, amelyek havonta négy napon át zajlanak, rendes körülmények között Strasbourg ad otthont, de néha további ülésekre is sor kerül Brüsszelben.

A lisszaboni szerződés 2009. decemberi hatálybalépésével az Európai Parlament bel- és igazságügy területén játszott szerepe jelentősen megnövekedett. A rendőri együttműködéssel kapcsolatos, parlamenti állásfoglalásokban kifejtett álláspontja azt a szándékát tükrözi, hogy megerősítse helyzetét, ugyanakkor azt is jól mutatja, hogy az uniós rendőri együttműködés még viszonylag korai szakaszában van. Ez utóbbi kérdéssel kapcsolatban a Parlament gyakran kifogásolja a belbiztonsággal kapcsolatos, ténylegesen összehangolt megközelítés hiányát. Az európai biztonsági stratégiáról szóló, 2015. július 9-i állásfoglalásában sajnálatát fejezte ki azzal kapcsolatban, „hogy a Parlament számos felhívása ellenére továbbra sem végezték el a meglévő uniós eszközök – többek között az új biztonsági fenyegetésekkel szembeni – hatékonyságának és a fennálló hiányosságok értékelését”, és azzal érvelt, hogy „el kell végezni az értékelést annak biztosítása

[42] *A szervezett bűnözés elleni küzdelem az Unióban* 2020.

érdekében, hogy az európai biztonsági politika hatékony, megfelelő, arányos, koherens és átfogó legyen". Gyakran hívta fel a figyelmet arra is, hogy a rendőri tevékenység és a bűnüldözés vonatkozásában a szabadság és a biztonság megfelelő egyensúlyára van szükség.

Az Európai Parlament másik prioritása, amint azt már fentebb is jeleztük, hogy intézményi szereplőként kialakítsa a belbiztonsággal kapcsolatos álláspontját. Míg a COSI hivatalosan kívül esik a parlamenti ellenőrzés hatókörén, a Parlament arra törekszik, hogy hangsúlyozza a saját, új, a rendőri együttműködésre vonatkozó hatásköreit. A Stockholmi Program félidős felülvizsgálatáról szóló, 2014. április 2-i állásfoglalásában emlékeztetett rá, hogy „az Európai Parlament mára a biztonságpolitikai terület teljes jogú intézményi szereplőjévé vált", és „központi szerepet kell játszania a belső biztonságpolitikák értékelésében és meghatározásában". Az európai biztonsági stratégiáról szóló, 2015. július 9-i állásfoglalásában a Parlament megismételte, hogy be kellene vonni a stratégia „politikai prioritásai és stratégiai célkitűzései meghatározásába". A Parlament vitathatatlanul jelentős hatást gyakorol a belső biztonságpolitikára. Az Europol reformjának részeként aktívan kiállt a nagyobb mértékű parlamenti ellenőrzés és a jobb adatvédelmi szabályok mellett. Felszólított továbbá az adatmegőrzési irányelv[43] hatályon kívül helyezésére, annak aránytalanságára hivatkozva, még mielőtt az irányelvet a Bíróság 2014. áprilisi, joggyakorlatot teremtő ítéletében megsemmisítette.

ENISA (European Network and Information Security Agency)

Az Európai Unió Hálózat- és Információbiztonsági Ügynökségét (ENISA) (a továbbiakban röviden: ENISA vagy Ügynökség) 2004-ben hívták életre a 460/2004/EK rendelettel. Az ENISA szakértői központként működik Európában, székhelye Görögországban, Kréta szigetén, Heraklionban található, az operatív iroda Athénban működik.

Az ENISA aktívan hozzájárul a magas szintű hálózat- és információbiztonság fenntartásához (NIS) az Európai Unión belül.

Az Európai Unió Hálózat-és Információbiztonsági Ügynökséget alapító rendeletét az 526/2013/EU rendelet váltotta fel, amely új szabályokat állapított meg, és amely a 2004-es EK rendeletet hatályon kívül helyezte.

Az ügynökség szorosan együttműködik a tagállamokkal és a magánszektorral azért, hogy tanácsot és megoldásokat találjon a kiberbiztonság megteremtéséhez. Ez magában foglalja nemcsak a páneurópai kiberbiztonsági gyakorlatok szervezését, fejlesztését, a *National Cyber Security* stratégiákat, a CSIRT-együttműködést és -kapacitásbővítést, hanem tanulmányok elkészítését a biztonságos *cloud-rendszerek* elfogadásáról, az adatvédelmi kérdésekről, az adatvédelmet erősítő technológiákról és a magánélethez kapcsolódó új technológiákról (eIDs, azaz e-személyigazolvány) is, és meghatározza a számítógépes fenyegetések és mások aktuális trendjeit. Az ENISA is támogatja, kidol-

[43] Az Európai Parlament és a Tanács 2006/24/EK irányelve.

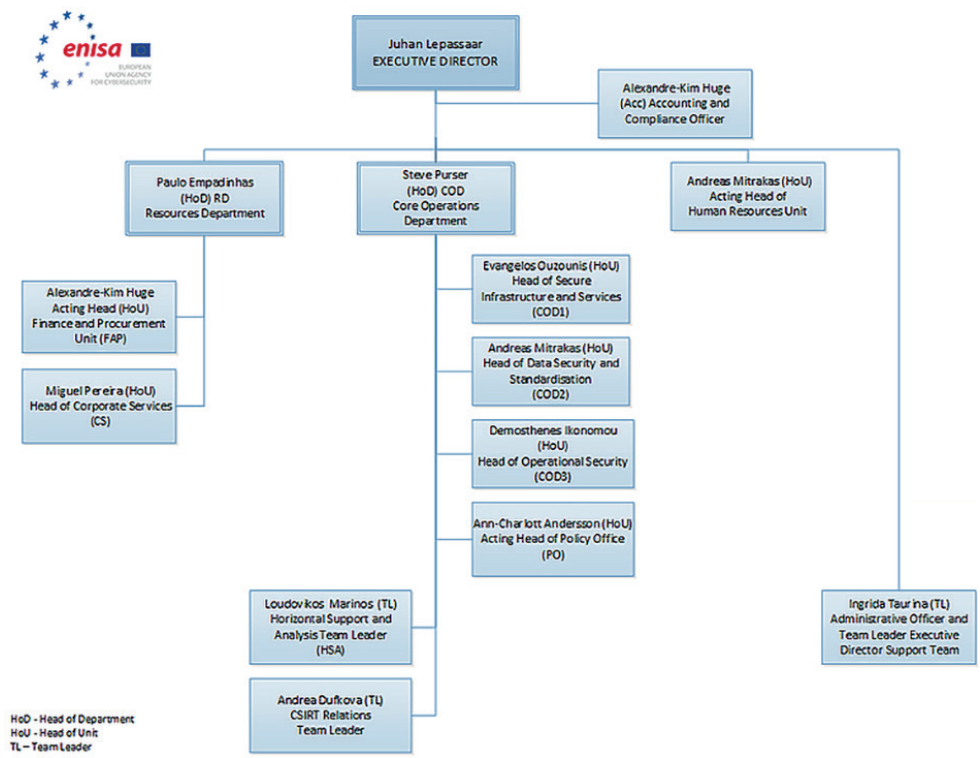
gozza és végrehajtja az Európai Unió kiberbiztonsági politikájával és az azokat érintő jogokkal kapcsolatos ügyeket.[44]

Az (EU) 2019/881 rendelet szerint az Ügynökség *testületei* a következőkből állnak:

Az *igazgatótanács* biztosítja, hogy az Ügynökség olyan körülmények között végezze feladatait, amelyek lehetővé teszik az alapító rendelettel összhangban történő szolgálatot. *A végrehajtó testület,* az igazgatóság előkészíti az igazgatótanács által elfogadandó határozatokat. Az *ügyvezető igazgató* felel az Ügynökség irányításáért, és feladatait függetlenül látja el. A *nemzeti összekötő tisztviselők hálózata (NLO)* megkönnyíti az információcserét az ENISA és az EU tagállamai között. A *tanácsadó csoport* az érdekelt felek szempontjából releváns kérdésekre összpontosít, és felhívja rájuk az ENISA figyelmét.

Az (EU) 2019/881 rendelet azt is előírja, hogy az ENISA segíti a Bizottságot az Európai Kiberbiztonsági Tanúsító Csoport (ECCG) titkárságának ellátásában, az ENISA pedig az érdekelt felek kiberbiztonsági tanúsító csoportjának (SCCG) titkárságát biztosítja.

Ad hoc munkacsoportok: az ügyvezető igazgató – az állandó érdekképviseleti csoporttal konzultálva – szakértőkből álló ad hoc munkacsoportokat hoz létre, amelyek konkrét műszaki és tudományos kérdésekkel foglalkoznak.



1. ábra: Az ENISA szervezeti ábrája

Forrás: www.enisa.europa.eu/about-enisa/structure-organization (A letöltés dátuma: 2020. 04. 03.)

[44] Szentgáli 2013, 296.

Az ENISA tevékenységének három területe:
- ajánlások;
- tevékenységek a politikai döntéshozatal és végrehajtás területén;
- *hands-on* munka (az ENISA közvetlen együttműködése az EU-n belüli műveleti csoportokkal).

Az 526/2013/EU rendelet pontosan meghatározza az Ügynökség feladatait, így:
- (23) segítenie kell az uniós intézményeket, szerveket, hivatalokat és ügynökségeket, valamint a tagállamokat a hálózat- és információbiztonság területét érintő problémák és váratlan események megelőzésével, észlelésével és kezelésével összefüggő, határokon átívelő képesség és felkészültség kialakítására és fokozására irányuló erőfeszítésekben az Ügynökségnek elő kell segítenie a Bizottság és más uniós intézmények, szervek, hivatalok és ügynökségek, valamint a tagállamok közötti együttműködést.
- (24) az Ügynökség elemezze a meglévő és a kialakulóban lévő kockázatokat. Ebből a célból az Ügynökségnek a tagállamokkal és a statisztikai szervekkel és másokkal együttműködve gyűjtenie kell a releváns információkat. Az Ügynökségnek emellett segítenie kell az uniós intézményeket, szerveket, hivatalokat és ügynökségeket, valamint a tagállamokat a hálózat- és információbiztonságra vonatkozó adatok gyűjtésére, elemzésére és terjesztésére irányuló tevékenységükben.
- (25) Feladatai végrehajtása során az Ügynökségnek elő kell segítenie az Unió és a tagállamok közötti együttműködést az uniós hálózat- és információbiztonság állapota ismertségének javítása céljából.
- (26) elő kell segítenie a tagállamok illetékes független szabályozó hatóságai közötti együttműködést, és ennek keretében támogatnia kell az oktatási és tudatosságnövelő programok területén a helyes gyakorlati megoldások és a standardok kialakítását, előmozdítását és cseréjét.
- (27) többek között segítenie kell az érintett uniós intézményeket, szerveket, hivatalokat és ügynökségeket, valamint a tagállamokat a végfelhasználók közoktatását szolgáló kampányokban.

Az ENISA *együttműködik még az EC3-vel és az Europollal* annak érdekében, hogy az Europol Kiberbűnözési Központja *(European Cybercrime Center – EC3)* és az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) közötti együttműködés fejlődjön, és annak érdekében, hogy az uniós tagállamok és az uniós intézmények segítséget kapjanak a kiberbűnözés megelőzésében és leküzdésében. A megállapodás nem terjed ki a személyes adatok megosztására.
Az *együttműködés* az alábbi elemeket tartalmazza:
- specifikus tudásanyag és szakértelem megosztása;
- az általános szituációs jelentések részletes kifejtése;
- a stratégiai elemzésekből és a helyes gyakorlatokból készülő jelentések;
- a kapacitásnövelés erősítése tréningeken és tájékoztató programokon keresztül az uniós szintű hálózati és információbiztonság megőrzése érdekében.

Az ENISA részt vesz az EC3 programtestületében *(EC3 Programme Board),* illetve az EC3 is tagja az ENISA-n belüli érdekelt felek állandó csoportjának *(Permanent Stakeholders Group),* amely az ENISA igazgatóját látja el tanácsokkal az éves munkatervet és a prioritásokat illetően. Az ENISA és az EC3 mindig is szorosan együttműködött a kiberbiztonság uniós szintű növelésében és a kiberbűnözés elleni harcban. Eddigi munkájuk eredményeként többek között kiadtak egy, a botnetek visszaszorításáról szóló közös tanulmányt; részt vettek az *Európai kiberbiztonsági hónapon (European Cyber-Security Month);* olyan kibergyakorlatokon vettek részt, mint amilyen a *CyberEurope;* a CERT-eknek szóló, helyes gyakorlatokat tartalmazó útmutatót adtak ki; szakmai műhelyek és konferenciák segítségével növelték a CERT-ek és a rendfenntartó erők közötti együttműködést.

Prof. Udo Helmbrecht, az ENISA ügyvezető igazgatója és Rob Wainwright, az Europol vezetője közös nyilatkozatot adott ki: „Ez a megállapodás egy fontos lépés abban a harcban, amit az egyre képzettebb kiberbűnözők ellen folytatunk, akik minden eddiginél több időt, pénzt és emberi erőforrást fordítanak a célzott támadások végrehajtására. A megállapodásunk jól példázza elkötelezettségünket, hogy saját szakterületünkkel járuljunk hozzá a közös erőfeszítéshez, és támogassuk egymás munkáját, amelynek célja, hogy Európában biztonságosabbá tegyük az online világot. Becslések szerint a kiberbűnözés éves szinten több mint 400 milliárd dollár kárt okoz a globális gazdaság számára. A szorosabb együttműködéssel és a szakértelem megosztásával erősebbé tesszük Európát a kiberbűnözők elleni harcban."[45]

CERT/CSIRT (Computer Emergency Response Team)

A *Computer Security Incident Response Team (CSIRT)* olyan információbiztonsági szakemberekből álló csoport, amelynek elsődleges feladata, hogy számítógépes biztonsági incidensek esetén beavatkozzon. Biztosítja az ezek kezeléséhez szükséges szolgáltatásokat, és támogatást nyújt vevőinek a rendszerfeltörések utáni helyreállításához.[46]

A CSIRT-hálózat tagjai kicserélik egymás között a biztonsági esemény technikai részleteit és elemzését, az IP-címeket, a fertőzöttségi mutatókat (IOC). Ezeket az információkat indokolatlan késedelem nélkül, de legkésőbb az esemény észlelése után 24 órával az ENISA rendelkezésére kell bocsátani.

A CERT-ek előnyei az ENISA által kiadott iránymutató szerint:

– Az információbiztonsági kérdések központi koordinációjának megvalósítása a szervezeten belül (kapcsolattartási pont).
– Az IT-incidensek központi és erre szakosodott kezelése, valamint az azokkal kapcsolatos beavatkozás.

[45] *A kiberbűnözés leküzdése: Stratégiai együttműködési megállapodást írt alá az ENISA és az Europol* 2014.

[46] Részletes leírás a CSIRT-csoportok létrehozásáról. WP2006/5. 1. sz. feladat (CERT D1/D2).

– Kéznél lévő szaktudás a biztonsági incidensek után a felhasználók által elvégzendő gyors helyreállítás támogatásához és segítéséhez.
– Jogi kérdések kezelése, a bizonyítékok megőrzése.
– A biztonság területén végzett fejlesztések nyomon követése.
– Az információbiztonsággal kapcsolatos együttműködés elősegítése, a tudatosságnövelés megteremtése.

A NIS-irányelv

A NIS-irányelv, azaz a hálózati és információs rendszerek biztonságáról szóló európai uniós irányelvet 2016-ban fogadták el, amely az uniós polgárok online védelmének javítását tűzte ki célul. A NIS-irányelv részletes bemutatását kerülni szeretném, ugyanakkor a fejezetben több szervezet és hivatal működésével kapcsolatban az abban foglaltak irányadók, így a legszükségesebb mértékben, pár mondat erejéig szükségesnek érzem, hogy foglalkozzunk vele. A kiberbiztonság fenntartásának egyik eszköze az elektronikus hálózati és információs rendszerek biztonsága, amibe beletartozik az adatok és információs rendszerek biztonsága is.

A hálózati- és információs rendszerek biztonsága azt jelenti, hogy megakadályozza mindazon fenyegetéseket, amelyek veszélyeztetik a bennük tárolt, továbbított, kezelt adatok vagy ezen rendszereken nyújtott, avagy a rajtuk keresztül elérhető, a hozzájuk kapcsolódó szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét és bizalmasságát. A kiberbiztonság (a hálózat- és információbiztonság együttese) ki kell, hogy terjedjen az elektronikus hírközlő hálózatokra, az adatvédelmi és a hálózatok ellenállását növelő szabályokra.

A NIS-irányelv egy olyan uniós szintű szabályozás, amely közös eszköztárat biztosít a tagállamok számára, továbbá egy európai uniós szintű együttműködés alapjait határozza meg jogi keretek között. Éppen ezért el lehet különíteni nemzeti és közösségi szinten végrehajtandó feladatokat. Az irányelv többek között az Európai Unió Kiberbiztonsági Ügynökségét (ENISA) mint kulcsszereplőt nevesíti, amely a NIS-irányelvben meghatározott feladatok és célok végrehajtásában és végrehajtatásában komoly szerepet játszó szervezet. Ezenfelül meghatározza az irányelv, hogy minden tagállamban ki kell jelölni szektoronként egy vagy több, számítógép-biztonsági eseményekre reagáló csoportot (CSIRT); lehet többet is, ezek az adott szektor kiberincidens-kezeléséért felelősek.

A NIS-irányelv hatályát tekintve két csoportot lehet megkülönböztetni:

Elsőként definiálja a gazdaság és a társadalom számára létfontosságú, úgynevezett alapvető szolgáltatásokat nyújtó szereplők csoportját, amelyhez a kritikus infrastruktúrák (létfontosságú rendszerelemek) meghatározott köre, az információs infrastruktúrák, az energetika, a közlekedés, a banki szolgáltatások, a pénzügyi szektor, az egészségügyi szektor és ágazatai tartoznak. A második csoportba a kulcsfontosságú információs szolgáltatók tartoznak.

Az alapvető szolgáltatásokat nyújtó szereplőknek a következő kötelezettségeket kell teljesíteni:

- Megfelelő és arányos műszaki és szervezési intézkedéseket kell tenniük a működésük során az általuk használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében (ilyen lehet a biztonsági kockázatmenedzsment keretében a sérülékenységi vizsgálatok, tesztek elvégzése).
- Az elektronikus információs szolgáltatás során megfelelő intézkedéseket kell tenni a hálózati és információs rendszerek biztonságát érintő biztonsági események megelőzésére és azok hatásainak csökkentésére a felsorolt szolgáltatások folytonosságának biztosítása céljából.
- Indokolatlan késedelem nélkül be kell jelenteni az illetékes hatóságnak vagy a létrehozott CSIRT-nek az általuk nyújtott szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági eseményeket.[47]

A polgári kiberbiztonság javítása fontos tényező, amely hozzájárul a hálózat- és információbiztonság általános ellenálló képességéhez. A hálózati és információbiztonságról (NIS) szóló irányelvjavaslat várhatóan javítja a nemzeti szintű felkészültséget, és erősíti a tagállamok közötti uniós szintű együttműködést mind stratégiai, mind operatív szinten. Ennek az együttműködésnek ki kell terjednie mind a kiberbiztonsági politikákat felügyelő nemzeti hatóságokra, mind a nemzeti CERT-ekre és a CERT-EU-ra. Az állami és magán NIS-platform célja a technológiai szempontból semleges bevált gyakorlatok azonosítása a kiberbiztonság fokozása érdekében, és ösztönzők kidolgozása a biztonságos IKT-megoldások elfogadására.

BEREC (Body of European Regulators for Electronic Communications)

BEREC Hivatala az uniós ügynökségek egyike, amelynek feladata, hogy szakmai és ügyviteli támogatást nyújtson az Európai Elektronikus Hírközlési Szabályozók Testületének (BEREC) (a továbbiakban röviden: BEREC vagy Testület).

A BEREC létrehozásának célja, hogy elősegítse az uniós szabályozás következetes végrehajtását, és ezáltal biztosítsa, hogy az elektronikus hírközlés egységes piaca megfelelően működjön.

A Testület tanácsokkal segíti az uniós intézmények munkáját ez utóbbiak felkérésére, illetve saját kezdeményezésre. A BEREC az úgynevezett *szabályozók tanácsából* áll, amelyet az egyes EU-országok nemzeti szabályozóinak vezetői (vagy kijelölt magas szintű képviselői) alkotnak.

Szervezeti felépítése: a BEREC Hivatalának élén az irányítóbizottság áll, amely az Európai Bizottság egy képviselőjéből és tagállamonként egy-egy tagból tevődik össze.

[47] Mezei 2019.

A BEREC Hivatala:
- szakmai és ügyviteli támogató szolgáltatásokat nyújt a BEREC szervezete számára;
- információkat gyűjt a nemzeti szabályozó hatóságoktól, valamint megosztja velük a bevált módszereket;
- segítséget nyújt a BEREC szabályozó tanácsa munkájának előkészítésében;
- szakértői munkacsoportokat állít fel.

A BEREC és közvetve a BEREC Hivatala a következő szervezeteket és egyéb érdekelt feleket szolgálja ki:
- európai, regionális és nemzeti intézmények az elektronikus hírközlés területén;
- az elektronikus hírközlési ágazatban működő vállalkozások és szakmai szövetségek;
- fogyasztók és fogyasztói egyesületek;
- tanácsadó irodák, kutatóintézetek, agytrösztök;
- tudományos dolgozók.

Európai Kiberbiztonsági Hálózat (European Network for Cyber Security – ENCS)

Az Európai Kiberbiztonsági Hálózat (ENCS) egy nonprofit tagszervezet, amely összehozza a kritikusinfrastruktúra-érdekeltségű tulajdonosokat és a biztonsági szakértőket azért, hogy biztonságos európai kritikusenergia-hálózatokat és -infrastruktúrákat telepítsen. A 2012-ben alapított ENCS elkötelezett kutatókkal és tesztelési szakemberekkel foglalkozik, akik az ENCS tagjaival és partnereivel együtt dolgoznak az alkalmazott kutatás területén, meghatározva a műszaki biztonsági követelményeket, a rendszerelemek és a végpontok közötti tesztelést, valamint az oktatást és képzést.[48]

2019. október 29-én felállítottak egy független stratégiai tanácsadó testületet, amelynek tapasztalati vezetői kérésre tanácsot adnak az ENCS igazgatótanácsa számára a stratégiai tervezés és a döntéshozatal folyamata során. A stratégiai tanácsadó testület tagjai nagykövetekként járnak el az ENCS igazgatótanácsa kérésére. A kapcsolatok fejlesztése és megerősítése fontos az ENCS-érdekelt felekkel, különösen az E.DSO[49]-val és az ENTSO-E[50]-vel és annak tagjaival.

A stratégiai tanácsadó testületnek hivatalosan nincs hatásköre, ezért nem szól bele az ENCS közgyűlése, a közgyűlés bizottsága és az igazgatóság hivatalos, ENCS-t érintő döntéseibe.[51]

[48] *ENCS – Our Mission* (é. n.)
[49] Európai Elosztórendszer-üzemeltetők *(European Distribution System Operators).*
[50] Átvitelrendszer-üzemeltetők Európai Hálózata *(European Network of Transmission System Operators).*
[51] *ENCS Strategic Advisory Board* 2020.

Európai Kiberbiztonsági Szervezet (European Cyber Security Organisation – ECSO)

Az Európai Kiberbiztonsági Szervezet (ECSO) egy teljes mértékben önfinanszírozású nonprofit szervezet, amelyet a belga törvények alapján hoztak létre 2016 júniusában.

Az ECSO képviseli az Európai Bizottság szerződésekben meghatározott partnerét a kiberbiztonsági szerződéses állami- és magánszféra partnerség (cPPP) végrehajtásában. Az ECSO-tagok széles körű érdekelt feleket, például nagyvállalatokat, kkv-kat és induló vállalkozásokat, kutatóközpontokat, egyetemeket, végfelhasználókat, üzemeltetőket, klasztereket és egyesületeket, valamint az Európai Unió helyi, regionális és nemzeti közigazgatásait, valamint az Európai Gazdasági Térség (EGT) és az Európai Szabadkereskedelmi Társulás (EFTA) és a Horizon 2020-hoz társult országokat segítik.
Az ECSO konkrét lépéseket tesz a céljaik elérése érdekében:

- együttműködik az Európai Bizottsággal és a nemzeti közigazgatásokkal a kutatás és innováció (K + I) előmozdítása érdekében a kiberbiztonság területén;
- javasolja a stratégiai kutatási és innovációs menetrendet (SRIA) és egy többéves ütemtervet annak rendszeres frissítéseivel;
- a piacfejlesztés, valamint a demonstrációs projektekbe és kísérleti projektekbe történő beruházások ösztönzése az innováció kiberbiztonsági piacra történő bevezetésének megkönnyítése érdekében;
- az európai kiberbiztonsági iparág (nagyvállalatok és kkv-k), valamint a végfelhasználók/üzemeltetők versenyképességének és növekedésének előmozdítása innovatív kiberbiztonsági technológiák, alkalmazások, szolgáltatások, megoldások révén;
- az innovatív kiberbiztonsági technológiák és szolgáltatások professzionális és magánfelhasználáshoz való legszélesebb körű és legjobb bevezetésének támogatása;
- elősegíti és segíti az európai kiberbiztonsági iparpolitika meghatározását és végrehajtását a kiberbiztonsági megoldások, valamint a biztonságos és megbízható IKT-megoldások használatának ösztönzése érdekében a digitális autonómia fokozása érdekében;
- támogatja a teljes kiberbiztonsági és IKT-biztonsági ökoszisztéma fejlesztését és érdekeit (ideértve az oktatást, a képzési tudatosságot stb.).[52]

Az Európai Rendőrségi Hivatal (Europol)

Az Europol 1999. július 1-jén kezdte meg teljes körű működését, azt követően, hogy a tagállamok ratifikálták az Europol-egyezményt. 2010. január 1-jén az ezen egyezmény helyébe lépő, az Európai Rendőrségi Hivatal (Europol) létrehozásáról szóló 2009. április 6-i, 2009/371/IB számú tanácsi határozat (tanácsi határozat) elfogadása után az Europol új jogi kerettel és kiterjesztett feladatkörrel rendelkező, teljes jogú uniós ügynökséggé vált.

Az Europol az Európai Unió bűnüldöző hatósága, amelynek fő feladata, hogy tevékenységével segítse az EU biztonságosabbá tételét. Az Európai Unió kormányközi,

[52] *About ECSO* 2020.

koordinációs és jogi végrehajtó szervezete. Feladatai közé tartozik az EU-tagállamok hatóságainak támogatása, a kölcsönös információmegosztás a nemzeti rendőrségekkel és a különböző bűnügyi adatok szakszerű elemzése. Hatáskörébe tartozik többek között a terrorizmus, a kábítószer-kereskedelem, a nemzetközi szervezett bűnözés, az ipari jog megsértése és a termékhamisítás, az illegális bevándorlás, továbbá a lopott autók csempészése, a pénzmosás és az euró hamisítása elleni fellépés és megelőzés.[53]

Hivatalos ügynökséggé 2010-ben vált, ezáltal egy sokkal integráltabb együttműködés kialakítása, kidolgozása lett a fő feladata. Az Europol célja, hogy javítsa az európai bűnüldöző hatóságok eredményességét és együttműködését a nemzetközi bűnözés súlyos formái, a szervezett bűnözés és a terrorizmus megelőzésében és leküzdésében. Az Europol szorosan együttműködve végzi a tevékenységét az Európai Unió 27 tagállamának bűnügyi hatóságaival, csakúgy, mint az USA, Kanada, Ausztrália és Norvégia bűnüldöző szerveivel. Ennek eredményeképp az Europol évi 13 500, határokon átnyúló nyomozáshoz nyújt hathatós segítséget elsősorban az adatbegyűjtés, -elemzés és -megosztás, valamint a koordináció eszközeivel. Az Europol eseti alapon részt vesz még a tagállamok területén tevékenykedő, úgynevezett *közös nyomozó csoportok* munkájában, ahol speciális eszközökkel és információkkal segíti a bűntények felderítését. Az Europol munkáját ezen felül segíti még a tagállamok és partnerországok által delegált, mintegy 145 összekötő tiszt is, akik az Europol székházában, Hágában tartanak fenn irodát, és a minél gyorsabb és hatékonyabb együttműködést, a személyes kapcsolatokat és a kölcsönös bizalom kiépítését segítik elő.

„Az Europol feladata, hogy támogassa és erősítse a tagállamok rendőri hatóságainak és egyéb bűnüldöző szolgálatainak tevékenységét, valamint a közöttük folytatott kölcsönös együttműködést a két vagy több tagállamot érintő bűncselekmények és a terrorizmus, valamint az uniós politikák alkalmazási körébe tartozó, közös érdekeket sértő bűnözési formák megelőzése és üldözése terén.

(2) Az Europol felépítését, működését, tevékenységi területét és feladatait rendes jogalkotási eljárás keretében elfogadott rendeletekben az Európai Parlament és a Tanács határozza meg. E feladatok a következőket foglalhatják magukban:

a) az információk, így különösen a tagállamok vagy harmadik országok hatóságai, illetve az Unión kívüli szervezetek által szolgáltatott információk összegyűjtése, tárolása, feldolgozása, elemzése és cseréje,

b) a tagállamok hatáskörrel rendelkező hatóságaival közösen vagy közös nyomozócsoportok keretében végzett nyomozati és operatív tevékenységek összehangolása, megszervezése és végrehajtása, adott esetben az Eurojusttal kapcsolatot tartva."[54]

Az Europol segíti az EU tagállamait a bűnüldözési tevékenységek során, például az alábbi területeken:[55]

- tiltott kábítószer-kereskedelem;
- terrorizmus;
- embercsempészet, emberkereskedelem és gyermekek szexuális kizsákmányolása;

[53] Tóth 2012, 72–73.

[54] Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata (2008).

[55] *Európai Rendőrségi Hivatal (Europol)* 2019.

– iparjogvédelmi jog megsértése és termékhamisítás;
– pénzmosás;
– pénz- vagy egyéb fizetőeszköz hamisítása – az Europol az euróhamisítás elleni küzdelem legfőbb európai felelőse.

Az Europol tagállamoknak nyújtott támogatása a következőket foglalja magában:
– az információcsere és a bűnügyi hírszerzés megkönnyítése az európai bűnüldöző hatóságok között az Europol információs és elemző rendszerei, valamint a biztonságos információcsere-hálózati alkalmazás (SIENA) segítségével;
– a tagállamok műveleteihez műveleti elemzés készítése, illetve támogatás nyújtása;
– a tagállamoktól vagy egyéb forrásból, illetve az Europoltól származó információk és adatok alapján stratégiai jelentések (például veszélyértékelések) és bűnügyi elemzések készítése;[56]
– szakértelem és technikai támogatás biztosítása az EU-n belüli nyomozásokhoz és műveletekhez, az érintett tagállamok felügyelete és jogi felelőssége mellett.

Az Europol a fentieken kívül a bűnügyi elemzések elősegítésével, a nyomozási technikák harmonizálásával és a tagállamokban adott képzésekkel is foglalkozik.

Ezen feladatai ellátásában segíti az *Europol Információs Rendszer* (továbbiakban: EIS), amely lényegét tekintve az Europol bűnügyi adatbázisa, elsődleges ellenőrző rendszere. A rendszer működtetésének célja, hogy az Europol mandátumába tartozó, súlyos megítélésű (a Btk. szerint legalább 5 év szabadságvesztéssel fenyegetett) és legalább két tagországot érintő bűncselekmények esetén a tagállamokban folyamatban levő nyomozásokat összekapcsolja, ezáltal orientálva és támogatva a nemzeti bűnüldöző hatóságok operatív, műveleti tevékenységét.[57]

Az EIS gyakorlati haszna abban áll, hogy segítségével megállapítható, hogy az Europol mandátumába tartozó ügyek esetében egy másik Europol-tagország rendelkezik-e a hazai nyomozáshoz kapcsolható információval. „Találat" esetén a tagállamok adatszolgáltató nyomozó szervei a nemzeti egységek közvetítésével kapcsolatba léphetnek egymással, és megállapodhatnak az információk felhasználhatóságát illetően. Magyarországon az Europol nemzeti egysége az Országos Rendőr-főkapitányság Nemzetközi Bűnügyi Együttműködési Központjában (ORFK NEBEK Iroda)[58] található.

Az Europol felállított egy csúcstechnológiai bűnözés elleni központot, amely 3 területen tevékenykedik munkacsoportokban:
– a gyermekek szexuális kizsákmányolása;
– készpénz-helyettesítő fizetési eszközzel kapcsolatos csalások;
– és a 3. munkacsoport, amelyből 2013 januárjában megalakult az EC3.[59]

[56] Europol Work Programmes.
[57] Brady 2008, 103–109.
[58] Hegyaljai 2012, 3–4.
[59] Simon 2018.

IOCTA – Internet Organized Crime Threat Assessment

Az Europol minden évben összesíti a számítógépes bűnözéssel kapcsolatos főbb trendeket és fenyegetéseket. Az Internet Organized Crime Threat Assessment (IOCTA) jelentése szerint a támadások tekintetében továbbra is a zsarolóvírusok jelentik a legnagyobb problémát.

Az internetes szervezett bűnözéssel foglalkozó részleg kurzusok szervezésével és technikai eszközök beszerzésével, fejlesztésével támogatja a tagállamok hatóságait, valamint a magánszektorral és a tudományos világgal is kapcsolatot tart a nyomozások fellendítése érdekében. Az internetes szervezett bűnözésről 2011 óta évente ad ki stratégiai elemzéseket, amelyek főleg az ilyen jellegű bűncselekmények értékeléseit tartalmazzák. Az Europol rendelkezik egy úgynevezett kiberbűnözési, több elemből álló platformmal, amelynek részei:

– az internetes bűncselekmények bejelentésére szolgáló online rendszer *(Internet Crime Reporting Online System, I-Cros).* Ebbe a rendszerbe a világhálón észlelt bűntettekkel kapcsolatos információkat lehet feltölteni;
– egy kiberbűnözési munkafájl;
– egy technikai szakismeretek bővítését ellátó internetes kriminalisztikai platform *(Internet Forensic Expertise Platform, I-Forex).*[60]

Europol Számítástechnikai Bűnözés Elleni Központ (European Cybercrime Centre, EC3)

Az Európai Bizottság 2012. március 28-án nyújtotta be javaslatát a számítástechnikai bűnözés elleni küzdelem európai központjának létrehozására, ami a Stockholmi Program egyik fontos eleme, célja a polgárok védelme, valamint a szervezett bűnözés és a terrorizmus elleni küzdelem javítása.[61]

A központot Hágában az Európai Rendőrségi Hivatalon belül hozták létre, működését 2013. január 11-én kezdte meg. A központ célja, hogy

– európai kapcsolattartó pontként működjön a számítástechnikai bűnözés elleni küzdelemben;
– részt vegyen az unión belüli rendészeti koordinációban;
– operatív támogatással segítse a tagállami rendészeti szerveket a konkrét nyomozások során.

A központ feladata elsősorban a számítógépes bűnözés elleni harc koordinálása, különös hangsúlyt fektetve a nagy nyereséggel járó bűnözés elleni tevékenységre. A további feladatok között megtaláljuk még a személyazonosság-lopás elleni küzdelmet, az elektronikus bankszolgáltatásokat érintő bűncselekmények elleni harcot, a gyermekek szexu-

[60] Tóth 2012.
[61] *Az Európai Tanács tájékoztatása. A Stockholmi Program* 2010.

ális kizsákmányolása elleni harcot, illetve az Európai Unió kritikus infrastruktúráinak és informatikai rendszereinek korlátozott védelmét.[62]

Az EC3 45 főből áll, többek között elsőrendű kibernetikai szakértőkkel kezdte meg tevékenységét, nincs önálló nyomozati jogköre.

A célok tükrében az EC3-nak 5 feladatköre van tehát:

Adatgyűjtés a számítógépes bűnözésről. Ezen adatok feldolgozása, egy számítógépes bűnözési helpdesk üzemeltetése a tagállami nyomozó hatóságok részére.

A számítógépes bűnözés elleni nyomozás támogatása a tagállamok számára azzal, hogy támogatja a közös nyomozócsoportok létrehozását egy vagy több tagállam együttműködésével, valamint megteremti és koordinálja a tagállamok közötti együttműködést a számítógépes bűncselekmények nyomozásában. Továbbá szoros együttműködést teremt az Eurojusttal és az Interpollal.

Értékeli és elemzi a kibertérből érkező fenyegetéseket, módszereket, és ezekből előrejelzi a számítógépes bűnözés alakulását.

A magánszférával történő szoros együttműködés, valamint a CERT-ekkel történő kapcsolattartás annak érdekében, hogy felkészültek legyenek a kibertámadásokkal szemben, és fel tudjanak lépni ellenük.

A K+F és a képzés során szorosan együttműködik a Cepollal, a tagállamok nyomozó hatóságaival és igazságügyi szervezeteivel, akiknek a folyamatos képzését, forenzikus eszközeik fejlesztését támogatja.

Az EC3 hatáskörébe tartozó fókuszpontok a számítógépek és a hálózati infrastruktúrák ellen végrehajtott bűncselekmények kivizsgálása, valamint a különböző internetes bűncselekmények *(FP Cyborg),* a gyermekek szexuális kizsákmányolása *(FP Twins)* mellett a bankkártyákkal történő csalások és a személyes adatokkal történő visszaélések is *(FP Terminal).*

A központ kiemelt feladata, hogy figyelmeztesse a tagállamokat az esetleges fenyegetettségekre. Szintén lényeges lépés az online szervezett bűnözői csoportok felkutatásának és azonosításának támogatása, ezt erősítve a központ tagállami szinten is képes segítséget nyújtani konkrét nyomozásokhoz.

Európai Kiberbűnözés Elleni Akciócsoport (European Union Cybercrime Task Force – EUCTF)

Az akciócsoportot 2010-ben alakították. A szakértői csoport az Europol, az Eurojust és az Európai Bizottság képviselőiből, valamint a tagállami, számítógépes bűnözéssel foglalkozó egységek vezetőiből áll. A csoport hozzájárul az informatikai bűncselekmények elleni küzdelem harmonizált európai megközelítésének fejlesztéséhez és támogatásához, valamint célba veszi azokat a problémákat, amelyeket az információs technológia bűncselekményekhez való felhasználása okoz.[63]

[62] Szentgáli 2013, 299–300.

[63] *Európai Rendőrségi Hivatal (Europol)* 2019.

Az EUCTF kiberbűnözéssel kapcsolatos céljai többek között:
- a számítógépes bűnözés és a számítógépes alapú bűncselekmények megelőzése és felderítése;
- a hatékony internetirányítás előmozdítása;
- a bűnügyi infrastruktúra megszakítása és szétszerelése;
- megakadályozza és leküzdheti a fekete gazdaságot *(underground economy)* az interneten;
- javítani kell az EU LEA[64]-információcserét és az operatív együttműködést;
- együttműködés az információbiztonsági iparral;
- a képzések és fejlesztésének felügyelete.

Az EUCTF-et egy külön testület irányítja, amely elnökből, alelnökből és igazgatósági tagból áll, akiket a tagság két évre választ. Ezen felül az igazgatótanács az EU Bizottsága és az Európai Kiberbűnözői Központ (EC3) egy-egy képviselőjéből áll.

Az EC3 állandó titkársági szolgáltatást nyújt az EUCTF és az igazgatóság munkájának támogatására.[65]

Stratégiai küldetése részeként a munkacsoport részt vesz az éves internetes szervezettbűnözés-fenyegetésről szóló (IOCTA-) jelentés elkészítésében.

A EUCTF feladatai közé tartoznak többek között olyan tevékenységek és javaslatok, amelyeket az egyes országok és országcsoportok az Europollal együttműködve képesek továbbfejleszteni az EMPACT operatív cselekvési terv keretében.

Az EUCF állandó képviselője az EUCTF testületének, és szoros együttműködésben működik a J-CAT-vel, előmozdítva működési tevékenységét az EUCTF tagjai között.[66]

The European Union's Judicial Cooperation Unit (Eurojust)

A szervezetet a Tanács 2002/187/IB határozata hozta létre, amelyet a Tanács 2008. december 16-i 2009/426/IB határozata módosított (Eurojust-határozat).[67] Az Eurojust feladata a nemzeti nyomozó hatóságok és ügyészségek hatékonyságának növelése a határokon átívelő, súlyos és szervezett bűncselekmények ügyeiben, és végső soron annak előmozdítása, hogy a bűncselekményt elkövetők felelősségre vonása gyorsan és eredményesen megtörténjék. Az Eurojust 2002-ben jött létre.

Hatásköre az Europol megbízhatóságához a szervezett bűnözés, súlyos bűncselekmények és a terrorizmus formáira terjed ki. Mindemellett az egyéb típusú bűncselekmények esetében az Eurojust tagállami megkeresés alapján nyújthat segítséget a nyomozásokban és a vádhatósági eljárásokban.

[64] LEA: Law Enforcement Agency.
[65] *EUCTF* (é. n.).
[66] *EUCTF* (é. n.)
[67] *Eurojust* 2020.

A 27 tagállam mindegyike magas beosztású nemzeti képviselőt delegál a Hága székhelyű Eurojusthoz, akik tapasztalt ügyészek, bírák vagy velük azonos hatáskörű rendőrtisztek. Ők végzik az Eurojust feladatait a nemzeti hatóságok nyomozásainak és ügyészi eljárásainak koordinálásában. Ugyanakkor a tagállamok jogrendszereinek különbözőségéből adódó nehézségeket és gyakorlati problémákat is megoldanak. A nemzeti tagokat helyetteseik, asszisztenseik és kiküldött nemzeti szakértők segítik. Azoknak a harmadik államoknak, amelyekkel az Eurojust együttműködési megállapodást kötött, összekötő ügyésze vagy bírója lehet az Eurojustnál. Ilyennel jelenleg Norvégia és az Egyesült Államok rendelkezik. Az EU-jog lehetővé teszi, hogy az Eurojust összekötő ügyészt vagy bírót küldjön harmadik államokba.

Az Eurojust ad otthont az Európai Igazságügyi Hálózatnak, a népirtás, emberiesség és háborús bűncselekmények elleni kontaktpontok hálózatának, továbbá a közös nyomozócsoportok szakértői hálózata titkárságának is.

Az Eurojust mintegy 260 fős EU-személyzettel rendelkezik, amely segíti a nemzeti hatóságok és az EU-szervek kéréseire való gyors reagálást is. Partnerei mind a nemzeti hatóságok, mind az olyan EU-formációk, mint például az Európai Igazságügyi Hálózat, az Europol, az OLAF (amennyiben az Európai Unió pénzügyi érdekeit érintő bűncselekményről van szó), a Frontex, a Sitcen, a Cepol, az Európai Igazságügyi Képzési Hálózat, továbbá minden más, a szerződések keretein belül elfogadott rendelkezések alapján kompetens szerv.[68]

Az Eurojust 2017-es éves jelentése alapján 70, számítógépes bűncselekményekkel összefüggő ügyben működött közre, és többek között aktívan részt vett a 2017-ben világszerte több kritikus infrastruktúrát is érő, a NotPetya-zsarolóvírus támadásaival kapcsolatos nyomozásokban.[69]

Join Investigation Team (JIT)

A közös nyomozócsoport (JIT) egy olyan nemzetközi együttműködési lehetőség, amely két vagy több állam illetékes hatóságai – mind az igazságügyi (bírók, ügyészek, nyomozási bírák), mind pedig a bűnüldöző szervek közötti megállapodásra épül, korlátozott időtartamra és meghatározott célra, nyomozások lefolytatására egy vagy több érintett államban. A közös nyomozócsoportok hatékony és eredményes együttműködési eszközt jelentenek, ami megkönnyíti a több államban párhuzamosan vagy határokon átnyúló ügyekben folytatott nyomozások és büntetőeljárások összehangolását.[70]

A közös nyomozócsoportokról szóló 2002/465/IB tanácsi kerethatározat 1. cikke (12) bekezdésének, valamint a 2000. évi, kölcsönös jogsegélyről szóló egyezmény vonatkozó rendelkezéseinek megfelelően az Eurojust és az Europol külön-külön és együttesen is részt vehetnek a közös nyomozócsoportokban. Ezenkívül az Eurojust és az Europol

[68] Buono 2012.
[69] *Eurojust – Éves jelentés 2017* 2019.
[70] *Eurojust – Joint Investigation Teams General Background* 2020.

közötti együttműködési megállapodás 6. cikke lehetővé teszi mindkét fél számára, hogy egy vagy több tagállam kérésére részt vegyenek a közös nyomozócsoport létrehozásában, és támogassák a nemzeti igazságügyi és bűnüldöző hatóságokat a közös nyomozócsoportok felállításában.

A gyakorlatban az Eurojust által a közös nyomozócsoportokhoz nyújtott támogatás különösen az alábbiakat foglalja magában:

– az esetek alkalmasságának értékelése a közös nyomozócsoport létrehozása esetében;
– segítségnyújtás a JIT-megállapodás kidolgozásában;
– jogi és gyakorlati támogatás a közös nyomozócsoport teljes élettartama alatt, ideértve a közös műveletek (koordinációs központok) támogatását is;
– a nyomozási és az ügyészi stratégiák összehangolása;
– joghatóság megállapítása és
– pénzügyi támogatás.

Az Európai Helyzetelemző Központ (EU INTCEN)

Az Európai Unió Helyzetelemző Központja (EU INTCEN) tulajdonképpen nem a rendőrségi együttműködés szerve, mivel az Európai Külügyi Szolgálat (EKSZ) részét képezi. Ettől függetlenül hozzájárul a rendőrségi együttműködéshez: a hírszerző szolgálatok, a katonaság, a diplomaták és a rendőrség által szolgáltatott információk alapján értékelést készít a fenyegetésekről. Az INTCEN tevékenysége operatív szempontból is hasznos, például a terroristák mozgásának célállomásaival, okaival és útvonalaival kapcsolatos, az EU egészére vonatkozó információk biztosítása révén.

Az INTCEN-nek két szervezeti egysége van. Az egyik az elemző-értékelő, míg a másik a nyílt forrású információkat feldolgozó osztály, amely az elérhető híroldalakat, a közösségi oldalakat folyamatosan monitorozza (7/24-es munkarendben, ezáltal megteremtve a valós idejű hírek figyelését).

Az INTCEN uniós kül- és biztonságpolitikát érintő, regionális vagy tematikus elemzéseket végez.

Fő feladata:

– az Európai Unió érdekszférájához tartozó térségek figyelemmel kísérése;
– korai előrejelző, stratégiai helyzetértékelő hírszerző jelentések készítése az EKSZ döntéshozói és főképviselői számára;
– helyzetértékelések és kockázatelemzések készítése azokról az országokról, ahol uniós műveletek folynak.

Az Európai Unió polgári műveleteket támogató, helyzetértékelő jelentéseit a szervezet 3-6 hónapra készíti el. Ezeket a jelentéseket megosztja a tagállamokkal is, ezen belül is a külügyminisztériumokkal, hírszerző szolgálatokkal, függetlenül attól, hogy az az adott tagállam vagy szolgálat bocsátott-e rendelkezésére információt a jelentéshez.[71]

[71] Marosi 2017.

A V4-ek és a Közép-európai Kiberbiztonsági Platform

A Visegrádi 4-ek, azaz a visegrádi együttműködés az Európai Unión belül 1991-ben létrejött regionális szervezet Magyarország, Lengyelország, Szlovákia és Csehország közreműködésével, a részt vevő országok közötti gazdasági, diplomáciai és politikai érdekeinek közös képviselete, esetleges lépéseinek összehangolása érdekében.

A nyilatkozatuk (deklarációjuk) célja, hogy eltüntessék a kommunista blokk maradványait Közép-Európában, megvédjék a demokráciát, a tagországok euroatlanti közösségéhez történő gyors együttműködését és gördülékeny csatlakozását elősegítsék. A folyamat befejezését követően újabb célkitűzéseket fogalmaztak meg a 21. században megjelenő globális kihívásokra és fenyegetésekre válaszul, amelyekkel szűkebb értelemben a tagállamok is szembe kellett, hogy nézzenek. Ausztria és Csehország kezdeményezésére Magyarország, Szlovákia és Lengyelország csatlakozásával létrehozták a Közép-európai Kiberbiztonsági Platformot *(Central European Cyber Security Platform – CECSP)* 2013-ban. A platform célja a szomszédos országok intenzív együttműködése a kiberbiztonság területén, különös tekintettel az információcserére és a know-how megosztására a kiberfenyegetések, valamint a potenciális és sikeres számítógépes támadások területén. A kiberbiztonsági intézkedésekkel kapcsolatos közös erőfeszítések megerősítik az államok pozícióit még a nemzetközi környezetben is. A kiberbiztonság biztosítása érdekében konszenzust kell találni az új biztonsági kihívásokkal való szembenézésben, és ezt európai szinten együttesen kell támogatni.[72]

Ennek megvalósítása érdekében öt pontban fogalmazták meg a feladatukat:

- Információ, know-how és a legjobb, leghatékonyabb gyakorlatok bemutatása, a kiberfenyegetésekkel szembeni ellenálló képesség javítása és az ahhoz szükséges felkészültség előmozdítása érdekében a tagállamok elkötelezik magukat, hogy megerősítik képességeiket, és ehhez rendszeresen megosztják az információkat és a legjobb gyakorlatokat a kiberbiztonság területén. A közös képzés, oktatás és gyakorlatok tervezése, szervezése is részét képezik a megállapodásnak.
- Biztonságos kommunikációs csatornák megtervezése és megvalósítása. A jövőbeli, a jelenlegi és a már megoldott, múltbeli kiberfenyegetésekkel összefüggő adatok, információk biztonságos továbbítása érdekében a tagállamainak (értsd V4 tagállamai) törekedni kell arra, hogy olyan információs csatornákat alakítsanak ki, amelyekhez illetéktelenek nem képesek hozzáférni és azokat lehallgatni.
- A definiálási és megegyezési besorolási rendszerre vonatkozóan az információk megosztása érdekében a tagállamoknak meg kell állapodniuk az érzékeny adatok tekintetében egy mindenki által elfogadott besorolási rendszerben. Olyan ajánlások megfogalmazása és lefektetése a cél, amelyek alkalmazásával könnyebbé válik az adott kiberbiztonsági incidens megértése és elemzése.
- Az egyéni álláspontok összehangolása és képviselete a nemzetközi fórumok előtt. A nyilatkozat szerint a résztvevőknek minden nagyobb nemzetközi szintű megbeszélés

[72] *Central European Platform for Cybersecurity* (é. n.).

előtt (NATO, EU, ENSZ, OSCE és ENISA) konzultálni kell a nemzeti álláspontjukat illetően a regionálisan átnyúló megközelítések harmonizálása érdekében.
– Gyakorlati munkacsoportok létrehozását is feladatul tűzték ki, amelyeknek speciális témák megvitatása céljából lehetőségük van alkalmi munkacsoportok létrehozására is. A legalább két tagállam részvételével működő munkacsoportok jellege attól függ, hogy milyen céllal, milyen alapon hozták azokat létre (például műveleti, politikai, irányítási, műszaki stb.). A közös ügyek, közös témák vonatkozhatnak szabványosításra és az adott aktuális fejlesztésekre is, mint az eszközök, hardverek beszerzésére, szoftverek hitelesítésére, határokon átnyúló együttműködésre.

A Közép-európai Kiberbiztonsági Platform tevékenysége és eredményességének oka a megalakulása óta főleg a felsorolt irányelveket szem előtt tartva leginkább a kölcsönös tapasztalatcseréről és a közös gyakorlatok megszervezéséről szólt, ami főleg az eltérő stratégiákban, a külpolitikai hangsúlyeltolódásokban, az információk és tapasztalatok megosztási hajlandóságának csökkentésében keresendő. Rajnai Zoltán, hazánk kiberbiztonsági koordinátora rámutatott arra, hogy Magyarország 2013-ban a tagállamok közül elsőként alkotta meg a Nemzeti Kiberbiztonsági Stratégiáját, de Csehország és Lengyelország átvette az innovatívabb szerepet. Ennek ellenére úgy látja, hogy van remény a visegrádi négyek kibervédelmének összeahangolására, de a cél eléréséig hosszú az út, ami kompromisszumok megteremtésével párhuzamosan az érintett államok közötti bizalom kiépítésével érhető el.[73]

A kibervédelem, a kiberbiztonság és a kiberbűnözés elleni harc nemzetközi szereplői

A címben szereplő három fogalom együttes használata nem véletlen tehát, ahogy az európai uniós szervezeteknél és szabályozásoknál is láthatjuk. A nemzetközi szervezetek esetében is törekedtem arra, hogy összegyűjtsem azokat a szervezeteket, értelemszerűen egy sokkal nagyobb földrajzi és jogszabályi területről, amelyek az EU-ban fellelhető szervezeteknek megfelelő feladatkörökkel, jogkörökkel rendelkeznek.

Gazdasági Együttműködési és Fejlesztési Szervezet (Organisation for Economic Co-operation and Development – OECD)

A Gazdasági Együttműködési és Fejlesztési Szervezetet 1948-ban hozták létre az Egyesült Államok által finanszírozott, a háború által elpusztított kontinens újjáépítésére szolgáló Marshall-terv végrehajtására. A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) hivatalosan 1961. szeptember 30-án született meg az arról szóló egyezmény hatálybalépésével, azért, hogy ösztönözze a gazdaságot.

[73] A Visegrádi Négyek helyzete a kibervédelem tekintetében (é. n.).

Az OECD 1983–1985 között készült jelentése négy jogsértő cselekményt nevezett meg:
- számítógépes csalás;
- számítógépes hamisítás;
- számítógépes szabotázs;
- szerzői jogi jogsértések.[74]

Az OECD ugyanakkor nemcsak kezdetben foglalkozott a számítógépes bűnözéssel és kibervédelemmel, 1992-ben kiadta az információs rendszerek biztonságára vonatkozó irányelveket, amely hozzájárult a biztonságkultúra kialakulásához és az „új gondolkodás- és viselkedésmódok meghonosításához".[75] Ezt az irányelvet 1997-ben felülvizsgálták.

Az információs rendszerek és hálózatok biztonságára vonatkozó OECD-irányelvek: Útban a biztonságkultúra felé címmel már kilenc alapelvet fogalmazott meg a biztonsági kultúra megvalósítása érdekben, amit az OECD-tanács ajánlásaként fogadták el a 2002. július 25-i 1037. ülésén. Alapelvei:

1. A *tudatosítás elve,* amely szerint az információs rendszerek és hálózatok hasznát csak úgy lehet élvezni, illetve a veszélyeiket úgy lehet elkerülni, ha azokat a biztonsági kockázatok tudatában használják.

2. A *felelősség elve* szerint ahhoz, hogy a biztonságot fenn lehessen tartani, minden alkalmazottnak tudatában kell lennie saját felelősségének, és ezt számon lehessen majd rajtuk kérni. A szervezeteknek rendszeresen felül kell vizsgálniuk saját szabályzataikat, gyakorlataikat, intézkedéseiket és eljárásaikat, ezeket értékelniük kell aszerint, hogy azok megfelelők-e.

3. A *válaszintézkedések elvének* megfelelően az alkalmazottaknak kellő időben, egymással együttműködve kell a váratlan biztonsági eseményeket megelőzni, észlelni, valamint ezekre a megfelelő válaszintézkedéseket megtenni. A szervezeteknek szükség szerint meg kell osztaniuk egymással a fenyegetésekkel és a sebezhetőséggel kapcsolatos információkat, valamint gyors és hatékony eljárásokat kell végrehajtani válaszul azért, hogy együttműködve megelőzzék, észleljék a váratlan biztonsági eseményeket, a megfelelő reagálás végett.

4. Az *etika elve* alapján az érintetteknek tiszteletben kell tartania mások jogos érdekeit. Az egyéneknek fel kell ismerniük, hogy a cselekedeteik vagy épp azok hiánya káros hatással lehet a többi munkavállalóra. Az érintetteknek törekedniük kell arra, hogy kialakítsák a jó gyakorlatot, és azt alkalmazzák is a biztonság igényének elfogadása és mások jogos érdekeinek tiszteletben tartása mellett.

5. A *demokrácia elve* szerint az információs rendszerek és hálózatok biztonságát megvalósító megoldásoknak a demokratikus társadalmak alapvető értékeivel összeférhetőnek

[74] *Computer-Related Criminality: Analysis of Legal Police* 1986, 28.
[75] *Az információs rendszerek és hálózatok biztonságára vonatkozó OECD-irányelvek: Útban a biztonságkultúra felé* 2003.

kell lenniük. A gondolatok és eszmék cseréjének szabadságát, az információ szabad áramlását, a személyes adatok megfelelő védelmét, azok nyitottságát és az átláthatóságot indokolatlan mértékben nem szabad korlátozni.

6. A *kockázatfelmérés elve* szerint a biztonság megtervezése és megvalósítása során a releváns kockázatokat fel kell mérni. A kockázatfelmérés lehetővé teszi a még elfogadható szervezeti kockázati szint meghatározását. Ezen felül segítséget nyújt az információs rendszerek és hálózatok biztonságát fenntartó megfelelő szabályozások kialakításában a megvédendő információk jellegével és fontosságával arányban. Figyelve az információs rendszerek összekapcsolására, a kockázatfelmérésnek ki kell térnie a másoktól származó vagy mások részére okozható hatásokra.

7. A *biztonságtervezés és végrehajtás elve* szerint az érintetteknek a biztonságot az információs rendszerek és hálózatok kialakítása során lényeges szempontként kell kezelni és azt megvalósítani.

8. A *biztonságmenedzsment elvének* jelentése, hogy az érintetteknek minden szempontra kiterjedő módon kell a biztonságmenedzsment-feladatokat végezni. A biztonságmenedzsmentnek kockázatfelmérésen kell alapulni, beleértve az érintettek tevékenységének és működésének minden vonatkozását.

9. Az *újraértékelés elvének* egyik fontos pontja, hogy folyamatosan megjelennek új és változó fenyegetések és sebezhetőségek, ezért az érintetteknek az információs rendszerek és hálózatok biztonságát folyamatosan felül kell vizsgálniuk és újra kell értékelniük. A biztonsági irányelvekben, gyakorlatokban, intézkedésekben és eljárásokban a szükséges módosításokat el kell végezniük.[76]

A jelenlegi – második fejezetben említett – kiberbiztonsági stratégiák közös elemei számos olyan fogalmat tartalmaznak, amelyek ösztönözhetik az OECD által alkotott és elfogadott iránymutatások kidolgozását a nemzeti politikai döntéshozatal szempontjából, például: 1. stratégiai megközelítés elfogadása; 2. erős vezetés támogatása; 3. a kiberbiztonság holisztikus kezelése – ideértve az adott ország kultúrájához és kormányzási stílusához igazított hatékony koordinációs mechanizmusokat; 4. a nem kormányzati érdekelt felek bevonása; 5. rugalmas politikai megoldások előmozdítása; 6. az önszabályozás és a köz- és magánszféra partnerségének ösztönzése; 7. az alapvető értékek tiszteletben tartása a megfelelő biztosítékok, ellenőrzések és egyensúlyok kialakításakor; 8. és a nemzetközi együttműködés előmozdítása, például a kibertérben a viselkedés általános normáinak elfogadásával.

Ahogy rámutat: „Az 1990-es évek eleje óta az OECD hatalmas szakértelemmel rendelkezik az információs rendszerek és hálózatok biztonságával és más ahhoz kapcsolódó területekkel összefüggésben, ideértve az elektronikus hitelesítést, a kriptográfiai politikát és a kritikus információs infrastruktúrák védelmét. Mindeddig az OECD digitális világban alkalmazott biztonságpolitikai megközelítésének célja olyan biztonsági politikai keretek kidolgozása volt, amelyek lehetővé teszik az IKT-k és az internetes gazdaság

[76] *Az információs rendszerek és hálózatok biztonságára vonatkozó OECD-irányelvek: Útban a biztonságkultúra felé* 2013.

új növekedési forrásai megragadását, az innováció előmozdítását és a társadalmi jólét fokozását. Az OECD fő eszköze, amint azt a 2002. évi biztonsági iránymutatások tükrözik (…), az a képessége, hogy magas szintű, rugalmas szakpolitikai elveken alapuló ajánlásokat dolgozzon ki, konszenzuson alapuló folyamat révén, valamennyi érdekelt felet bevonva."[77]

FIRST (Forum of Incident Response and Security Teams)

A FIRST 1990-ben alakult meg, reagálva egyes eseményekre, amelyek előzménye volt egy 1988 novemberében bekövetkezett számítógépes biztonsági esemény, az úgynevezett *internetes féreg* támadása, ami az internet jelentős részét térdre kényszerítette. Az incidensre az érintettek eltérően reagáltak, és nem volt összhang, ami sokszorosított erőfeszítésekhez és ellentmondásos megoldásokhoz vezetett. Hetekkel később létrejött a CERT Koordinációs Központ. Az elkövetkező két évben az eseményekre reagáló csoportok száma tovább növekedett, mindegyik saját céllal, finanszírozással, jelentéstételi kötelezettséggel és érdekelt (érintett) felekkel rendelkezik. A csapatok közötti interakció nehézségekbe ütközött a nyelv, az időzóna, valamint a nemzetközi szabványok vagy egyezmények eltérései miatt. 1989 októberében a *Wank-féreg* elnevezésű súlyos esemény rámutatott a jobb kommunikáció és a csapatok közötti koordináció szükségességére.[78]

A FIRST-tagság sokféle szervezetből áll, így az oktatási, kereskedelmi, szállítói, kormányzati és katonai szervezetek eseménykezelő csoportjaiból.

A FIRST szervezeti felépítése csúcsán áll az igazgatóság, amely olyan személyek csoportja, akik felelősek az általános működési politikákért, eljárásokért és a kapcsolódó kérdésekért, amelyek a társaság egészét érintik. Az igazgatóság két részből áll: az egyik az állandó igazgatóság, emellett működik az úgynevezett ad hoc jellegű igazgatóság.

A szervezet titkársága adminisztratív feladatokat lát el, míg a FIRST Bizottságának – amelynek tagjait az igazgatóság nevezi ki – feladata, hogy támogassa a tagsági jelentkezési és felülvizsgálati folyamatokat, a tagság felvétele és megtartása tekintetében döntsön, és áttekintse a tagsági folyamatot és a kommunikációt.

Ötödik szervezete a rendes közgyűlés, amely évente megvitatja a szervezet igazgatótanácsának évente megüresedett helyére jelentkező jelöltek személyét.

A FIRST számos, számítógépes biztonsági eseményekre reagáló csoportot is létrehoz a kormányzati, kereskedelmi és oktatási szervezetekből. Az FIRST célja az együttműködés és a koordináció előmozdítása az események megelőzése terén, az eseményekre való gyors reagálás ösztönzése, valamint a tagok és az egész közösség közötti információcsere előmozdítása. A FIRST a bizalmi hálózaton kívül – amelyet

[77] *Cybersecurity Making at Turning Point…* 2012.
[78] *FIRST* (é. n.).

a globális eseményekre reagáló közösségben alkot – *hozzáadottérték-szolgáltatásokat* is nyújt. Néhány ezek közül:

- a tagok számára hozzáférés a legfrissebb, bevált gyakorlati dokumentumokhoz;
- műszaki vizsgák a biztonsági szakértők számára;
- gyakorlati órák szervezése és tartása;
- éves eseményekre reagáló konferenciákat tart a kiberbiztonsági eseményekkel kapcsolatban;
- kiadványok és webszolgáltatások nyújtása;
- speciális érdekcsoportok kialakítása.[79]

Jelenleg a FIRST több mint 500 taggal rendelkezik Afrikában, Amerikában, Ázsiában, Európában és Óceániában.

A FIRST-nek különleges érdekcsoportjai vannak *(SIGs, Special Interest Groups),* ahol a szervezet tagjai megvitathatják mindazon témákat, amelyek az incidenskezelő közösség érdeklődésére számot tarthatnak. A SIG egy olyan csoport, amely a FIRST-tagokból és a meghívott felekből áll, és általában azért jönnek össze, hogy azokon megvitassanak egy-egy érdeklődésre számot tartó területet vagy egy meghatározott technológiai területet azzal a céllal, hogy együttműködjenek és megosszák tapasztalataikat a közös kihívások kezelése érdekében. Ilyen különleges érdekcsoportok:

- munkacsoportok *(working groups);*
- szabványügyi csoportok;
- vitacsoportok;
- *Bird of a Feather Sessions (BoF).*

A munkacsoportokat az igazgatótanács szavazással kezdeményezi, egy tag által javasolt alapszabály alapján. A jelenlegi munkacsoportok a következőket foglalják magukban:

- tudományos biztonsági SIG;
- *Big Data* SIG;
- CSIRT keretfejlesztési SIG;
- kiberbiztonsági fenyegetések figyelése és jelzése (*Cyber Threat Intelligence* SIG);
- *DNS Abuse* SIG;
- etikai SIG;
- információmegosztási SIG;
- *Red Team* SIG;
- *Security Lounge*[80] SIG;
- a biztonsági rés jelentése és adatcsere;
- sebezhetőség koordinációja.[81]

[79] *FIRST* (é. n.).

[80] A magyar fordítása nem adja vissza ennek a munkacsoportnak a feladatait. Ennek a SIG-nek a kiberbiztonsági versenyek, gyakorlatok szervezése és nyilvántartása a feladata.

[81] *Special Interest Groups (SIGs)* (é. n.).

A szabványügyi csoportok célja a belső használatra vagy a külső közzétételre vonatkozó szabvány kidolgozása. A kezdeményezés alapszabálya és az igazgatóság szavazása alapján indul. A jelenlegi szabványcsoportok a következők:
- közös biztonsági rés pontozási rendszere (CVSS);
- információbiztonsági cserepolitika;
- érzékeny információk megosztásának jelzésére irányuló, úgynevezett *jelzőlámpa-protokoll (Traffic Light Protocol – TLP);*
- passzív DNS-csere *(Passiv DNS-Exchange).*[82]

A vitacsoportok kevésbé strukturált csoportok a többihez képest, ezáltal lehetővé téve egy-egy adott téma megvitatását. A vitacsoportok nem igényelnek chartát, és általában nem is kapnak közvetlen forrásokat a szervezettől. A jelenlegi vitacsoportok a következők:
- malware-elemzés;
- mérőszámok;
- ipari vezérlőrendszerek *(Industrial Control System – ICS).*[83]

Európai Biztonsági és Együttműködési Szervezet (EBESZ)

Az Európai Biztonsági és Együttműködési Szervezet *(Organization for Security and Cooperation in Europe – OSCE)* jogelődje az Európai Biztonsági és Együttműködési Értekezlet.

Az EBESZ szervezete integráns része az euroatlanti intézmények rendszerének. Feladata a konfliktusok korai előrejelzése és megelőzése, a válságok kezelése és enyhítése, valamint a válság utáni időszak rehabilitációja és a konfliktusok utókezelése.[84]

A szervezet irányításáért a mindenkori soros EBESZ-elnökséget ellátó tagállam a főtitkárral együtt felel. 57 európai, észak-amerikai és közép-ázsiai részt vevő államból és 11 partnerállamból álló páneurópai biztonsági szervezet. Mivel az EBESZ a biztonság minden területét más szervezettel együttműködve kezeli, annak valamennyi részével külön-külön foglalkozik, amiben mind az 57 államnak egyenlő jogai vannak.

Az EBESZ folyamatosan alkalmazkodik az új biztonsági környezet okozta elvárásokhoz, és felvette a küzdelmet az új típusú fenyegetések ellen, mint például a terrorizmus, az ember- és kábítószer-kereskedelem, a szervezett bűnözés vagy a kiberbűnözés.

Az EBESZ Állandó Tanácsa – azért, hogy fokozza az egyéni és a kollektív erőfeszítéseket – 2012. április 29-én létrehozta az információs és kommunikációs technológiák átfogó kezelésének érdekében a kiberügyekkel foglalkozó informális munkacsoportot *(Informal Working Group – IWG),* amelynek feladatául a kiberbiztonsági bizalomépítő intézkedések *(Confidence Building Measures – CBMs)* kidolgozását határozta

[82] *Special Interest Groups (SIGs)* (é. n.).
[83] *Special Interest Groups (SIGs)* (é. n.).
[84] Remek 2017.

meg az államközi együttműködés, átláthatóság, kiszámíthatóság és stabilizáció, valamit az IKT-k használatából eredő félreértések, eszkalációk és konfliktusok kockázatának csökkentése érdekében.

Az összesen 16 bizalomépítő intézkedést tartalmazó 1202-es döntés alapján az abban részt vevő országok az alábbi feladatokat vállalták:

- Önkéntesen megosztják egymással a nemzeti álláspontjukat a nemzeti és a transznacionális fenyegetések különböző aspektusairól és az IKT-k használatáról.
- Önkéntesen elősegítik a kompetens nemzeti szervezeteik közötti együttműködést és információcserét az IKT-k vonatkozásában.
- Önkéntes alapon konzultációkat tartanak az IKT-k használata kapcsán felmerülő félreértésekből adódó politikai és katonai feszültségek csökkentése céljából.
- Önként megosztják a nyílt, interoperábilis, biztonságos és megbízható internet biztosításának céljából meghozott intézkedéseiket.
- Az EBESZ-t párbeszédek lefolytatására, az úgynevezett *jó gyakorlatok* megosztására, az IKT-k biztonságára vonatkozó kapacitásnövelés megvitatására és az egyes támadásokra adott hatékony válaszlépések megosztására alkalmas platformként kezelik és alkalmazzák.
- Olyan nemzeti szabályozásokat kívánnak létrehozni, amelyek lehetővé teszik a kompetens hatóságok, kiemelten a bűnüldöző szervek közötti kétoldalú együttműködéseket.
- Önként megosztják a nemzeti stratégiáikat, irányelveiket és programjaikat, beleértve az együttműködésüket az állami- és magánszférával, illetve az IKT-k biztonságát és alkalmazását.
- Kijelölnek egy kapcsolattartó pontot, megosztják a nemzeti struktúra egyes elemeihez tartozó kapcsolattartási adatokat, amelyeket egy esetlegesen bekövetkező incidens alkalmával használnak. Ezeket az adatokat évente frissítik.
- A közös terminológia hiányából adódó esetleges félreértések elkerülése végett egy magyarázatokkal és definíciókkal ellátott listát készítenek az IKT-k használatára és biztonságára vonatkozó terminológiákból.
- A kiberbiztonsági bizalomépítő intézkedésekkel kapcsolatos kommunikáció megkönnyítése érdekében az EBESZ-platformok és -mechanizmusok felhasználásával önkéntes alapon folytatnak eszmecserét.
- A kijelölt tagállami szakértők szintjén évente legalább 3 alkalommal találkoznak az IWG keretein belül, hogy a bizalomerősítő intézkedések tárgyalását, megvalósítását és továbbfejlesztését illetően döntsenek.
- Workshopok, szemináriumok, kerekaszta- beszélgetések szervezése és megtartása által támogatják az információmegosztást és az államok közötti információcserét.
- Elősegítik, hogy a tisztviselők és a szakértők védett és engedélyezett csatornákon keresztül kommunikáljanak a lehetséges félreértések, konfliktusok és eszkalációk megelőzése és csökkentése érdekében.
- Népszerűsítik az állami és a magánszféra közötti együttműködést.

– Elősegítik a regionális és kistérségi együttműködés kiépítését a kritikus infrastruktúrák biztonságáért felelős hatóságok között.
– Ösztönzik a felelős információmegosztást az IKT-k biztonságát és használatát érintő sérülékenységekre vonatkozóan, hiszen minden ilyen jellegű tájékoztatás és kommunikáció elősegíti az EBESZ-t érintő, régión belüli együttműködéseket.[85]

Egyesült Nemzetek Szervezete (ENSZ)

Az Egyesült Nemzetek Szervezete részéről több dokumentum foglalkozik az informatikai bűncselekmények megelőzéséről, kezeléséről, az információs technológiák elleni harcról.[86] Az 1994-ben kiadott kézikönyv – a számítógépes bűncselekmények megelőzéséről és kezeléséről – a számítógépes bűncselekmény *(computer crime),* valamint a számítógéppel kapcsolatos bűncselekmény *(computer-related crime)* fogalmakat még nem határolja el. Felsorolja ugyanakkor a kézikönyv a számítógépes bűncselekmények leggyakoribb típusait: a számítógép manipulációjával elkövetett csalás, a számítógépes hamisítás, a károkozás számítógépes adatokban vagy programokban, illetve a számítógépes adatok vagy programok megváltoztatása, a jogosulatlan hozzáférés számítógépes rendszerekhez és szolgáltatásokhoz, a jogi védelem alá eső számítógépes programok jogosulatlan reprodukálása.

A kézikönyv támaszkodik az 1989-ben született, az Európa Tanács által elfogadott ajánlásra.[87] Felismerték, hogy a számítógépes környezetben elkövetett bűncselekményekkel szemben nem elegendő a területi védekezés, mivel az a deliktum jellege miatt egy kiterjedtebb kört veszélyeztet.

Ugyanakkor a gyermekpornográfia bűncselekménye vagy épp a *cyberbullying,* más néven elektronikus zaklatás miatt kiemelést érdemel az 1989-es, a gyermekek jogairól szóló New York-i egyezmény, amely több szabályt is tartalmaz a gyermek káros tartalmakkal szembeni védelméről.

Az ENSZ közgyűlése a 2000-ben elfogadott határozatában már az információs technológiák bűncselekményekhez való felhasználásával szembeni harcra hívja fel a figyelmet, és olyan intézkedéseket azonosított, amelyek segítenek az információs technológiákkal való visszaélés megelőzésében, illetve az információs technológiákkal való visszaélések elleni fellépés érdekében. Így például az államok jogszabályai és joggyakorlata számolja fel a védett zónákat az információs technológiákkal való visszaélések esetében. Az információs technológiákkal való nemzetközi visszaélések esetében koordinálni kell az érintett államok között a nyomozó hatóságok együttműködését a nyomozásban

[85] Decision No.1202.

[86] *Az ENSZ kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről* 1994; az ENSZ Közgyűlésének 55/63. számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról; az ENSZ Közgyűlésének 56/121 számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról.

[87] *UN Manual on the Prevention and Control of Computer-Related Crime* 1994, vagyis az ENSZ számítógépes bűnözés megelőzéséről és szabályozásáról szóló tanulmánya.

és a vádemelésben. Fontos, hogy információmegosztás legyen az államok között, a nyomozó hatóságok személyzetének kiképzése és felszereléssel ellátása megoldott legyen. A jogrendszereknek védeniük kell az adatok számítógépes bizalmasságát, integritását és elérhetőségét a jogosulatlan megkárosítástól, és biztosítaniuk kell, hogy a visszaéléseket büntetni rendelik. A jogrendszereknek lehetővé kell tenniük a bűnügyi nyomozásokkal kapcsolatos elektronikus adatok megőrzését, és az ezekhez való gyors hozzáférést. A határozat rámutat, hogy a nyilvánosság figyelmének felhívására, a személyes szabadságjogok és a magánélet védelmének, valamint a kormányzat cselekvési lehetőségeinek megőrzésére az ilyen jellegű visszaélések elleni küzdelemben hangsúlyt kell fektetni.

ITU, azaz az International Telecommunications Union

Az ENSZ szervezete, az International Telecommunications Union (röviden ITU) a fejlesztési irodáján keresztül együttműködik a tagállamokkal, a partnerekkel és a regionális/nemzetközi szervezetekkel a nemzeti és regionális szintű kapacitásépítés, a képességek telepítése, valamint a nemzeti CIRT-k létrehozásának és fejlesztésének elősegítése érdekében. Az ITU eddig közel 80 CIRT-készségértékelést készített azért, hogy segítse az országokat nemzeti kiberbiztonságuk felmérésében.

Az ITU-nak a kiberbiztonsággal kapcsolatos feladata – többek között –, hogy segítséget kell nyújtania a fejlődő és a legkevésbé fejlett országok számára a kiberbiztonsággal kapcsolatos nemzeti politikák kidolgozásában és előmozdításában. Az ITU-nak a segítséget kell nyújtania a fejlődő és a legkevésbé fejlett országok számára a kiberbiztonsági események globális perspektíva elleni küzdelemre irányuló nemzeti, regionális és nemzetközi stratégiáinak kidolgozásában, segítenie kell a kormányokat olyan politikák és stratégiák kidolgozásában, amelyek célja a kiberbiztonsági kezdeményezések nemzeti, regionális és nemzetközi szintű koordinációjának javítása. A szervezet további segítséget nyújt az országoknak azok sajátos szükségleteire való reagálás szervezeti struktúrájának kialakításában, figyelembe véve az erőforrások rendelkezésre állását, az állami és magánszféra partnerségét, valamint az egyes országok IKT-fejlesztésének szintjét, a több érdekelt fél közötti együttműködés szellemében, amint azt vázolják a WSIS[88] eredményeiben.[89]

Az informatikai bűncselekmények elleni nemzetközi fellépés szükségessége, az internacionális együttműködés hatékonysága nem lehet kétséges a deliktumok országok határait átlépő jellege miatt. A digitális világ védelmében és biztonságának megőrzésében, azaz összefoglaló néven a kiberbiztonság eszközeinek tekinthető intézkedések megtételéhez relatíve egységes fogalmak kellenek. A kiberbiztonság jogi, technikai és szervezeti kihívásokat jelent, és mivel ezek globális jellegűek, így szükségessé vált egy koherens, nemzetközi együttműködés keretein belüli stratégia kialakítása. Csak ilyen jellegű stratégia az, amely alkalmas az érintett országok szerepének meghatározására, illetve a már

[88] WSIS: *World Summit on the Information Society,* azaz az információs társadalomról szóló csúcstalálkozó.
[89] Schjølberg 2008.

létező stratégiák számbavételére. A nemzetközi együttműködés szükségességét felismerve több internacionális szervezet foglalkozik a kiberbiztonság kérdésével. Ezek közül is kiemelkedik az ITU az általa megalkotott *Global Cybercrime Agenda*-val és a *Global Cybersecurity Index*-szel, valamint az *Európai Unió kiberberbiztonsági stratégiája*.

Az ITU létrehozta a *High Level Experts Groupot (HLEG),* azaz a magas szintű szakértői csoportot, ami a szervezet főtitkárának a kiberbiztonsággal kapcsolatos tanácsadói testülete. Ez a szakértői testület a világ elismert szakembereiből áll. A magas szintű szakértői csoport (HLEG), amelynek tagjait az ITU főtitkára nevezte ki, figyelembe véve mind a földrajzi sokféleséget, mind a szakértelem körét a több érdekelt fél közötti képviselet biztosítása érdekében. Több mint száz világhírű kiberbiztonsági szakemberből áll, akik széles körű háttérrel rendelkeznek, beleértve az ITU tagállamainak adminisztrációit, az ipart, a regionális és nemzetközi szervezeteket, a kutatást és az akadémiai intézményeket.

A HLEG fő feladatai többek között a konkrét stratégiák kidolgozása és javaslata a globális kiberbiztonsági menetrend fő céljainak elérése érdekében, jelentések vagy tájékoztató dokumentumok, műszaki know-how, tudás és szakértelem formájában a kiberbiztonság különböző aspektusaival kapcsolatban, valamint útmutatás nyújtása a lehetséges hosszú távú stratégiákról és a kiberbiztonság felmerülő tendenciáiról.[90]

A *Global Cybersecurity Index (GCI, Globális kiberbiztonsági felmérés)* egy olyan referencia, amely méri az országok elkötelezettségét a kiberbiztonság mellett.

A GCI 25 mutatót egy referenciaértéken egyesít azért, hogy figyelemmel kísérje és összehasonlítsa az országok kiberbiztonsági elkötelezettségének szintjét a globális kiberbiztonsági menetrend (GCA) öt pillére mentén:

- jogi intézkedések;
- technikai intézkedések;
- szervezeti intézkedések;
- képességfejlesztés és
- együttműködés.

Ebből az öt szempontból származó értékelések alapján összesített pontszámokat kapnak az egyes országok.[91]

Európa Tanács (ET)

Az Európa Tanács, amely nem tévesztendő össze az Európai Unió Tanácsával, egy nemzetközi szervezet, székhelye Strasbourg.

Az ET 2001. november 23-án Budapesten fogadta el a *Számítástechnikai bűnözésről szóló egyezményt (Convention of Cybercrime).* Az egyezmény 2004. július 1-jén lépett

[90] *ITU Global Cybersecurity Agenda* 2007.

[91] Magyarország 2018-ban a 19. helyen végzett az értékelt országok között.

életbe. Az Európa Tanács 5 tagállama – így Magyarország[92] is – ratifikálta a konvenciót. 2011. október 1-ig az Európa Tanács 31 tagja, valamint az Egyesült Államok részéről is az egyezmény elfogadása és törvénybe iktatása megtörtént. A számítástechnikai bűnözésről szóló egyezményt a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyv[93] követte.

Az Európa Tanács 12(81) sz. ajánlása a gazdasági bűncselekményekről elsőként foglalt össze néhány bűncselekményt *computer crime* elnevezéssel, igaz csupán példálózva.

Az Európa Tanács 9(89) sz. ajánlása a számítógépes környezetben elkövetett bűncselekményekről *(computer related crime)* a címében átfogó elnevezést használ, tartalmi meghatározás nélkül. Ez a dokumentum nemcsak, hogy leír egy minimális és egy fakultatív listát, hanem a szankcionálni javasolt bűncselekményeket is definiálja.

Az ET minimális listája:

1. *Számítógépes csalás (computer-related fraud):* Aki azzal a szándékkal, hogy a maga vagy más személy számára jogtalan előnyhöz jusson, számítógépes adatokat vagy programokat bevisz, megváltoztat, töröl, illetőleg hozzáférhetetlenné tesz, vagy az adatfeldolgozást bármilyen egyéb módon befolyásolja úgy, hogy azok hatással vannak az adatfeldolgozás eredményére, ezáltal más személynek gazdasági vagy birtokbeli kárt okoz, számítógéppel kapcsolatos csalást követ el.

2. *Számítógépes hamisítás (computer forgery):* Aki a nemzeti jog által meghatározott módon vagy körülmények között számítógépes adatokat vagy programokat bevisz, megváltoztat, töröl, illetőleg hozzáférhetetlenné tesz, vagy az adatfeldolgozást bármilyen egyéb módon befolyásolja úgy, hogy az megfelel a hamisítás bűntettének, amennyiben az ilyen típusú bűncselekmények hagyományos tárgyára tekintettel követte el, számítógépes hamisítást követ el.

3. *Számítógépes adatokban és programokban történő károkozás (damage to computer data or programs):* Aki számítógépes adatot vagy programokat jogtalanul töröl, károsít, eltérít vagy hozzáférhetetlenné tesz, kárt okoz.

4. *Számítógépes szabotázs (computer sabotage):* Aki azzal a szándékkal, hogy egy számítógép vagy telekommunikációs rendszer működését gátolja, számítógépes adatokat vagy programokat bevisz, megváltoztat, töröl vagy hozzáférhetetlenné tesz, a számítógépes rendszer működését befolyásolja, számítógépes szabotázst követ el.

5. *Jogellenes behatolás (unauthorized access):* Számítógépes rendszerbe vagy hálózatba történő jogosulatlan bejutás a biztonsági intézkedések megsértése révén.

6. *Jogosulatlan lehallgatás (unauthorised interception):* Jogosulatlan lehallgatás olyan kommunikációtechnikai módszerrel, amely számítógépes rendszer vagy hálózat útján valósul meg.

[92] 2004. évi LXXIX. törvény.

[93] A számítástechnikai bűnözésről szóló egyezménynek a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyve (é. n.).

7. *Védett számítógépes programok jogellenes másolása (unauthorised reproduction of a protected computer program):* Aki jog által védett számítógépes programot jogtalanul reprodukál, terjeszt vagy a nyilvánosság számára hozzáférhetővé tesz, bűncselekményt követ el.

8. *A félvezető topográfiák jogellenes másolása (unauthorised reproduction of a topography):* Aki jog által védett félvezető termék topográfiáját jogtalanul reprodukálja, vagy a félvezető terméket reprodukálás céljából jogtalanul hasznosítja, importálja, vagy jogtalanul félvezető terméket gyárt topográfia használatával, bűncselekményt követ el.[94]

Az ET fakultatív listája:

1. *Számítógépes adatok és/vagy programok megváltoztatása (alteration of computer data or computer programs):* Aki a számítógépes adatokat vagy programokat jogosulatlanul megváltoztatja, bűncselekményt követ el.

2. *Számítógépes kémkedés (computer espionage):* Aki kereskedelmi vagy üzleti titkot jogtalanul, illetve jogi felhatalmazás nélkül, helytelen eszközökkel megszerez, közzétesz, átruház vagy felhasznál azzal a szándékkal, hogy a titok jogosultjának gazdasági veszteséget okozzon, illetőleg magának vagy másnak jogtalan gazdasági előnyt szerezzen, bűncselekményt követ el.

3. *Számítógép jogellenes használata (unauthorised use of a computer):* Aki a számítógépes rendszert vagy hálózatot jogosulatlanul oly módon használja, hogy

– elfogadja a jelentős kockázatát annak, hogy a rendszer használatára jogosult személynek kára keletkezik, vagy a rendszerben, illetve annak működésében kár keletkezik;
– a szándéka arra irányul, hogy a rendszer használatára jogosult személynek kára keletkezzen, vagy a rendszerben, illetve annak működésében kár keletkezzen;
– a rendszer használatára jogosult személynek kára keletkezik, vagy a rendszerben, illetve annak működésében kár keletkezik,
– bűncselekményt követ el.

4. *Védett programok jogellenes használata (unauthorised use of a computer program):* Aki a jog által védett és jogtalanul reprodukált számítógépes programot jogtalanul használ azzal a szándékkal, hogy magának vagy másnak jogtalan gazdasági előnyt szerezzen vagy a jog tulajdonosának kárt okozzon, bűncselekményt követ el.[95]

A számítástechnikai bűnözésről szóló egyezmény védeni kívánja a számítástechnikai rendszerek, a hálózatok, az adatok hozzáférhetőségének sérthetetlenségét, az ilyen rendszerek titkosságát. Biztosítani kívánja a rendszerek, a hálózatok, az adatok visszaélésszerű használatának megelőzését és bűncselekménnyé nyilvánítását is. Továbbá meghatározza a számítógépes bűnözés elleni hatékony fellépést lehetővé tévő felderítést, a nyomozást és bűnüldözést nemzeti és nemzetközi szinten. Az értelmező rendelkezések körében az egyezmény több alapfogalmat definiál, mint számítástechnikai rendszer *(computer system),* számítástechnikai adat *(computer data),* szolgáltató *(service*

[94] Sorbán 2015.
[95] *Computer-Related Crime* 1990.; Nagy 1993.

provider), illetve forgalmi adat *(traffic data),* viszont a számítástechnikai bűncselekmény *(cybercrime)* fogalmának meghatározásával adós marad. Az egyezmény a büntető anyagi jogi szabályok körében négy csoportra osztja a bűncselekményeket. Az első csoportot a számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények, a második csoportot a számítógéppel kapcsolatos bűncselekmények, a harmadik csoportot a számítástechnikai adatok tartalmával kapcsolatos bűncselekmények, a negyedik csoportot pedig a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények jelentik.

A Miniszteri Bizottság R(95) 13 számú ajánlása a büntetőeljárás információs technológiával kapcsolatos problémáiról: A Miniszteri Bizottság újabb ajánlást fogadott el, amelyben 7 pontban foglalta össze azokat a problémákat, amelyek a büntetőeljárás során felmerülhetnek a számítógépes bűncselekmények kapcsán. Ezek:

1. *Átvizsgálás és lefoglalás (search and seizure):* A számítógépes rendszerek átvizsgálásának, valamint a bennük tárolt adatok lefoglalásának és az átvitel közben keletkező adatok lehallgatásának jogi elhatárolását kétség nélkül kell felvázolni és alkalmazni. A büntetőeljárási jognak meg kell engednie a nyomozó hatóságok számára, hogy átvizsgálják a számítógépes rendszereket, és az adatokat hasonló feltételekkel lefoglalják, mint a hagyományosnak nevezett házkutatás és lefoglalás esetében. A rendszerért felelős személyt tájékoztatni kell a rendszer átvizsgálásáról és a lefoglalt adatok típusáról. Azoknak a jogorvoslatoknak, amelyek egyébként is alkalmazhatók a hagyományos házkutatás és lefoglalás esetében, ugyanúgy alkalmazhatóknak kell lenniük a számítógépes rendszerek átvizsgálására és a bennük tárolt adatok lefoglalására is. Az átvizsgálás végrehajtása alatt a nyomozó hatóságoknak megfelelő biztosítékok mellett rendelkezniük kell azzal a jogosítvánnyal, hogy kiterjesszék a keresést egyéb, a joghatóságuk alá tartozó olyan számítógépes rendszerekre, amelyek hálózaton keresztül össze vannak kapcsolva, illetve lefoglalják a bennük található adatokat, amennyiben azonnali intézkedésre van szükség. Ahol az automatikusan feldolgozott adat megfelel egy tradicionális dokumentumnak, a büntetőeljárási jog dokumentumok átvizsgálásával és lefoglalásával foglalkozó szabályainak ezekre is ki kell terjednie.

2. *Megfigyelés (technical surveillance):* Az információtechnológia és a telekommunikáció konvergenciájának szempontjából felül kell vizsgálni a bűnügyi nyomozások célját szolgáló technikai intézkedéseket (így például a telekommunikációs eszköz lehallgatását), és ahol szükséges, ott módosítani kell ezeket az alkalmazhatóságuk biztosítása miatt. Itt tárgyalják azokat a problémákat, amelyek a megfigyeléssel, a lehallgatással és a forgalmi adatok összegyűjtésével kapcsolatosak. Kiemelik itt is, hogy szükséges a jelenlegi szabályozás felülvizsgálata.

3. *A nyomozó hatóságokkal való együttműködés kötelezettsége (obligations to co-operate with the investigating authorities):* A legtöbb jogrendszer megengedi, hogy a nyomozó hatóságok utasítsanak bizonyos személyeket arra, hogy adják át a birtokukban lévő azon tárgyakat, amelyekre a bizonyítás során szükség van.[96] A nyomozó hatóságoknak

[96] Sorbán 2015.

rendelkezniük kell azzal a képességgel, hogy utasítsák azokat a személyeket, akiknek adatai az információs rendszerben benne vannak, azért, hogy átadják azokat az információs rendszerhez, valamint a benne tárolt adatokhoz való hozzáféréshez szükséges információt is. A büntetőeljárási jognak továbbá biztosítani kell azt is, hogy hasonló utasítást lehessen adni az olyan személyeknek is, akik tudással rendelkeznek az információs rendszer működéséről, vagy azokról az intézkedésekről, amelyeket az abban tárolt adatok védelmének érdekében használtak. A telekommunikációs szolgáltatásokat nyilvános vagy magánhálózatokon kínáló speciális kötelezettségeket kell megállapítani azért, hogy olyan információkat adjanak át, amelyekkel azonosítható a felhasználó, ha a nyomozó hatóság erre utasítást ad.

4. *Elektronikus bizonyítékok (electronic evidence):* El kell ismerni a közös igényt az elektronikus bizonyítékok olyan módon történő összegyűjtésére, megőrzésére és bemutatására, ami a legjobban biztosítja és visszatükrözi azok integritását és hitelességét úgy a nemzeti büntetőeljárásban, mint a nemzetközi együttműködésben. Ezért azokat az eljárásokat és technikai módszereket, amelyek az elektronikus bizonyítékok kezelésére vonatkoznak tovább kell fejleszteni úgy, hogy azok biztosítsák az államok közötti kompatibilitást.

5. *Titkosítás használata (use of encryption):* Olyan intézkedéseket kell bevezetni, amelyek minimalizálják a bűncselekmények nyomozása során a kriptográfia használatának negatív hatásait anélkül, hogy a szükségesnél jobban érintenék azok legitim használatát.

6. *Kutatás, statisztika és képzés (research, statistics and training):* Tovább kell vinni az informatikai bűncselekményekkel összefüggően keletkezett adatok elemzését, beleértve a *modus operandi* és a műszaki szempontok vizsgálatát. Speciális szakegység létrehozásának megfontolása szükséges a speciális bűncselekmények nyomozásának végrehajtásához.

7. *Nemzetközi együttműködés (international co-operation):* Az átvizsgálás jogának kiterjesztését más számítógépes rendszerekre azokban az esetekben is alkalmazni kell, amikor a rendszer más ország joghatósága alá tartozik, amennyiben azonnali intézkedésre van szükség. Annak érdekében, hogy elkerülhető legyen a nemzeti szuverenitás, illetve a nemzetközi jog megsértése, az ilyen kiterjesztett átvizsgálásra és lefoglalásra egyértelmű jogi szabályokat kell alkotni. Elérhetőnek kell lennie az olyan gyorsított és megfelelő eljárásoknak, amelyek alapján a nyomozó hatóságok igényelhetik azt, hogy a külföldi hatóságok is gyűjthessék a(z) (elektronikus) bizonyítékokat. A megkeresett hatóságoknak felhatalmazással kell rendelkezniük a telekommunikációval kapcsolatos forgalmi adatok megosztására, a telekommunikációs rendszerek és eszközök lehallgatására, illetve azok forrásának beazonosítására. Ennek okán a jelenlegi kölcsönös jogsegély eszközeit ki kell egészíteni.

A Bűnügyi Rendőrség Nemzetközi Szervezete (International Criminal Police Organization – Interpol)

A Bűnügyi Rendőrség Nemzetközi Szervezete – közismertebb nevén Interpol – jelenleg 194 tagországgal rendelkezik. Valamennyi tagországban segítik a tagállami rendőrséget az együttműködés terén, ennek érdekében a bűncselekményekkel és bűnözőkkel kapcsolatos adatokat osztanak meg, továbbá biztosítják a tagállomok közötti technikai és operatív támogatást.

Az Interpol a tanulmányban felsorolt szervezetek között az egyik legrégebbi, hiszen az 1923-ban Bécsben megalakult Nemzetközi Bűnügyi Rendőrség Bizottság volt az Interpol alapja. Végül 1927-ben hozták létre az Interpol Nemzetközi Irodát.

A második világháborút követően, 1946-ban az Interpol székhelye Párizsba, majd azt követően, 1989-ben Lyonba költözött.

Az Interpol[97] egyik célja, hogy globális szinten összefogja és koordinálja a számítógépes bűncselekmények felderítését.[98] A feladataik ellátásához megalakították a *Digital Crime Centert,* amely leginkább a kutatással és az innovációval kapcsolatos teendőket látja el. Ezen központ mellett létrejött még a *Cyber Fusion Center,* amely a szervezet tagországainak nyújt segítséget a nyomozás kezdetétől annak befejezéséig. A két egység létrehozta a forenzikus tevékenységével kapcsolatos szakértői laborját is, a *Digital Forensic Laboratory-t.*

Az Interpol feladata, hogy koordinálja és összehangolja a 190 tagállam közötti együttműködést a bűnüldözés területén, a technológiai és technikai fejlődés figyelemmel kísérése mellett a szakemberek folyamatos oktatása, felkészítése a számítógépes bűncselekmények változásainak megfelelően.

NAT – North Atlantic Treaty Organization

A NATO, vagyis az Észak-atlanti Szerződés Szervezete Kooperatív Kibervédelmi Kiválósági Központja (NATO CCD COE) egy nemzetközi katonai szervezet, amelyet a NATO Észak-atlanti Tanácsa 2008-ban akkreditált *Kiválósági Központnak.* A Kiválósági Központ Észtországban, Tallinnban található, jelenleg Észtország, Németország, Magyarország,[99] Olaszország, Lettország, Litvánia, Hollandia, Lengyelország, Szlovákia, Spanyolország és az Egyesült Államok támogatja. A központ nem része a NATO parancsnokságának vagy erőstruktúrájának, és a NATO sem finanszírozza. Ez azonban egy szélesebb keret részét képezi, amely támogatja a NATO Parancsnoki Megállapodásait.

A NATO 1999-ben észlelt kibertámadásokat a rendszerei ellen, amelyeket a koszovói *Fekete kéz* hackercsoport követett el, amit a kínai és orosz hackerek folytattak, jellemzően DDoS-támadásokat[100] végrehajtva.

[97] *Annual Report 2017* 2017.
[98] Az Interpol nem rendelkezik nyomozati jogkörrel.
[99] Magyarország 2010-ben csatlakozott a Központhoz.
[100] Tóth 2018.

Amint azt az Észak-atlanti Szerződés Szervezetének 2010. novemberi, a *NATO szervezetének védelmére és biztonságára vonatkozó stratégiai koncepció*ban megállapítják, a NATO-tagállamok felismerték, hogy a rosszindulatú kibertevékenységek elérhetik azt a küszöböt, amely veszélyezteti a nemzeti és euroatlanti jólétet, biztonságot és stabilitást.[101] A NATO a területe és lakossága biztonságának biztosítása érdekében elkötelezte magát amellett, hogy folytatja alapvető feladatait, többek között a felmerülő biztonsági kihívások, például a számítógépes fenyegetések megakadályozása és megvédése érdekében.

A NATO Alapokmányának 5. cikkelye kimondja, hogy: „A Felek megegyeznek abban, hogy egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek, és ennélfogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. cikke által elismert jogos egyéni vagy kollektív védelme jogát gyakorolva támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Féllel egyetértésben azonnal megteszi azokat az intézkedéseket – ideértve a fegyveres erő alkalmazását is –, amelyeket a békének és biztonságának az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart."

A NATO 2008-ban megalapította a Kooperatív Kibervédelmi Kiválósági Központot *(Cooperative Cyber Defence Centre of Excellence – CCDCOE),* amelyet a szövetséges fegyveres erők transzformációs főparancsnoka 2006-ban engedélyezett. A központ a kiberműveletek és a kiberbiztonság oktatásával, kutatásával és fejlesztésével foglalkozik, és a műszaki technológiai aspektuson kívül vizsgálja az etikai és jogi kihívásokat. Mindezek mellett közreműködik a nemzetek kibervédelmi stratégiájának létrehozásában, fejlesztésében és módosításában.

Cyber Defence Management Authority – DMA

A NATO létrehozta még többek között a Számítógépes Védelmi Irányító Hatóságot *(Cyber Defence Management Authority – CDMA)* is, amely a brüsszeli székhelyű Számítógépes Védelmi Irányító Tanács *(Cyber Defence Management Board – CDMB)* alárendeltségében látja el a szövetségi szintű, centralizált, számítógépes védelem megteremtésének és irányításának feladatait.

A CDMA alapvető feladatai:

- közreműködés informatikai rendszerek sérülékenységi vizsgálatainak végrehajtásában, illetve a feltárt hálózati sérülékenységek elhárításában;
- a hatáskörébe tartozó kormányzati, állami, valamint állami háttérintézmények rendelkezésére álló naplóállományainak elemzése, valamint azok hiánya esetén a szükséges munkafolyamatok kialakítása;
- közreműködés a hatáskörébe tartozó kormányzati, állami, valamint állami háttérintézmények elektronikus incidenseinek kezelésében, illetve azok rendszerein történt elektronikus visszaélések kivizsgálásában;

[101] *Active Engagement, Modern Defence…* 2010.

– az állami rendszerek üzemeltetésével összefüggésben szakértői, minőségbiztosítási tevékenység végzése;
– gondoskodás elektronikus információbiztonsági és tudatossági programok szervezéséről;
– stratégiai és taktikai együttműködés az EU és a NATO társszervezeteivel, valamint a tagállamok CDMA-szervezeteivel.

A Számítógépes Védelmi Irányító Hatósághoz kapcsolódva alakították ki az úgynevezett gyorsreagálású csoportokat *(Rapid Reaction Teams – RRT),* amelyek gyorsan települve az adott országba nemzeti szinten nyújtanak segítséget a számítógépes támadások ellen.

A számítógépes szükséghelyzeteket elhárító csoportok *(Computer Emergency Response Team – CERT)* rendszerét a CDMA mellett alakították ki. A CERT koncepciója 1988-ban jelent meg – függetlenül a NATO-tól – a Carnegie Mellon Egyetemen, az Egyesült Államokban. A CERT tulajdonképpen egy szakértőkből álló „testület", amely a nemzeti számítógépes hálózatok felügyeletét, illetve adott esetben védelmének kidolgozását és – a lehető leggyorsabb reagálással – annak végrehajtását végzi. Ma több mint 250 ilyen CERT létezik, beleértve a magyarországiakat is. Bevett gyakorlattá vált, hogy az államok pénzügyi támogatásával ezek a csoportok látják el a nemzeti kibervédelmi felügyeletet, ezzel is erősítve a CDMA munkáját.

A G8 feladatai a kiberbűnözés elleni harcban és a kiberbiztonság megteremtésében

A *Group of Eight* a G7 és Oroszország együttműködési fóruma, amelynek tagjai Kanada, Franciaország, Németország, Olaszország, Japán, az Egyesült Királyság, az Amerikai Egyesült Államok és Olaszország.

A G8-ak információs miniszterei 1995. február 25–26-án Brüsszelben tartott megbeszélésükön megvitatták az „innováció és az új technológiák fejlesztésének, ösztönzésének és előmozdításának szükségességét, ideértve különösen a nyílt, versenyképes és világszerte működő információs infrastruktúrák megvalósítását". A konferencia annak a kísérleti projektnek a meghatározásával zárult le, amely a nemzetközi együttműködésből profitálna. Ezeket a projekteket hivatalosan elfogadták.

A G8-ak az igazságügyi és belügyminisztereik találkozóján – 1997. decemberben – egy hálózat létrehozására szólítottak fel, amelynek alapja azon kinyilvánításuk volt, hogy „[a] csúcstechnológiával kapcsolatos bűnözés kapcsán el kell ismernünk azt, hogy az új számítógépes és telekommunikációs technológiák példátlan lehetőségeket kínálnak a globális kommunikációhoz. Ahogy a nemzetek egyre inkább támaszkodnak ezekre a technológiákra, ideértve a vezeték nélküli kommunikációt is, a csúcstechnológiájú bűnözők általi kihasználásuk egyre nagyobb veszélyt jelent a közbiztonságra".[102]

[102] Dougherty 1998.

Létrehozták a *G8 24/7 hálózatot,* amely egy úgynevezett pont-pont hálózat *(Point to Point Network);* a kiberbűnözéssel kapcsolatos feladata:

- a sürgős segítségnyújtás;
- egyetlen kapcsolattartó pont (POC) létrehozása;
- amely elérhető a nap 24 órájában, a hét 7 napján;
- a POC-nak ismerettel kell rendelkeznie a kiberbűnözéssel kapcsolatos ügyekben végrehajtandó feladatokról.

A hálózat elsődleges célja az adatok megőrzése a kölcsönös jogi segítségnyújtási csatornákon keresztül, majd az azokon történő későbbi információtovábbítás.

A hálózat célja, hogy használatához a külföldi résztvevőktől segítséget kérő bűnüldöző szervek kapcsolatba lépjenek a saját államukban vagy autonóm bűnüldözési joghatóságukban található 24 órás kapcsolattartó ponttal, amely adott esetben felveszi a kapcsolatot a külföldi résztvevővel. A hálózat résztvevői kötelezettséget vállaltak arra, hogy minden tőlük telhetőt megtesznek annak biztosítása érdekében, hogy az internetszolgáltatók a lehető leggyorsabban szolgáltassák a kérelmező fél által kért információkat.

A G8-nak ugyanakkor komoly szerepe van a kiberbiztonság területén is. Az egyik legjelentősebb dokumentum a 2000. július 22-i okinawai csúcstalálkozón a G8 által aláírt okirat, amellyel elfogadták a globális információs társadalom chartáját (a továbbiakban: Okinawa Charta).

Az *Okinawa Charta* preambuluma kimondja, hogy az IKT-k „gyorsan válnak a világgazdaság létfontosságú motorjává". Azt is rögzíti, hogy az IKT-k képesek átalakítani a gazdaságokat és a társadalmakat, mivel „képesek segíteni az egyéneket és a társadalmakat a tudás és az ötletek felhasználásában". Az Okinawa Charta a befogadás elvét vallja, amely szerint „mindenkinek lehetővé kell tenni, hogy mindenki részt vehessen azon, és senkit sem szabad kizárni a globális információs társadalom előnyeiből".

Felhívta a charta a figyelmet arra is, hogy az együttműködést a globális hálózatok optimalizálása, a hálózat integritását aláásó visszaélések elleni küzdelem, a digitális megosztottság áthidalása, az emberekbe történő befektetés, valamint a globális hozzáférés és részvétel előmozdítása érdekében kell fejleszteni.

Az Okinawa Charta második része arra összpontosított, hogy az IKT-k számára jobb politikai és szabályozási környezetet kell létrehozni, hogy pozitív hatást gyakoroljon. A magánszektor „vezető szerepet játszik", de „a kormányok feladata, hogy hozzanak létre kiszámítható, átlátható és megkülönböztetéstől mentes politikai és szabályozási környezetet".

A dokumentum hangsúlyozta a szellemi tulajdonhoz fűződő jogok és a nemzetközi liberalizáció, különösen az e-kereskedelem érvényesítésének fontosságát. Az OECD fent említett erőfeszítéseihez hasonlóan az Okinawa Charta a jövőben fontosnak tartotta a magánélet védelmét, az elektronikus hitelesítést és a biztonságot.

A G8-nak a kiberbiztonság feladataival kapcsolatos bemutatása során szükségesnek érzem a *Dot Force* említését. A kormányokat, a magánszektort, a nonprofit szervezeteket és a nemzetközi szervezeteket képviselő szervezetekből összesen 43 csoportot

állítottak össze, hogy „meghatározzák azokat a módszereket, amelyek a digitális forradalom előnyei lehetnek minden embernek, különösen a legszegényebb és leginkább marginalizált csoportoknak". Első ülése 2000. november 27–28-án volt Japánban.[103]

Közvetlenül a New York-i World Trade Center és a Pentagon elleni, 2001. szeptember 11-én elkövetett támadások után a G8 vezetői kevésbé foglalkoztak a Dot Force-ban is megvitatott, többek között a kiberbiztonságra irányuló kérdésekkel.

A hazai kiberbűnözés és kibervédelem szervezetei

Az uniós és nemzetközi szervezetek bemutatása, ismertetése mellett úgy gondolom, hogy nélkülözhetetlen legalább érintőlegesen a hazai kibervédelemmel és kiberbűnözéssel foglalkozó szervezeteket bemutatni.

A rendőrség

Magyarország közbiztonságáért, a rendvédelmi, bűnüldözési és bűnmegelőzési feladatok ellátásáért a Belügyminisztériumhoz tartozó rendőrség felelős. A rendőrség feladatait elsősorban a rendőrségről szóló 1994. évi XXXIV. törvény (Rtv.) szabályozza, de munkája során tekintettel kell lennie a büntetőeljárásról szóló 2017. évi XC. törvényre, a Büntető Törvénykönyvről szóló 2012. évi C. törvényre, illetve a rendőrség hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendeletre, amely a rendőrség szervezeti tagolódását szabályozza. Ezen jogszabályokon kívül a nyomozó hatóság a nyomozás és az előkészítő eljárás részletes szabályairól szóló 100/2018. (VI. 8.) Korm. rendelet és további belső utasítások alapján látja el feladatait.

A rendőrség meghatározott jogok és kötelezettségek szem előtt tartásával végzi feladatait, mindeközben védi az állampolgárok biztonságát, és a gondoskodik a törvények betartásáról és betartatásáról. Ugyanakkor a rendőrség feladata talán az egyik legösszetettebb, hiszen a közrendvédelmi, bűnügyi és szabálysértési terület mellett ellát egyéb feladatokat is. A rendészeti tevékenység alapvető irányultsága a rend, a biztonság fenntartása, megőrzése, emeli ki Madai.[104]

Minden büntetőeljárás megindításánál az első lépés a hatáskör és az illetékesség vizsgálata, amely alapján az elkövetés helye, jellege, a bekövetkezett kár mértéke alapján folytatja le az arra jogosult szerv a vizsgálatot. Továbbá az Európai Unió tagállamai között folytatott bűnügyi jogsegély, a bűntetőügyekben folytatott együttműködés, valamint európai elfogatóparancs alapján folytatott átadási eljárás,[105] illetve a nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény alapján segítik a határon átnyúló bűncselekményekkel kapcsolatos kényszerintézkedések végrehajtását, az elkövetők elfogását és azok kiadatását, átadását. Többek között ez utóbbi két jogszabály, valamint nemzetközi

[103] Hart 2005.
[104] Madai 2016, 265.
[105] 2012. évi CLXXX. törvény.

szerződések (két vagy több fél által megkötött bi- vagy multilaterális szerződések) is segítik a számítógépes bűncselekmények nemzetközi jellegével összefüggő nehézségek leküzdését a nyomozó hatóságok között.

Mivel a nyomozással kapcsolatos problémák elsődlegesen a rendőrség feladatainak végrehajtása során fordulnak elő, így összességében azzal kívánunk foglalkozni, míg a fejezetben az Alaptörvényhez igazodva, a rendőrség mellett a nemzetbiztonsági szervezetek számítógépes bűnözés miatt jelentkező kibervédelmi és kiberbiztonsági kihívásait is tárgyaljuk.

Terrorelhárítási Központ

Az Rtv. hatálya alá tartozó szervezet továbbá a Terrorelhárítási Központ (TEK), amellyel nem a számítógépes bűncselekmények, sokkal inkább a kibervédelemmel kapcsolatos feladataik ellátása miatt szükséges röviden foglalkozni. Ez a szervezet a terrorcselekmények elhárításával, megakadályozásával és megelőzésével foglalkozik.

A Terrorelhárítási Központ feladatait egyrészt az 1994. évi XXXIV. törvény határozza meg, másrészt a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól szóló 295/2010. (XII. 22.) Korm. rendelet. A rendőrségről szóló törvény és az említett kormányrendelet alapján a TEK nyomozati jogkört nem gyakorol; ugyanakkor a 2012. évi C. törvényben, a Büntető Törvénykönyv 314–316. §-aiban taglalt terrorcselekménnyel összefüggésben az internet felhasználásával történő szerveződést, terrorsejtek szerveződését, az ezekkel összefüggésben történő szerveződéseket, csoportokat, személyeket felderít és megfigyelhet, valamint a kritikus infrastruktúrák vagy az azokon kívüli kiemelt létesítmények – akár azok informatikai rendszereinek – védelmében, az ellenük történő támadás megakadályozásában, felderítésében és azok védelmére vonatkozó nemzeti program kidolgozásában, a veszélyeztetettség értékelésében és biztonsági intézkedési tervek kidolgozásában rész vesz.[106]

Ahogy említettük, nem rendelkezik a klasszikus értelemben vett nyomozati jogkörrel, így a törvényben előírt tevékenysége során az Rtv. 7/E. §-a alapján együttműködik a rendőrséggel, valamint a magyar nemzetbiztonsági szolgálatokkal és a külföldi titkosszolgálati szervezetekkel is.

Nemzeti Adó- és Vámhivatal (NAV)

A Nemzeti Adó- és Vámhivatal feladatai közé tartozik a klasszikus adó- és illetékkiszabások mellett a büntetőeljárások lefolytatása. A NAV Bűnügyi Főigazgatóság Központi Nyomozó Főosztály Információtechnológiai Osztály feladata a különböző, informatikai eszköz felhasználásával elkövetett jogellenes cselekmények nyomozása. A főigazgatóság hatáskörébe tartozik az egymilliárd forintot meghaladó értékre üzletszerűen vagy bűnszövetségben elkövetett bűncselekmények, a bűnszervezetben elkövetett

[106] 295/2010. (XII. 22.) Korm. rendelet 3. § (1) bekezdés *c)* pont.

bűncselekmények, valamint az olyan bűncselekmények nyomozása, amelyeket az elkövető személye vagy az elkövetés körülményei, illetve a bűncselekmény társadalomra veszélyességének kiemelkedő foka miatt a Bűnügyi Főigazgatóság a hatáskörébe vont, illetve utalt. Feladata továbbá:

- az interneten elkövetett bűncselekmények felderítés és nyomozása;
- az internetes keresés, monitorozás, nyomrögzítés és az online szemlék;
- helyszíni adatmentések *(live forensic);*
- együttműködés a magyarországi jogvédő szervezetekkel (Pro Art, Artisjus), a Készenléti Rendőrség Nemzeti Nyomozó Irodával és a Nemzeti Kibervédelmi Intézettel;
- nemzetközi együttműködés, bűnügyi jogsegélyek teljesítése (például Europol Copy, IOS-akciók);
- konferenciák és képzések tartása.

A szerzői jogok vagy a szerzői joghoz kapcsolódó jogok bűncselekményei kapcsán az IT-osztály feladata az internetes monitorozás, annak során a jogsértések feltárása, a jogsértés módjának meghatározása, továbbá az okozott vagyoni hátrány meghatározása, a jogsértő azonosítása, a Btk. 77. §-a alapján a jogsértő adat eltávolítására tett indítvány és annak ellenőrzése.

A magyarországi kibervédelemmel és kiberbiztonsággal foglalkozó szervezetek

A számítógépes bűncselekmények mellett több szakirodalom is említi a kibervédelmet és a kiberbiztonságot is. Amennyiben az elmúlt években bekövetkezett globális kibertámadásokra gondolunk, amelyek veszélyeztették az államok biztonságát, a társadalmat és a gazdaságot, érzékeny adatokat és információkat szereztek meg vagy tettek hozzáférhetetlenné, ezen esetekben kiemelt feladataik voltak nemcsak a számítógépes bűncselekményekkel foglalkozó szervezeteknek, hanem a kibervédelemmel és a kiberbiztonsággal összefüggő állami és a magánszférához tartozó szerveknek is. A feltűnt zsaroló- és trójai vírusokkal, a malware-ekkel elkövetett támadásokra, azok veszélyére és a kötelező, illetve ajánlott cselekvésekre adnak választ az országok kibervédelmi stratégiái, valamint az azok végrehajtására felhatalmazott szervezetek.

Nemzeti Kibervédelmi Intézet

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (röviden: NBSZ NKI) rövid ismertetése szintén megkerülhetetlen. Habár közvetlenül nem is tartozik a számítógépes bűncselekmények nyomozását végző szervezetek közé, ennek ellenére feladatuk szorosan összefügg a számítógépes, pontosabban a kibertérben elkövetett jogellenes cselekményekkel, amikor is riasztást, jelzést és értesítést tesz közé a hivatalos honlapján és közösségi médián keresztül a rosszindulatú kibertámadásokkal, interneten vagy más kommunikációs eszközön keresztül érkező adathalász levelekkel, infokommunikációs

eszközöket és rendszereket érő sebezhetőségekkel kapcsolatban, továbbá a többi kibervédelemmel foglalkozó szervezeteknek (CERT-eknek), és együttműködnek a nyomozást folytató hatóságokkal is.

Az információbiztonságról szóló törvény (Ibtv.) 2015. évi módosításának eredményeként 2015. október 1-jén megalakult a Nemzeti Kibervédelmi Intézet – a Nemzetbiztonsági Szakszolgálat keretei között –, amelyen belül három szakmai szervezeti területet különítettek el a tevékenységüknek megfelelően:

– a kibertérből érkező támadásokkal és fenyegetettségekkel közvetlenül foglalkozó incidenskezelési szakterület (a Kormányzati Eseménykezelő Központ, azaz a GovCERT);
– a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó hatósági szakterület, a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH);
– a védelmi képességek fejlesztését és üzemeltetését támogató biztonságirányítási és sérülékenységvizsgálati (GovCERT) szakterület.[107]

A három terület mellett az NKI feladata még többek között a honvédelmi és a kritikus információs infrastruktúrák védelme, de a kibertámadásokkal kapcsolatos védelmi feladatok elvégzése is.

A *GovCERT* alapvető feladata az állami és önkormányzati szervek informatikai biztonsági támogatása, ami egyrészt preventív jellegű (értve ez alatt a szoftversérülékenységek és információbiztonsági fenyegetések nyomon követését és a sérülékenységmenedzsmentet), másrészt pedig reaktív jellegű, a védett szerveknél bekövetkező biztonsági események (incidensek) kivizsgálására és – több állami szervet érintően – a kezelésük koordinációjára irányul.

A sérülékenységmenedzsment során a GovCERT információkat gyűjt a szoftversérülékenységekről és a káros szoftverekről, megvizsgálja azok relevanciáját az állami IT-rendszerek tekintetében, és általános körben vagy célzottan tájékoztatja a fenyegetés kiváltotta biztonsági esemény megelőzése érdekében az ezen rendszereket üzemeltetőket. Az incidenskezelési tevékenység során a GovCERT 24 órás ügyeletet működtet, ahol folyamatosan fogadja az IT-rendszereket érő incidensek bejelentéseit, és megteszi az alapvető intézkedéseket (incidens nyilvántartásba vétele, bejelentő visszatájékoztatása, alapvető információk azonosítása stb.). A bejelentett incidens felszámolása során a következő lépés a jogosultsággal és/vagy képességgel rendelkező szerv/személy tájékoztatása a teendőkről, szükség esetén kapcsolattartás a bejelentővel, valamint az érintett incidens felszámolásának nyomon követése (incidenskoordináció). Amennyiben szükséges, az incidensre utaló jelek alapján a GovCERT összegyűjti az incidens felderítéséhez szükséges információkat (például naplóadatok), és ezek elemzésével megkísérlik rekonstruálni az incidens kiváltó okait, egyúttal javaslatot tesznek a hasonló incidensek megelőzését vagy az okozott kár enyhítését támogató informatikai védelmi intézkedésekre.

[107] *NKI* (é. n.)

A Nemzeti Kibervédelmi Intézet mellett a kibertérrel összefüggő veszélyekkel és támadásokkal kapcsolatban egyéb – a disszertációhoz nem kapcsolható – feladatai vannak a Katonai Nemzetbiztonsági Szolgálatnak, a Magyar Honvédségnek, de ezeket most nem szerettük volna részletezni.

Irodalomjegyzék

About ECSO (2020). Brüsszel, ECSO. Elérhető: www.ecs-org.eu/about (A letöltés dátuma: 2020. 04. 17.)

Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation (2010). Adopted by Heads of State and Government at the NATO Summit in Lisbon 19–20 November 2010. Lisszabon, NATO. Elérhető: www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf (A leltöltés dátuma: 2020. 04. 12.)

A kiberbűnözés leküzdése: Stratégiai együttműködési megállapodást írt alá az ENISA és az Europol (2014). Heraklion, ENISA. Elérhető: https://news.cision.com/global/enisa–-european-union-agency-for-network-and-information-security/r/a-kiberbonozes-lekuzdese–strategiai-egyuttmokodesi-megallapodast-irt-ala-az-enisa-es-az-europol,c9607505 (A letöltés dátuma: 2020. 03. 31.)

Annual Report 2017 (2017). Lyon, Interpol.

A szervezett bűnözés elleni küzdelem az Unióban (2020). Brüsszel, Európai Tanács – Az Európai Unió Tanácsa. Elérhető: www.consilium.europa.eu/hu/policies/eu-fight-against-organised-crime-2018-2021/ (A letöltés dátuma: 2020. 03. 20.)

A Visegrádi Négyek helyzete a kibervédelem tekintetében (é. n.). *Kutatói blog.* Budapest, Antall József Tudásközpont. Elérhető: www.ajtk.hu/kutatoi-blog/219/a-visegradi-negyek-helyzete-a-kibervedelem-tekinteteben-/ (A letöltés dátuma: 2020. 04. 11.)

Az ENSZ kézikönyve a számítógéppel kapcsolatos bűncselekmények megelőzéséről és kezeléséről (1994). New York, ENSZ.

Az Európai Bizottság (2020). Brüsszel, Európai Bizottság. Elérhető: https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_hu (A letöltés dátuma: 2020. 04. 01.)

Az európai digitális menetrend (2010). Brüsszel, Európai Bizottság. Elérhető: www.europarl.europa.eu/factsheets/hu/sheet/64/az-europai-digitalis-menetrend (A letöltés dátuma: 2020. 04. 11.)

Az Európai Tanács tájékoztatása. A Stockholmi Program (2010). Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Ajl0034 (A letöltés dátuma: 2020. 04. 16.)

Az Európai Unió Belső Biztonsági Állandó Bizottsága (COSI) által meghatározott stratégiai célok a kiberbűnözés ellen harc terén a 2014–2017 közötti időszak tekintetében (2013). Elérhető: www.cert-hungary.hu/node/212 (A letöltés dátuma: 2020. 03. 30.)

Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér (2013). JOIN (2013)01 final. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A52013JC0001 (A letöltés dátuma: 2020. 04. 02.)

Az információs rendszerek és hálózatok biztonságára vonatkozó OECD-irányelvek: Útban a biztonságkultúra felé (2003). (oecd Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.) Párizs, OECD. Elérhető: www.oecd.org/sti/ieconomy/15582292.pdf (A letöltés dátuma: 2020. 04. 12.)

Berki Gábor (2016): Kiberháborúk, kiberkonfliktusok. In *Műhelytanulmányok,* 2016/1. sz. 245–284. Elérhető: http://real.mtak.hu/80322/1/246_kiberhaboru16182.pdf (A letöltés dátuma: 2020. 04. 04.)

Boda József szerk. (2019): *Rendészettudományi szaklexikon.* Budapest–Pécs, Dialóg Campus Kiadó. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/14690/743_Rendeszettudomanyi_Szaklexikon_e.pdf?sequence=1 (A letöltés dátuma: 2020. 03. 27.)

Bodó Attila Pál – Zámbó Nóra (2018): Újdonságok a kibervédelmi szabályozásban. In Deák Veronika szerk.: *Célzott kibertámadások.* Budapest, Nemzeti Közszolgálati Egyetem. 7–21. Elérhető: https://nke-repo.uni-nke.hu/xmlui/bitstream/handle/123456789/7229/C%E9lzott%20kibert%E1mad%E1sok.pdf;jsessionid=CE32777BB02B4FAAB18DF6EF83EAC4D7?sequence=1 (A letöltés dátuma: 2020. 04. 12.)

Brady, Hugo (2008): Europol and the European Criminal Intelligence Model: A Non-state Response to Organized Crime. *A Journal of Policy and Practice,* Vol. 2, No. 1. 103–109. DOI: https://doi.org/10.1093/police/pan014

Buono, Laviero (2012): Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (EC3). *Sage Journals,* Vol. 3, No. 3–4. 332–343. DOI: https://doi.org/10.1177%2F2032284412003003O7

Central European Platform for Cybersecurity (é. n.). National Security Authority, Slovakia. Elérhető: www.nbu.gov.sk/en/cyber-security/partnership/central-european-platform-for-cybersecurity/index.html (A letöltés dátuma: 2020. 04. 03.)

Computer-Related Crime (1990). Recommendation No. R (89) 9. Strasbourg, Council of Europe Legal Affairs – European Committee on Crime Problems.

Computer-Related Criminality: Analysis of Legal Police (1986). Paris, OECD.

Cybersecurity Making at Turning Point – Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy (2012). Párizs, OECD. Elérhető: www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf (A letöltés dátuma: 2020. 04. 12.)

Dougherty, Thomas (1998): *G7 24/7 Cybercrime Network.* Elérhető: https://rm.coe.int/1680303ce2 (A letöltés dátuma: 2020. 04. 07.)

ENCS – Our Mission (é. n.). Elérhető: https://encs.eu/our-mission/ (A letöltés dátuma: 2020. 04. 18.)

ENCS Strategic Advisory Board (2020). Hága, ENCS. Elérhető: https://encs.eu/encs-strategic-advisory-board/ (A letöltés dátuma: 2020. 04. 17.)

ENISA – Strucuture and Organization (2019). Elérhető: www.enisa.europa.eu/about-enisa/structure-organization (A letöltés dátuma: 2020. 04. 03.)

EUCTF (é. n.). Elérhető: www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf (A letöltés dátuma: 2020. 04. 16.)

Eurojust (2020). Elérhető: www.eurojust.europa.eu/Pages/languages/hu.aspx (A letöltés dátuma: 2020. 03. 20.)

Eurojust – Éves jelentés 2017 (2019). Luxemburg, Publications Office of the European Union. Elérhető: https://op.europa.eu/en/publication-detail/-/publication/4e8e4f95-6183-11e9-b6eb-01aa75ed71a1/language-hu/format-PDF (A letöltés dátuma: 2020. 04. 04.)

Eurojust – Joint Investigation Teams General Background (2020). Elérhető: www.eurojust.europa.eu/Practitioners/JITs/Pages/historical-background.aspx (A letöltés dátuma: 2020. 04. 12.)

Európai biztonsági stratégia – Biztonságos Európa egy jobb világban (2009). Luxemburg, EU. Elérhető: www.consilium.europa.eu/media/30811/qc7809568huc.pdf (A letöltés dátuma: 2020. 04. 05.)

Európai Rendőrségi Hivatal (Europol) (2019). Elérhető: https://europa.eu/european-union/about-eu/agencies/europol_hu (A letöltés dátuma: 2020. 04. 12.)

European Union Cybercrime Task Force (EUCTF) (é. n.). Elérhető: www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf (A letöltés dátuma: 2020. 04. 03.)

FIRST (é. n.). Elérhető: www.first.org/about/history (A letöltés dátuma: 2020. 04. 14.)

Gyaraki Réka (2019): *A számítógépes bűnözés nyomozásának problémái.* Doktori értekezés. Pécs, Pécsi Tudományegyetem.

Haig Zsolt – Kovács László (2008): Fenyegetések a cybertérből. In *Nemzet és Biztonság,* 1. évf. 5. sz. 61–69. Elérhető: www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf (A letöltés dátuma: 2020. 04. 03.)

Hart, Jeffrey A. (2005): The G8 and the Governance of Cyberspace. In Fratianni, Michele – Kirton, John J. – Rugman, Alan M. – Savona, Paolo eds.: *New Perspectives on Global Governance: Why American Needs the G8.* Farnham, Ashgate. 137–151. Elérhető: www.researchgate.net/publication/277323800_The_G8_and_the_Governance_of_Cyberspace (A letöltés dátuma: 2020. 05. 31.) DOI: 10.4324/9781315248035-9

Hegyaljai Mátyás (2012): A nemzetközi bűnügyi együttműködés. *Kül-Világ,* 9. évf. 4. sz. 2–14.

ITU Global Cybersecurity Agenda (2007). Genf, ITU. Elérhető: www.itu.int/osg/spuold/cybersecurity/gca/hleg.html (A letöltés dátuma: 2020. 04. 12.)

ITU-T X.1205. Series X: Data Networks, Open System Communications and Security. Telecommunication Security. Overview of Cybersecurity (2008). Genf, ITU. Elérhető: www.itu.int/rec/T-REC-X.1205-200804-I (A letöltés dátuma: 2020. 04. 03.)

Jelentés „A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: A globális kiberbiztonság felé" című dokumentumról (2011). Brüsszel, Európai Parlament. Elérhető: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0167+0+DOC+XML+V0//HU (A letöltés dátuma: 2020. 04. 11.)

Jelentés az európai biztonsági stratégia végrehajtásáról – A biztonság megteremtése a változó világban (2008). Brüsszel, Európai Tanács. Elérhető: www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/HU/reports/104644.pdf (A letöltés dátuma: 2020. 04. 11.)

Komanovics Adrienne (2007): *Információszabadság az Európai Unióban.* Doktori értekezés. Pécs, Pécsi Tudományegyetem. Elérhető: https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/komanovics-adrienne/komanovics-adrienne-vedes-ertekezes.pdf (A letöltés dátuma: 2020. 04. 06.)

Kovács László (2018): *Kiberbiztonság és -stratégia.* Budapest–Pécs, Dialóg Campus Kiadó. Elérhető: https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_Kiberbiztonsag_es_strategia.pdf (A letöltés dátuma: 2020. 04. 02.)

Közös jövőkép, közös fellépés: Erősebb Európa – Globális stratégia az Európai Unió közös kül- és biztonságpolitikájára vonatkozóan (2016). Brüsszel, EEAS. Elérhető: www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_hu_.pdf (A letöltés dátuma: 2020. 04. 13.)

Maciejewski, Mariusz – Næss, Kristine – Gouardères, Frédéric – Hess, Arthur-Edouard (2020): *Az európai digitális menetrend.* Brüsszel, Európai Parlament. Elérhető: www.europarl.europa.eu/factsheets/hu/sheet/64/az-europai-digitalis-menetrend (A letöltés dátuma: 2020. 04. 11.)

Madai Sándor (2016): Integrációs változatok a rendészetben. In Horváth M. Tamás – Bartha Ildikó: *Közszolgáltatások megszervezése és politikái.* Budapest–Pécs, Dialóg Campus Kiadó.

Marosi Zsuzsanna (2017): Az Európai Unió hírszerzési együttműködésének helyzete és lehetőségei. *Nemzetbiztonsági Szemle,* 5. évf. 2. sz. 5–18. Elérhető: www.epa.hu/02500/02538/00018/pdf/EPA02538_nemzetbiztonsagi_szemle_2017_02.pdf (A letöltés dátuma: 2020. 04. 11.)

Mezei Kitti (2019): *A kiberbűnözés egyes büntetőjogi szabályozási kérdései.* Doktori értekezés. Pécs, Pécsi Tudományegyetem. Elérhető: https://pea.lib.pte.hu/bitstream/handle/pea/23209/mezei-kitti-phd-2019.pdf?sequence=1&isAllowed=y (A letöltés dátuma: 2020. 04. 04.)

Molnár Anna (2019): Az Európai Uniónak a biztonsági közösségtől a kollektív védelemig terjedő folyamata. In Molnár Anna – Marsai Viktor – Wágner Péter szerk.: *Nemzetközi biztonsági szervezetek.*

Budapest–Pécs, Dialóg Campus Kiadó. 81–97. Elérhető: http://real.mtak.hu/104072/7/web_PDF_Nemzetkozi_biztonsagi_szervezetek-82-98.pdf (A letöltés dátuma: 2020. 04. 17.)

Munk Sándor (2018): A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* 28. évf. 1. sz. 113–131. Elérhető: http://real.mtak.hu/77921/1/HT20181_115_133_u.pdf (A letöltés dátuma: 2020. 03. 30.)

Nagy Zoltán (1993): Konferencia az információtechnikai bűnözésről. *Magyar Jog,* 40. évf. 2. sz. 102–104.

Paráda István (2018): A NATO kibervédelmi irányelveinek fejlődése. *Honvédségi Szemle,* 146. évf. 3. sz. 3–13. Elérhető: https://honvedelem.hu/files/files/110428/hsz_2018_3_beliv_003_013.pdf (A letöltés dátuma: 2020. 04. 04.)

Remek Éva (2017): AZ EBESZ II. története, helye, szerepe és jellemzői a nemzetközi szervezetek rendszerében. *Hadtudományi Szemle,* 10. évf. 2. sz. 143–162. Elérhető: http://real.mtak.hu/85315/1/17_2_bp_remek_2.pdf (A letöltés dátuma: 2020. 04. 03.)

Schjølberg, Stein (2008): *Report of the Chairman of HLEG.* Moss–Genf, ITU Global Cybersecurity Agenda (GCA) – High Level Experts Group (HLEG). Elérhető: www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf (A letöltés dátuma: 2020. 04. 14.)

Simon Béla (2018): Az EU rendészeti szerveinek együttműködése a kiberbűnözés ellen. *Nemzetbiztonsági Szemle,* 6. évf. 4. sz. 21–47. Elérhető: http://epa.oszk.hu/02500/02538/00027/pdf/EPA02538_nemzetbiztonsagi_szemle_2018_04.pdf (A letöltés dátuma: 2020. 04. 12.)

SOCTA – European Union Serious And Organised Crime Threat Assessment 2017 (2017). Hága, Europol–SOCTA/OCTA. Elérhető: www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 (A letöltés dátuma: 2020. 03. 23.)

Sorbán Kinga (2015): Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. *Themis,* 2015. június. 343–375. Elérhető: https://edit.elte.hu/xmlui/bitstream/handle/10831/34602/Themis_2015_jun_Sorban_Kinga_p_343-375.pdf;jsessionid=FC00541AF57CDB36B4BD04FCF31EFA02?sequence=1 (A letöltés dátuma: 2020. 04. 10.)

Special Interest Groups (SIGs) (é. n.). Cary, NC, FIRST. Elérhető: www.first.org/global/sigs/ (A letöltés dátuma: 2020. 04. 17.)

Szentgáli Gergely (2013): Az Európai Unió kiberbiztonsági törekvései és szervezetei II. *Hadmérnök,* 8. évf. 1. sz. 295–305.

Tóth Tamás (2012): Az Europol tevékenysége. *Nemzet és Biztonság,* 5. évf. 5–6. sz. 59–78.

Tóth Tamás (2018): A NATO Kibervédelmi Kiválósági Központ bemutatása. *Nemzetbiztonsági Szemle,* 6. évf. 4. sz. 48–62.

UN Manual on the Prevention and Control of Computer-Related Crime (1994). Az Egyesült Nemzetek Szervezete Számítógépes bűnözés megelőzéséről és szabályozásáról szóló tanulmánya. New York, United Nations. Elérhető: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf (A letöltés dátuma: 2020. 04. 12.)

Urszán József (2011): A súlyos és szervezett bűnözés elleni fellépés feladatai az Európai Unióban. *Nemzet és biztonság,* 4. évf. 2. 59–71. Elérhető: www.nemzetesbiztonsag.hu/letoltes.php?letolt=406 (A letöltés dátuma: 2020. 03. 12.)

Várnay Ernő – Papp Mónika (2005): *Az Európai Unió joga.* Budapest, KJK Kerszöv.

Jogforrások

Magyarország Alaptörvénye

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai bűnözésről szóló egyezményének kihirdetéséről. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A0400079.TV&searchUrl=/gyorskereso%3Fpagenum%3D5 (A letöltés dátuma: 2020. 04. 10.)

A számítástechnikai bűnözésről szóló egyezménynek a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyve (é. n.).

2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáró

295/2010. (XII. 22.) Korm. rendelet a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól. Elérhető: https://net.jogtar.hu/jogszabaly?dbnum=1&docid=A1000295.KOR&mahu=1 (A letöltés dátuma: 2020. 03. 21.)

1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845 (A letöltés dátuma: 2020. 04. 03.)

60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról

Az ENSZ Közgyűlésének 55/63. számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról

Az ENSZ Közgyűlésének 56/121. számú határozata az információs technológiák bűncselekményekhez való felhasználása elleni harcról

Lisszaboni szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról (2007). Lisszabon, 2007. 12. 13. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A12007L/TXT (A letöltés dátuma: 2020. 04. 04.)

Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata (2008). Elérhető: https://europaialkotmanyjog.eu/?p=404 (A letöltés dátuma: 2020. 04. 08.)

EUMSZ – Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata (2012). Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A12012E%2FTXT (A letöltés dátuma: 2020. 04. 03.)

Az Európai Parlament és a Tanács 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32006L0024&from=HU (A letöltés dátuma: 2020. 04. 04.)

Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32013L0040 (A letöltés dátuma: 2020. 03. 21.)

Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0881&from=EN (A letöltés dátuma: 2020. 04. 04.)

A Tanács 2005/222 IB kerethatározata az információs rendszer elleni támadásokról. Elérhető: https://publications.europa.eu/hu/publication-detail/-/publication/708d86d8-ab9a-4e18-9bda-ac37405a3185 (A letöltés dátuma: 2020. 03. 20.)

Bizottsági rendelkezések az „ARGUS" általános sürgősségi riasztórendszerről. COM (2005)662, 2005. 12. 23.

A Bizottság 2006/25/EK határozata (2005. december 23.) a belső eljárási szabályzata módosításáról. HL L 19/20–22. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=OJ:L:2006:019:FULL&from=IT (A letöltés dátuma: 2020. 04. 16.)

A Bizottság (EU) 2017/1584 ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról. HL L 239/36–58. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32017H1584&from=EN (A letöltés dátuma: 2020. 04. 10.)

A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről – Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása [SEC(2009) 399, SEC(2009) 400]. Elérhető: https://op.europa.eu/hu/publication-detail/-/publication/0561fc28-3997-41b2-ab7b-c54fc8c24836/language-hu (A letöltés dátuma: 2020. 04. 11.)

Decision No.1202 OSCE Confidence-Building Measures Toreduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies (2016). Elérhető: www.osce.org/pc/227281?-download=true (A letöltés dátuma: 2020. 04. 03.)

Rövidítések jegyzéke:

BEREC *(Body of European Regulators for Electronic Communications):* Európai Elektronikus Hírközlési Szabályozók Testülete
CBMs *(Confidence Building Measures):* az EBESZ kiberbiztonsági bizalomépítő intézkedései
CDMA *(Cyber Defence Management Authority):* Számítógépes Védelmi Irányító Hatóság (NATO)
CDMB *(Cyber Defence Management Board):* Számítógépes Védelmi Irányító Tanács (NATO)
CECSP *(Central European Cyber Security Platform):* Közép-európai Kiberbiztonsági Platform
COSI: Európai Unió Belső Biztonsági Állandó Bizottsága
cPPP: állami- és magánszféra-partnerség
CSIRT: *Computer Security Incident Response Team*
DAE: Európai Digitális Menetrend
E.DSO *(European Distribution System Operators):* Európai Elosztórendszer-üzemeltetők
EBESZ: Európai Biztonsági és Együttműködési Szervezet
EC3 *(European Cybercrime Centre):* Számítástechnikai Bűnözés Elleni Központ (Europol)
ECCG: Európai Kiberbiztonsági Tanúsítócsoport titkársága
EGT: Európai Gazdasági Térség
ENCS *(European Network for Cyber Security):* Európai Kiberbiztonsági Hálózat
ENISA *(European Network and Information Security Agency):* Európai Hálózat- és Információbiztonsági Ügynökség
ENSZ: Egyesült Nemzetek Szervezete
ENTSO-E *(European Network of Transmission System Operators):* Átvitelrendszer-üzemeltetők Európai Hálózata
EU INTCEN: Európai Helyzetelemző Központ
EU LEA: Law Enforcement Agency
EUCTF *(European Union Cybercrime Task Force):* Európai Kiberbűnözés Elleni Akciócsoport
EUMS INT: Európai Unió Katonai Törzsének Hírszerzési Osztálya
Eurojust *(The European Union's Judicial Cooperation):* Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége
Europol: Európai Rendőrségi Hivatal
FIRST: *Forum of Incident Response and Security Teams*
GCI *(Global Cybersecurity Index):* Globális Kiberbiztonsági Felmérés
GDPR: általános adatvédelmi rendelet
HLEG *(High Level Experts Group):* az ITU magas szintű szakértői csoportja
I-CROS *(Internet Crime Reporting Online System):* internetes bűncselekmények bejelentésére szolgáló online rendszer
Interpol *(International Criminal Police Organization):* Bűnügyi Rendőrség Nemzetközi Szervezete
IOCTA *(Internet Organized Crime Threat Assessment):* Az internetes szervezett bűnözéssel foglalkozó részleg éves értékelése
ITU *(International Telecommunications Union):* Nemzetközi Távközlési Egyesület
IWG *(Informal Working Group):* az EBESZ kiberügyekkel foglalkozó informális munkacsoportja
JIT *(Join Investigation Team):* közös nyomozócsoport
K + I: kutatás és innováció
NATO *(North Atlantic Treaty Organization):* Észak-atlanti Szerződés Szervezete
NATO CCD COE *(Cooperative Cyber Defence Centre of Excellence):* Észak-atlanti Szerződés Szervezetének Kooperatív Kibervédelmi Kiválósági Központja

NIS-irányelv: a hálózati és információs rendszerek biztonságáról szóló európai uniós irányelv
OECD *(Organisation for Economic Co-operation and Development):* Gazdasági Együttműködési és Fejlesztési Szervezet
ORFK NEBEK: Országos Rendőr-főkapitányság Nemzetközi Bűnügyi Együttműködési Központ
SCCG: Kiberbiztonsági Tanúsítócsoport titkársága
SIAC: egységes információelemzési kapacitás
SIENA: biztonságos információcsere-hálózati alkalmazás
SIG's *(Special Interest Groups):* a FIRST különleges érdekcsoportjai
SITROOM: helyzetelemző központ
SRIA: stratégiai kutatási és innovációs menetrend

VÁKÁT OLDAL

Téglásiné Kovács Júlia

Az információbiztonság megalapozásának egyes adminisztratív eszközei
Az adatvédelmi jog mint a jogrendszert átható jogréteg?

Bevezetés

Az információnak a társadalomban és a gazdaságban betöltött szerepe egyre nagyobb hangsúlyt kap. A nyugati civilizáció negyedik ipari forradalmának, a digitalizációnak a korszakát éljük, amikor a gyors technológiai fejlődés és a globalizáció új kihívások elé állítja az információs önrendelkezési jog és a megfelelő tájékoztatáson alapuló információhoz való jog érvényesülését.

A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt, és kissé önellentmondásos módon az emberek egyre nagyobb mértékben hoznak nyilvánosságra és tesznek globális szinten (közösségi oldalakon keresztül) elérhetővé személyes adatokat, míg másfelől a személyes adatok védelméhez fűződő össztársadalmi igény egyre erőteljesebb.[1] A technológia az üzleti szféra és a közhatalmi szervek számára tevékenységük folytatásához a személyes adatok felhasználását minden eddiginél nagyobb mértékben lehetővé teszi.

Egyrészről ugyan az állami hatalomgyakorlás ma már egyenesen elképzelhetetlen információk nélkül, és voltaképpen a közigazgatás – információs szempontból – nem más, mint „szakadatlan adatkezelés":[2] mind a polgárok személyes adatainak a kezelése, mind a közhatalom-gyakorlás során létrejött információk, közérdekű adatok létrejöttének tekintetében.[3] Másfelől az állam feladata a fennhatósága alatt élő személyek biztonságának megteremtése, jogaik érvényesülésének a kikényszerítése. Az alapjogok érvényesítése kapcsán az állam elsődleges feladata, hogy az egyének személyes adatait védje, azok felhasználhatóságát megfelelő korlátok közé szorítsa, így az adatvédelem kérdése kapcsán a klasszikus alapjogi ember-állam megközelítésen túl a magánszférában is érvényesülő érintett-adatkezelő jogviszonyára is szükséges kitérnünk.

A pozitivista jogfelfogáson alapuló jogrendszer egyik legnagyobb kritikája, hogy nehezen követi le a társadalomban bekövetkező változásokat, és ez a kritika az információ-

[1] Szőke Gergely László – Pataki Gábor (2017): Az online személyiségprofilok jelentősége – régi és új kihívások. *Infokommunikáció és jog,* 14. évf. 69. sz. 63-70.

[2] Patyi András (2018): A közigazgatási eljárásjog és perjog változásai és összefüggései. In Benisné, Győrffy Ilona szerk.: *Tizennegyedik Magyar Jogászgyűlés: Balatonalmádi 2018. október 4–6.* Budapest, Magyar Jogász Egylet. 150–160.

[3] Lásd erről Péterfalvi Attila – Révész Balázs – Szalai András (2013): A közigazgatás adatkezelő tevékenysége. In Temesi István szerk.: *A közigazgatás funkciói és működése.* Budapest, Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. 265–295.

technológia fejlődésével és a kibertér növekedésével kapcsolatban álló jogok esetében még erőteljesebb.

A Big Data korában a jog mást nem tehet, minthogy egyfajta „alkut" köt a technológiai fejlődéssel, mivel a változások okozta tempót követni nem bírja, de a jog uralmára épülő jogrendszerekben csak azzal tudja a technológia jogszerű magatartását kikényszeríteni, ha enyhébb (betarthatóbb) szabályokat ír elő, hogy a jogi rendelkezések és a jogállamiság ne legyen puszta *lex imperfecta.* Az uniós jogalkotó alkut köt, és például a direktmarketing-tevékenység kapcsán kimondja, hogy a gazdasági érdek alapján korlátozható az információs önrendelkezési jog, ezen elismert jogos érdekek azonban nem minősülnek olyan meghatározott alapjogoknak vagy alkotmányos értékeknek, amelyekre tekintettel alkotmányosan korlátozható lehetne a személyes adatok védelméhez fűződő jog.

Hazánkban az alapjogok korlátozásának általános mércéjét, az úgynevezett szükségességi-arányossági tesztet ilyen formában nem találhattuk meg a korábbi Alkotmány normaszövegében, hanem azt az Alkotmánybíróság – több mint húszéves – gyakorlata alakította és kristályosította ki. Ez a teszt aztán az Alaptörvény 2011. évi elfogadásával került be az alkotmány normaszövegében, amely alapvető követelményként határozza meg, hogy milyen esetben lehetséges alapvető jogot korlátozni. Így az I. cikk (3) bekezdése szerint „[a]z alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható". E tanulmány központi kérdésköre a GDPR 6. cikk (1) bekezdés *f)* pontjában meghatározott jogos érdeken alapuló adatkezelési jogalap, amely szerint az adatkezelés akkor jogszerű, ha az az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek, valamint a jogalapot alátámasztó érdekmérlegelési-teszt horizontális és vertikális vizsgálatára irányul.

A jogos érdek mint jogalap a közhatalmi szervek esetében nem alkalmazható. A közhatalom gyakorlójaként ugyanis az államnak megvan az a lehetősége, hogy jogszabályokat alkosson, ezáltal jogi normába foglalja és expressis verbis kinyilvánítsa a saját „jogos érdekét".

A jogalapok sorában az utolsó az úgynevezett jogos érdeken alapuló adatkezelés, amelynek alkalmazásához szükséges az úgynevezett érdekmérlegelési teszt lefolytatása, amely egy „kvázi alapjog-korlátozási teszt", annyi különbségtétellel, hogy ez nem a klasszikus közjogi, vagyis az állam-egyén közötti jogviszonyokban, hanem magánjogi, tehát magánfelek közötti jogviszonyokban alkalmazandó. E jogalap alkalmazásának lényege, hogy az adatkezelő a saját (vagy más harmadik fél) érdekében kezel adatokat, és az adatkezelő ezen érdekeivel szemben mérlegeli azokat az érdekeket, amelyek a magánszféra, illetve magánélet körében az érintettek oldalán keletkeznek. Amennyiben a mérlegelés arra vezet, hogy az adatkezelő érdeke erőteljesebb az érintettek érdekeivel

szemben, akkor az adatkezelés ilyen esetekben is jogszerű.[4] Az érdekmérlegelés akkor szolgálhat jogalapként, ha más jogalap nem alkalmazható érvényesen, tehát ultima ratio. Ez a jogalap alkalmazandó a munkahelyi adatkezelések esetében, ugyanis részletesen kidolgozott törvényi jogalap nem áll az adatkezelő rendelkezésre, az érintett hozzájárulása pedig a munkáltató oldalán fennálló erőfölény miatt nem értékelhető önkéntesként.[5]

A kiinduló hipotézisem, hogy *minden adatkezelés,* amely nem az érintett kifejezett, önkéntes és megfelelő tájékoztatásán alapuló hozzájárulásán alapul, *az információs önrendelkezési jog korlátozásának minősül.* Ugyan az információs önrendelkezési jog mint alapjog korlátozása a klasszikus alkotmányjog-dogmatikai értelemben elsődlegesen az állam és az egyén viszonylatában értelmezendő, az alapjogok horizontális – harmadik irányú – hatálya (német terminológiával Drittwirkung), magánjogi jogviszonyokban való érvényesülése is felmerül a jogos érdek alkalmazása kapcsán.

A tanulmány során egyrészről arra keresem a választ, hogy horizontális értelemben – mint a tagállami jogba épült jogi előírás alkotmányjogi felülvizsgálata kapcsán – mennyiben egyeztethető össze a jogos érdek alkalmazásának előfeltételeként alkalmazott „érdekmérlegelési teszt" az alkotmányjogi dogmatikájában kiérlelt alapjogkorlátozási tesztekkel. Ennek kapcsán arra, hogy az adatkezelő vagy más harmadik fél jogos érdeke mennyiben egyeztethető össze az alapjog-korlátozási klauzulákban meghatározott „*más alapjog vagy alkotmányos érték"*, avagy az Alapjogi Chartában meghatározott törvényben rögzített „jogszerű ok" követelményekkel. Jogforrástani értelemben mennyiben egyeztethető össze az uniós jogi rendeleti szint az alkotmányokban és az Alapjogi Chartában meghatározott törvényi szinttel? *Az alapjog-korlátozás címzettje* esetében már nem az állam, aki a szükségességi-arányossági tesztet lefolytatja, hanem *az adatkezelő* (mindenféle képesítési előírás vagy jogvégzett személyhez kötött eljárás nélkül). Tekintettel arra, hogy a jogos érdek mint jogalap közhatalmi jogosítvány gyakorlása során (az állami tevékenység körében) nem alkalmazható, így nem beszélünk közjogi jogviszonyban történő alapjog-korlátozásról. Vajon a jogos érdek alkalmazása kapcsán felállított biztosítékrendszer (hatásvizsgálat, érdekmérlegelési teszt, az adatkezelési tájékoztatóban való jogszerű érdekre való utalás) mennyiben elegendő a jogszerű – magánjogi jogviszonyban történő – alapjog-korlátozáshoz? A tagállami jogalkotónak vajon áll-e fenn további jogalkotási kötelezettsége a jogos érdek alkalmazását megelőző érdekmérlegelési teszt szempontrendszerének kialakításában? Egyáltalán van-e lehetősége az EU-rendeletben meghatározott kérdéseket, kifejezett felhatalmazás nélkül megalkotni?

Vertikális (Magyarország–EU) szempontból pedig a tagállamok alapjog-korlátozási szuverenitásának a kérdésére vagyok kíváncsi. Kérdés, hogy az EU-nak milyen lehetőségei vannak, hogy az alapjogok korlátozása kapcsán minden tagállamra egyforma

[4] Szabó Endre Győző (2019): A személyes adatok védelméhez és a közérdekű adatok megismeréséhez fűződő jog. In Schanda Balázs – Balogh Zsolt szerk.: *Alkotmányjog–Alapjogok.* Budapest, Pázmány Press. 257.

[5] Uo.

kötőerővel rendelkező alapjog-korlátozási követelményt írjon elő, mégha ez az alapjog-korlátozás nem is a klasszikus állam és egyén viszonyában történik, hanem (elsősorban) a magánjogi jogviszonyokon belül. Vajon a jogos érdek mint alapjog-korlátozási klauzula alkalmazása jelent-e bármiféle hatáskörtúllépést az EU jogalkotása terén? Az EU adatvédelmi rendszere a jogos érdek megteremtésével alapjog-korlátozásra is felhatalmazást ad, ám kérdés, hogy ez mennyiben egyeztethető össze az Alaptörvény E) cikkében foglalt szuverenitástranszfer-klauzulával és az állami szuverenitás kérdésével.

A kutatási módszertan meghatározása

A vizsgálódások szempontjából, ami ebből az alapjog-korlátozási klauzulából a jogos érdek vizsgálata kapcsán felmerül, az egyrészről az, hogy az információs önrendelkezési jogot, a *személyes adatok védelméhez fűződő jogot tekinthetjük-e alapvető jogként?* E kérdésre az Alaptörvény VI. cikkében, valamint a nemzetközi egyezményekben megfogalmazottakra tekintettel – ahogy azt az általános részben részletesebben is kifejtették – egyértelműen igennel válaszolhatunk.

A tanulmány megírásához az általánosból a speciálisra fókuszáló módszertant választottam, így a dolgozat első felében az információs önrendelkezési jog általános kérdéseivel foglalkozom, majd ezt követően térek rá a fent megfogalmazott kérdések vizsgálatára.

Az általános részben áttekintjük az információs önrendelkezési jog mibenlétét, illetőleg annak korlátozhatóságának alkotmányjogi doktrínáját, így a tanulmány első fejezetében áttekintem az információs jogok létrejöttének társadalmi igényét, vagyis azt, hogy mi volt az a társadalmi „hívószó", amely miatt a nemzetközi jogi emberi jogi szerződések, valamint a magyar alkotmány az emberi jogok szintjére emelte e kérdést. Ennek kapcsán kitekintés jelleggel áttekintjük az információs önrendelkezési jog – nemzetközi, uniós és hazai – jogforrásait, majd az alapjogi dogmatika lényeges elemeit, így az információs önrendelkezési jog és a magánszféra tárgyát képező személyes adat fogalmát, valamint ennek mélyebb rétegeit, alanyát és címzettjét, valamint az alapjog tartalmát meghatározó követelményeket (így az alapelveket és a jogalapokat) is. A *különös részben* foglalkozom a jogos érdek jogalapjának fent ismertetett horizontális és vertikális kérdéseivel.

A kutatáshoz elsődlegesen *primer jogforrásoknak,* így az EU elsődleges jogforrásainak, Magyarország Alaptörvényének, a vonatkozó alkotmánybírósági határozatoknak, NAIH álláfoglalásainak, az uniós jogi aktusok és vonatkozó rendelkezéseinek az áttekintésére törekedtem, a másodlagos jogforrások és az azokat értelmező munkacsoporti vélemények feldolgozásával. *A szekunder források* között főként a hazai alapjogvédelmi és alkotmányjogi jogirodalom releváns publikációit tekintettem át, így különösen a Péterfalvi-féle *Magyarázat a GDPR-ról* című művet, amely egy olyan alapműnek tekinthető, amely az adatvédelmi szakjogászok „bibliájának" is felfogható. Emellett feldolgoztuk az elmúlt 10 év jogos érdeket vizsgáló szakirodalmi forrásait.

Az alapvető jogokra vonatkozó szabályok – az információs önrendelkezési jog jellege

A vizsgálódások szempontjából, ami az Alaptörvény I. cikk (3) bekezdésében meghatározott alapjogkorlátozási-klauzulából a jogos érdek vizsgálata kapcsán felmerül, hogy az információs önrendelkezési jogot, a *személyes adatok védelméhez fűződő jogot tekinthetjük-e alapvető jognak.* Ennek kapcsán az Alaptörvény VI. cikkében, valamint a nemzetközi egyezményekben megfogalmazottokra tekintettel áttekintjük az információs önrendelkezési jog alapjogi mivoltát és annak részelemeit.

A személyes adatok védelméhez fűződő jogot – az alapjogok generációk szerinti besorolása alapján – általában az alapjogok harmadik generációjához szokták sorolni, azonban véleményem szerint nem feltétlenül hordozza magán azokat a harmadik generációs alapjogi jegyeket, amelyek alapján a besorolása ennyire egyértelmű lenne. Ugyanis nagyon erőteljesen kötődik az emberi méltósághoz, amelyet az alapjogok első generációjához szokás sorolni, másfelől megjelenését tekintve harmadik generációs alapjogi jegy, hogy előbb jelenik meg a nemzetközi jogi színtéren, és csak ezt követően szivárog be a nemzeti alkotmányok szintjére. A harmadik generációs jogokkal szemben felhozott kritikákat – miszerint az alapjog tartalma, alanya nem határozható meg, a jogi igényérvényesítés nehézkes, mint például a környezethez való jog vagy a népek békéhez való joga kapcsán – tartók számára elég, ahogy arra a következőkben rámutatok, hogy igenis konkrét az információs önrendelkezési jog alapjog-dogmatikai rendszere.

Az információs önrendelkezés emberi jogi megjelenése

Az információs önrendelkezési jog az emberi méltóságból eredeztetett magánszférának a részét képezi, így a személyes adatok védelméhez fűződő jog a magánszféra emberi jogi fejlődésével együtt alakult ki. Az általános nemzetközi emberi jogi dokumentumok között alapvető fontosságúak az Emberi Jogok Egyetemes Nyilatkozatában,[6] az Emberi Jogok Európai Egyezményében,[7] valamint a Polgári és Politikai Jogok Nemzetközi Egyezségokmányában[8] foglalt rendelkezések. Továbbá az általános alapjogi dokumentumok

[6] 12. cikk: Senkinek magánéletébe, családi ügyeibe, lakóhelye megválasztásába vagy levelezésébe nem szabad önkényesen beavatkozni, sem pedig becsületében vagy jó hírnevében megsérteni. Minden személynek joga van az ilyen beavatkozásokkal vagy sértésekkel szemben a törvény védelméhez.

[7] 8. cikk: Magán- és családi élet tiszteletben tartásához való jog. 1. Mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák. 2. E jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges.

[8] 17. cikk: 1. Senkit sem lehet alávetni a magánéletével, családjával, lakásával vagy levelezésével kapcsolatban önkényes vagy törvénytelen beavatkozásnak, sem pedig a becsülete és jó hírneve elleni jogtalan támadásnak. 2. Ilyen beavatkozás vagy támadás ellen mindenkinek joga van a törvény védelmére.

között kell megemlítenünk az EU alapító szerződéseivel azonos kötőerővel rendelkező Alapjogi Charta vonatkozó rendelkezéseit is.[9]

Az adatvédelemre vonatkozó *speciális* szabályozások kapcsán szükséges megemlíteni az 1980-ban elfogadott OECD-irányelveket,[10] valamint az Európa Tanács által 1981-ben elfogadott, *Az egyének védelméről a személyes adatok gépi feldolgozása során* címet viselő egyezményt.

A személyes adatok védelméhez fűződő jog az Európai Unióban mind az elsődleges jogban (a szerződések szintjén), mind pedig a másodlagos jog (rendeletek, határozatok, irányelvek) szintjén elismert. A másodlagos források közül – az 1995-ben elfogadott adatvédelmi irányelvi szabályozást felváltva – 2016-ban fogadták el az általános adatvédelmi rendeletet[11] (a továbbiakban: GDPR), amely általános területi, tárgyi és személyi hatállyal rendelkezik az adatvédelmi kérdésekről, valamint az úgynevezett bűnügyi irányelvet,[12] amely a személyes adatok bűnüldözési célból történő kezelésének határozza meg az uniós kereteit, a tagállami szabályozásra bízva a részletszabályok megalkotását. Az uniós adatvédelmi szabályozás két alapvető célt tűzött ki maga elé: a személyes adatok védelmének magas szintű biztosítását a tagállamokban és a személyes adatok szabad áramlását a belső piacon. Az Európa Tanács, valamint az Európai Unió tagjaként a fenti dokumentumok kötelezőek Magyarországra nézve, azok kikényszerítése az EJEB, illetve az Európai Unió Bíróságának hatáskörébe tartozik.[13]

A nemzetközi egyezmények között meg kell megemlítenünk azokat a szektorális két- vagy többoldalú nemzetközi megállapodásokat, amelyek valamilyen határon átnyúló jogviszonyokhoz kötődő adatcserék rendjét szabályozzák. Számos ilyen szerződés létezik, szabályozva például a légi közlekedési, bűnüldözési, vízumkiadási és egyéb célú

[9] 7. cikk: A magán- és a családi élet tiszteletben tartása. Mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát és kapcsolattartását tiszteletben tartsák.
8. cikk A személyes adatok védelme. (1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. (2) Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni. (3) E szabályok tiszteletben tartását független hatóságnak kell ellenőriznie.

[10] A gazdaságpolitikai fórumként működő Gazdasági Együttműködési és Fejlesztési Szervezet az információs technológia és a számítógépes adatfeldolgozás elterjedését észlelve adta ki irányelveit a magánélet védelmének és a személyes adatok határon átívelő áramlásának tárgyában, amelyek később a nemzeti jogszabályokra is nagy hatással voltak. Sziklay Júlia (2012): A személyes adatok védelme. In Péterfalvi Attila szerk.: *Adatvédelem és információszabadság a mindennapokban.* Budapest, HVG ORAC. 37–39.

[11] A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló 2016/679/Európai Parlament és Tanács rendelete (HL L 119., 2016.5.4.)

[12] A személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló 2016/680. számú irányelv.

[13] Szőke Gergely László (2013): Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció és Jog,* No. 3. 107–112.

adatcseréket. Ezek a szerződések általában egy-egy külföldi állam viszonylatában rögzítik az adatok kezelésének szabályait, és ilyen módon érvényesítik a személyes adatok védelmére vonatkozó hazai elvárásokat nemzetközi téren is.[14]

A nemzetközi jogi dokumentumok többsége nagy hangsúlyt fektet a magánszféra és a személyes adatok védelmére egyaránt. A szoros kapcsolódás mellett szükséges megemlíteni, hogy a magánszféra védelmével nem teljesen azonos a személyes adatok védelme, hiszen számos személyes adat (például munkahelyi elérhetőség) nem tartozik a magánélethez.

E nemzetközi szintű alapjogi elismertség az információs jogok tagállami alkotmányokba való elismertségén és jogérvényesítési lehetőségein túl a szupranacionális jogorvoslati utakat is megnyitja, erre tekintettel az információs jogok értelmezésébe e jogorvoslati fórumok által kidolgozott gyakorlatot is szükséges figyelembe venni.

Az információs önrendelkezési jog tárgya, alanya, címzettje

Az információs önrendelkezési jog tárgya: Első ránézésre a laikusokban felmerülhet, hogy az *információ* áll az információs önrendelkezési jog középpontjában, azonban az információ tartalma alapján más alapjogok érvényesülése kerül a vizsgálódás középpontjába. Az *információ és az adat fogalmának viszonya* kapcsán, a hatályos jogi szabályozás[15] az adat legkisebb egységének tekinti az információt, amely adatok összességéből áll össze. Egy-egy adat – tartalmától függően – lehet személyes, közérdekű, de az alapjogi védelmen túlmutató egyéb vonású is (például nyilvános, üzleti, statisztikai, elhunyt személyekre vonatkozó adat stb.).

Amennyiben az emberhez mint *egyénhez fűződő információk* védelméről beszélünk, akkor a személyes adatok védelme, azon belül is az egyén magánszférájának a védelme kerül a középpontba, amely az *információs önrendelkezési jogot* képezi. Alkotmányjogi rendeltetését tekintve a személyes adatok *az emberek magánéletét, magánszféráját* (privacy) védik.

Az állam működése során létrejött adatokat *közérdekű adatoknak* nevezzük, a társadalmi rendeltetése szempontjából *információszabadságnak* hívjuk. A közérdekű adatok megismerésének és terjesztésének alkotmányjogi funkciója végsősoron az állam demokratikus működését szolgálja – amelynek előkövetelménye többek között az „átlátható állam", a megfelelő tájékoztatáson alapuló demokratikus közvélemény kialakítása, amely a véleménynyilvánítás szabadságának is az alapja. Az adatok tartalmát és jellegét

[14] Szabó 2019, 255.

[15] A hatályos szabályozás általános megfogalmazását a GDPR és az Infotv. között fennálló hatálybeli kérdések teszik szükségessé. Az adatok védelmét uniós szinten, generálisan a GDPR rendelkezései határozzák meg, azonban a tagállami szuverenitáshoz tartozó kifejezett kérdések tekintetében, például a honvédelmi, nemzetbiztonsági, bűnüldözési célú adatkezelések keretét illetően az Infotv. meghatározó; a GDPR-ban a tagállami hatáskörbe tartozó egyéb adatkezelési kérdéseket is (felügyeleti hatóság, elhunyt személyek adatkezelése stb.) az Infotv. szabályozza.

tekintve tehát el kell különítenünk a személyes adatokat a közérdekű adatoktól, azonban ezen adatok információtartalma alapján sokkal árnyaltabb képet kapunk.

Az Alaptörvény VI. cikke kifejezett védelemben részesíti a magán- és családi életet, az otthon nyugalmát, az egyén kapcsolattartásait – az ember magánszféráját.[16] Ami a magánszféra meghatározását illeti, az angolszász jogban használatos *privacy,* a magyar jogban használt *magánszféra* és a strasbourgi bíráskodás kiindulópontjaként szolgáló *magánélet* rokon fogalmak,[17] azonban eltérések adódnak az eltérő jogrendszerek létrejöttét indikáló gondolkodásmód fejlődése okán, így alapvető eltérés mutatkozik az angolszász és a kontinentális magánszféra-felfogások között.[18] Az eltérések alapja abban az alkotmányosérték-választásbeli különbségben leledzik, miszerint az európai alkotmányosság központi eleme az emberi méltóság, míg Amerikában a legfontosabb alkotmányos érték az emberi szabadság.[19]

A hatályos fogalom-meghatározás szerint *személyes adat az érintettre vonatkozó bármely információ, amely alapján az adott természetes személy azonosított vagy azonosítható.* Az adatvédelmi jogi rendelkezések rendezik az *azonosítható természetes személy* fogalmát is: az, aki közvetlen vagy közvetett módon, különösen valamely azonosító – például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján – azonosítható.

A személyes adatok legérzékenyebb kategóriái közé tartoznak a különleges, valamint a bűnügyi adatok – ezek az információk nyilvánvalóan olyan mértékben mutatnak rá az érintett legbensőbb vonásaira, amelyek már az ember magánszférájának legbensőbb rétegeit érintik.

A különleges adatok körét mind a GDPR, mind az Infotv. taxatív jelleggel határozza meg, amelyeknek – így a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatoknak, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatoknak, az egészségügyi adatoknak és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatoknak – *kezelése fő szabály szerint tilos.*[20]

A *bűnügyi személyes adat* az, amely a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben a büntetőeljárás lefoly-

[16] Koltay András (2012): A magánszféra, a személyes adatok, a képmás és a hangfelvétel védelme. In Koltay András – Nyakas Levente szerk.: *Magyar és európai médiajog.* Budapest, Magyarország. Complex Kiadó. 323–337.

[17] Szabó 2019, 255.

[18] A magánszféra fogalmának alakulásáról lásd bővebben: Csink Lóránt – Török Réka (2017): A magánszféra átalakulása – 21. századi kihívások. In Csink Lóránt szerk.: *A nemzetbiztonság kihívásainak hatása a magánszférára.* Budapest, Pázmány Press. 96.

[19] Sziklay Júlia idézi James Q. Whitman *The Two Western Culture of Privacy* című művét. Sziklay 2012, 29.

[20] GDPR 9. cikk.

tatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozik. A bűnügyi személyes adatok kezelése a mindennapokban az erkölcsi bizonyítványok kezelése kapcsán merül fel.[21]

Az információs önrendelkezési jog alanya: A személyes adatok védelméhez fűződő jog általános alanya, állampolgárságától függetlenül, az az élő természetes személy lehet, akit az adatvédelmi jog érintett*ként* határoz meg. A fogalom-meghatározás szerint *é*rintett a bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

A személyiségi jogok természetéből következik, hogy az ember jogképessége halálával megszűnik, mivel a személyiségi jogok alanya csak jogképes ember lehet.[22] Az ember halála után tovább él a személyiségének és társadalmi tevékenységének hatása, emiatt az elhunyt emléke és az elhunyttal kapcsolatos személyes adatok kezelése kihatással lehet a hozzátartozók magánszférájára.[23]

Az adatvédelem különleges védelmi szabályokat alkalmaz a kiszolgáltatott helyzetben lévő egyéb személyekre, így az adatvédelem különleges alanyaiként tekinthetünk a gyermekekre, az idősekre, valamint a fogyatékkal élő személyekre.

Az információs önrendelkezési jog címzettje: Mint minden alapjognak, így a személyes adatok védelméhez fűződő jognak is az első számú kötelezettje az állam. Az állam elsődleges kötelezettsége, hogy az alapjogokat konkretizáló jogszabályok megalkotásával, vagyis jogi és intézményi garanciákkal biztosítsa érvényesülésüket.

Az adatvédelem *horizontális természetű hatályára* tekintettel azonban a személyes adatok védelmével összefüggésben az érintetti adatokat kezelő jogi és természetes személyeknek, az adatkezelőnek[24] is vannak kötelezettségei. Az adatkezelői oldal meglehetősen sokrétű, hiszen a magánjogi jogviszonyokban meglehetősen szerteágazó szerződéses viszonyok csak tovább specifikálják a kötelezetti oldalt. Az adatkezelő nevében adatkezelési műveleteket végrehajtó személyeket az adatvédelem adatfeldolgozóként[25] határozza meg, míg a közös elhatározásból született adatkezelési célokat és eszközöket

[21] A bűnügyi adatkezelésekre 780/2016.számú irányelv vonatkozik, amelynek rendelkezéseit az Infotv.-be átültették.

[22] Eszteri Dániel (2018): A GDPR tárgya és hatálya. In Péterfalvi Attila – Révész Balázs – Buzás Péter szerk.: *Magyarázat a GDPR-ról.* Budapest, Wolters Kluwer Hungary. 51.

[23] Eszteri 2018, 51–53.

[24] Adatkezelő az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.

[25] Az adatfeldolgozó az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

meghatározó személyeket közös adatkezelőként nevesíti az adatvédelmi jog. Az adatkezelői oldalon megjelenik továbbá az adattovábbítás címzettjének kategóriája is, aki lényegében az a személy lesz, akivel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azonban a szabályozás rögzíti, hogy azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek.

Az információs önrendelkezés tartalma

A személyes adatok védelméhez fűződő jog alkotmányos tartalmát, így az alapelveket és a legfontosabb követelményeket a 15/1991. (IV. 13.) határozatában – a német alkotmánybíróság 1983-as népszámlálásdöntéséhez hasonló módon – az Alkotmánybíróság a következőképp határozta meg:„a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezi, hanem annak aktív oldalát is figyelembe véve, információs önrendelkezési jogként. Az Alkotmány 59. §-ában biztosított személyes adatok védelméhez való jognak eszerint az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csakis az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát. Kivételesen törvény elrendelheti személyes adat kötelező kiszolgáltatását, és előírhatja a felhasználás módját is. Az ilyen törvény korlátozza az információs önrendelkezés alapvető jogát, és akkor alkotmányos, ha megfelel az Alkotmány 8. §-ában megkövetelt feltételeknek."

Az Alkotmánybíróság kifejtette az adatvédelem további fő követelményeit is: így azt, hogy az adatkezelésnek átláthatónak kell lennie, biztosítani kell a tájékoztatáshoz, a helyesbítéshez, valamint a törléshez való jogot, továbbá az ezen jogok érvényesítéséhez szükséges előfeltételeket (például az adattovábbítási nyilvántartás vezetését). A két legfontosabb biztosítékként az Alkotmánybíróság a célhoz kötöttséget, valamint az adatok továbbításának és nyilvánosságra hozatalának korlátozását jelölte meg.

A Sólyom László nevéhez fűződő alaphatározat egészen a GDPR megjelenéséig meghatározta a magyar adatvédelmi jog kereteit. Ennek kifejeződése, hogy a fentiekben meghatározott alapjogi követelményeket követve, minősített 2/3-os többségű törvényként született meg a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény, majd e törvénynek a koncepcióját és szabályait átvéve született meg az Alaptörvény felhatalmazása szerint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, amelynek egyetlen sarkalatos törvényi minősített tárgyköre a NAIH jogállására és feladatkörére vonatkozó rendelkezés, amely az 1992-es törvényben létrehozott adatvédelmi ombudsmani rendszert váltotta fel.

Alapelvek

A személyes adatok kezelésére vonatkozó alapelveket az Alkotmánybíróság a – már idézett – 15/1991. (IV. 13.) AB határozatában kijelölte, amely alkotmányos követelmények mind a magyar jogban, mind az uniós szintű adatvédelmi szabályozásban megjelennek. Az 1991-ben íródott határozat leegyszerűsítő sémájához képest bebizonyosodott, hogy az adatkezelés jogalapjára nézve sokkal részletesebb, illetve némiképp megengedőbb szabályozásra van szükség. Amellett ugyanis, hogy az érintett hozzájárulását adja az adatkezeléshez, vagy törvény kötelező adatkezelést rendel el, lehetséges, hogy az adatkezelés egy szerződés előkészítéséhez vagy végrehajtásához szükséges, vagy valamilyen szerződésből fakadó jogi kötelezettség teljesítéséhez nélkülözhetetlen. Ezen túl olyan esetek is elképzelhetők, amikor az adatkezelőnek jogos érdeke fűződik az adatkezeléshez, és sem az érintett hozzájárulása, sem törvényi felhatalmazás nem áll rendelkezésre, mégis, az érintett és az adatkezelő érdekeinek mérlegelése alapján arra jutunk, hogy az adatok kezelése révén megvalósuló jogkorlátozás arányban áll az érvényesíteni kívánt érdekekkel. Ennek kapcsán, a GDPR-ban meghatározott alapelvek mentén minden adatkezelésnek meg kell felelnie az alapelvi követelményeknek.

A jogszerűség, tisztességes eljárás és átláthatóság követelménye szerint a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. Ezeknek az alapelveknek az érvényesülését szolgálja a kezelt adatok *jogalapokhoz* való kötöttsége. Az adatkezelés jogalapja a jog által absztrakt módon meghatározott azon esetek köre, amikor a személyes adatok kezelését legitimnek ismeri el. A jogszabályba foglalt esetekben a legitimitás mellé legalitás, jogszabályban rögzítettség társul.[26] A *tisztességes eljárás követelményét* többek között az érintetti jogok gyakorlásával összefüggésben kell alkalmazni, míg ezen érintetti jogok érvényesülésével és a tisztességes eljárás követelményével együtt jelenik meg az átláthatóság követelményének a teljesítése, amely az adatkezelésre vonatkozó érintetti tájékoztatások és adatkezelői nyilvántartások vezetésében mutatkozik meg.

A célhoz kötöttség alapelve szerint a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból kell történjen, úgy, hogy azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. A GDPR 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés. *Az adattakarékosság (adatminimalizáció) alapelve* szerint az adatkezelés céljai megfelelőek és relevánsak kell hogy legyenek, és a szükségesre kell korlátozódniuk. *A pontosság alapelve* szerint a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék. *A korlátozott tárolhatóság alapelve* szerint a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes

[26] Péterfalvi Attila szerk. (2012): *Adatvédelem és információszabadság a mindennapokban.* Budapest, HVG-ORAC. 90.

adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a GDPR 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel. *Az integritás és bizalmas jelleg (adatbiztonság) alapelve* alapján, az adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve. Amennyiben az adatok biztonsága sérül, úgy adatvédelmi incidensről beszélünk. Ezt az adatkezelő minden esetben köteles a nyilvántartásába felvezetni, amennyiben az incidens az érintettek jogaira nézve is valószínűsíthetően magas kockázattal jár, az incidenst a tudomásszerzést követő 72 órán belül be kell jelenteni a NAIH-nak, valamint az adatok alanyait is tájékoztatni kell.

Az elszámoltathatóság elve szerint az adatkezelő felelős az összes alapelvnek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására. Ez az adatvédelmi jog „szuperelve". Az általános bizonyítási teher megfordul, és az adatvédelem kapcsán minden esetben az adatkezelőnek kell bizonyítania, hogy az adatkezelési tevékenysége megfelel a jogszabályokban meghatározott követelményeknek.

Jogalapok

A korábbi hazai szabályozás a személyes adatok kezelését főszabály szerint két jogalapon tette lehetővé: egyrészt az érintett – előzetes tájékoztatáson alapuló – hozzájárulása alapján, másrészt kötelező jelleggel, amennyiben azt törvény vagy törvény felhatalmazása alapján az abban meghatározott körben helyi önkormányzat rendelete közérdeken alapuló célból rendelte el.

A magyar adatvédelmi jog hagyományosan *dichotóm* adatkezelési jogalaprendszerének következménye volt, hogy a hozzájáruláson alapuló adatkezelések körét túlzottan kitágították, másrészt felmerült az a kérdés is, megfelel-e a magyar szabályozás ezen a ponton az irányelvnek. Az Infotv. ezért bevezette a „másodlagos" jogalapokat.[27]. Az irányelv már a GDPR előtt is tartalmazta széles körű jogalap-katalógusát, tehát számos olyan jogalapot ismert el lehetséges adatkezelési jogalapként, amely az információs önrendelkezési jog doktrínája és a korábban hatályos Avtv. 3. § (1) bekezdésében foglalt szabályozás szerint a magyar adatvédelmi jogban sokáig nem volt önálló adatkezelési jogalap.[28] Megjegyzendő, hogy az Avtv. 2003. évi módosítása az irányelv 7. cikkében szereplő jogalapokat adatkezelési céllal vezette be a törvény szövegébe. Az Avtv. 5. § (4)

[27] Jóri András (2018a): Az adatkezelő vagy harmadik fél jogos érdekeinek érvényesítése mint jogalap („érdekmérlegeléses" jogalap). In Jóri András szerk.: *A GDPR magyarázata.* Budapest, HVG-ORAC. 160.
[28] Jóri 2018a, 161.

bekezdése szerint: a személyes adatot – akár az érintett hozzájárulásával, akár jogszabály alapján – különösen akkor lehet kezelni, ha ez közérdekű feladat, vagy az adatkezelő törvényi kötelezettségének teljesítéséhez, az adatkezelő vagy az adatátvevő harmadik személy hivatalos feladatának gyakorlásához, az érintett létfontosságú érdekeinek védelméhez, az érintett és az adatkezelő között létrejött szerződés teljesítéséhez, az adatkezelő vagy harmadik személy jogos érdekének érvényesítéséhez, társadalmi szervezetek jogszerű működéséhez szükséges.

Ennek következtében a magyar adatvédelmi jog adatkezelési jogalapokat illető rendelkezései jellemzően szigorúbbak voltak az EU tagállamaiban ismert adatvédelmi szabályoknál. E magasabb szintű alapjogi védelem azonban – egyes nézőpontokból – olyan jogi önkorlátozó tényezőként merült fel, amely a gazdasági versenyben a hazai résztvevőket hátrányosabb helyzetbe hozta a többi tagállam gazdasági szereplőihez képest.[29] Jóri András véleménye szerint „[e]gyes, az EU területén mindennapos adatkezelések – mint például a közvetlen üzletszerzés céljait szolgáló úgynevezett listakereskedelem [list broking] – Magyarországon jogellenesnek minősültek. Ez kétségtelenül hasznos az állampolgárok magánszféráját tekintve, ugyanakkor fölöslegesen korlátozónak minősül a magyar versenyszféra szempontjából. Számos esetben a szabályozás ráadásul indokolatlanul tett különbséget adatkezelők között – míg a profitorientált közvetlen üzletszerző cégek számára a direktmarketing célú adatkezelések széles körére törvény ad felhatalmazást, addig nonprofit szervezetek hasonló lehetőségekkel nem élhettek; míg főszabály szerint valamely gazdasági társaság csak az érintett hozzájárulására támaszkodva továbbíthatta adósának adatait követeléskezelő cég számára, addig egyes területeken működő cégek számára ez a lehetőség adott volt".

E kérdés megítélése azon alapul, hogy korlátozásnak tekinthető-e a magasabb szintű alapjogvédelmi intézményrendszer. Ez tehát abszolút nézőpont kérdése. Az alapjog-korlátozás szempontjait érintően is különféle elméletek ismertek. Külön válasza van a természetjogi, a pozitivista, az utilitarista (haszonelvű) és a moralista szemléletnek. Míg a természetjogi és a moralista – bár más-más szempontból, de – nem ismer el teljes korlátozást, addig a pozitivista-haszonelvű megközelítés a személy érinthetetlen dimenziójával nem számol.[30]

A fenti elméletek azon kérdés mentén alakultak ki, hogy miként lehet az egyén és a közösség érdekeit összeegyeztetni. A központi kérdés, hogy van-e az egyén szabadságának, autonómiájának egy olyan határa, amely semmilyen körülmények között nem sérthető meg, avagy a közösség haszna érdekében bármilyen korlátozás, beavatkozás megengedett.[31] Mindkét megközelítés lehetővé teszi az alapjog-korlátozást, de míg az első a korlátozásnak határt szab, addig az utóbbinak nem. Ugyanakkor megjelenhetnek úgy is, mint két szélsőség: az egyik, amely olyan tágra nyitja az egyén sérthetetlenségi

[29] Jóri 2018a, 162.
[30] Balogh Zsolt (2019): Általános rész. Az alapjogok korlátozása. In Schanda Balázs – Balogh Zsolt szerk.: *Alkotmányjog–Alapjogok*. Budapest, Pázmány Press. 41.
[31] Balogh 2019, 41–42.

dimenzióját, hogy az már a közösségi szempontok elenyészéséhez vezet, míg a másik esetén – szélsőséges esetben – a közösség érdekei az egyén elnyomását eredményezik, az egyén eszközzé válik a közösség céljai érdekében.[32]

A teljesség kedvéért, az információs önrendelkezési jog korlátozásának egyes fokozatai (és a szabályozásban megtalálható sorrendiség) mentén – amely ugyan nem jelent hierarchiát az egyes jogalapok alkalmazása kapcsán – tekintsük át az uniós szinten létrehozott jogalap-katalógus elemeit és azoknak legesszenciálisabb követelményeit!

A GDPR 6. cikk (1) bekezdésében található felsorolás – Osztopáni Krisztián véleménye szerint – nem jelent rangsort a jogalapok között. Ugyanakkor elismeri: azáltal, hogy a jogalapok ismertetése a hozzájárulással kezdődik, a szabályozás implicite kiemeli azt, hogy az adatvédelem alapvetően az információs önrendelkezési jogra, vagyis arra épül, hogy a saját személyes adataival – a törvény által meghatározott keretek között – mindenki maga rendelkezhet.[33]

Az első jogalap, amely az önrendelkezési jog teljes értékű érvényesülését szolgálja az, ha az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez. A hozzájárulás érvényességének fogalmi feltétele, hogy az adatkezeléshez az érintett akaratának kinyilvánítása önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű legyen, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez. Ez alapján a hierarchikus jogviszonyokban (például munkaviszonyban) meglehetősen szűk körben alkalmazható ez a jogalap.

A további jogalapok kapcsán az információs önrendelkezést korlátozták. Így kifejezetten akkor, ha az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges, bár a szerződés megkötési szándék főszabály szerint az érintett saját akaratából, elhatározásából jön létre, így még az egyén autonómiája (ha nem is kifejezetten a személyes adatainak felhasználása végett) azért valahol mégicsak tetten érhető. Másfelől előfordulnak olyan esetek is, amikor az egyéni önrendelkezési jog a szerződéskötés kapcsán nem egyértelmű, például közüzemi szerződések létrejötte, közszolgáltatások igénybevétele esetén, amelyeknek a jogi kereteit jogszabály állapítja meg. A jogi keretek törvényben vagy törvényi felhatalmazás alapján önkormányzati rendeletben való szabályozása már átvezet az adatkezelés adatkezelőt érintő jogi kötelezettség teljesítésére vonatkozó jogalap alkalmazásához, valamint a közérdekű vagy a közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges jogalaphoz.

A fenti jogalapokon túl az információs önrendelkezési jogot a közösség vagy más személyek érdekeivel szemben a leginkább – nem törvényi szinten meghatározott – korlátozó jogalapok a következők: a létfontosságú érdekei védelmének jogalapja és az adat-

[32] Balogh 2019, 41–42.

[33] Osztopáni Krisztián (2018): Jogalapok. In Péterfalvi Attila – Révész Balázs – Buzás Péter szerk.: *Magyarázat a GDPR-ról.* Budapest, Wolters Kluwer.

kezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges jogalap. A jogos érdek mint jogalap a közhatalmi szervek vonatkozásában nem alkalmazható. A közhatalom gyakorlójaként az államnak meg van az a lehetősége, hogy jogszabályokat alkosson, ami által jogi normába foglalhatja a saját „jogos érdekét".

A jogos érdek kérdésének jogforrási szintje

A második kérdés, amely felmerül a jogkorlátozás alapjogi dogmatikájának vizsgálta során, hogy *az alapjog-korlátozás törvényi jogforrási szintet* kíván meg az alapjogok tartalmának és korlátjainak megállapítása tekintetében.

Az uniós és tagállami jog jogalkotási jellegének viszonya tekintetében fontos rögzíteni, hogy míg a törvény tagállami hatáskörben – az állampolgárok által közvetlenül választott országgyűlési képviselők által, a törvényhozói hatalmat gyakorló – az Országgyűlés által elfogadott, a köztársasági elnök által kihirdetett olyan jogalkotási eredmény, amelynek a legitimációja közvetlenül visszavezethető a népre, addig a GDPR-t uniós rendeleti formában alkotta meg több tagállam képviselője, és közvetlenül alkalmazandó. A belső „integrált" jogforrási hierarchiában[34] magasabb szinten áll a hazai törvényeknél, de kérdés a tárgykör szabályozhatóságának felhatalmazása, mivel a rendeleti jogi aktus demokratikus legitimációs láncolata közvetettebb, így e kérdéskör kapcsán merül fel *a hatáskör-átruházás* kérdése. A törvényi rögzítettség kapcsán idetartozik továbbá a „*törvényi felhatalmazáson"*[35] alapuló jogos érdek, amely esetben szintén szükséges az érdekmérlegelési teszt lefolytatása.

A hipotézis szerint az érdekmérlegelési teszt lefolytatásának követelményeit, valamint a jogos érdek alkalmazhatóságának körét törvényi szinten lenne szükséges rögzíteni

[34] Patyi András – Varga Zs. András (2012): *Általános közigazgatási jog (az Alaptörvény rendszerében).* Budapest, Dialóg Campus. 52.
Az úgynevezett „integrált" jogforrási rendszer elmélete alapján a magyar jogrendszer három jogrend, nevezetesen a belső jog, az uniós jog, valamint a nemzetközi jog forrásaiból épül fel. Az Alaptörvény hatálybalépését követően az integrált jogforrási rendszer:
Alaptörvény, az Alaptörvény módosításai – „Integrációálló alkotmánymag",
Nemzetközi szerződések, EU elsődleges jogforrásai,
Európai Unió Bíróságának döntései,
AB döntései,
Kúria önkormányzati és jogegységi döntései,
EU közvetlen hatályú és közvetlenül alkalmazandó másodlagos jogforrásai,
sarkalatos törvény,
törvény,
kormányrendelet, a Magyar Nemzeti Bank elnökének rendelete,
kormány tagjának rendelete,
önálló szabályozó szerv elnökének rendelete,
helyi önkormányzati rendelet,
közjogi szervezetszabályozó eszközök.
[35] Osztopáni 2018.

(törvényi felhatalmazás). E követelmények meghatározása vajon mennyire egyeztethető össze az EU-bíróság gyakorlatával?

Az információs önrendelkezési jog tartalmának jogforrástani vizsgálata

Az alapjog-korlátozás formai követelményei röviden: korlátozni csak törvényben és előre meghatározott eljárás szerint szabad.[36] Az előre meghatározottság kérdését, a jogos érdek alkalmazásának előfeltételét az érdekmérlegelési teszt előzetesen betölti formális szempontból, azonban tartalmi meghatározása hiányzik a belső jogrendszerből, ami véleményem szerint jogbizonytalansághoz vezet.

Az Európai Unió alapjait és működését meghatározó az alapítószerződések – mint elsődleges jogforrások – nemzetközi szerződéseknek minősülnek, amelyeknek megkötésével az unió tagállamai abban állapodtak meg, hogy egyes, a joghatóságuk alá tartozó kérdésekben őket megillető hatásköreiket a többi tagállammal közösen, az alapítószerződésekben meghatározott mechanizmusok, intézmények útján gyakorolják.

Az Alaptörvény E) cikke e hatáskör-átruházás kapcsán általánosan kimondja, hogy Magyarország az európai népek szabadságának, jólétének és biztonságának kiteljesedése érdekében közreműködik az európai egység megteremtésében. A következő bekezdésben azonban alkotmányos szinten meghatározzák, hogy Magyarország az Európai Unióban tagállamként való részvétele érdekében nemzetközi szerződés alapján – az alapító szerződésekből fakadó jogok gyakorlásához és kötelezettségek teljesítéséhez szükséges mértékig – az Alaptörvényből eredő egyes hatásköreit a többi tagállammal közösen, az Európai Unió intézményei útján gyakorolhatja. A második bekezdés szerinti hatáskörgyakorlásnak összhangban kell állnia az Alaptörvényben foglalt alapvető jogokkal és szabadságokkal, továbbá nem korlátozhatja Magyarország területi egységére, népességére, államformájára és állami berendezkedésére vonatkozó elidegeníthetetlen rendelkezési jogát.

Bendik Tamás tűpontossággal állapítja meg, hogy a GDPR megalkotásából fakadó alapvető változás a szabályozás eszközéül választott jogforrás jogi természetének a következménye. EUMSz 288. cikkében meghatározottak szerint a rendeleti jogforrás az abban szabályozott jogviszonyok tekintetében közvetlenül hatályosul és alkalmazandó a tagállami jogrendszerekben, így az teljes egészében egységes jogi szabályozást eredményez a hatálya alá tartozó minden címzett vonatkozásában.[37] Maga a GDPR [9] preambulumbekezdése is kinyilvánítja, hogy a rendeleti jogforrási szintű szabályozási technika abból a meggyőződésből fakadt, hogy a tagállami adatvédelmi előírások egymástól való lényeges eltérésének egyik legfontosabb kiváltó oka a jogforrás jellegében volt keresendő.[38]

[36] Balogh 2019, 47–53.

[37] Bendik Tamás (2018): A tagállami jog és a GDPR viszonya – Az Infotv. szerepe a megváltozott szabályozási környezetben. In Buzás Péter – Péterfalvi Attila – Révész Balázs szerk.: *Magyarázat a GDPR-ról*. Budapest, Wolters Kluwer. 37.

[38] Bendik 2018, 37.

Az általános adatvédelmi rendelkezéseket magában foglaló jogforrás *rendeleti* jellege az ahhoz kapcsolódó tagállami szabályozási technika tekintetében alapvetően eltér a korábbi *irányelvi* jogforrás által megkövetelt szabályozási technikától. Az irányelvi rendelkezések címzettje a tagállam, nem annak joghatósága alatt álló jogalanyok. Ebből fakadóan az irányelvek előírásait a tagállam tartalmilag is a belső jog részévé köteles tenni. A közvetlenül hatályosuló és alkalmazandó rendeleti szabályok ezzel szemben tipikus esetben minden tagállamban azonos, egységes tartalommal érvényesülnek, azok a belső jogban nem ismételhetők meg. A tagállam kötelezettsége, hogy a rendeleti szabályok akadálymentes alkalmazhatóságát biztosítsa, egyrészt a rendeleti szabályokkal tartalmilag ellentétes belső jogi szabályok deregulációjával, másrészt a rendeleti szabályok érvényesüléséhez nélkülözhetetlen kiegészítő jogalkotási és egyéb intézkedések útján.[39]

Az EUMSz 16. cikke (az EKSz. korábbi 286. cikke) általánosan kimondja, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. A második bekezdésben megteremti a rendeleti jogalkotásra történő felhatalmazást, amely szerint a természetes személyeknek az uniós intézmények, szervek és hivatalok által, illetve az uniós jog alkalmazási körébe tartozó tevékenységeik során a személyes adataiknak a tagállamok által végzett feldolgozása tekintetében történő védelmére, valamint az ilyen adatok szabad áramlására vonatkozó szabályokat rendes jogalkotási eljárás keretében az Európai Parlament és a Tanács állapítja meg. E szabályok tiszteletben tartását független hatóságok ellenőrzik.

Bendik Tamás is megállapítja, hogy azon tárgykörök, amelyek tekintetében az uniós tagállamok szuverenitásuk gyakorlását nem ruházták át az uniós intézményekre, nemzeti jogalkotási és jogalkalmazási hatáskörben maradtak.[40] Így a személyes adatok védelme vonatkozásában is korlátozott az Európai Unió jogalkotási hatásköre.[41] Azon tárgykörökben, amelyek nem tartoznak az uniós jog hatálya alá, sem a charta, sem az alapítószerződések, sem az azok alapján megalkotott másodlagos uniós jogi aktusok nem alkalmazandók.[42] Ezt a korlátozott tárgyköri hatályt az adatvédelmi csomagban elfogadott uniós jogi aktusok is rögzítik.[43] Bendik Tamás rámutat, hogy a tagállami jogalkotónak tehát uniós jogi szempontból alkotmányos kötelezettsége, hogy azon tárgykörök, tevékenységek adatkezelési jogviszonyait szabályozza, amelyek az uniós jog hatályán kívül esnek.[44] Azonban az uniós alapítószerződések, a másodlagos uniós jogi aktusok nem adnak olyan konkrét felsorolást, amely az uniós jog hatálya alá tartozó vagy éppen annak hatálya alá nem tartozó tárgyköröket pontosan és kimerítő módon azonosítaná. A GDPR és a bűnügyi irányelv

[39] Bendik 2018, 40.
[40] Bendik 2018, 38.
[41] Bendik 2018, 38.
[42] Bendik 2018, 38.
[43] Bendik 2018, 38.
[44] Bendik 2018, 38–42.

preambulumbekezdései is csupán a nemzetbiztonsággal kapcsolatos tevékenységet mint egy példát említik ezen tárgykörök vonatkozásában.[45]

A fentiekkel egyetértve annyival egészíteném ki az uniós jogalkotási hatáskör kérdését, hogy álláspontom szerint, a jogos érdek jogalapjának létrehozására és a hozzá kapcsolódó érdekmérlegelési teszt követelményének előírására az EU-nak nincs explicit felhatalmazása. A charta 52. cikke, és az Alaptörvény E) cikk (2) bekezdése is az alapjogok gyakorlásának (korlátozásának) követelményeit tagállami hatáskörben, törvényi szinten rendeli rendezni. E kérdéskör irányelvi szinten történő meghatározása még összeegyeztethető lett volna a magyar Alaptörvény E) cikkében foglaltakkal, azonban a jelenlegi megoldás nem tartja tiszteletben a magyar alkotmányjogi hagyományokat.

Hatáskör-átruházás vagy tagállami hatáskör? A „jogos érdek" megalkotásának uniós jogi felhatalmazása

Az információs önrendelkezési jog tartalmának és korlátozásának kapcsán az Emberi Jogok Európai Bíróságának konzekvens gyakorlata, amelyet a *Leander-ügyben* összegzően megállapított, és amelyet azóta több ügy[46] kapcsán is megerősített, hogy akkor megfelelő a korlátozás, ha több követelmény teljesülése mellett (legitim célból, demokratikus társadalomban való igazoltság mellett) azt törvény írja elő, azaz a belső jogban meg kell határozni azt a jogalapot, amelyen a jogkorlátozás alapul.[47] Ez a jogi szabályozottság ugyan nem formai, hanem tartalmi kritérium, meg kell felelnie a jogbiztonság azon követelményének, miszerint kellően meghatározottnak és az emberek számára hozzáférhetőnek kell lennie.[48]

A vizsgálódások szempontjából az Alaptörvényben foglalt alapvető jogokkal és szabadságokkal való összhang kitétele a leghangsúlyosabb, amely magába foglalja az alapvető jogok korlátozására vonatkozó követelményeket is.

Ennek kapcsán az EUSz. 6. cikk (1) bekezdésének megfelelően az unió elismeri a charta szövegében foglalt jogokat, szabadságokat és elveket; és e charta ugyanolyan jogi kötőerőjű, mint a szerződések. A charta 8. cikkében foglalt, személyes adatok védelméhez való alapvető jog szorosan kapcsolódik a charta 7. cikkében szereplő, a magánélet tiszteletben tartásához való joghoz. Ugyanakkor a személyes adatok védelméhez való jog nem abszolút jog, hanem a társadalomban betöltött szerepének függvényében kell figyelembe venni. Ennek megfelelően a charta 8. cikkének (2) bekezdése lehetővé teszi a személyes adatok kezelését, ha teljesülnek bizonyos feltételek.

[45] Bendik 2018, 38–42.

[46] Rotaru vs. Romania. Lásd: Nagy 2015): Az információs önrendelkezési jog. In Smuk Péter szerk.: *Alkotmányjog III.: Alapjogok.* Győr, Universitas-Győr Nonprofit Kft. 209–230.

[47] P. G. and J. H. vs. the United Kingdom. Lásd: Nagy 2015, 210.

[48] P. G. and J. H. vs. the United Kingdom. Lásd: Nagy 2015, 210.

E tekintetben az említett rendelkezés szerint a személyes adatokat csak „tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni". Ezenfelül a charta 52. cikkének (1) bekezdése kimondja, hogy a chartában elismert jogok és szabadságok gyakorlása *csak a törvény által* és e jogok lényeges tartalmának tiszteletben tartásával korlátozható. Az arányosság elvére figyelemmel korlátozásukra csak akkor és annyiban kerülhet sor, ha és amennyiben az elengedhetetlen és ténylegesen az unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja.

A charta az alapjogok jogforrásai kapcsán differenciál: az alapjogok korlátozása kapcsán a (tagállami hatáskörben megalkotott) törvényi szinten történő meghatározását, míg az 52. cikk (5) bekezdése az uniós intézmények alapjog-érvényesítése kapcsán jogalkotási és végrehajtási aktusokra, valamint az uniós jog végrehajtására irányuló jogi aktusokra hivatkozik.[49] Azonban álláspontom szerint *az* EUMSz 16. cikkében meghatározott jogalkotási felhatalmazás az alapjog korlátozására vonatkozó követelmények megállapítására nem ad felhatalmazást.

A fentiek kapcsán Bendik is elismeri arra, hogy sem a charta, sem a másodlagos jogalkotási aktusok jogalapjául is szolgáló EUMSz 16. cikke korlátozást nem tartalmaz, megalapozottan kérdőjelezhető meg, hogy az adtavédelmi csomagban elfogadott aktusok e tekintetben az elsődleges uniós joggal maradéktalanul összhangban vannak-e azt illetően, hogy az érintettek alapjogainak védelmét e tárgyi hatályon kívül eső területen nem biztosítják.[50] Bendik rámutat, hogy a magyar jogalkotót az Alaptörvény, valamint vállalt nemzetközi jogi kötelezettségei arra kötelezik, hogy a személyes adatok védelméhez fűződő jog mint alapjog érvényesülését minden, a joghatósága alá tartozott jogviszonyban biztosítsa: a magyar jogrendszerben a személyes adatok védelméhez fűződő jog alapjogi jellegéből fakadóan ezen alapjog érvényesülésének biztosítékaira, a személyes adatok kezelésére vonatkozó feltételrendszerre, az adatkezelőt terhelő kötelezettségek és az érintetteket megillető jogosítványok körére, továbbá az alapjog érvényesülésének ellenőrzésére létrehozott intézmény feladat- és hatáskörére vonatkozó szabályokat törvényi szintű jogszabályok állapítják meg.[51]

A magyar alapjog-korlátozási doktrína formai kritériumként következetesen a törvényi szabályozást írja elő. Az alapjog-korlátozás formai követelményei röviden: korlátozni csak törvényben és előre meghatározott eljárás szerint szabad.[52] Az előre meghatározottság

[49] (5) Az ebben a chartában foglalt, alapelveket megállapító rendelkezések a saját hatásköreik gyakorlása során az Unió intézményei, szervei és hivatalai által elfogadott jogalkotási és végrehajtási aktusok, illetve a tagállamok által elfogadott, az uniós jog végrehajtására irányuló jogi aktusok útján hajthatók végre. E rendelkezésekre bíróság előtt kizárólag az ilyen jogi aktusok értelmezése, illetve jogszerűségének megítélése tekintetében lehet hivatkozni.

[50] Bendik 2018, 39.

[51] Bendik 2018, 341.

[52] Balogh 2019, 47–53.

kérdését, a jogos érdek alkalmazásának feltételét az érdekmérlegelési teszt előzetes lefolytatásának követelménye betölti formális szempontból, azonban tartalmi meghatározása hiányzik a belső jogrendszerből, ami véleményem szerint jogbizonytalansághoz vezet.

Törvényi felhatalmazás a jogos érdek jogalapjának alkalmazására

A jogbiztonság követelményét szolgálná az a megoldási mechanizmus, amennyiben a jogos érdekre vonatkozó féltételeknek (érdekmérlegelési teszt szempontjainak) és magának a jogos érdekre való hivatkozásnak törvényi jogalapja (felhatalmazás) lenne. Így a követeléskezelő és az engedményező közötti engedményezési szerződés esetében nincs törvényi jogalap az adós adatkezelésre. A törvénynek szükséges ezeket a felhatalmazásokat megadnia. Vagy említhető a lakcímnyilvántartás kérdése, amikor az igénylő a jogos érdekére alapozza a megismerni kívánt adatot, de az adatkiadására a közhatalmat gyakorló ügyintézőnek nincs kifejezett jogosultsága.

A jogos érdek alapjogi tartalmának vizsgálata

E fejezet központi kérdése, hogy a *jogos érdek fogalma* mennyiben egyeztethető össze a „más alapjog vagy alkotmányos érték" fogalmával, valamint az érdekmérlegelési teszt az alkotmánybíróság által kidolgozott alapjogkorlátozási teszttel. Ehhez az információs önrendelkezési jog korlátozása kapcsán kialakított teszt, majd az érdekmérlegelési tesztek kerülnek a fókuszba.

Az alapvető jog és az alkotmányos érték fogalma

Az alapjogoknak több kategóriáját is meg lehet különböztetni: az alapvető jogok és az emberi jogok csoportját. Amennyiben az alapvető jog fogalmát olyanképpen fogjuk fel, hogy az az alapjogok azon csoportját képezi, amelyet a nemzeti alkotmányok alapvető jogként ismernek el.[53]

Emberi jogok alatt azt értjük, hogy léteznek olyan jogosultságok, amelyek az embereket emberi mivoltuknál fogva illetik meg, amelyeket nem az állam teremt, de köteles

[53] Halmai Gábor és Tóth Gábor Attila szerint az „alapvető jogok" kifejezés és az „alapjogok" szó szinonimák, s gyakran még az alkotmányos jogok kifejezés is ezzel azonos jelentésben fordul elő. Halmai Gábor – Tóth Attila (2008): *Emberi jogok.* Budapest, Osiris Kiadó. 29. Ez a megállapítás Gárdos-Orosz Fruzsina álláspontja szerint téves, mert „alkotmányos jognak nevezhető minden, az alkotmányon alapuló alanyi jog, így azok is, amelyek nem az emberi jogok alkotmánybeli megfogalmazásai (például az országgyűlési képviselők jogosultságai)". Gárdos-Orosz Fruzsina (2009): 8. § [Alapjogok korlátozása]. In Jakab András szerk.: *Az Alkotmány Kommentárja.* Budapest, Századvég Kiadó. 392. Az Alaptörvény ezen fogalmi meghatározásokhoz képest leginkább az alapvető jog terminológiáját alkalmazza, ezen belül is az ember alapvető egyéni és közösségi jogait, illetve ezen jogok és kötelezettségek természetüknél fogva a törvény alapján létrehozott jogalanyok jogait nevezi meg.

elismerni és tiszteletben tartani, és amely jogok minden embert egyenlően illetnek meg.[54] Az emberi jogok olyan erkölcsi és egyben alanyi jogok, amelyek azon alapulnak, hogy a jogosult emberi lény, akit emberhez méltó bánásmód illet meg.[55] Ma már azonban emberi jogok csoportja nem csupán az egyénnek az államhoz fűződő viszonyáról nyújt eligazítást, hanem az egyén és közösségei viszonyáról *más egyénekhez és közösségekhez* is. A különféle, méltánylást érdemlő emberi igényeket egyre nagyobb számban minősítik emberi jognak, és fokozatosan bővül az emberi jogok érvényesülési köre.[56]

Az alkotmányos érték már kisebb védelmi szintet élvez az alapjogokkal szemben, így többek között a jogi igényérvényesítés lehetősége is kisebb. Az alkotmányos érték, az államcél egyfajta állami önkötelezést fejez ki, amelynek az Alaptörvényben való kifejeződése leginkább az alapvetések között jelenik meg az egyes intézmények védelme kapcsán, de az alapjogok korlátozása kapcsán legitim célként állja meg a helyét.

A jogos érdek fogalma

A fentiekben meghatározott alkotmányban való rögzítettségnél alacsonyabb szintű jogforrásban való megjelenés is elegendő a jogos érdek igazolására. E feltételezés alátámasztására elsőként a hazai jogrendszer jogosérdek-fogalmát vizsgálom meg a jogszabályok, valamit a hazai adatvédelmi hatóság gyakorlata szerint, majd rátérek az uniós adatvédelmi szabályozásban fellelhető támpontokra, így a GDPR-ban való meghatározás mellett, a 29. munkacsoport véleményére is.

A jogos érdek fogalma a magyar jogszabályok kontextusában: A jogos érdek fogalmát a magyar jog számos esetben, így a közigazgatási jog az ügyfél fogalmának meghatározásánál, valamint a polgári eljárásjog a *beavatkozás intézményének szabályozásánál* is használja.[57] A bírói gyakorlat szerint „jogos érdek fogalma alatt a jogszabályon alapuló, jog által védett érdeket kell érteni. A fél érintettsége a kereshetőségi jogban (perbeli legitimáció, legitimatio ad causam) valósul meg".[58] Jóri András véleménye szerint felmerülhet továbbá olyan értelmezés is, amely szerint a jogos érdek megegyezik a *méltányolható*

[54] Az emberi jogok általános jellegét illetően három nézetet különböztet meg Takács Péter. Az első nézet szerint – Mauric Cranston Cranston *What are Human Rights?* című műve alapján – az emberi jogok gyakorlatilag természetes jogok, csupán más az azokat alátámasztó érvek rendszere. A másik – szélesebb körben elterjedt – felfogás szerint az emberi jogok valójában erkölcsi jogok. „Egy emberi jog úgy határozható meg, mint egy egyetemes erkölcsi jog; mint valami olyasmi, amivel minden embernek, mindenütt és mindig rendelkeznie kellene; valami, amitől senkit sem lehet megfosztani anélkül, hogy súlyosan meg ne sértenék az igazságosságot; s ami minden emberi lényt pusztán azért illet meg, mert ember." Végül, egy harmadik álláspont szerint az emberi jogok a jogok önálló csoportját jelentik, amelyben a természetes és az erkölcsi jogok egyes elemei csak kiegészítő szerepet játszanak. Takács Péter (2011): *Az emberi jogok jogelméleti kérdései.* Elérhető: http://jog.unideb.hu/documents/tanszekek/jogbolcseleti/tansegdletek/2011-12/2011-12-2/takcs_p_-_az_emberi_jogok_jogelmleti_krdsei__a_jogok.pdf (a letöltés dátuma: 2016. 01. 29.)

[55] Halmai–Tóth 2008, 28.

[56] Halmai–Tóth 2008, 29.

[57] Jóri 2018a,168.

[58] Jóri 2018a,168.

érdek, sőt akár a *gazdasági érdek* fogalmával. Jóri szerint ez a széles értelmezés a fenti jogalapok szinte korlátlan alkalmazhatóságához vezetne. A német irodalom szerint jogos érdek az, *ami nem ellentétes a „Treu und Glauben" elvével.*[59]

A jogos érdek fogalma a NAIH joggyakorlata szerint: A NAIH tiszteletben tartva az uniós jogalkotó szándékát, és a meghatározott felügyeleti hatáskörét túl nem lépve foglalkozik a jogos érdek meghatározásával. E jogalapot eljárásai során inkább az érdekmérlegelési szempontrendszernek felelteti meg, mintsem hogy explicit módon meghatározná, melyek azok a jogos érdeknek számító tények, amely alapján jogszerű a GDPR 6. cikk (1) bekezdés *f)* pontjának az alkalmazása. Így a NAIH 2018. évi beszámolójában[60] kifejtette, hogy „[ha] az adatkezelés jogalapja a jogos érdek, akkor az adatkezelőnek előzetesen érdekmérlegelési tesztet kell elvégeznie, továbbá a tájékoztatási kötelezettsége keretében az érintettet a tiltakozáshoz való jogáról is külön tájékoztatnia kell. Az általános adatvédelmi rendelet példálózóan megemlít két esetet, melyeknél ennek a jogalapnak az alkalmazása gyakran előfordul, nevezetesen azokat, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll".

A NAIH gyakorlata konzekvensen képviseli azt az álláspontot, amely szerint a közhatalmi tevékenységgel összefüggő adatkezelés esetében nem alkalmazható a jogos érdek mint jogalap. „Az adatkezelő közfeladatait meghatározó jogszabályi rendelkezéseken alapuló adatkezelések jogalapja tehát a GDPR 6. cikk (1) bekezdés *e)* pontja. Fontos kiemelnünk azt is, hogy egy közhatalmi tevékenységet vagy egyéb közfeladatot ellátó szerv – mint költségvetési szerv – minden közjogi és magánjogi jogviszonyának, és az ahhoz járulékosan kapcsolódó adatkezelési jogviszonyainak kizárólag közfeladatai ellátásával összefüggésben lehet alanya, ettől eltérő minősége fogalmilag kizárt. Ebből fakadóan e jogalap, mintegy magába olvasztja, elnyeli a további adatkezelési jogalapokat."[61]

Jóri András ezzel kapcsolatban kimondja, hogy a NAIH jogosérdek-fogalmáról általában elmondható, hogy ezen értelmezések az adatkezelőknek kedvező, széles értelmezést tesznek lehetővé, ami Jóri szerint gyengítette a jogvédelem szintjét.[62] E megállapítás alátámasztására példaként hozza fel Jóri a Google Street View-ügyet, amelynek kapcsán a NAIH úgy foglalt állást, hogy „[a] fentiek értelmében az adatkezelés jogalapjainak elemzése kapcsán az Adatvédelmi Irányelv 7. cikk *f)* pontját is figyelembe vettem, mivel úgy ítélem meg, hogy a Google-nek a GSV szolgáltatás bevezetéséhez és működtetéséhez olyan jogszerű érdeke fűződik, amelynek érvényesítéséhez szükséges lehet az érintett adatainak kezelése, és amely arányban áll az érintettek személyes adatai védelméhez fűződő jogának esetleges korlátozásával".[63]

[59] Jóri 2018a, 169. Idézi: Liber Ádám (2012): A jogos érdeken alapuló adatkezelésről. *Infokommunikáció és Jog,* 2. sz. 79–88.
[60] 2018. évi NAIH beszámoló
[61] 2018. évi NAIH beszámoló 36.
[62] Jóri 2018a, 169.
[63] 2012. évi NAIH beszámoló 57.

Ennek kapcsán szükséges megvizsgálni, a NAIH GDPR-alkalmazását követő joggyakorlatát is. Ennek kapcsán, a NAIH/2019/2402/9. számú határozatában, már szűkebben értelmezte a jogos érdek fennállásának létét, így kimondta, hogy „telefonszám jogérvényesítéshez szükségessége indokolatlan, mert a követeléskezelés nem jogi eljárás, hanem egy olyan a végrehajtást megelőző »eljárás«, [a]mely a felek kölcsönös együttműködését és konszenzusát kívánja elősegíteni. A Kérelmező telefonszámának kezelése a követelés behajtásához és a Kérelmezővel történő kapcsolattartáshoz nem elengedhetetlenül szükséges, hiszen a Kötelezett a Kérelmezővel történő kapcsolattartásához a Kérelmező lakcímadatát kezeli. A telefonszám kezelése a gépjármű forgalomból való kivonásához sem szükséges".[64]

A NAIH/2019/2528. számú állásfoglalásában az iskolai évkönyv elkészítése során felmerülő adatvédelmi vonatkozású kérdések kapcsán igazolhatónak találta a jogos érdek fennálltát. „A fentiekkel összhangban, miszerint elkülönülő adatkezelési műveletnek minősül egy felvétel elkészítése és annak különböző módon történő felhasználása (évkönyvben, illetve nyilvános sajtófelületen), amely adatkezelési műveletek különböző célból lehetnek szükségesek, azokhoz az iskolának műveletenként eltérő érdeke fűződhet, így fontos, hogy az érdekmérlegelési teszt egyértelműen tartalmazza, hogy melyik adatkezelési művelet elvégzése pontosan miért áll jogos érdekében az iskolának."

A jogszerű érdek fogalma a 29. munkacsoport szerint: A jogszerű érdek fogalmát, az Adatvédelmi Irányelv 7. cikk (1) bekezdés *f)* pontjában megfogalmazott jogalapot, a 29. cikk szerinti munkacsoport is értelmezte, amely külön véleményt szentelt e kérdésnek.[65]

A munkacsoport először is rögzíti a különbséget a célhozkötöttség elvéhez kapcsolódó cél és az érdek fogalma között, amelyek kapcsán példát is hoz, miszerint „a »cél« az a különös ok, amely miatt az adatot feldolgozzák, vagyis ez az adatfeldolgozás célja és szándéka. Az érdek azonban egy tágabb fogalom; az az érdek, amellyel az adatkezelő rendelkezik az adatfeldolgozásban, illetve az az előny, amelyet az adatkezelő származtat – vagy a társadalom származtathat – az adatfeldolgozásból. Például egy vállalatnak lehet érdeke a nukleáris erőművében dolgozók egészségének és biztonságának biztosítása. Ehhez kapcsolódóan a vállalatnak lehet célja bizonyos hozzáférést ellenőrző eljárások megvalósítása, ami igazolja meghatározott személyes adatok a dolgozók egészségének és biztonságának elősegítése érdekében végzett feldolgozását [kezelését]." Az érdeknek egyértelműen megfogalmazottnak kell lennie, és az is feltétel, hogy az az *adatkezelő által érvényesített* legyen; ezen túl a szöveg „valós és fennálló érdeket feltételez, olyat, amely megfelel a jelenlegi tevékenységeknek vagy a közeljövőben várható előnyöknek". A vélemény szerint a „homályos vagy elméleti érdekek nem megfelelőek".[66]

[64] Elérhető: https://naih.hu/files/NAIH-2019-2402_hatarozat.pdf (a letöltés dátuma: 2019. 01. 29.)

[65] 06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról

[66] 06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról. 25–26.

A munkacsoport megkülönbözteti továbbá az érdekeket abból a szempontól is, hogy azok „lényegesek és előnyösek" a társadalom számára, vagy sem. Előnyösnek minősíti a média azon érdekét, hogy a kormányzati korrupcióról szóló információkat közzé tegye, vagy a tudományos kutatásokhoz fűződő érdeket. Ugyanakkor a vállalatok azon gazdasági érdeke, hogy minél többet tudjanak meg a lehetséges ügyfeleikről annak érdekében, hogy jobban megtervezhessék a termékeikről és szolgáltatásaikról szóló hirdetéseket vagy kevéssé pozitívan, vagy kifejezetten ellentmondásosan hat a társadalom egészére a munkacsoport véleménye szerint. Ez önmagában nem a jogszerűség megítélésével kapcsolatban fontos, hanem az érdekmérlegelési teszt során az érdekek súlyát megállapító mérlegeléssel kapcsolatban.

Összességében az érvényesített érdekkel kapcsolatban a munkacsoport szerint három konjunktív követelmény fogalmazható meg:

– *törvényesnek* kell lennie (vagyis meg kell felelnie a vonatkozó uniós és nemzeti jognak);
– kellően *egyértelműnek* (vagyis kellően pontosnak) kell lennie annak érdekében, hogy a mérlegelési tesztet el lehessen végezni az érintettek érdekeire és alapvető jogaira vonatkozóan;
– *valós és fennálló érdeknek* kell lennie (vagyis nem lehet elméleti).

Ami a jogszerűség fogalmát illeti, a munkacsoport megállapítja, hogy „a jogszerű érdek fogalma érdekek széles körét foglalhatja magában, legyenek azok jelentéktelenek vagy lényegesek, egyértelműek vagy ellentmondásosak". Az adatvédelmi munkacsoport gyakorlata tágabban határozza meg a jogos érdek fogalmát, mivel abba a nem közvetlenül jogszabályi rendelkezésen alapuló jogszerű érdekek és szükségletek is beletartoznak.[67]

Jogszerű érdekekre a munkacsoport által hozott példák: a szólás- vagy információszabadsághoz való jog gyakorlása többek között a médiában és a művészetekben; hagyományos módú közvetlen üzletszerzés és az üzletszerzés vagy reklám más formái; nem kereskedelmi kéretlen üzenetek, többek között politikai kampányokhoz vagy jótékonysági adománygyűjtéshez; jogi kérelmek végrehajtása, ideértve a peren kívüli eljárások útján történő követelésbehajtást; csalás, szolgáltatásokkal való visszaélés vagy pénzmosás megelőzése; dolgozók biztonsági vagy vezetési célú ellenőrzése; belső informátori (visszaélés-jelentési) rendszerek; fizikai biztonság, informatikai és hálózati biztonság, történelmi, tudományos vagy statisztikai célú adatfeldolgozás, kutatási célú adatfeldolgozás (ideértve a piackutatást).

A fentieken túl Liber Ádám még a következő tíz jogos érdeken alapuló adatkezelési köröket gyűjtötte össze a munkacsoport tevékenysége alapján: a munkavállalói adatok kezelése, bírósági tárgyalásokat megelőző vizsgálat, külföldi hatóságtól származó, bírság terhével történő idézés, internetes keresőmotorok, belső visszaélés-jelentés, a fertőző betegségek elleni fellépés, földrajzi helymeghatározási szolgáltatások, kamerás megfigyelés, intelligens fogyasztásmérők adatkezelése.[68]

[67] Liber 2012, 79–88.
[68] Liber 2012, 79–88.

Jogos érdek fogalma a GDPR preambuluma szerint: Bizonyos érdekeket jogszerű érdeknek ismer el a GDPR preambuluma (egyéb feltételek teljesülése mellett). Így azokat az eseteket, amikor releváns és megfelelő kapcsolat áll fenn az érintett és az adatkezelő között, például olyan esetekben, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll. A jogos érdek fennállásának megállapításához mindenképpen körültekintően meg kell vizsgálni többek között, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor. Idetartozik továbbá a csalásmegelőzés érdekében végzett adatkezelés; a közvetlen üzletszerzési célú adatkezelés; a vállalkozáscsoport vagy „központi szervhez kapcsolódó intézmények részét képező adatkezelők" azon érdeke, amely ahhoz fűződik, hogy a vállalkozáscsoporton belül belső adminisztratív célból személyes adatokat továbbítsanak, ideértve az ügyfelek és az alkalmazottak személyes adatainak a kezelését is.

Jogos érdekként ismeri el a GDPR *a hálózati és információbiztonság védelméhez fűződő érdeket:* „az érintett adatkezelő jogos érdekének minősül a közhatalmi szervek, számítástechnikai vészhelyzetekre reagáló egység [CERT], hálózatbiztonsági incidenskezelő egységek [CSIRT], elektronikus hírközlési hálózatok üzemeltetői és szolgáltatások nyújtói, valamint biztonságtechnológiai szolgáltatók által végrehajtott olyan mértékű személyes adatkezelés, amely a hálózati és informatikai biztonság garantálásához feltétlenül szükséges és arányos, vagyis adott titkossági szinten az érintett hálózat vagy információs rendszer ellenálló képessége az e hálózatokon és rendszereken tárolt vagy továbbított adatok, valamint az e hálózatok és rendszerek által nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, integritását és bizalmas jellegét sértő véletlen eseményekkel, illetve jogellenes vagy rosszhiszemű tevékenységekkel szemben. Ez magában foglalhatja például az elektronikus kommunikációs hálózatokhoz való engedély nélküli hozzáférés és a rosszindulatú programterjesztés megakadályozását, továbbá a szolgáltatás megtagadásával járó támadások, valamint a számítógépes és elektronikus kommunikációs rendszerekben való károkozás megállítását".

A fejezet megállapítása

E fejezetben összemért alapjog- és alkotmányosérték-fogalom, valamint a jogos érdek fogalma egyértelműen azt az eredményt hozta, hogy nem beszélhetünk egy szinten álló védelemről. Míg az alapjog és az alkotmányos érték esetében az alkotmányjogban való rögzítettség (még az implicit alapjogi elismertség is idetartozik, amikor expressis verbis az alkotmány szövege nem utal ezekre az alapjogokra, alkotmányos értékekre, de a nemzetközi jogi kötelezettségvállalásokból vagy az alkotmánybíróság gyakorlatából ezek a jogok levezethetők – lásd például élelemhez való jog) az alapjog-korlátozási teszt

előfeltétele, addig a jogos érdek jogszabályban való rögzítettsége sem alapvető követelmény annak alkalmazásakor.[69]

A vezérfonalat nem elhagyva, miszerint az alapjog-korlátozás alapvetően az egyén és az állam viszonyában értelmezhető, a magánjogi jogviszonyokban való alapjog-korlátozáskor az államnak feladata megteremteni azokat a jogi kereteket, amelyek során a magánfelek közötti jogkorlátozás is megfelel a jogbiztonság követelményéből fakadó normavilágosság követelményének. Ellenkező esetben a jogos érdek fogalmának eltúlzott használata túlságosan tág keretet biztosít az információs önrendelkezési jog korlátozására, valamint hasonló élethelyzetekben alkalmazott jogos érdek jogalap használata – ellenkező jogértelmezésre is vezethet (attól függően, milyen érdekmérlegelési teszt minőséget képes az adatkezelő igazolni).

Az érdekmérlegelési teszt és a szükségességi-arányossági teszt összevetése, jogos érdek alkalmazása kapcsán felállított biztosítékrendszer

Az információs önrendelkezési jog korlátozásának feltételei a GRPR hatálybalépése előtt: A személyes adatok védelméhez való jog nem abszolút jog, azt az arányosság elvével összhangban, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal. A GDPR kimondja, hogy a személyes adatok kezelését az emberiség szolgálatába kell állítani.

Az információs jogok tartalmát a GDPR és az Infotv. bontja ki. Az Infotv. rendelkezései a személyi szám általános alkalmazhatóságának jogellenességét kimondó 15/1991. (VI. 13.) AB határozatba foglalt elvi alapokra nagyban támaszkodik: a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezi, hanem annak aktív oldalát is figyelembe véve információs önrendelkezési jogként. A határozat kifejtette, hogy az információs önrendelkezési jog gyakorlásának feltétele és garanciája a célhoz kötöttség, ami azt jelenti, hogy személyes adatot feldolgozni csak pontosan meghatározott és jogszerű célra szabad, amelyet törvénnyel kell szabályozni. *Személyes adatot felvenni és felhasználni általában csak az érintett hozzájárulásával szabad.* Az átláthatóság követelményének teljesítése kapcsán mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát. A határozat rögzítette továbbá, hogy *kivételesen törvény elrendelheti a személyes adat kötelező kiszolgáltatását, és előírhatja a felhasználás módját is; az ilyen törvény azonban, mivel korlátozza az információs önrendelkezési jogot, meg kell hogy feleljen az alapjog-korlátozás általános követelményeinek.* Az ilyen rendelkezést tartalmazó törvény korlátozza az információs önrendelkezés alapvető jogát, ami pedig akkor alkotmányos, ha megfelel az általános alapjogkorlátozási teszt által meghatározott feltételeknek [15/1991. (IV. 13.) AB határozat].

[69] Vö. Pozsár-Szentmiklósy Zoltán (2016): *Alapjogok mérlegen: Az általános alapjogi tesztek dogmatikája.* Budapest, HVG-ORAC.

Az Alkotmánybíróság az információs önrendelkezési jog korlátozásának feltételeit az alapjog-korlátozás általánosan alkalmazott tesztjéhez (szükségesség-arányosság) képest konkretizálta. A személyes adatok védelméhez való jog korlátozására is irányadó alapjogi teszt alkalmazásakor *az Alkotmánybíróság az alapjog-korlátozás szükségessége körében értékeli a célhoz kötöttség követelményének érvényesülését:* azt, hogy a személyes adat feldolgozásának van-e pontosan meghatározott és jogszerű célja, s az adatkezelés minden szakasza megfelel-e a bejelentett és közhitelűen rögzített célnak. Az információs önrendelkezési jog gyakorlásának tehát feltétele és egyben legfontosabb garanciája a célhoz kötöttség. Ez azt jelenti, hogy személyes adatot feldolgozni csak pontosan meghatározott és jogszerű célra szabad. Az adatfeldolgozásnak minden szakaszában meg kell felelnie a bejelentett és közhitelűen rögzített célnak. A célhoz kötöttségből következik, hogy a meghatározott cél nélküli, „készletre", előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és -tárolás alkotmányellenes [15/1991. (IV. 13.) AB határozat].

Jóri András rámutat, hogy az Alkotmánybíróság a 46/1995. (VI. 30.) határozatában a személyes adatok védelméhez való jog korlátozása kapcsán természetszerűleg állapította meg, hogy a korlátozásnak„meg kell felelnie az alapjogi korlátozás mindenkori alkotmányos feltételeinek, azaz az Alkotmány 8. § (2) bekezdésében foglalt követelményeknek. Ez azt jelenti, hogy az információs önrendelkezési jogot, az Alkotmány 59. § (1) bekezdésében biztosított szabadságjogot mint alapjogot csak elkerülhetetlen esetben lehet alkotmányosan korlátozni, akkor ha a korlátozás elkerülhetetlenül szükséges és az a korlátozással elérni kívánt célhoz képest arányos",[70] és a korlátozás során a jogalkotónak a cél eléréséhez alkalmas legenyhébb eszközt kell választania.[71] A 90-es évek közepén kialakult alkotmánybírósági gyakorlat szerint a személyes adatok védelméhez fűződő jog korlátozását *nem indokolhatja önmagában közérdek,* így például célzott vagy ígért gazdasági növekedés, tartós gazdasági növekedés feltételeinek kibontakoztatása, illetőleg az ehhez fűződő közérdek az információs önrendelkezési jog korlátozásnak nem elegendő alkotmányos indoka.[72]

Az információs önrendelkezési jog alapjog-korlátozási doktrínája egészen a GDPR hatálybalépéséig meghatározta a hazai adatvédelmi jog kereteit. Ennek sajátossága volt, hogy az információs önrendelkezési jogot értelmező alkotmánybírósági határozatokban foglalt követelményeket követve született, a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény, majd a 2011-ben elfogadott Alaptörvény okozta jogrendszerbeli változásokat követően megalkotott információs önrendelkezési jogról és az információszabadságról szóló 2011. év CXII. törvény (Infotv.) az adatkezelő jellegétől (hogy az közhatalmi szerv vagy magánjogi jogalany) függetlenül használta a duális jogalaprendszert.[73]

[70] 46/1995. (VI. 30.) AB határozat, ABH 1995, 219, 223

[71] Jóri András (2018b): Adatvédelem: az alapjogvédelmi teszttől az érdekmérlegelésig. *Alkotmánybírósági Szemle,* 2018/1. 16.

[72] „[A] közérdek fennállásának és alkotmányos indokának a vizsgálatánál is a szükségesség—arányosság ismérveit alkalmazza" [46/1995. (VI. 30.) AB határozat, ABH 1995, 219, 224], vagy 60/1994. (XII. 24.) AB határozat. Idézi Jóri 2018b. 16.

[73] Jóri 2018b. 16.

Az érdekmérlegelési teszt mint a magánjogi jogviszonyok alapjog-korlátozása?
A GDPR 6. cikk (1) bekezdés *f)* pontjában meghatározott jogos érdek (jogszerű) alkalmazásának előfeltétele az érdekmérlegelési teszt lefolytatása. Ennek elmaradása a NAIH konzekvens gyakorlata szerint jogellenes adatkezelést eredményez.

Az érdekmérlegelési teszt annak igazolására szolgál, hogy az adatkezelő megfelelően azonosította a jogos érdekét, és erre alapozva olyan módon végzi az adatkezelést, amely nem jelent aránytalan korlátozást az érintett érdekeire, jogaira és szabadságaira nézve.[74] Osztopáni Krisztián rámutat, hogy a gyakorlatban számos módszertan alkalmazható az érdekmérlegelési teszt elvégzésére.[75]

Hét lépésből álló módszertant ajánl a 29. cikk szerinti Adatvédelmi Munkacsoport a 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról szóló 06/2014. számú véleményében az adatkezelőknek.

1. lépés: Melyik a potenciálisan alkalmazható jogalap a 7. cikk a)–f) pontja közül?
2. lépés: Az érdek jogszerűségének vagy jogszerűtlenségének megállapítása.
3. lépés: Az adatfeldolgozás az érdek érvényesítéséhez való szükségességének megállapítása.
4. lépés: Ideiglenes egyensúly elérése annak mérlegelésével, hogy az adatkezelő érdekeivel szemben elsőbbséget élveznek-e az érintettek alapvető jogai vagy érdekei.
5. lépés: Végleges egyensúly elérése a kiegészítő biztosítékok figyelembevételével.
6. lépés: A megfelelés bizonyítása és az átláthatóság biztosítása.
7. lépés: Mi történik, ha az érintett él a tiltakozási jogával?

Öt lépésből álló tesztet javasol az adatkezelőknek a NAIH a 2016. november 16-án megjelent, a munkahelyi adatkezelésekről szóló tájékoztatójában.[76]

1. lépés: az adatkezelőnek a tervezett adatkezelés megkezdése előtt át kell tekintetnie, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése: rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél.
2. lépés: az adatkezelői jogos érdek lehető legpontosabb meghatározása.
3. lépés: annak meghatározása, hogy mi az adatkezelés célja, milyen személyes adatok meddig tartó adatkezelését igényli a jogos érdek.
4. lépés: annak meghatározása, hogy az érintettnek mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (például azok a szempontok, amelyeket az érintettek felhozhatnának az adatkezeléssel szemben).

[74] Osztopáni 2018
[75] Osztopáni Krisztián kifejti, hogy ezek a módszertanok segítséget jelentenek, támpontot adnak az érdekmérlegelés jogalapjának alkalmazásához, ugyanakkor ezen túlmenően valamennyi olyan megoldás elfogadható a NAIH részéről is, amelyből egyértelműen kiderül, hogy milyen jogos érdek teszi szükségessé az adatkezelést, és az adatkezelés miért korlátozza arányosan az érintettek jogait és szabadságait. Osztopáni 2018, 131–132.
[76] Elérhető: www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf (a letöltés dátuma: 2019. 01. 29.)

5. lépés: annak meghatározása, hogy miért korlátozza arányosan az adatkezelői jogos érintetti jogokat, várakozásokat. Az érdekmérlegelésen alapuló adatkezelések esetében többek között a fokozatosság elvének érvényesülése és az érintett jelenléte többlet biztosítékként szolgálják az adatkezelés szükségesség-arányosságát.

Az érdekmérlegelés tesztje két különálló érdek azonosítására: az adatkezelő (vagy más harmadik fél) és az érintett érdekeinek a kiegyensúlyozására épül. Az érdekmérlegelési teszt tehát nem végezhető el anélkül, hogy az adatkezelő ne azonosítaná azokat a jogokat és elvárásokat, amelyekre a szóban forgó adatkezelés hatással lesz.[77]

Minden adatkezelés elsődlegesen az érintett információs önrendelkezési jogára van hatással, hiszen a személyes adatok kezelésére az érintett hozzájárulása nélkül kerül sor oly módon, hogy az adatkezelés körülményeit maga az adatkezelő alakítja ki.[78] Ezen túlmenően különböző adatkezelések számos, a chartában, az EUMSz-ben vagy pedig Magyarország Alaptörvényében rögzített jogot vagy szabadságot érinthetnek, így például az adatkezelés hatással lehet az érintett magánszférához való jogára, a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához való jogára, a jó hírnév védelméhez fűződő jogára, a gondolat-, a lelkiismereti és a vallásszabadságára, a szabad véleménynyilvánításhoz való jogára is.[79] Az adatkezelőnek mindemellett fel kell tárnia, hogy *milyen elvárásokat támaszthat az érintett* a szóban forgó adatkezeléssel szemben, melyek lehetnek az érintett érdekei. Ilyennek tekinthető például az érintettek azon joga, hogy a személyes adataik kezelésére a lehető legrövidebb ideig kerüljön sor, a személyes adataikhoz csak egy szűk személyi kör férhessen hozzá.[80] Az érintettek elvárásai az adatkezelés végrehajtásának a módjához igazodóan határozhatók meg.[81]

Szükségesség és arányosság vizsgálata elemi feltétele az érdekmérlegelési teszt lefolytatásának, ugyanúgy, mint az alapjogok korlátozása esetén, csak más szempontrendszerek alapján. A *szükségesség* körében alapvetően két kérdés vizsgálata indokolt. Az egyik, hogy az adatkezelő mely tevékenysége teszi szükségessé a személyes adatok kezelését, a másik, pedig az adatkezelőnek ki kell fejtenie azt is, hogy ez a tevékenység miért nem végezhető más módszerrel, mint a személyes adatok kezelésével, vagyis van-e alternatívája az adatkezelésnek.[82] A szükségesség mellett az adatkezelőknek azt is elemezniük kell, hogy az adatkezelés arányos korlátozást jelent-e az érintettek személyes adatai vonatkozásában.

[77] Osztopáni 2018, 131–132.
[78] Osztopáni 2018, 131–132.
[79] Osztopáni 2018, 134.
[80] Osztopáni 2018, 134–135.
[81] Osztopáni 2018, 135.
[82] Osztopáni 2018, 135.

Ennek során az elemzésben ki kell térni arra, hogy *milyen érintetti körre* vonatkozik az adatkezelés.[83] A kiszolgáltatottabb helyzetben lévő érintettek esetén az adatkezelőnek még több garanciális intézkedést kell meghoznia annak érdekében, hogy az adatkezelés arányos legyen. Az arányosság kapcsán vizsgálni kell továbbá, hogy *milyen kapcsolat van az érintett és az adatkezelő között,*[84] valamint, hogy *milyen időszakot ölel fel az érintett és az adatkezelő közötti kapcsolat*.[85]

Amennyiben *harmadik fél jogos érdeke* indokolja az érdekmérlegelés jogalapjának az alkalmazását, akkor az adatkezelőnek meg kell vizsgálnia, hogy valóban szükséges-e a személyes adatok továbbítása a harmadik személy számára, illetve hogy milyen célból és milyen adatkezeléséhez használná fel a személyes adatokat.[86] Ezzel kapcsolatban annak vizsgálata is lényeges lehet, hogy *a harmadik fél milyen hátrányt, sérelmet szenvedne el abban az esetben, ha az adatkezelő nem továbbítaná számára a személyes adatokat,* illetve milyen nehézségekbe ütközhetne az, ha az érintettek hozzájárulását kellene beszerezni az adattovábbításhoz.[87]

Az arányosság elemzése során lényeges szempont, hogy *milyen személyes adatra terjed ki az adatkezelés*.[88] Amennyiben különleges adatokra vonatkozna az adatkezelés, akkor az érdekmérlegelés jogalapja önállóan nem alkalmazható.[89]

Abban az esetben, ha az érdekmérlegelés alapján végzett adatkezelés hozzáadott értékkel rendelkezik az érintettek által vásárolt termék vagy általuk igénybe vett szolgál-

[83] Amennyiben kiszolgáltatottabb helyzetben levő érintettekre irányul az adatkezelés (például idősek, beteg személyek), akkor vélhetően kevésbé lehet arányos az érdekmérlegelés jogalapjának az alkalmazása, vagy pedig plusz garanciális intézkedések bevezetését igényli az adatkezelők részéről. A GDPR kiemeli, hogy különös jelentőségű az érdekmérlegelés jogalapjának alkalmazásában, ha az érintett gyermek. Ezen érintetti kör ugyanis kevésbé lehet tisztában a személyes adatok kezelésével összefüggő kockázatokkal, következményekkel vagy például az ahhoz kapcsolódó garanciákkal, jogaival. GDPR (38) preambulumbekezdés.

[84] Az ügyfélviszony, munkaviszony vagy a cégek közötti kapcsolat (üzleti partner, jövőbeli ügyfél) jobban igazolhatja az arányosság követelményének teljesülését, míg egy olyan érintett vonatkozásában, aki még soha nem vette igénybe az adatkezelő szolgáltatását (vagy nem vásárolt az adatkezelőtől terméket), vagy nem állt kapcsolatban az adatkezelővel, nehezebben alkalmazható a jogalap. Osztopáni 2018, 136.

[85] Amennyiben a kapcsolat folyamatos, úgy az érintettek inkább számíthatnak arra, hogy az adatkezelő jogos érdeke alapján kerül sor az adatkezelésre, míg ha az adatkezelést megelőzően semmilyen kapcsolat nem volt az érintett és az adatkezelő között, akkor kevésbé láthatnak előre egy ilyen természetű adatkezelést. Osztopáni 2018, 136.

[86] Osztopáni 2018, 135.

[87] Osztopáni 2018, 136.

[88] Osztopáni 2018

[89] Az adatkezelőnek a GDPR 9. cikk (2) bekezdésében szereplő esetkörrel is kell rendelkeznie az érdekmérlegelés jogalapjával végzett adatkezelés jogszerűségéhez. Ha nincs olyan esetkör, amely illeszkedne az adatkezelő tevékenységéhez, akkor legfeljebb az érintett kifejezett hozzájárulásával kezelhet különleges adatot [GDPR 9. cikk (2) bekezdés *a)* pont], feltéve, hogy annak valamennyi követelménye érvényesül a konkrét helyzetben. További vizsgálandó szempont az is, hogy az adatkezelő milyen forrásból jut hozzá a személyes adatokhoz. Ha a személyes adatok forrása közvetlenül az érintett, akkor az inkább feltételezi az adatkezelés arányosságát, mint az, ha más forrásból származnak a személyes adatok. Osztopáni 2018, 135.

tatás tekintetében, vagy más előnnyel jár az érintettekre nézve, akkor ez is az adatkezelés arányosságát igazolhatja.[90]

Másfelől az adatkezelés arányossága ellen hat, ha az adatkezelés negatív módon befolyásolja az érintett joggyakorlási lehetőségét (például az adatkezelés során alkalmazott technológia sajátosságából fakadóan nem tudja a személyes adatai módosítását kérni), vagy az érintett számára indokolatlanul nem kívánt hátrány vagy negatív következmény jelentkezik (például az adatkezelés kihat a korábban már részletezett, az érintettet megillető jogra vagy szabadságra).

Az információs önrendelkezési jog korlátozását ellensúlyozó biztosítékok

Ugyan az információs önrendelkezési jog nem abszolút jog, azonban *a lényeges tartalma nem korlátozható.* Ez véleményem szerint jelenti, hogy *az érintettek részére legalább azt kell tudnia az adatkezelőnek biztosítani, hogy hozzáférése legyen azokhoz az információkhoz, hogy az adatait milyen adatkezelési tevékenység kapcsán, milyen célból, milyen jogalappal, milyen többlet biztosítékokkal kezelik.*

Ezt a követelményt szolgálja jogszabályi szinten az *adatkezelő tájékoztatási kötelezettsége* a GDPR 12–14. cikkekben foglaltak alapján, másfelől az érintett hozzáférési joga (amely adott esetben a jogos érdeken alapuló adatkezelés érdekmérlegelési tesztjét is magában foglalja), valamint a további érintetti jogok alkalmazása például a tiltakozási joga is a jogos érdeken alapuló adatkezelés esetén.[91] A hatásvizsgálat lefolytatása, valamint az adatvédelmi tisztviselő kötelező bevonása a hatásvizsgálatba.

Az adatkezelőknek a fenti jogi követelmények teljesítésén, az általános érintetti jogok érvényesítésén túlmenően *a jogos érdek alkalmazása kapcsán többletgaranciák beépítéséről kell gondoskodniuk*, hogy az adatkezelés arányosan korlátozza az érintettek jogait, tehát az információs önrendelkezési jog lényeges tartalma ne sérüljön.[92] A beépítendő garanciák egyrészt lehetnek az *adatkezelés végrehajtásához kapcsolódó* biztosítékok: a kezelt adatok körének, az adatkezelés idejének minimalizálása, a személyes adatok álnevesítése.[93] Másrészt olyan *szervezési-logikai biztosítékok,* hogy a személyes adatokhoz hozzáférő személyek köre minimalizálódik, vagy az, ha az adatkezelés során kezelt adatokhoz csak többszintű azonosítást követően lehet hozzáférni.[94] Garanciális

[90] Előfordulhat olyan eset, amikor az adatkezelés az érintett érdekében is áll, vagy egybeesnek az érintettek és az adatkezelő érdekei. Így például a parkolóház megfigyelésére szolgáló kamerarendszer, hiszen a gépjárművek védelme egyrészt a parkolóházat (és a kamerarendszert) üzemeltető cég, másrészt az érintettek érdeke is (saját gépjárműveik vonatkozásában). Amennyiben akár helyi, akár széles körű társadalmi érdeknek tekinthető az adatkezelés, akkor az szintén az arányosságot erősítő tényező (például a veszélyes anyagok őrzése érdekében alkalmazott kamerák). Osztopáni 2018, 136.

[91] Osztopáni Krisztián szerint is az információs önrendelkezési jog magasabb szintű érvényesülését szolgálja, ha például az adatkezelő többféle formában további tájékoztatást nyújt az adatkezelésről (például az érdekmérlegelési tesztet e-mailen továbbítja az érintett számára).

[92] Osztopáni 2018, 136.

[93] Osztopáni 2018, 136.

[94] Osztopáni 2018, 136.

intézkedések lehetnek az *informatikai természetű biztosítékok is*, mint például az elérhető legjobb technológiával biztosítani az adatbázis védelmét (tűzfalvédelem, titkosítás), vagy ha az érintettek a felhasználói profiljukban ki tudják kapcsolni az adatkezelést, vagy online módon hozzáférhetnek azon személyes adataikhoz, amelyet az adatkezelő az érdekmérlegelés jogalapjának alkalmazásával kezel.[95] Az érintett számára kontrollt biztosító garanciának minősül, ha az érdekmérlegelés jogalapjának alkalmazásával végzett munkáltatói ellenőrzést úgy vezeti be a munkáltató, hogy előtte kikéri a munkavállalók érdekképviseletének a véleményét.[96]

Mindezeken túlmenően az érdekmérlegelés jogalapján végzett adatkezelés további garanciája, ha *az adatkezelőn kívüli szervezet működik közre ezen adatkezelés kialakításában.* Így például, ha az adatkezelő tőle független szervezetet (például ügyvédi irodát, szakmai tanácsadót) bíz meg az érdekmérlegelési teszt elvégzésével. Ilyen külső garancia továbbá a tanúsítási mechanizmus alkalmazása, a magatartási kódexhez való csatlakozás.

Véleményem szerint azonban az adatkezelői többletgaranciák érvényesíthetősége kapcsán ezek maximum jó gyakorlatként értékelhetők, a fenti garanciák nincsenek jogszabályban előírva, így ezeknek kikényszerítése (bírsággal való sújtása) álláspontom szerint nem egyeztethető össze a normavilágosság és a jogbiztonság követelményével.

Összegzés – De lege ferenda javaslatok

Tanulmányomban az érdekmérlegelési teszt alapjog-korlátozási jellegének a vizsgálatára tettem kísérletet. Ennek kapcsán kiindulópontként szolgált, hogy hazánkban az alapjogok korlátozása kapcsán az Alkotmánybíróság több mint húszéves gyakorlata alatt kialakított alapjog-korlátozási tesztje az Alaptörvény 2011. évi elfogadásával emelkedett fel az alkotmány normaszövegébe, amely alapvető követelményként határozza meg, hogy milyen esetben lehetséges alapvető jogot korlátozni. Így az I. cikk (3) bekezdése szerint: „Az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható."

A vizsgálódások szempontjából ami ebből az alapjog-korlátozási klauzulából a jogos érdek vizsgálata kapcsán felmerül az egyrészről, hogy az információs önrendelkezési jogot, a *személyes adatok védelméhez fűződő jogot értékelhetjük-e alapvető jogként?* E kérdésre az Alaptörvény VI. cikkében, valamint a nemzetközi egyezményekben megfogalmazottokra tekintettel egyértelműen igennel tudunk válaszolni. A jogos érdek jogalapjának elemzése kapcsán megállapítható, hogy ugyan itt nem egy klasszikus értelemben vett alapjog-korlátozásról van szó az állam és az egyén viszonyában (ugyanis maga a GDPR zárja ki, hogy közhatalmi szervek e jogalappal kezelhessenek személyes adatot), hanem *az alapjogok magánjogi jogviszonyokban történő kollíziójáról van szó,*

[95] Osztopáni 2018, 136.
[96] Osztopáni 2018, 136.

de az államnak az egyének jogérvényesítésének elősegítése kapcsán fennálló feladata körében szükséges e korlátozási körülményeket – az érdekmérlegelési teszt szempontrendszerét – törvényben meghatároznia.[97]

A második kérdés, amely felmerült, hogy az Alaptörvény által előírt *törvényi jogforrási forma* – az alapjogok tartalmának megállapítása tekintetében – mennyiben érvényesül az adatvédelem kapcsán ismert jogos érdekmegjelenítés kapcsán.

A törvény a tagállami hatáskörben – az állampolgárok által közvetlenül választott országgyűlési képviselők által, a törvényhozói hatalmat gyakorló – az Országgyűlés által elfogadott, a köztársasági elnök által kihirdetett olyan jogalkotási eredmény, amelynek a legitimációja közvetlenül visszavezethető a népszuverenitásra. Ezzel szemben a GDPR-t rendeleti formában alkották meg, amelynek közvetlen demokratikus legitimációja hosszabb láncolaton megy keresztül, mint a törvényé. E kérdéskör kapcsán merült fel *a szuverenitási transzfer* kérdéskörének a vizsgálata, amelynek kapcsán megállapítható, hogy ugyan az adatvédelem szabályzására az EU ugyan jogalkotási hatáskörrel rendelkezik, az információs önrendelkezési jogot korlátozó jogos érdek jogalapjának a bevezetésével a hatáskörét feltehetőleg túllépte – az alapjog-korlátozásnak minden esetben az alkotmányokban meghatározott követelményeknek kell megfelelnie.

A normavilágosság követelményének megfelelően álláspontom szerint szükséges az érdekmérlegelési teszt szempontrendszerét törvényben meghatározni, másfelől pedig a jogalkotó által körülhatárolható esetekben adatkezelési felhatalmazásként megjeleníteni a jogos érdeket törvényi szinten. Amennyiben törvényi szinten nem konkretizálják a jogos érdek alkalmazásához szükséges érdekmérlegelési tesztet, úgy az jogbizonytalansághoz vezet, a helyzet sérti a normavilágosság követelményét. Az adatkezelők az alkalmazott teszt jogszerűsége kapcsán bizonytalan bírságkockázatnak és bírósági jogérvényesítési kockázatnak vannak kitéve.

Mindezeken túl azonban nem lehetünk álszentek. A digitális korszak mindennapi életviteléhez *szükség van a jogos érdeken alapuló adatkezelésére* mint a jogalapok „jolly jokerére", hiszen alapvetően az emberiség szolgálatába kell állítani az adatvédelmet és az alapjogok korlátozását, ahogy ezt a [4] preambulumbekezdés is írja, azonban *megfelelő alkotmányos bástyák nélkül ezt nem lehet a jogállamiság keretein belül megtenni.* Azért is szükséges ez, hogy e jogalap ne legyen túl tág értelemben alkalmazható, és az adatkezelők ne kezelhessék az adatainkat eltúlzott rugalmassággal felfogott értelemben, hogy az érintett alapjogai ne sérüljenek, vagy ha ezek mégis sérülnek, akkor megfelelő jogi keretek között lehessen magát a jogsértést értelmezni és megfelelő módon lehessen jogorvoslattal élni.

A NAIH gyakorlata során gondosan kimunkált érdekmérlegelési tesztet (hasonlóan az Alkotmánybíróság által kidolgozott alapjogkorlátozási teszt analógiájára) álláspontom szerint *törvényi szintre szükséges emelni.* Eme törvényi szintű meghatározás (és nem többlet követelmény kialakítása) összhangban áll az Európai Bíróság adatvédelmi jog

[97] Vö. Gárdos Orosz Fruzsina (2011): *Alkotmányos polgári jog? Az alapvető jogok alkalmazása a magánjogi jogvitákban.* Budapest–Pécs, Dialóg Campus Kiadó.

tekintetében kimunkált joggyakorlatával. Persze ez további kérdéseket vet fel, a tekintetben, hogy az EU területén más tagállamok joghatósága alá tartozó adatkezelők érdekmérlegelési tesztjét, hogyan fogadhatja el a magyar hatóság, viszont magyar alkotmányjog dogmatikai szempontokat figyelembe véve szükség van e konkretizálásra, más különben felmerül az alkotmányos mulasztás kérdése.

Felhasznált szakirodalom

Baka Péter – Dudás Gábor – Filipovits Viktória – Freidler Gábor et al. (2012): *Adatvédelem és információszabadság a mindennapokban.* Budapest, HVG-ORAC.

Balogh Zsolt (2019): Általános rész. Az alapjogok korlátozása. In Schanda Balázs – Balogh Zsolt szerk.: *Alkotmányjog–Alapjogok.* Budapest, Pázmány Press.

Bendik Tamás (2018): A tagállami jog és a GDPR viszonya – az Infotv. szerepe a megváltozott szabályozási környezetben. In Buzás Péter – Péterfalvi Attila – Révész Balázs szerk.: *Magyarázat a GDPR-ról.* Budapest, Wolters Kluwer.

Csink Lóránt – Török Réka (2017): A magánszféra átalakulása – 21. századi kihívások. In Csink Lóránt szerk.: *A nemzetbiztonság kihívásainak hatása a magánszférára.* Budapest, Pázmány Press.

Eszteri Dániel (2018): A GDPR tárgya és hatálya. In Buzás Péter – Péterfalvi Attila – Révész Balázs szerk.: *Magyarázat a GDPR-ról.* Budapest, Wolters Kluwer.

Gárdos-Orosz Fruzsina (2011): *Alkotmányos polgári jog? Az alapvető jogok alkalmazása a magánjogi jogvitákban.* Budapest–Pécs, Dialóg Campus Kiadó.

Gárdos-Orosz Fruzsina (2009): *8. § [Alapjogok korlátozása].* In Jakab András szerk.: *Az Alkotmány Kommentárja.* Budapest, Századvég Kiadó.

Halmai Gábor – Tóth Attila (2008): *Emberi jogok.* Budapest, Osiris Kiadó.

Jóri András (2018): Adatvédelem: az alapjogvédelmi teszttől az érdekmérlegelésig. *Alkotmánybírósági Szemle.* 2018/1. 16.

Jóri András (2018): Az adatkezelő vagy harmadik fél jogos érdekeinek érvényesítése mint jogalap („érdekmérlegeléses" jogalap). In Jóri andrás szerk.: *A GDPR magyarázata.* Budapest, HVG-ORAC. 160.

Jóri András – Hegedűs Bulcsú – Kerekes Zsuzsanna szerk.: *Adatvédelem és információszabadság a gyakorlatban.* Budapest, Complex Kiadó.

Koltay András (2012): A magánszféra, a személyes adatok, a képmás és a hangfelvétel védelme. In Koltay András – Nyakas Levente szerk.: *Magyar és európai médiajog.* Budapest, Complex Kiadó. 323–337.

Köbel Szilvia (2018): *Információszabadság és adatvédelem. Az információs önrendelkezési jog jogi garanciái.* Konferencia-előadás.

Liber Ádám (2012): A jogos érdeken alapuló adatkezelésről. *Infokommunikáció és Jog,* 2012/2. 79–88.

Nagy Klára (2015): Az információs önrendelkezési jog. In: Smuk Péter szerk.: *Alkotmányjog III. Alapjogok.* Győr, Universitas-Győr Nonprofit Kft. 209–230.

Osztopáni Krisztián (2018): Jogalapok. In Buzás Péter – Péterfalvi Attila – Révész Balázs szerk.: *Magyarázat a GDPR-ról.* Budapest, Wolters Kluwer.

Patyi András – Varga Zs. András (2012): Általános közigazgatási jog (az Alaptörvény rendszerében). Budapest–Pécs, Dialóg Campus.

Patyi András (2018): A közigazgatási eljárásjog és perjog változásai és összefüggései. In: Benisné Győrffy Ilona szerk.: *Tizennegyedik Magyar Jogászgyűlés: Balatonalmádi 2018. október 4–6.* Budapest, Magyar Jogász Egylet.

Péterfalvi Attila – Révész Balázs – Szalai András (2013): A közigazgatás adatkezelő tevékenysége. In Temesi István szerk.: *A közigazgatás funkciói és működése.* Budapest, Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. 265–295.

Péterfalvi Attila szerk. (2012): *Adatvédelem és információszabadság a mindennapokban.* Budapest, HVG-ORAC.

Péterfalvi Attila (2013): Az adatvédelem a magyar jogvédelem mechanizmusában. In: Cserny Ákos szerk.: Ünnepi tanulmányok Rácz Attila 75. születésnapja tiszteletére. Budapest, Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. 333–345.

Pozsár-Szentmiklósy Zoltán (2016): *Alapjogok mérlegen: Az általános alapjogi tesztek dogmatikája.* Budapest, HVG-ORAC.

Sabjanics István (2013): Adatvédelem és terrorellenes intézkedések az Egyesült Államokban: A MATRIX modellkísérlet története és visszhangjai. In Gerencsér Balázs Szabolcs szerk.: *Modellkísérletek a közigazgatás fejlesztésében: Az úgynevezett „pilotprojektek" határai elméletben és gyakorlatban.* Budapest, Pázmány Press.

Sepsi Tibor (2019): *GDPR útikalauz adatkezelőknek.* Budapest, Wolters Kluwer.

Szabó Endre Győző (2019): A személyes adatok védelméhez és a közérdekű adatok megismeréséhez fűződő jog. In Schanda Balázs – Balogh Zsolt szerk.: *Alkotmányjog–Alapjogok.* Budapest, Pázmány Press.

Szádeczky Tamás (2017): Adatvédelem és adatbiztonság az elektronikus okmányoknál. *Hadmérnök,* 12. évf. 2. Különszám. 181–195.

Szendrei Ferenc (2019): Az adatvédelemmel kapcsolatos feladatok. In Nyeste Péter – Szendrei Ferenc szerk.: *A bűnügyi hírszerzés kézikönyve.* Budapest, Dialóg Campus Kiadó. 173–180.

Sziklay Júlia (2012): A személyes adatok védelme. In Péterfalvi Attila szerk.: *Adatvédelem és információszabadság a mindennapokban.* Budapest, HVG-ORAC.

Szikora Veronika – Árva Zsuzsanna szerk. (2019): Újratervezés – Fogyasztói szabályozási modellek, digitalizáció, adatvédelem. Debrecen, Debreceni Egyetem.

Szőke Gergely László – Pataki Gábor (2017): Az online személyiségprofilok jelentősége – régi és új kihívások. *Infokommunikáció és Jog,* 14. évf. 2. sz. 63–70.

Szőke Gergely László (2013): Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció és Jog,* 3. sz. 107–112.

Takács Péter (2011): Az emberi jogok jogelméleti kérdései. Elérhető: http://jog.unideb.hu/documents/tanszekek/jogbolcseleti/tansegdletek/2011-12/2011-12-2/takcs_p_-_az_emberi_jogok_jogelmleti_krdsei__a_jogok.pdf (a letöltés dátuma: 2016. 01. 29.)

Wellmann Barna Bence (2018): A munkajogi adatvédelem aktuális kérdései. In Erdős Csaba szerk.: *Doktori Műhelytanulmányok 2018 – Doctoral Working Papers 2018.* Budapest, Gondolat.

VÁKÁT OLDAL

Csaba Makó – Miklós Illéssy

Platform Work in Hungary: A Preliminary Overview

(Innovation in the Age of the 4th Industrial Revolution)

Introduction[1]

The usual vocabulary of change is no longer adequate for describing the paradigmatic transformation in the capitalist development. Mazzucato (2020) stresses the trinity of the current crisis: we have to face not only with the coronavirus COVID-19 pandemic and the resulting economic crisis but also with the long debated climate crisis. Besides this triple crisis of capitalism, it is worth calling attention to another revolutionary change: the shift in the techno-economic paradigm.[2] In this relation, the following two major technological breakthroughs could be distinguished. The first one is the 4th industrial revolution driven by the digitisation/automation/robotisation and artificial intelligence (AI). Industry 4.0 as a terminology represents "a vision of increasing digitisation of production. The concept describes how the so-called Internet of Things (IoT), data and services will be a change in the future production, logistics and work processes […]. They are alluding to a new organisation and steering of the entire value chain, which is increasingly becoming aligned with individual customer demands".[3] The second technological breakthrough is the platform-based business model of capitalism. Unfortunately, a generally accepted terminology of this digitally based platform economy – in spite of the fast growing literature – is still missing. Among the great number of definitions, we prefer to use the concept of platform, according to which platforms "…operate as "match-makers" between previously fragmented and unconnected groups of users. In the course of pervasive digitisation, platforms have fundamentally transformed domains as diverse as the market for goods (e.g. Amazon, eBay), mobility (e.g. Uber, Lyft), labour (e.g. Upwork, TaskRabbit), funding (e.g. Kickstarter, Prosper) and of course, the entire field of online search, socialising and content production (e.g. Facebook, Google, YouTube)".[4]

[1] The authors would like to express their appreciation for the helpful participation of Katalin Bácsi, Budapest Corvinus University, in the first version of this paper.

[2] Perez 2010.

[3] Buhr 2015, 4. It is worth mentioning, that the term Industry 4.0 was not an academic invention but first systematically used by a working group chaired by the Rober Bosch Gmbh; Acatech aimed to work on Industry 4.0 even before the terminology Industry 4.0 was introduced at the well-known Hannover Fair in 2011 (Kopp et al. 2016).

[4] Grabher–Tuijl 2020, 4.

This paper intends to describe the impacts of the second strand of technological transformation (i.e. platform economy) – often called the Uberisation of economy – in terms of job structure, working conditions, employment status and collective voice of platform workers. The core text is based on the review of both academic and grey literature on platform work and lessons drawn from the preliminary fieldwork (i.e. interviews with trade unionists, leaders of platform owners, researchers, blog writers and other experts) carried out in Hungary.

In relation with the development of platform technology, we share the following perspective that insists: "Technologies – the cloud, big data, algorithms and platform – *will not dictate* our future. How we deploy and use these technologies will. When we look at the history of innovations such as electric utility grids, call centres and the adoption of technology standards, we find that the market and social outcomes of using new technologies vary across countries. Once we start on a technology path, it frames our choices, but *the technology does not determine in the first place exactly which trajectory we will follow.*"[5]

The structure of this paper follows the guideline elaborated by the EU funded CrowdWork21[6] international research consortium. The first section gives an overview on the scientific debates about the digital platform workers. Results of the European survey – including Hungary – are outlined in the next section. The third section describes the main features of the national debate in Hungary based on a variety of sources (e.g. national media, web search, blogs, etc.). The fourth section intends to identify the position of social actors on the practice of platform work. In this section, the authors are using the Uber story as a lens to illustrate the social-economic and legal challenges for the social actors and institutions. The concluding section summarises the main lessons of the analysis.

Platform work and its institutional filters

Before presenting in detail the public and scientific debate about digital platform workers in Hungary, it is worth briefly describing the main features of the Hungarian industrial relations system as well as the state-of-the-art of the international scientific debate about platform work in general. These two issues represent the most important contextual factors and therefore are necessary to be briefly summarised in order to interpret in an adequate way what is happening in the country in this particular field. The project aims to understand the multiform strategies of stakeholders, (trade unions, employers' association, governments, self-organised platform workers' organisations) and this cannot be achieved without a deeper understanding of the varieties of the national systems of industrial relations.

[5] Kenney–Zysman 2016, 14.
[6] Source: https://crowd-work.eu/ (Accessed: 22.05.2020.)

Platform work: Lack of consent-based terminology and the heterogeneous character of platform work

The digital platform work is a new coordination form of economic activities where transactions between the partners involved are carried out through a digital platform. According to Mateescu and Nguyen, its main features are the followings:

- "Prolific data collection and surveillance of workers through technology
- Real-time responsiveness to data that informs management decision
- Automated or semi-automated decision-making
- Transfer of performance evaluation to rating systems or other metrics, and
- The use of "nudges" and penalties to indirectly incentivise workers behaviours"[7]

The comparison of the results of different empirical research in the field is often hindered by the lack of the harmonious use of terminology on digital labour and by the insufficiently systematic and uncoordinated data collection. This 'knowledge deficiency' syndrome makes cross-country comparison of platforms difficult, as well as inquiry into concerted policy actions on both national and EU level public governance that are aimed at regulating the online labour market. The source of the lack of consent is not due to the shortage of definitions but rather a plethora of terminology. Sedláková, for instance, identified the following terms most often used to describe platform work: crowdsourcing, sharing economy, collaborative economy, collaborative consumption, share economy, click-work, on demand economy, crowdworker, platform work, crowdwork, platform economy, gig work, platform labour.[8]

In a similar vein, Heeks (2017) made a systematic analysis of the literature on digital labour and found nearly 30 different terms to describe the intersection between work, connectivity and digital technologies. Based on a literature review, he suggested using the following "prime terms".

Table 1: Terms used and the implied differences in their focus

Main focal point	Prime terms to be used
Work (labour)	Online labour, crowdwork, digital labour, microwork
Clients	Online outsourcing, microsourcing
Overall domain	Gig economy, platform economy

Source: Compiled by the authors based on Heeks 2017, 2.

In this respect, it is worth citing the definition of Eurofound as the largest labour research institute in Europe, coordinating multiple European wide surveys and case study research in the field of work and employment. Eurofound suggests the following definitions of digital platform work: "Platform work is a form of employment that uses an online plat-

[7] Mateescu–Nguyen 2019, 3.
[8] Sedláková 2018, 6.

form to enable organisations or individuals to access other organisations or individuals to solve problems or to provide services in exchange for payment. The main characteristics of platform work are the following:

– Paid work is organised through an online platform.
– Three parties are involved: the online platform, the client and the worker.
– The aim is to carry out specific tasks or solve specific problems.
– The work is outsourced or contracted out.
– Jobs are broken down into tasks.
– Services are provided on demand".[9]

The CrowdWork research consortium plans to focus on work and labour in the perspective of finding new strategies to organise labour in Europe.[10] With this orientation in mind, we intend to recommend the simultaneous use of online digital labour or platform work together with the indication of the platform, which permit identification of the variety of professional profiles of the participants on the digital labour market. As concerning the varieties of platform workers, another important outcome of our literature review is the fact that the use of such "umbrella terms" as crowdwork, platform work, gig work, etc. hides important differences among these types of employees in terms of skill requirements, wages and other dimensions of working conditions.

Pongratz (2018) further distinguishes three types of platform work according to their core characteristics as the average skill level of the tasks performed, the average wage level, and how they address their online workers, themselves and their client companies. This is summarised in the following table.

Table 2: The main types and semantics of various platforms

	Microtask	Freelance platforms	Specialised platforms
Task complexity	Low	High	High
Payment	Low-paid	Higher wages	Higher wages
Workers are addressed	As workers	As freelancers	As freelancers
Jobs are labelled	Task	Project	Varies according to the purpose (design, translation, etc.)
Platform designation	Platform or marketplace	Platform or marketplace	Platform or marketplace
Buyers are called	Customers, clients, buyers	Customers, clients, buyers	Customers, clients, buyers

Source: Compiled by the authors based on Pongratz 2018, 63–64.

Furthermore, we can distinguish between platforms that are about mediating physical services and require personal presence (e.g. Uber, Babysitter.hu, Airbnb, Delivero, Bolt, etc.) from those involving an intermediary between digital services fulfilled without personal presence (e.g. Upwork, Guru, Cloud Factory, Amazon Mechanical Turk etc.).

[9] Eurofound 2018a, 9.

[10] The Project title: *Crowdwork – Finding new strategies to organise labour in Europe (CrowdWork21),* Call for proposal: VP/2018/004 Improving expertise in the field of industrial relations.

To put it in a more formalised way, Pajarinen et al. (2018) classified 2 different types of platform workers: "(a) Online Labour Markets (OLMs), in which an outcome of a job task is electronically transmittable; and (b) Mobile Labour Markets (MLMs), in which the delivery of a service requires personal presence."[11] We can further add that platform work of both OLM and MLM can belong to the category of 'low-skilled and low-paid' as well as 'high-skilled and high-paid' jobs as presented in Table 3.

Table 3: Types of labour markets and platform work: Low vs. high-skilled work

Types of the labour market	Micro work (low-skilled – low-paid)	Specialised work (medium to high-skilled – medium to high-paid)	High-skilled freelancers work (medium to high-paid)
Online Labour Market (OLM)	Amazon Mechanical Turk (AMT)	99designs, Article One Partners, CastingWords, crowdSPRING	UpWork
Mobile Labour Market (MLN)	Uber, Taxify, Bolt		UrbanSitter, Medicast (MD house calls)

Source: Compiled by the authors based on Pajarinen et al. 2018, 5; Pongratz 2018, 72–73.

As Pongratz (2018) rightly stresses: "The choice of terminology by different types of platforms is neither random nor arbitrary. The term 'worker' emphasises the mere status of being employed and evokes associations of routine tasks and tough working conditions. 'Freelancer' on the other hand, stresses the independence and responsibility of self-employment, including prospect of demanding jobs and reasonable income. Thus, they refer deliberately to the established discourses of work and employment in order to arouse interest among target groups with suitable skills and ambitions."[12]

Using such characteristics of job quality (JQ) as wages, education and training, working conditions, employment quality, work life balance, etc., we may avoid the oversimplification in such inexact terminology as 'crowdworker' and thus avoid the possible misinterpretation of the research outcomes. Semiotic analysis of the 44 global English language platforms calls attention to "…the diversity of the occupational groups involved […]. It impedes any attempt to find an overarching category for all online works as no one category is widely used across all types of platforms."[13]

During the desktop research, we analysed the data available on one of the most popular platform company website (Upwork) and found substantially differing jobs. On the Upwork freelance platform, the following professionals were represented:

– Software developers, web designers
– IT and networking professionals
– Data scientists and analytics expert
– Engineers

[11] Pajarinen et al. 2018, 5. It is worthy of note that the authors distinguish short-term work assignment as an additional essential characteristic of platform work.
[12] Pongratz 2018, 64.
[13] Pongratz 2018, 64.

- Designers and creative workers
- Writing assistant
- Translators
- Legal experts

Table 4 illustrates the professional profiles of the Upwork platform in the CrowdWork21 research consortium countries. Among the countries, Germany has the leading role, followed by Spain, Portugal and finally Hungary. The difference between the frontrunner Germany, Spain and the trailing edge Hungary is more than double regarding the aggregate number of the Upworkers. The most populated professions are as follows: translation, writing and software development and web design. These professions are the most populated in the leading edge countries (Germany and Spain). However, in the trailing edge countries (Portugal and Hungary), the differences are less sharp in the case of "IT and Networking" (Portugal: 355 – Hungary: 345) and "Data Science and Analytics" (Portugal: 255 – Hungary: 245).

Table 4: Upwork platform workers by professional profile: The Case of the CrowdWork21 project countries (2019)

Countries	Total	Software Development and Web Design	IT and Networking	Data Science and Analytics	Engineers	Design and Creative	Writing	Translation	Legal experts
Hungary	4,891	1,235	345	245	332	1,304	493	1,304	17
Germany	13,489	3,206	706	730	594	3,381	2,214	4,307	45
Portugal	7,565	1,518	355	255	425	2,111	1,266	3,000	27
Spain	12,200	2,150	524	420	574	3,375	2,075	4,447	58

Source: Hungarian National Research Team, Nasib Jafarow owns calculation based on Upwork.com as of 4 April 2019.

Institutional filters: Erosion of the Hungarian Industrial Relations System (IRS)[14]

Varieties of Capitalism (VoC) and employment regimes in Europe. National systems of industrial relations are just as diverse as the platform workers are, so it is worth taking a short overview on this topic. Technological changes may have different social and economic impacts in different countries according to the country-specific institutional arrangements. These key regulatory institutions – such as education and training, labour market regulation and industrial relations systems, welfare regimes, tax systems, etc. – play a crucial filtering role in shaping the national effects of even such mega-trends as the emerging and rapidly growing practice of platform work. It is also obvious that the intensity and the 'quality' of public discourse on platform work are also conditioned by these institutional filters to a great extent.

[14] For the sake of clarity, we will use the term industrial relations and labour relations as synonyms.

Institutions have been in the focus of social sciences from the beginning of their history, but the most current wave on institutional diversity can be traced back to the seminal work of Hall and Soskice (2001) on variety of capitalism (VoC). They called attention to the important interactions that exist between employment and working practices and the differences in the national systems of education and training, labour relations, labour market polices, etc. They identified three major institutional clusters of capitalism: liberal market economy (LME), coordinated market economy (CME) and Mediterranean economy. Presently, the VoC approach is one of the cornerstones of the evolutionary theory of economics. The binary model of the typology of capitalism was challenged – among others by Andre Sapir who distinguished four types of European social models. (It should be noted that an obvious disadvantage of the binary model is that not all countries easily fit into one of the two categories.) Sapir's model is based on two axes of a welfare system: efficiency and equity. For the sake of brevity, we only present the classification of countries along the four types of social models proposed by Sapir.

Table 5: Typology of European social models

		Efficiency	
		Low	*High*
Equity	*High*	'Continental' (AT, BE, **DE,** FR, LU)	'Nordic' (DK, FI, NL, SE)
	Low	'Mediterranean' (**ES,** GR, IT, **PT**)	'Anglo-Saxon' (IE, UK)

Source: Sapir 2005, 9.

However, the VoC school of evolutionary economics produced less developed comparative knowledge on the institutional variety of the capitalist development among the post-socialist countries, mainly due to the historically short experiences of capitalism in these countries. Fortunately, there have been notable efforts recently aimed to overcome this knowledge deficiency by applying the VoC approach for the CEE countries, too: Morawski (2019), Makó and Illéssy (2016), Bohle and Greskovits (2012), Szelényi and Wilk (2011) and Martin (2008). From among these and other attempts, the theory of employment regimes developed by Duncan Gallie is worthy of note in the context of the CrowdWork project.

Roughly speaking, the employment regime theory extends the analysis of VoC in the perspective of production regime theories by bringing in the characteristics of employment relationship, employment policy and industrial relations system. In contrast to the previous typologies, Gallie distinguished 3 types of employment regimes within the European economies. *Inclusive* employment regimes aim to increase the level of employment and at the same time the employees' rights as much as possible. *Dualis*t employment regimes guarantee extended rights for the core employees, while peripheral employees have much reduced workers' rights and job security. In the *market-based* employment regimes, state intervention remains at the lowest possible level, labour regulation is weak, but market relations usually leads to higher levels of employment.

European IRS institutions: Visible cross-country differences

This section briefly presents one of the most recent attempts aimed at classifying the varieties of industrial or labour relations systems in Europe. The Industrial Relations System (IRS) represents: "…collective relationships between workers, employers and their respective representatives, including the tripartite dimension where public authorities at different levels are involved. Social dialogue refers to all communications between social partners and government representatives, from simple information exchanges to negotiations. Social partners are employees' organisations (such as trade unions) as well as employers' organisations."[15]

An industrial relations system is an interaction between autonomous actors; nevertheless, it evolves in time. It results in a complex situation in case of post-socialist countries as the trade unions, with the exception of the Polish Solidarnosc, were not autonomous institutions at all during the socialist political regime when state party dominated all area of civil life, and the role of trade unions was reduced to be a 'transmission belt' aimed at mediating the will of the state party towards the rank-and-file employees and the management. In the following table we present the classification of the EU Member States according to different employment regimes.

Table 6: Employment regimes in the European Union

Liberal market economy	Nordic	Continental coordinated	State-coordinated	Transitional
United Kingdom	Denmark Finland Norway Sweden	Austria Belgium **Germany** Luxemburg Netherlands Slovenia	France Greece Italy **Portugal** **Spain**	Czech Republic Estonia **Hungary** Latvia Poland Romania Slovakia

Source: Gallie 2011, 11.

It is not at all surprising, therefore, that after the collapse of state-socialist systems the trade union density rates[16] fell dramatically in all countries of the region as their role and credibility had been compromised by this "forced coalition" with the mono-party state. This general decline has been continuing ever since. According to the OECD data, this declining trend is not specific for any political regime since the vast majority of the Member States show the same pattern, as it can be seen from the following table.

[15] Akgüc et al. 2018, 3.

[16] Here we define trade union density rate as the proportion of trade union members compared to the total number of wage and salary earners.

Table 7: Union density rates in Europe (%)

Year	1998	2003	2008	2012	2013	2014	2015	2016
Country								
Austria	38	35	30	28	28	28	27	27
Belgium	55	54	54	55	55	54	54	..
Czech Republic	32	22	17	15	14	13	12	..
Denmark	75	71	66	67	67	66	65	..
Estonia	17	12	7	7	..	..	..	..
Finland	78	73	69	67	66	67	..	65
France	8	8	8	8	8	8	..	..
Germany	**26**	**23**	**19**	**18**	**18**	**18**	**18**	**17**
Greece	27	..	24	22	22	..	..	..
Hungary	**27**	**18**	**14**	**12**	**..**	**11**	**..**	**11**[y]
Ireland	41	35	31	34	33	..	..	..
Italy	35	33	33	36	37	36	36	..
Latvia	..	21	15	13	..	..	..	..
Lithuania	..	14	9	9	8	8	8	8
Luxembourg	43	43	37	35	..	34	..	..
Netherlands	24	21	19	19	18	18	18	17
Poland	20	19	15	13	13	12	..	..
Portugal	**23**	**21**	**21**	**19**	**..**	**17**	**16**	**16**[x]
Slovak Republic	36	26	17	14	13	12	11	..
Slovenia	43	44	27	22	21	..	..	..
Spain	**19**	**16**	**17**	**17**	**17**	**16**	**14**	**14**[x]
Sweden	82	76	69	67	..	..	67	..
United Kingdom	30	29	27	26	25	..	..	..

Source: Data extracted on 10 October 2019 07:15 UTC (GMT) from OECD.Stat.
Legend:.. means no data available; [x] means data is from 2015; [y] means data is from 2014.

As we can see from Table 7, there is no country in Europe where the union density rate would increase between 1998 and 2016. There are some countries, like Belgium from the upper end and Italy from the middle segment of the density scale, where it has remained relatively stable, and those countries with the highest rates in 1998 experienced less significant decrease. In contrast, the most spectacular decline was observable in the post-socialist countries where union density rates generally trend downward since. Another important indice that is frequently used to describe industrial relations system is the collective bargaining coverage rate,[17] so it is worth taking a look at this indicator, too.

[17] The definition of collective bargaining coverage is the share of employees covered by a collective agreement compared to the total number of wage and salary earners.

Table 8: Collective bargaining coverage rates in European countries[18]

Year	2000	2005	2010	2015
Country				
Austria	98.00	98.00	98.00	98.00
Belgium	96.00	..	96.00	96.00
Czech Republic	47.95	41.63	51.06	46.27
Denmark	85.00	85.00	83.00	84.00
Estonia	..	28.00	24.00	18.60
Finland	85.00	87.70	77.81	89.32
France	..	96.08	98.00	98.46
Germany	**67.75**	**64.90**	**59.76**	**56.80**
Greece	82.00	82.00	64.00	..
Hungary	**42.42**	**24.75**	**27.33**	**22.80**
Ireland	44.22	41.73	40.49	33.52
Italy	80.00	80.00	80.00	80.00
Latvia	..	15.00	20.36	14.85
Lithuania	..	10.73	11.14	7.05
Luxembourg	60.00	58.00	54.22	55.00
Netherlands	81.70	86.83	89.65	79.41
Poland	25.00	..	14.86	..
Portugal	**78.43**	**83.20**	**76.74**	**72.26**
Slovak Republic	51.00	40.00	35.00	24.40
Slovenia	100.00	100.00	80.00	65.00
Spain	82.87	76.01	76.94	76.93
Sweden	94.00	94.00	88.00	90.00
United Kingdom	36.40	34.90	30.90	27.90

Source: Data extracted on 10 October 2019 08:45 UTC (GMT) from OECD.Stat.

Note: The OECD uses adjusted collective bargaining coverage rate, which means that the share of covered employees is compared not to all employees but only to those that have bargaining rights.

One of the most striking observations is that the differences between Old and New Member States are much higher in case of collective bargaining coverage rate compared to the union density. Collective bargaining is an important institution of social dialogue

[18] It is more difficult to collect this type of data; therefore, in missing cases we used the next data available. To be more accurate, for example, in case of Hungary we used the data from 1999 instead 2000, which was missing. Further 'adjustments' are as follows: for Denmark, Estonia, France and Slovakia we used data from 2004 to replace the missing data from 2005. For the similar year, we used data from 2006 in case of Lithuania. For 2010, we used data from 2008 in case of Belgium, data from 2009 for Estonia, France and Ireland, and data from 2011 in case of Luxemburg, Poland, Slovakia and Sweden, and for 2015, we used data from 2014 in case of France, Hungary, Ireland and Luxemburg.

that can counterweight the declining trend of unionisation rate, at least for the employees having bargaining rights. For the sake of simplicity, we compare the latest available data from 2015. In all countries, except for Lithuania, the collective bargaining coverage rate is higher than the union density rate, the difference being significant in most of the cases. For example, in Austria the unionisation rate is 27%, which is paired with a collective bargaining coverage rate of 98%. A similar phenomenon can be observed in the Netherlands where low unionisation rate (18%) is combined with a coverage rate of almost 80%. The following table summarises this compensation effect.

Table 9: Compensation effect of collective bargaining coverage rate

		Collective Bargaining Coverage Rate		
		Low	**Medium**	**High**
Union Density Rate	Low	Estonia Hungary Latvia Lithuania Poland **Portugal** Slovakia U.K.	Czech Republic **Germany**	Netherlands Austria France Portugal Slovenia **Spain**
	Medium		Ireland Luxemburg	Italy
	High			Belgium Denmark Finland Sweden

Source: Compiled by the authors based on OECD Statistics.

There is obviously no country where the low collective bargaining coverage rate would be combined with low union density rate but as we can see from the data, the leverage or compensation effect does not prevail in all countries at the same extent. In case of the Netherlands, Austria, France, Portugal, Slovenia and Spain, the difference between the two rates are the highest, while in case of Italy, the medium level of unionisation rate is paired with a high level of collective bargaining coverage. It is obvious that the coverage rate is high in Belgium, Denmark, Finland and Sweden as the highest density rates are found in these countries as well. This leverage effect occurs in the Czech Republic and Germany but to a lesser degree since these two countries can be characterised by a low level of union density rate and medium level of collective bargaining coverage rate. There is no such compensation effect in case of Ireland and Luxemburg, where both rates are at medium level. The country group in the least advantageous position in this regard is composed by the U.K. and the vast majority of the post-socialist countries (Estonia, Hungary, Latvia, Lithuania, Poland, Portugal and Slovakia), where both rates are the lowest. These results are not surprising as these are the countries where the extension of multi-employer or sectoral level collective bargaining agreements has the weakest tradition.

What is more surprising, however, is that a more detailed analysis of the interplay between the collective bargaining coverage rate and organisational density of social partners on both the employees' and the employers' side shows that this leverage effect is due to the higher unionisation rate mostly in the Nordic countries, where trade unions are more organised than employers' association. In contrast: "In continental western and southern Europe, coverage rates are two to three times higher than the union density rate and much more driven by high rates of employer organisation and the legal extension of collective agreements to nonorganised firms by the state."[19] At the other extreme of the scale, we find primarily Central and Eastern European Countries, where both trade unions and employers' associations are weakly organised, and collective agreements are more sparsely extended, even if the labour regulation allows this practice.

Inspired by Visser's industrial relations regimes approach,[20] a recent Eurofound study tried to establish a similar typology based on more recent data.[21] The cluster analysis is built upon indicators covering four dimensions of industrial relations:

- Associational governance, which is aimed at characterising the relationship between governmental bodies and social partners (e.g. involvement of social partners in government decision on employment and economic policy, mechanisms for collective bargaining agreement extension, employer organisation density, coordination and main locus of collective bargaining, etc.).
- Representation and participation rights, including three variables measuring the strength of indirect participation at company level and representation rights at board level (board-level employee representation rights, Works Councils' rights, status of works councils).
- Social dialogue at company level, including employee representation coverage, incidence of information provided to the employee representation body by management, influence of employee representation in workplace-level decision-making, share of companies holding regular meetings where employees can directly express their views about the organisation.
- Strengths of trade unions and government intervention in industrial relations, including unionisation rate and government intervention in collective bargaining and the setting of minimum wage.

The typology based on the cluster analysis distinguishes six types of industrial relations regimes, the first being the social partnership, which can be characterised by a high level of collective bargaining coverage rate. However, this is not due to strong unions but rather to highly organised employers' association and strong intervention of the state in the coordination of collective bargaining, in wage-setting mechanisms. Besides, as the study notes: "At company level, this cluster includes some of the countries that have granted the

[19] Visser 2009, 51.
[20] Visser 2009, 49.
[21] Eurofound 2018b.

most extensive legal rights to works councils (Austria and the Netherlands) and the most extensive board-level employee representation rights (Belgium is an exception to this)."[22]

The second cluster is the so-called 'organised corporatism' regime, the group of countries with high collective bargaining coverage based on highly coordinated and centralised collective bargaining and strong decentralised coordination structures: "A key defining feature of this cluster is the positive combination of collective autonomy and high associational governance *(i.e. high collective bargaining coverage).* It includes countries that provide extensive rights to works councils, particularly Germany and Sweden, where co-determination rights are established by law. It is also worth noting that national and sectoral collective agreements in the Nordic countries provide higher standards for information sharing and consultation than legal provisions."[23]

The third cluster is the state-centred model, which is characterised by high collective bargaining coverage rate (although somewhat lower than in the case of the previous two clusters) and a weak social dialogue at company level. This is the result of a unique institutional arrangement in which "centralised but quite uncoordinated collective bargaining institutions that have greater dependence on state regulation. Indeed, this cluster records the highest scores in collective bargaining state intervention, which are matched by low trade union densities. While mandatory works councils exist at company level, they are granted less wide-ranging legal."[24]

The fourth cluster is characterised by "company-centred governance" where unionisation rate is low, collective and wage bargaining is decentralised and uncoordinated. The role of the state is residual and mostly limited to the set-up of the national minimum wage and to a relatively extended right of works councils guaranteed by the labour legislation. "[A] defining feature of this cluster is its comparatively high performance in the industrial democracy sub-dimension of representation and participation rights at company level, which is higher than the southern cluster and close to the Nordic one. This is due to the existence of far-reaching rights provided to works councils/employee representative bodies, and some of the highest board-level employee representation rights in the EU."[25]

The fifth cluster of 'voluntarist associational governance' is similar to cluster 4 and 6 in terms of the uncoordinated and decentralised collective bargaining system but the coverage rate is somewhat higher. While differences are higher when it comes to company level collective bargaining, this cluster records the lowest score in the industrial democracy sub-dimension of representation and participation rights at company level. Countries have the voluntary character of the liberal system of employee participation in common, in which works councils or employee representative bodies are voluntary (even where these are mandated by law, and there are no legal sanctions for non-observance). Moreover, board-level employee representation rights are not available in most of the

[22] Eurofound 2018b, 37.
[23] Eurofound 2018b, 38.
[24] Eurofound 2018b, 39.
[25] Eurofound 2018b, 40.

countries under this cluster. Social dialogue performance at company level is comparatively low, although higher than in Cluster 3.[26] Contrary to cluster 4 and 6, employers' associations are strong.

The sixth cluster is the most market-oriented, with weak social partners and more generally the worst values for the variables in the associational governance[27] sub-dimension. The uncoordinated and decentralised collective bargaining system is combined with the weak role of state intervention. Despite these differences, the last three country groups show significant similarities with low level of collective bargaining coverage and weak trade unions. As the study notes: "A clear division between two main groups: the Nordic and continental countries, which record the best scores in industrial democracy, and the southern, liberal and central and eastern-European (CEE) countries, which perform far worse in this dimension. A more detailed typology enables six clusters to be distinguished that show a high degree of stability between the two periods analysed."[28] The following table presents the composition of the different clusters.

Table 10: The industrial relations cluster in Europe

No.	Characteristic	Countries
1.	Social partnership	Austria, Belgium, Luxembourg and the Netherlands
2.	Organised corporatism	**Germany,** Denmark, Finland and Sweden
3.	State-centred associational governance	France, Italy, **Portugal,** Slovenia and **Spain** (and Greece for 2008–2012)
4.	Company-centred governance	Croatia, **Hungary** and Slovakia
5.	Voluntarist associational governance	Bulgaria, Cyprus, the Czech Republic, Ireland, Latvia, Lithuania, Malta and Romania (and Greece for 2013–2017)
6.	Market-oriented governance	Estonia, Poland and the U.K.

Source: Eurofound 2018, 37.

The country-specific institutional arrangements are partly the heritage of the past, partly the result of the global financial crisis and economic downturn in 2008, after which severe deregulation took place in the field of industrial relations in many countries. In relation with the former, it is necessary to mention the effect of the collapse of the state-socialist political-economics system at end of 1980s and the beginning of the 1990s. This political-economic regime termination was followed – with slight variations in the CEE countries – with the mass privatisation and fast restructuring of the national economies. For example, the dominance of large state-owned companies in socialism was replaced

[26] Eurofound 2018b, 40.

[27] Associational governance means in this context that the government relies heavily on tripartite consultation bodies and other forms of social dialogue when it comes to decision-making processes. In the industrial relations index, it is measured by the following five indicators: 1. union density rate; 2. employer organisation density; 3. institutionalised bipartite consultation bodies; 4. collective bargaining coverage; 5. Routine involvement of unions and employers in government decisions on social and economic policy (Eurofound 2018b, 20).

[28] Eurofound 2018b, 36.

by the dominance of the micro firms and the SME sector. This disruptive change in the size-structure in the economy speeded up the decline of trade unions and the IRS through dismantling the previous regulatory and institutional framework of the economy and society (e.g. monolithic political architecture, transmission role of the trade unions between the ruling party and the economic management of the national economy, etc.) The loosing influence of the IRS resulted in not only the decline in interest representation of the wage earners in general but also contributed to the weakening of public control on the privatisation. Social partners had difficulties to influence the shares and distribution of winners and losers of the radical changes in ownership and governance structure of the economy and society in Hungary. The outcomes of this transformation process resulted in the weakening bargaining positions of the trade unions in the CEE region.

The majority of the post-socialist countries were also hit by the deregulative labour market "reforms" as a result of an external pressure of either the Troika[29] or the country-specific recommendations of the so-called European Semester. However, it is interesting to note that Hungary was a rather unique exception, where "policies undermining industrial democracy have been approved in the absence of external pressure. Since 2010, the Hungarian Parliament has approved radical reforms that have restricted strike and trade union rights, and allowed collective agreements and individual employment contracts to deviate from labour law".[30]

This striking example of "voluntary austerity" can only be understood if we take a closer look at the most recent changes in the Hungarian economic policy and politics. It dates back to the 2010 elections when Viktor Orbán won and achieved a supermajority in the Hungarian Parliament. We can observe a rather sharp regime change affecting all important areas of the social, economic and legal institutional arrangement. Neumann and Tóth describe the nature of these changes as "a statist and nationalist economic-policy turn and a shift from welfare to a workfare-based social policy".[31] This policy turn consists of neoliberal measures that aim to massively deregulate the labour market and to cut back welfare and wage expenditure in order to maintain some sort of competitiveness of the country,[32] combined with large-scale economic and regulatory expansion of the state in the name of economic nationalism.[33]

Hungarian trade unions had been fragmented and politically divided, lacking the necessary resources, constantly loosing support and trust from some of the employees so they were not prepared to counter-attack the measures of a government that had the support of two thirds of the MPs. Instead, they often focused on the interests of core employees

[29] Troika is a popular designation for the political decision-making group composed by the European Commission, the European Central Bank and the International Monetary Fund.

[30] Eurofound 2018b, 9.

[31] Neumann–Tóth 2018, 135.

[32] This is the so-called low road of development based – among others – on low wages, medium-level skills, employer-friendly flexibility schemes and limited room for collective industrial action.

[33] We have to note, however, that the boundaries between state, the governing party and the favoured interest groups (oligarchs) are blurred.

at the expense of such peripherical employees as temporary agency workers.[34] The characteristics of this political turn are important in the context of the CrowdWork project as these measures further limit the opportunities for employees to express their voice.

Labour law regulation and platform work in Hungary[35]

In Hungarian labour law, platform workers are mostly independent contractors, as Hungary does not have the third labour law category. Independent contractors are self-employed workers, whose work relationships are covered by the Civil Code (contract for service). The Civil Code does not provide any employment protection in the framework of such contracts for service, contrary to the Labour Code provisions on employment relationships.

The Hungarian labour law is unprepared to cope with the regulation of platform work. It is presently characterised by a rigid 'binary model' of employment regulation consisting of employment contracts and civil law contracts: "universal" versus "zero" legal protection. In the perspective of the binary regulation, platform workers have either an "employee status" entitled to complete labour law protection guaranteed by the Labour Code (LC), or have the status of "self-employed" working without any legal protection under the scope of the Civil Code.

The Hungarian labour law does not regulate the third type of employment status: economically dependent worker or dependent contractor or worker. There is no special legal regulation on this third category of workers in the Labour Code. Moreover, it is impossible to use in a mechanistic way the legal regulations covering the standard (typical) and non-standard (atypical) employment relationships in the Labour Code. The major legislative issue is whether the regulation of the third employment status (economically dependent worker) would be an appropriate solution for the protection of platform (gig) workers. However, the third labour law status could only partly solve the particular problems created by gig work. Certainly, there are various issues related to platform work, which require rather particular legal solutions due to its special characteristics.

In this relation, one of the particular features of platform work is the rating system and its legal consequences. The Hungarian regulation is totally missing on "digital ratings". Therefore, it is impossible to guarantee the transparency of online evaluation and to question its correctness (i.e. legal remedy). Beyond transparency, the transferability of ratings is also a fundamental issue without legal guarantees. Online rating has two consequences: disciplinary sanctions or termination of the legal relationship (inactivation). According to the Labour Code, disciplinary sanctions may be levied if the collective agreement or the employment contract allows it.[36] As a contrast, in civil law the parties may agree on

[34] Neumann–Tóth 2018, 145.

[35] This section is based on the contributions of Dr. Tamás Gyulavári (labour lawyer, Department of Labour Law, Péter Pázmány Catholic University, Budapest) and Dr. Bankó Zoltán (labour lawyer, University of Pécs, Faculty of Law). The authors are grateful to them.

[36] Act 1 of 2012 (Labour Code), Article 56(1).

such legal consequences. In case of termination of employment (inactivation), platform workers usually lack any protection against termination due to the unilateral regulation of the employer (conditions of work on the website).

Furthermore, platform workers are not fully entitled to seemingly universal social rights, such as prohibition of child work and discrimination. In relation to child work, in principle the Labour Code provisions on the protection of young employees could be a satisfactory solution (i.e. in case of employees under 18, it is obligatory to apply the LC articles on the protection of young employees).[37] Unfortunately, it is unclear whether the special rules on establishment of employment in relation to young employees (the age limit) shall be applied outside the employment contract. As for the equal treatment principle, the Equal Treatment Act (125 of 2003) shall be applied in all legal relationships aimed at work. Therefore, the nature of the work relationship is not relevant, since the equal treatment provisions must be applied in all circumstances.[38]

Collective rights and especially the right to conclude collective agreements are not ensured outside the scope of the Labour Code. In the Hungarian labour market, collective agreements exist almost exclusively at workplace level. Collective agreements may be concluded by a trade union (or their federation), if at least 10% of the employees are union members.[39] However, if workers are lacking the employee status, they cannot be covered by a collective agreement. Works council agreements may provide an alternative or quasi collective agreement.[40] In this case, a Works Council (WC) must be elected, but establishment of a WC requires – again – the votes of employees (only). In this way, the "employee status" is the exclusive basis of employee rights, whether collective or individual.

Sector level collective agreements would be the ideal solution covering legal relations beyond employment relationships, covering also platform work. For instance, if a sector level collective agreement were operational on the entire personal transport sector, it would be possible to extend it over digital platforms providing taxi services. However, sector level collective agreements hardly exist in Hungary.[41] While Act 74 of 2009 on sector level social dialogue regulated the role of sector level dialogue committees and middle level social dialogue, this Act only covers interest representation of employees.[42] In addition, the constraints of EU competition law regarding the conclusion of collective agreements by non-employees are present in Hungarian law, too.

As a consequence, the Hungarian labour law presently hardly addresses in any substantial way questions related to the protection of platform workers. Therefore, it would be necessary to create a separate and detailed legal regulation regarding workers outside the scope of employment relationships, with particular attention to platform workers.

[37] Act 1 of 2012 (Labour Code), Article 4.
[38] Act 125 of 2003, Article 5.d and 3(1)a–b.
[39] Act 1 of 2012 (Labour Code), Article 276(1)–(2).
[40] Act 1 of 2012 (Labour Code), Article 268.
[41] Except the health sector. Source: www.aeek.hu/-/kollektiv-szerzodes-az-egeszsegugyben-unnepelyes-alairas (Accessed: 21.09.2019.)
[42] Act 74 of 2009, Article 1–2, 15(1).

Lack of comprehensive empirical evidence on platform work: Hungarian experience in European perspective

Although the gig-economy as such is a popular topic in the international scientific debates, this topic is rather undervalued in the Hungarian context. This is even more true when it comes to platform workers, the discussion about their jobs' content, working conditions and employment status, as well as their voice with management and collective bargaining power. This is partly because it is a rather new phenomenon, and partly because labour related issues are of secondary importance in the present practice of the Hungarian social sciences.

Therefore, international research projects represent the most important source of knowledge on platform work instead of the Hungarian ones. The first attempt to estimate the size of platform workers in 14 European countries has been made by the COLLEEM survey.[43] The survey results are shown in the next table in a somewhat simplified version.

Table 11: The number of platform workers as a percentage of the total adult population (2017)

Country	Adjusted estimate
U.K.	12.0
Spain	11.6
Germany	10.4
Netherlands	9.7
Portugal	10.6
Italy	8.9
Lithuania	9.1
Romania	8.1
France	7.0
Croatia	8.1
Sweden	7.2
Hungary	6.7
Slovakia	6.9
Finland	6.0
Total	**9.7**

Source: Pesole et al. 2019, 15 (COLLEEM dataset).

According to the estimates of the COLLEEM project, a non-negligent share of the Hungarian adult population (6.7%) makes some earnings from platform works. This ration is well below of the rates of such project partner countries as Spain (11.6%), Portugal (10.6%) or Germany (10.4%).

[43] Pesole et al. 2019.

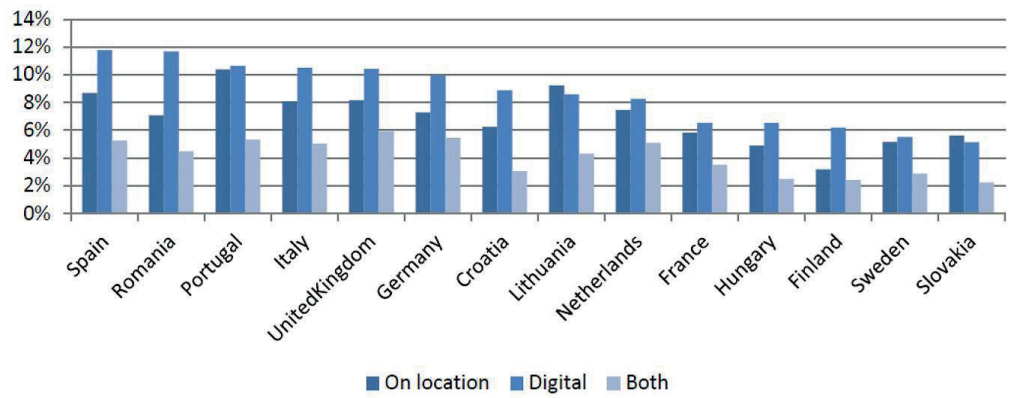


Figure 1: Types of provided service by country (2017)
Source: Pesole et al. 2019, 35 (COLLEEM dataset).

Except for Lithuania, in all countries surveyed, the 'digital service' dominates. In relation with the CrowdWork21 research consortium countries, it is necessary to call attention to the leading roles of Spain, Portugal in comparison with Germany and especially with Hungary. The other interesting result of the survey: Nordic countries who have the highest level of "digital literacy" are among the "trailing edge" countries. As we mentioned earlier, the COLLEEM survey was the first attempt to map the quantitative and qualitative characteristics of platform workers in some selected European countries by using an empirical survey.

The IRSDACE (Industrial Relations and Social Dialogue in the Age of Collaborative Economy) project funded by the DG EMPL of the European Commission is another recent research project on platform work. Its aim is to explore new strategies of traditional stakeholders (trade unions, employers' association, governmental bodies, etc.) towards the challenges of the collaborative economy. As part of the project, case studies were carried out about platform workers and platform companies in Hungary. This is the most recent and most comprehensive qualitative research in the country, therefore, we will briefly summarise its main results and findings.[44]

During the project, 13 interviews were made and additionally two focus group interviews were conducted with six platform workers. The sectors covered by the research were: 1. local personal transport; 2. housework; and 3. accommodation service. All three sectors belong to the category of mobile labour where personal presence is required for the service delivery. These three sectors differ greatly in terms of wages, skill level of the jobs, social status and interest representation. Baby-sitting works, for example, are regarded as the least desirable jobs, while those participating in the Airbnb business rarely consider themselves platform workers but rather entrepreneurs and real estate investors. Taxi drivers, in contrast, form a socio-professional group with traditionally string identity and collective representation.

[44] For the whole report see Meszmann 2018.

However, a rapid growth was observable in all three sectors during the last decades. This was due to the global financial crisis and the subsequent economic downturn that gave a rise for both the demand and the supply side of this special segment of the labour market through the increased cost sensitivity of households (demand side) and through the increased popularity of extra income generating service platforms (supply side). As the final research report concludes, the regulation of platform work is at the heart of the public debate while job quality and employees' voice are not prioritised. Regulation is a tricky issue because all three sectors can be characterised by a high level of informality. Household work (baby-sitting) and other accommodation services (Airbnb) are minimally regulated, while the local personal transport sector is meticulously regulated.

This informality has a direct (negative) impact on the employment relations, as platform workers are usually self-employed or simply are not declared at all: "Such employment forms also do not provide solid ground for self-organization of labour. Those working in the platform economy typically do not have formal contracts and are thus deprived from enjoying rights stemming from employment contracts in addition to social rights. Micro-workers, or individual entrepreneurs, fulfil the criteria for membership with some civil and interest based associations, but do not fulfil the set criteria to become members affiliated with trade unions."[45] Most platform workers are typically either self-employed small entrepreneurs or registered natural persons working as service providers. This represents a further barrier to self-organisation of the workers as they are rarely entitled to join any existing trade union or create a new one. The social dialogue is even more cumbersome due to the fact that platform companies typically deny that they are employers of the platform workers but are serving only as an intermediary, bringing together buyers and sellers via an ICT platform. As concerning the buyers, it is worth noting that they are just as atomised individually as the workers are and have no social or economic interest to form any employer-type of collective entity. On the other hand, as employer organisations of the traditional (offline) subsectors have been vocal against platform companies, the most important emerging "battlefield" is not focused on the working conditions and job quality of platform workers but most often on fair competition and tax avoidance.

The general perception of the most relevant stakeholders on platform work are summarised as follows: "Workers and service providers praised the efficiency of platforms to provide opportunities for earning income and, in some cases, job generation. Many highlighted the lack of introductory education regarding the risks and requirements of working for the platforms. On the other hand, traditional employers and service providers in local transport and accommodation expressed both caution and hostility towards the platform economy. This group highlighted unfair competition due to low regulation as causing undeclared employment and thus tax evading practices of the new competitors. Platform companies and platform based employers stressed the innovative and income generating dimension of their enterprise. Employers in the accommodation sector, and also small service providers using platforms for their service providing market, stressed the benefi-

[45] Meszmann 2018, 5.

cial, very different, personalized, detailed nature of services they delivered to customers. Finally, public authorities did not have a general stance towards platform companies."[46]

Social dialogue is generally weak in Hungary, and consequently is even weaker when it comes to platform work. The social prestige of trade unions is low, Hungarian workers tend to consider themselves employees only if they have a full time employment contract. In addition, Hungarian trade unions do not prioritise highly platform workers as a potential recruitment base but take a more traditional approach. As mentioned previously, systemic efforts have been made from within the government that are aimed at weakening the role of the social dialogue at all levels. On the national level, the tripartite dialogue has been considerably limited in its scope and agenda, the power of the sectoral level social dialogue committees, established during the 2000s, has decreased to an even greater extent.[47] It seems that there is a vicious cycle in the institutional framework of the interest representation in Hungary: the trade unions traditionally tend to represent the core workforce and leave precarious workers aside,[48] while employees tend to neglect the significance of trade unions and see them as an ineffective, old-fashioned and excrescent tool that can generally be ignored.

National debate reflected in the social media[49]

As the social science community has generally paid little attention to the social and economic consequences of platform work in Hungary, the same is true for public debate and for the traditional as well as online media. The majority of the articles written about platform work emphasises the advantages of platform work, while tends to understate the dark side of this form of work. There is also an interesting division between the mainstream media, which essentially ignores the topic, and some specialised blogs that are extensively focused on platform work.

For our analysis, web data on platform work were gathered and analysed. The figures presented below graphically represent where the discussion on sharing economy took place. According to the Hungarian keywords examined, the issue appeared most commonly in blogs (Figure 2). The majority of web links (HTML resources) are classified as blogs (more than 60%), which is followed by academia and media, both slightly above 10%. Websites of interest groups appeared in 5%, among them the appearance of traditional social partners (trade unions) was rare. The majority of the discussion is happening on unofficial fora, as blogs. Taking into consideration the PDF documents, these files are mostly published by the academia (approximately 40%), the interest groups are in the second place by approximately 10%. In the ratio of sources, there is no significant change between 2018 and 2019.

[46] Meszmann 2018, 37.
[47] Meszmann 2018, 18.
[48] Neumann–Tóth 2018, 144.
[49] Some parts of this section are based on the contributions of Gergő Benedek who is a blog writer, owner of freelancer.hu. The classification of the web data (Figures 2 and 3) was made by Katalin Bácsi, Budapest Corvinus University.

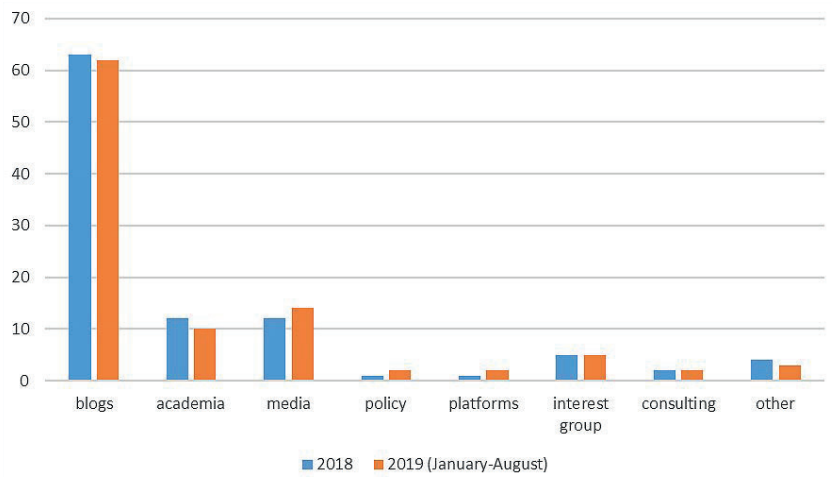


Figure 2: Classification of web data: HTML documents using native key terms

Source: Google search and own calculations. Key terms: közösségi gazdaság (sharing economy), platform gazdaság (platform economy), hakni gazdaság (gig economy), online gazdaság (online economy), digitális munka (digital labour).

The presence of debates on these topics is rare on television or radio, and only a few podcasts and news sources exist, and these are mainly connected to platforms of public transport (Lime, Mol Bubi). In magazines and newspapers, related articles are mainly connected to newly established platforms, to defining and usage of the sharing economy, and to what it means to be a freelancer. The blogs are primarily connected to platforms and freelancers.

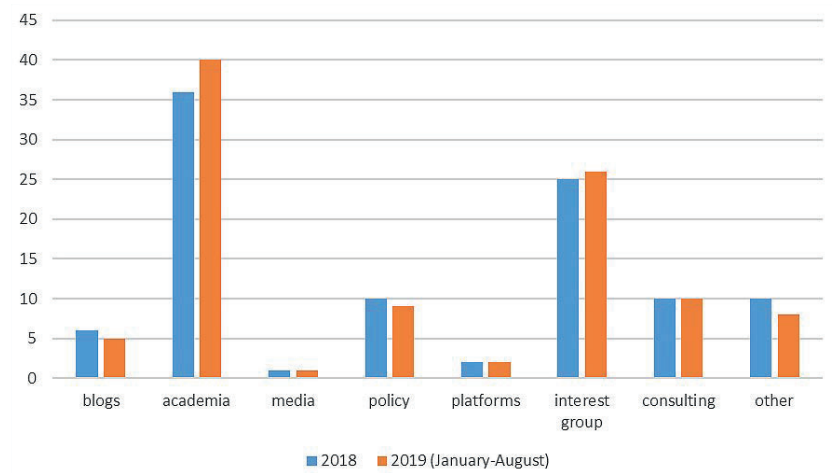


Figure 3: Classification of web data: PDF documents using native key terms

Source: Google search and own calculations. Key terms: közösségi gazdaság (sharing economy), platform gazdaság (platform economy), hakni gazdaság (gig economy), online gazdaság (online economy), digitális munka (digital labour).

The PDF documents are mainly connected to policy makers, focusing primarily on defining the sharing economy related to accommodation services and local transportation.

Interest representation (collective voice) and the platform work

Platform work is a marginal issue in the current Hungarian public and scientific discourse in comparison with such topics as the growing number of Hungarians working abroad and the subsequent labour shortage on the Hungarian labour market, and more recently the social and economic impact created by the COVID-19 pandemic.

In this context, it is not at all surprising that the debate about the precarious employment practices of platform work is not so intensive. As we will examine, the majority of the public debates around such pioneering platform companies as Uber and Airbnb is primarily about the economic regulation-related effects these new business models. It is, therefore, somewhat obvious that the traditional stakeholders (trade unions, employers' associations) are less active in organising themselves around these topics, while new or grassroots interest representative associations have been slowly emerging. In the followings, we will briefly summarise the stance of the most relevant stakeholders towards platform work through the lens of some of the few initiatives and actions that have been found during the desktop research and the preliminary fieldwork, interviewing selected groups of stakeholders.

Hungarian trade unions: Slow exploration of the new forms to organise platform workers[50]

Preliminary remarks: More European than national level initiatives. Digitalisation and platform working are new topics for the Hungarian trade unions and the confederations. While there are 6 confederations and more than 150 trade unions, the movement is very fragmented and weak. In this context, it is a hard work to disseminate new topics (e.g. working time reduction, gender questions, platform work), because of current pressing challenges: low salaries, employees' unfriendly legislation ('slavery law' from 2018), low TU density, weaknesses of the collective bargaining power, poor working conditions in the public sector, etc. The Hungarian confederations are participating on the international trade union movement, and while the ETUC, the EPSU and other European organisations are involved and interested in the digitalisation and the platform working, the Hungarian trade unions are less open and active in the field of platform work than in other parts of Europe. A recent Eurofound study examined the newest or most innovative practices and found quite large varieties as to how the social partners address and deal with such

[50] This section is based on the contribution of János Véber, Deputy President of the Hungarian Union of Cultural Institutions and Public Collections Employees (KKDSZ) and Member of the Committee of Labour Market and Employment of the European Trade Union Confederation (ETUC). The authors are grateful to him.

new topics as for example platform work. The authors distinguished three main groups of countries that are shown in the following table.

Table 12: Social partners exploring new topics since 2000 – main results (2015)

Patterns of addressing new topics	Countries exploring these patterns
Mainly shadowing EU-level developments and initiatives	Cyprus, Czech Republic, Estonia, Croatia, Hungary, Malta, Lithuania, Latvia, Poland, Romania, U.K.
Exploring also additional topics	Bulgaria, Slovakia, Slovenia
Exploring new topics	France, Luxembourg, Italy
With significant changes after 2008	Greece, Ireland, Portugal, Spain
Exploring a broad range of new topics	Austria, Belgium, Germany, Netherlands
Plus initiating organisational changes and labour market/ welfare reforms	Denmark, Finland, Norway, Sweden

Source: Eurofound 2016, 64.

As we can see from the table above, Hungarian social partners belong to the category of the least open and active countries in terms of addressing new issues emerging from such global trends like the growing number of platform workers. From the CrowdWork21 research consortium countries, data show that social partners are more innovative in Portugal and Spain, especially since the global economic and financial crisis, while German social partners are traditionally good in exploring a broad range of new topics, although to a lesser extent than their Scandinavian counterparts. This was reinforced by our own preliminary research as well, where we found that trade union leaders admitted they lacked the financial and human (expert) resources and background to initiate comprehensive actions in that field. However, we found there are some initiatives at national and international level they have been involved in recently.

Selected EU trade union involved projects on digital economy: Weak involvement of the Hungarian trade unions[51]

International projects of ETUC (European Trade Union Council): Workers Participation – The Key to Fair Digitalisation (2016–2018)

www.etuc.org/en/key-fair-digitalisation

ETUC had a project entitled *Workers' Participation: The Key to Fair Digitalisation.* This project examined practices responding to the key challenges and questions surrounding workers' participation, considering the changes brought about by digitalisation. ETUC and ETUI organised conferences and seminars in this topic. ETUI published a research paper about the new challenges of digitalisation, which were based on an international sur-

[51] The rare exception of the involvement of the National Association of Works Council (Munkástanácsok Szövetsége) in a recent, EU supported project on platform work (Kun–Rácz 2019).

vey. The Hungarian Trade Unions and confederations were represented in the seminars, conferences. The published report on these events can be found on the following link:

www.etuc.org/sites/default/files/publication/file/2018-09/Voss%20Report%20EN2.pdf

As a part of this project, ETUC published the first report on platform economy (edited by Jeremiah Prassl):

www.etuc.org/sites/default/files/publication/file/2018-09/Prassl%20report%20maquette.pdf

Establishing workers representation and social dialogue in the platform and app economy (2019–)

The last Conference of the ETUC (held in Vienna, May 2019) underlined the importance of the new ways of employment, e.g. digitalisation and platform working. In this light, ETUC in partnership with the French institute IRES and the organisation ASTRESS has started the project *Establishing workers representation and social dialogue in the platform and app economy,* funded by the European Commission. The project started in March 2019, with a two years duration and has three specific objectives: 1. setting up and running a European Observatory for the development of workers participation in digital platforms; 2. identifying and accompanying new and innovative practices that aim at improving representation, organisation and protection of platform workers (two collective coaching sessions are planned); and 3. proposing a European regulatory framework to establish worker representation in platforms and fair working conditions in these companies. The first meeting of the observers from the ETUC side was held on 18 September, and while there was no representation from the Hungarian Trade Unions, they will be informed as the project continues.

National level initiatives: Domination of the information campaign domination – The Future of Work (2016)

The MASZSZ (The Hungarian Trade Union Confederation) and the FES (Friedrich Ebert Stiftung) organised a conference in Budapest in 2016 on the topic: *The Future of Work.* Speakers, scientists and trade union leaders identified digitalisation and platform working as a key element of employment in the future:

http://szakszervezet.net/images/kepek/2017/11_november/A_munka-jovoje_konferencia-Program-20161122.pdf

Report for the National Economic and Social Council of Hungary (2018)

Trade unions presented a working paper in the NGTT (The National Economic and Social Council), which is the highest level forum for social dialogue between the government, trade unions and employers' association. The paper was prepared by a working group of Hungarian trade union confederations on the topic of digitalisation. This working paper was submitted in autumn 2018. The NGTT has discussed and accepted this information paper without any recommendations for the social partners of the NGTT.

A grassroot initiative: When platform owners (operators) organise themselves – The case of the Hungarian Sharing Economy Association (HSEA)

One of the weakest points of the Hungarian industrial relation system is the weak organisation of the employer's side. This is due to multiple reasons, the most important one being the lack of interest and incentive to do so. This is not the case, however, in the field of platform work. Although trade unions are struggling with organising individualised platform workers, we already found the rudiment of a self-organising employers' association. The term might be misleading as they do not define themselves as employers, so it would be more adequate to call them business groups; nevertheless, this is a rather unique initiative.

The Hungarian Sharing Economy Association was established in March 2017 to promote the development of sharing economy in Hungary. Their members strongly believe that exploiting the potential of sharing helps all the players in the economy to operate efficiently and sustainably.[52] Currently they have 14 member organisations. Their *main goals* relative to platform work are as follows: 1. Support (to create a general framework for the functioning of the community economy representing the interest of businesses and consumers in every possible forum; 2. Knowledge Deepening (to increase understanding about the community economy, and promoting the aspirations of enterprises operating in the spirit of sharing economy); and 3. Influence Regulatory Framework (to promote the development of legal guidelines and tax regulations that are tailored for the functioning of community economic models and are ideal for all stakeholders).

The member organisations are recruited primarily from the person-to-person (P2P) markets and include both mobile labour market (MLM) and online labour market (OLM) companies (see section *Platform work: Lack of consent-based terminology and the heterogeneous character of platform work* of this report for a precise definition).
Platforms active on the mobile labour markets:

- Oszkár[53] (Oscar), car sharing company for longer distance trips, mainly inland
- a Miutcank.hu[54] (ourstreet.hu), a community building platform that aims at exploring the hidden opportunities and resources of one's neighbourhood, thus promoting sustainability
- Click4work,[55] casual work for students
- Loffice,[56] office, event space and coworking
- Boatly,[57] boat renting

[52] Source: www.sharingeconomy.hu/?lang=en (Accessed: 22.05.2020.)
[53] Source: www.oszkar.com/ (Accessed: 22.05.2020.)
[54] Source: https://miutcank.hu/hu.html (Accessed: 22.05.2020.)
[55] Source: https://clickforwork.hu/ (Accessed: 22.05.2020.)
[56] Source: https://budapest.lofficecoworking.com/about_us (Accessed: 22.05.2020.)
[57] Source: https://boatly.hu/ (Accessed: 22.05.2020.)

- Veddbérbe[58] (takearent.hu), renting a broad range of tools (utensils, casual clothes, office instruments, vehicles, etc.)
- Dooroffice,[59] event space and coworking
- Kaptár[60] (Hive), community office
- Roomly,[61] renting a premise
- Meló-diák,[62] student work

Platform members active on the online labour markets (OLM):

- Tikething,[63] ticket sales
- Barion,[64] online payment
- Rukkola,[65] online booksharing
- Tőkeportál,[66] crowdfinance

The activities of the association cover three main areas:

1. Supporting: They help to create a general framework for the functioning of the community economy representing the interest of businesses and consumers in every possible forum.
2. Find answers: They support to deepen the knowledge about community economy and promote the aspirations of enterprises operating in the spirit of a sharing economy.
3. Shape regulation: their members agree to promote the development of legal guidelines and tax regulations that are tailored for the functioning of community economic models that are ideal for all stakeholders.

As it can be seen from the mission statement and the main activities, the Hungarian Sharing Economy Association is a lobbying organisation aimed to promote the idea of sharing rather than a classical employer's association, but this can change over time and might play a significant role especially by its shaping regulation activities.

Dominance of informal and grassroots initiatives in interest articulation

Irrespective of where they work, there are many references in the literature to factors relating to how difficult it is to organise labour working in these platforms. Akgüc et al.

[58] Source: https://veddberbe.hu/ (Accessed: 22.05.2020.)
[59] Source: https://dooroffice.hu/ (Accessed: 22.05.2020.)
[60] Source: https://kaptarbudapest.hu/ (Accessed: 22.05.2020.)
[61] Source: www.roomly.io/ (Accessed: 22.05.2020.)
[62] Source: https://business.melodiak.hu/ (Accessed: 22.05.2020.)
[63] Source: www.tickething.hu/ (Accessed: 22.05.2020.)
[64] Source: www.barion.com/hu/ (Accessed: 22.05.2020.)
[65] Source: https://rukkola.hu/ (Accessed: 22.05.2020.)
[66] Source: https://tokeportal.hu/ (Accessed: 22.05.2020.)

(2018), for example, revealed a number of reasons why platform workers tend to refuse attempts from the side of trade unions to cover these workers:

1. A general declining trend in unionisation rate, as was described in the previous section.
2. Low wage earners tend to prefer to use time for executing another task rather than to attend meetings where they could be organised.
3. As platform work may involve very different tasks and activities, it is often not clear which sector platform workers belong to and therefore they are often uncertain which union would be most appropriate.
4. Platform workers carry out their tasks in a relatively individualised way and this isolated, atomised way of working does not favour organising workers for collective actions.
5. Platform work often involves short-term, temporary commitments, secondary jobs, while unionisation requires long-term common interests in one's main job.
6. The tradition of collective action varies greatly across countries, as was extensively elaborated on in the first section.[67]

The same issues apply in the Hungarian context. One of our experts interviewed, however, indicated that there are in fact significant differences among platform workers according to their type of jobs. Freelancers who carry out highly skilled jobs tend to regard themselves as self-entrepreneurs and in some cases view their experience as the first step in an evolution of learning how to become an entrepreneur. They build informal structures, in many cases by using online tools (chat rooms, forums, Facebook groups, etc.), to share some problems and offer solutions for them. The most important topics for these workers are the following:

1. Psychological problems like solitude.
2. Productivity: how to work effectively in a home working environment.
3. Attracting new clients: how to create brand, make new deals, promote their talent to stand out in the crowd.
4. Pricing: it is a crucial point in the freelancers' work as in most of the cases there is no general scheme for pricing, each and every work is bargained individually.
5. Working conditions: how to ensure the best working conditions, opportunities and threats of flexible working arrangement, continuous training.
6. Employment status and problems related to taxation and accountancy.

In addition to the different online "communities of practices", there are regular meet-ups, where these problems are discussed in person with the direction of experts of the field.

[67] Akgüc et al. 2018, 6.

Uber failure in Hungary: Unfair competition not tolerated by social actors[68]

Uber appeared in Hungary during the early 2010s and its business model became a hot topic automatically. There were two main concerns about their activities: first, Uber paid its company tax outside Hungary. Second, their business model was based on unfair competitive advantages. Uber claimed that they are not a taxi company but only a high-tech firm and application developer through which they link customers and individual service providers who were (self-) entrepreneurs. Rival taxi companies, however, protested against them for several reasons:

1. Uber did not pay the obligatory deposit every other taxi company had to pay.
2. Uber did not have to comply with strict environmental requirements regarding fleets.
3. Uber did not have any obligations towards their quasi-employees and
4. The Uber drivers did not have to make the same exams and tests that every other taxi driver had to.

The main root of all of these issues was Uber's business model and the fact that Uber refused to be acknowledged as a taxi company. Taxi drivers represent a traditionally strong interest group in Hungary and in this case, they found a powerful ally in the Hungarian Government because of the tax evasion. The taxi drivers' trade unions organised demonstrations and petitions against Uber that was promoted by taxi drivers and taxi company owners. The Hungarian Trade Union for Taxi Drivers (Magyar Taxisok Szakszervezete) blocked Budapest in January 2016 with a demonstration that effectively shut down traffic in the city centre. Following this demonstration, the Hungarian Parliament adopted a new regulation, which practically prohibited providing services in a similar way to Uber, and on 13 July 2016, Uber announced they would leave Hungary. However, it is worthy of note that the employment status and the working conditions of the taxi drivers working for traditional taxi companies are rather similar to those working for Uber; therefore, the public debate around Uber focused mainly on unfair competition and tax avoidance, while deeper problems related to job quality, working conditions and employment status have been overshadowed. The destiny of Uber in Hungary was rather similar to the German case where "…Uber never got off the ground. The overarching taxi association mounted an immediate cease and desist order which framed Uber as a threat to the public interest and themselves as defender of the rule of law. The debates therefore moved quickly away from the public to the judicial arena".[69] There is, however, a similar company, originally called Taxify, renamed Bolt, that operates in Budapest and uses an app essentially identical to the one used by Uber for drivers and clients to connect and pay for rides electronically.

[68] The authors would like to thank the significant contributions of Tibor Meszmann (research fellow and activist, Central European Labour Studies Institute [CELSI], Bratislava) that were an invaluable help in preparing the present report.

[69] Thelen 2019, 3.

Platform work and digitalisation of catalogues, records of public collections

The Hungarian public collections (libraries, museums, archives, etc.) usually have limited catalogues or inventory, and because the staff of these public institutions is limited in their ability to conduct digitalisation for these documents, small companies have been established to carry out digitisation tasks. These companies usually hire librarians and archivers, some of whom normally work in the public sector as civil servants, as part-time workers or via self-employment. The Union of Cultural Institutions and Public Collections Employees (KKDSZ) considers these workers a target group (self-employed or part-time workers) but the organising of such a group is complicated. The KKDSZ will organise a conference in 2020 on the topic of digitalisation, they submitted an application for funding the Friedrich Ebert Stiftung in Budapest.

Platform workers versus entrepreneurs: The case of Airbnb[70]

There has been a steady growth in the accommodation services beginning in the late 1970s in Hungary, although this subsector is geographically concentrated around Budapest and Lake Balaton. The accession to the European Union in 2004 had an additional rise in the number of nights spent by international tourists in the country, and another wave has coincided with the emergence of Airbnb, which has proven to be a major disruptor of the lodging industry. Contrary to the case of Uber, the presence of Airbnb did not provoke any major social protests, mainly because of the much softer regulation: while Uber would have had to spend significant resources to meet all requirements resulting from the severe regulative environment, Airbnb has been completely free to operate. Thus, the company is not even registered in the country, running its daily operation through its two main European affiliates: Airbnb Ireland UC and Airbnb Payments UK Ltd.

According to some estimates, the number of apartments advertised through Airbnb is between seven and ten thousand. The Hungarian Hotel and Restaurant Association is the most powerful stakeholder on the employers' side, and the association has been a vocal advocate against Airbnb since it entered onto the Hungarian market. Although the unionisation rate is extremely low in the sector (0.9%) it has a relatively well performing social dialogue committee. The Association often invites foreign experts to these meetings, and several background papers have been elaborated under their supervision. Three of these expert documents deal exclusively with the impacts of platform economy[71] on the sector: the first *The emergence of sharing economy on the market of accommodation services* was published in 2015, the second *Analysis of experiences on renting private apartments as a commercial activity* was published in 2016, and the third *Demand and supply on the private apartments market between 2010–2017* came

[70] This section is based on Meszmann 2018 with some updates and complements.

[71] They use the term sharing economy but we will refer to it as platform economy for the sake of consistency.

out in 2018.[72] The Association considers Airbnb a strong competitor and attempts to lobby against it. Their arguments can be regrouped into three main streams: 1. unfair competition; 2. poor working conditions; and 3. reliance on foreign investors, who take profits outside of Hungary.

The first line consists of the well-known arguments on fair competition, the quality standards of the services and the taxation issues. As we mentioned earlier, Airbnb is not registered in Hungary and consequently it does not pay any taxes after the income generated in the country. In contrast, it is the owners of the apartments that would pay the taxes. While tax avoidance practices are not common in case of big real estate companies who recognise the legal risks involved, this is not necessarily the case for the individual lessors.

A second group of arguments deals with the poor working conditions of employees working in the platform economy. This was a hot topic in 2017 during the sectoral social dialogue committee meetings: "The session of late 2017 covered the issue of platform economy in the accommodation sector, and in this session, the employers' side posited that platforms indirectly threaten job security, quality of employment of workers in the traditional proxy sector, and created highly precarious, unregistered employment."[73] It is important to stress that this was the only example we found where the working conditions of those engaged in the platform economy emerged as a key topic in the context of formal or institutionalised social dialogue.

A third group of arguments call attention to the wider negative impacts of short-term renting activities. As the market prices are lower in Budapest than in other European capitals, short-term renting proved to be a good investment for foreign investors, especially as the interest rates have been close to zero in the recent years. The appearance of Airbnb has led to an exponential growth of prices both for renting and for buying, and represents a major social risk for a growing number of people residing in Budapest, although the impact of the coronavirus pandemic on tourism and real estate has yet to be understood.

However, the majority of these arguments have not created much public interest so far, and the functioning of Airbnb can generally be regarded as smooth. The only social group that has been relatively successful when protesting against Airbnb have been the residents of inner districts of Budapest, where many young tourists rent apartments for a long week-end for partying, primarily young tourists who visit Budapest to celebrate bachelor days, birthdays and visit the ruin pubs. In this case, the debate is not around taxation or working conditions but rather on how to regulate this market in order to ensure the repose of residents of these central districts. (Budapest is not alone in having alcohol-fuelled, budget-airline-driven tourism cause disruptions in residential areas. Krakow, Prague and other destinations in Central Europe have experienced similar issues.)

[72] The documents can be found on the following link www.hah.hu/elemzesek/sharing-economy.
[73] Meszmann 2018, 24.

It is also worth calling attention to the fact that this special group of apartment owners differs greatly from all other types of platform workers in that they do not consider themselves platform workers. Other platform workers – be they micro-workers or highly skilled freelancers – also regard them as real estate investors and/or entrepreneurs who have nothing to do with "real" platform workers.

Concluding remarks

The analysis of the available quantitative and qualitative literature on platform work indicates that the online labour market has produced a visible growth since the global financial crisis and economic downturn (2008). The most recent survey on the use of platform work among internet users (COLLEEM database) shows that in such leading edge countries as Spain, Germany and Portugal, the estimated number of platform workers may exceed one-tenth of the adult population.[74] In less active countries, such as Hungary, the share of occasional or regular platform workers is much lower, i.e. about 7% of the adult population. However, it is also worth highlighting that the frequency of usage of platform works does not necessarily tell us much about its real role in terms of income generated by, or working hours spent on platform work. More detailed analyses suggest that this type of employment remains residual compared with the standard employment form that are based on full-time working contracts on the offline labour market. Nonetheless, it is crucially important to regularly monitor the development trends in this field. At present, we lack reliable data from methodologically well-designed surveys that make cross-country comparisons and especially longitudinal analysis ponderous if not impossible.

The first step in this direction would be reaching a consensus on the definition of platform work and a tentative typology to classify its most important forms. Currently there exists a plethora of definitions describing the wide variety of forms in this emerging and evolving sector of employment. The jobs differ greatly by several key factors: skill level required by the tasks or projects, length of time involved (which may range from passing keys to Airbnb clients to long-term contracts for software coding projects), as well as by the wages accessible for and the perceived social status of the workers. In addition, there are other features, such as online vs. physical presence that are being increasingly blurred as the coronavirus alters the workplace and more people are working online from home. What is common, however, in all types of platform jobs is the fact that the workers have a precarious employment status, being either self-employed or natural persons with some special legal and tax regulation. There is a vivid debate among labour law specialists on the question of whether it would be beneficial to create a special employment status for platform workers since platform companies deliberately avoid considering themselves employers of these workers. Such a special status would allow to clarify and "whiten"

[74] Pesole et al. 2019.

this grey sector of the economy and allow platform workers to be paid a more equitable compensation for their level of social contributions.

Despite the lack of public debate on these issues, the employment status of the platform workers, their job content and their working conditions may raise serious concerns among not only social scientists but among trade unionists as well. A more detailed analysis of the national industrial relations system shows that the chances of the platform workers to be unionised or be represented by a trade union varies greatly according to country-specific institutional arrangement and culture of social dialogue. Platform workers are in an especially precarious situation in Hungary. Trade unions are generally weak, but their bargaining has been systemically further weakened since 2010. Instead of collective interest representation, individual bargaining has always been the prevailing form of solving workplace conflicts. In addition, the trade unions are also discredited for the majority of employees because of their compromised role in the state-socialist system and due to the dominance of the SMEs in the current employment landscape. Finally, the trade unions themselves tend to overlook platform work in part due to a lack of the necessary financial resources to organise, but primarily because it is extremely hard to organise this highly individualised, scattered group of workers.

Furthermore, we need more international comparative research on this topic. In addition to the COLLEEM project, which gathered quantitative information on platform workers, the only research project in Hungary that attempted to map the opportunities and threats of interest representation of platform workers has been the IRSDACE project. Labour law represents the only exemption, and labour law experts are relatively active in this field. Several PhD dissertations and higher level scientific papers have been recently made about how to regulate the precarious employment status of the platform workers. Perhaps not independently from the generally weak interest of social scientists in examining platform work in Hungary, the public debate is also virtually non-existent.

It is mainly the employers and their associations organised in the traditional segments of the same sector that are vocal about platform employment, focusing their complaints of how the companies and their workers are circumventing regulation, lessening quality standards and engaging in tax avoidance all of which result in unfair competition. The poor working conditions of platform workers were raised only in 2017 in the sectoral social dialogue committee of the hotel and tourism sector.

Although Uber and Airbnb have much in common in their business models, the appearances of the two global platforms in the Hungarian market have had completely different social impacts. This calls attention to the decisive role of such institutional filters, including the regulatory framework (being high in case of the local transport and low in case of accommodation), the professional identity of different socio-professional groups (strong in case of the local transport and weak in case of accommodation), and the sector-specific characteristics of sector level social

dialogue.[75] One major research challenge is to better understand this filtering role of meso and macro level institutions in shaping the concrete country-specific local forms of such global practices as platform work. Another relevant research question is whether traditional forms of collective interest representation are suitable tools to organise such highly individualised workers, and if this is not the case, what are the more appropriate ways to ensure a minimum level of job quality and employment protection for the platform workers. Thirdly, it would be important to have reliable quantitative data on the spread of platform economy, in order to see to what extent it is interlinked with the changing demand of the offline labour market.

References

Akgüc, Mehtap – Beblavy, Miroslav – Cirule, Elina – Kilhoffer, Zachary (2018): *Industrial Relations and Social Dialogue in the Age of Collaborative Economy (IRSDACE). Comparative Report.* Jobs and Skills Unit – CEPS.

Andjelkovic, Branka – Sapic, Jelena – Skocajic, Milica (2019): *Digging into Gig Economy in Serbia: Who are the digital workers from Serbia and why do they work on global platforms?* Belgrade, Public Policy Research Centre.

Berki Erzsébet (2019): Munkaügyi akciók 2010 és 2019 között Magyarországon, különös tekintettel a sztrájkokra [Labour Action between 2010–2019, with Special Attention to the Strike Activity]. Budapest, Friedrich Ebert Stiftung.

Bohle, Dorothee – Greskovits, Béla (2010): *Capitalist Diversity on Europe's Periphery.* Ithaca–London, Cornell University Press.

Borbély, Szilvia – Neumann, László (2019): Neglected by the State: The Hungarian Experience of Collective Bargaining. In Müller, Torsten – Vandaele, Kurt – Waddington, Jeremy eds.: *Collective Bargaining in Europe: Towards an Endgame?* Brussels, European Trade Union Institute (ETUI). 295–314.

Buhr, Daniel (2015): *Social Innovation Policy for Industry 4.0.* Bonn, Friedrich Ebert Stiftung. 17. Source: www.fes-2017plus.de (Accessed: 22.05.2020.)

Eurofound (2016): *New topics, new tools and innovation policies adopted by the social partners.* Luxemburg, Publications Office of the European Union.

Eurofound (2018a): *Employment and working conditions of selected types of platform work.* Research Report. Luxemburg, Publications Office of the European Union.

Eurofound (2018b): *Measuring varieties of industrial relations in Europe: A quantitative analysis.* Luxembourg, Publications Office of the European Union.

Galgóczi, Béla – Leschke, Janine – Watt, Andrew (2009): Intra-EU labour migration: flows, effects and policy responses. *ETUI Working Paper,* No. 3. Source: https://ssrn.com/abstract=2264049 (Accessed: 22.05.2020.)

[75] In case of local transport, the well-organised employers reached a mutual agreement with the taxi drivers who had a strong professional identity, and they managed to chase down Uber relatively soon. In case of accommodation, the similarly well-organised employers' association was unable to successfully lobby against Airbnb. To some extent, it was due to the lack of unionised workforce, the unionisation rate being below 1% in this sector.

Gallie, Duncan (2011): Production Regimes, Employee Job and Skill Development. *LLAKES Research Paper,* No. 31. Source: www.llakes.ac.uk/sites/default/files/31.%20Gallie.pdf (Accessed: 22.05.2020.)

Gallie, Duncan (2018): Quality of work and innovative capacity: implications for social equality. *QuInnE Working Paper,* No. 8.

Grabher, Gernot – Tuijl, Erwin van (2020): Uber-production. From global networks to digital platforms. *Environment and Planning A,* Vol. 52, No. 4. 16.

Hall, Peter – Soskice, David eds. (2001): *Varieties of Capitalism. The Institutional Foundations of Comparative Advantage.* Oxford, Oxford University Press.

Heeks, Richard (2017): Digital Economy and Digital Labour Terminology: Making sense of the "Gig Economy", "Online Labour", "Crowd Work", "Microwork", "Platform Labour", etc. *Centre for Development Informatics – Global Development Institute (SEED), Working Paper,* No. 70.

Kopp, Ralf – Howaldt, Jürgen – Schultze, Jürgen (2016): Why Industry 4.0 needs Workplace Innovation: a critical look at the German debate on advanced manufacturing. *European Journal of Workplace Innovation,* Vol. 2, No. 1. 7–24.

Kenney, Martin – Zysman, John (2016): The Rise of the Platform Economy. *Issues in Sciences and Technology,* Vol. 32, No. 3. 15. Source: https://issues.org/the-rise-of-the-platform-economy (Accessed: 22.05.2020.)

Kun, Attila – Rácz, Ildikó (2019): *National Report on Industrial Relations – The Case of Hungary, iRel – Smarter Industrial Relations to Address New Technological Challenges in the World of Work. European Commission, Agreement no. VS/2019/0081 (2019–2021).* Budapest, Munkástanácsok Szövetsége (National Association of Works Council).

Lehdonvirta, Vili (2018a): Flexibility in the Gig Economy: Managing Time on Three Online Piecework Platforms. *The New Technology, Work and Employment,* Vol. 33, No. 1. 13–29.

Lehdonvirta, Vili (2018b): The rise of online labour markets: freelancing and gig working via internet platforms. *IAB Forum,* 20 December 2018. Source: www.iab-forum.de/en/the-rise-of-online-labour-markets-freelancing-and-gig-working-via-internet-platforms/ (Accessed: 22.05.2020.)

Makó, Csaba – Illéssy, Miklós (2016): Segmented Capitalism in Hungary: Diverging or Converging Development Paths? In Delteil, Violaine – Kirov, Vassil N. eds.: *Labour and Social Transformation in Central and Eastern Europe. Europeanization and Beyond.* New York, Routledge. 77–97.

Mandl, Irene (2019): *Platform work: Maximising the potential while safeguarding standards?* Luxemburg, Publications Office of the European Union.

Martin, Roderick (2008): Post-socialist segmented capitalism: The case of Hungary. Developing business systems theory. *Human Relations,* Vol. 61, No. 1. 131–159.

Mateescu, Alexandra – Nguyen, Aiha (2019): Explainer: Algorithmic Management in the Workplace. *Data and Society,* 6 February 2019. Source: https://datasociety.net/library/explainer-algorithmic-management-in-the-workplace/ (Accessed: 22.05.2020.)

Mazzucato, Mariana (2020): Capitalism's Triple Crisis. *Project Syndicate,* 30 March 2020. Source: www.project-syndicate.org/commentary/covid19-crises-of-capitalism-new-state-role-by-mariana-mazzucato-2020-03?barrier=accesspaylog (Accessed: 22.05.2020.)

Meszmann, Tibor (2018): *Industrial Relations and Social Dialogue in the Age of Collaborative Economy (IRSDACE), National Report: Hungary.* Bratislava, Central European Labour Studies Institute (CELSI).

Morawski, Witold (2019): Researching Capitalism in Poland: Economic Interests as a Cultural Construction. *Journal of Management and Business Administration. Central Europe,* Vol. 27, No. 1. 84–107.

Neumann László (2018): A munka jövője – a szakszervezetek jövője [The Future of Work – The Future of Trade Unions?]. *Magyar Tudomány,* Vol. 179, No. 1. 77–89.

Neumann, László – Tóth, András (2018): Hungarian unions under political and economic pressure. In Lehndorff, Steffen – Dribbusch, Heiner – Schulten, Thorsten eds.: *Rough waters – European trade unions in a time of crises.* Brussels, ETUI. 135–159.

Owczarek, Dominik (2019): Country Background: Poland. In *Don't Gig Up! State of the Art Report.* Brussels, European Commission. 54–63.

Pajarinen, Mika – Rouvinen, Petri – Claussen, Jörg – Hakanen, Jari – Kovalainen, Anne – Kertschmer, Tobias – Poutanen, Seppo – Seifried, Mareike – Seppänen, Laura (2018): *Upworkers in Finland. Survey Results.* Helsinki, ETLA Report 85. Source: https://pub.etla.fi/ETLA-Raportit-Reports-85.pdf (Accessed: 22.05.2020.)

Perez, Carlota (2010): Technological Revolution and Techno-Economic Paradigms. *Cambridge Journal of Economics,* Vol. 34, No. 1. 185–202.

Pesole, Annarosa – Urzi Brancati, Cesira – Fernandez-Macias, Enrique – Biagi, Federico – Gonzáles Vázquez, Ignacio (2018): Platform Workers in Europe. Evidence form the COLLEEM Survey. *JRC Sciences for Policy Report, JRC112157,* Joint Research Centre.

Pesole, Annarosa – Fernandez-Macias, Enrique – Urzi Bracanti, Cesira – Gomez Herrera, Estrella (2019): How to quantify what is not seen? Two proposals for measuring platform work. *JRC Working Papers Series on Labour, Education and Technology,* No. 1.

Riso, Sara (2019): *Digital Age: Mapping the Contours of the Platform Economy.* Dublin, Eurofound.

Pongratz, Hans J. (2018): Of crowds and talents: discursive constructions of global online labour. *New Technology, Work and Employment,* Vol. 33, No. 1. 58–73.

Sapir, Andre (2006): Globalization and the reform of European Social Models. *Journal of Common Market Studies (JCMS),* Vol. 44, No. 2. 369–390.

Sedláková, Mária (2018): *Industrial Relations and Social Dialogue in the Age of Collaborative Economy (IRSDACE), National Report: Slovakia.* Bratislava, Central European Labour Studies Institute (CELSI).

Szelényi, Iván – Wilk, Katarzyna (2010): Institutional Transformation in European Post-Communist Regimes. In Morgan, Glenn – Campbell, John L. – Crouch, Colin – Pedersen, Ove K. – Whitley, Richard eds.: *The Oxford Handbook of Comparative Institutional Analysis.* Oxford, Oxford University Press.

Thelen, Kathleen (2019): Regulating Uber: The politics of the platform economy – Public lecture by Kathleen Thelen. *STIAS: The Stellenbosch Institute for Advance Studies,* 27 March 2019. Source: https://stias.ac.za/2019/03/regulating-uber-the-politics-of-the-platform-economy-public-lecture-by-kathleen-thelen/ (Accessed: 22.05.2020.)

Valenduc, Gérard (2018): *Technological revolutions and societal transitions.* Brussels, ETUI Foresight Unit.

Visser, Jelle (2009): The Quality of Industrial Relations and the Lisbon Strategy. In Visser, Jelle ed.: *Industrial Relations in Europe 2008.* Luxembourg, Office for Official Publications of the European Communities. 45–72.

Warhurst, Chris – Hunt, Wil (2019): Digitisation of Future Work and Employment. Possible Impact and Policy Responses. *JRC Working Paper Series on Labour, Education and Technology,* No. 5.

Warhurst, Christopher – Erhel, Christine – Dhondt, Steven – Hamon-Cholet, Sylvie et al. (2019): *D2.1. Guidance paper on key concepts, issues and development of conceptual framework guide and working paper.* Technical Report.

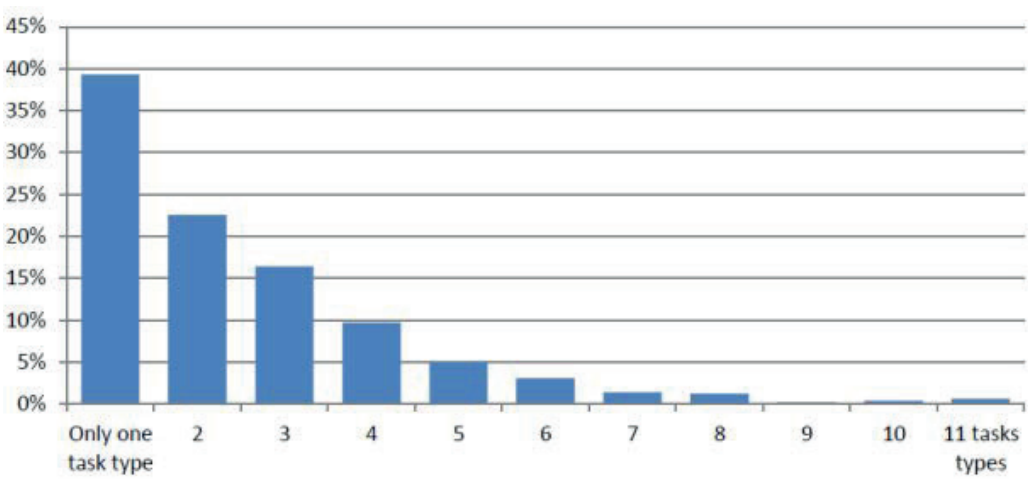
Warhurst, Christopher – Gallie, Duncan – Erhel, Christine – Guergoat-Larivière, Mathilde – Illéssy, Miklós – Makó, Csaba – Muñoz de Bustillo, Rafael – Wright, Sally (2017): Work Package 3: Integrative Framework and Analysis. In *Quality of Jobs and Innovation Generated Employment Outcomes.* Periodic Technical Report, QuInnE, No. 649497.

World Travel and Tourism Council (2018): *Economic Impact 2018: Hungary.* Source: https://turizmus.com/html/data/cikk/115/6991/cikk_1156991/WTTC_Hungary2018.pdf (Accessed: 22.05.2020.)

	I	II	III	IV	V	VI	VII	VIII
	1. Frequency		**2. Hours**		**3. Income**			
	% monthly or more	Estimate signif. frequency	10 or more hours pw	Estimate signif. hours	25% income or more	Estimate signif. income	*50% income or more*	*Estimate signif. income*
United Kingdom	82.5%	9.9%	56.1%	6.7%	71.0%	8.5%	*35.7%*	*4.3%*
Spain	80.5%	9.4%	56.7%	6.6%	52.1%	6.1%	*17.6%*	*2.0%*
Germany	78.3%	8.1%	63.1%	6.6%	62.8%	6.5%	*23.9%*	*2.5%*
Netherlands	89.1%	8.7%	55.0%	5.4%	66.8%	6.5%	*29.8%*	*2.9%*
Portugal	67.2%	7.1%	56.1%	6.0%	39.6%	4.2%	*15.4%*	*1.6%*
Italy	79.7%	7.1%	61.0%	5.4%	61.0%	5.4%	*20.4%*	*1.8%*
Lithuania	65.0%	5.9%	61.3%	5.6%	60.9%	5.6%	*17.7%*	*1.6%*
Romania	79.5%	6.4%	55.8%	4.5%	47.7%	3.8%	*9.7%*	*0.8%*
France	84.2%	5.9%	59.7%	4.2%	69.1%	4.8%	*25.8%*	*1.8%*
Croatia	64.3%	5.2%	63.9%	5.2%	36.6%	3.0%	*12.8%*	*1.0%*
Sweden	74.6%	5.3%	49.2%	3.5%	64.1%	4.6%	*23.0%*	*1.6%*
Hungary	74.8%	5.0%	62.0%	4.1%	52.7%	3.5%	*19.2%*	*1.3%*
Slovakia	73.4%	5.1%	39.6%	2.7%	53.5%	3.7%	*12.5%*	*0.9%*
Finland	68.7%	4.1%	48.9%	2.9%	54.4%	3.3%	*10.7%*	*0.6%*
Total	80.1%	7.7%	58.2%	5.6%	61.8%	6.0%	*24.0%*	*2.3%*

Annex 1. Frequency of use of and the estimated income generated by the platform work (2017)

Source: Pesole et al. 2019, 18 (COLLEEM dataset).



Annex 2. Number of task types performed by platform workers

Source: Pesole et al. 2019, 36 (COLLEEM dataset).

List of abbreviations used in the report

ASTREES	Association Travail Emploi Europe
CELSI	Central European Labour Studies Institute
COLLEEM	Collaborative Economy and Employment
CEE	Central and Eastern European Countries
EPSU	European Public Service Union
ETUC	European Trade Union Confederation
ETUI	European Trade Union Institute
FES	Friedrich Ebert Foundation
IRSDACE	Industrial Relations and Social Dialogue
IRES	Institut de Recherche Économique et Sociales
KKDSZ	Hungarian Union of Cultural Institutions and Public Collections Employees
MASZSZ	Hungarian Trade Union Confederation
NOVA FCSH	University Lisbon – Faculty of Social Sciences and Humanities
NGTT	National Economic and Social Council
OECD	Organisation for Economic Co-operation and Development
VoC	Variety of Capitalism

II. Kiberdiplomácia

VÁKÁT OLDAL

1. Bevezetés a kiberdiplomáciába

VÁKÁT OLDAL

Mártonffy Balázs[1]

Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták

„A kibertér és a hozzá kapcsolódó fogalmak esetében nem kérdéses, hogy […] távol állunk az együttműködéshez szükséges mértékű egységes értelmezéstől. Ez részben a »kiber« jelzővel jellemezhető fogalmi rendszer viszonylagos újdonságából, részben az általa leírt dolgok, jelenségek, objektumok napjainkban is tapasztalható változásaiból következik."[2]

Ahogy fentebb Dr. Munk Sándor, a Nemzeti Közszolgálati Egyetem egyetemi tanára is írja, a kibervilágban, és azon belül is a kiberdiplomácia világában, való hatékony navigációhoz 2020 derekán még nincs kellő munícióink. E fejezet ezen szeretne változtatni, vagy legalábbis iránymutatást adni az olvasónak, hogy az egyet nem értések és vitapontok területén el tudjon igazodni. Így e fejezet általános bevezetést nyújt a kiberdiplomácia, és részben a kiberbiztonság világába.

Írásom célja, hogy bemutassam, hogyan lehet a kiberdiplomáciát koncepcionálisan értelmezni, valamint hogy hogyan alkalmazzák a fogalmat a szakpolitikákban és a tudományos szaklapokban. Megjegyzendő, hogy a kiberdiplomácia viszonylag új fogalom a nemzetközi kapcsolatok világában. Valamivel elterjedtebb ugyan a médiában, de ott sokszor túl tág fogalomként,valamint pontatlan meghatározásokkal együttesen használják. Így e fejezetben fontos tisztázni néhány kulcsfontosságú kifejezést a kiberdiplomácia megismeréséhez és megértéséhez.

Amikor a kibervilág kérdéseire és különösen a kiberdiplomáciára gondolunk, kiemelten fontos az alapfogalmak tisztázása. Általánosságban elmondható, hogy a „kiber" előtag a számítógépes és az elektromágneses spektrumhoz kapcsolódó tevékenységekhez köthető dolgokra utal. Ezek a fogalmak magukba foglalják többek között a hálózatba kapcsolt számítógépeket, az internetet, valamint az intranetet, a mobil technológiákat, az optikai kábeleket és a szatelliten történő kommunikációkat is. Fontos ugyanakkor kiemelni, hogy a kibertérnek van egy fizikai infrastruktúra rétege is, amely alátámasztja a kiberteret. De ahogy Joseph Nye amerikai professzor is írja, a kibertér önmaga nem pusztán ez a fizikai infrastruktúra, hanem az infrastruktúra által létrehozott tér is.[3] A tér ez esetben a kibertér, a kiberdiplomácia helyszíne.

[1] A szerző szeretne köszönetet mondani Urbanovics Annának, a Nemzeti Közszolgálati Egyetem hallgatójának, a kutatómunkában nyújtott segítségért.

[2] Munk 2018.

[3] Nye 2008.

Alapfogalmak a kibervilágban

A kiber mint kifejezés a 21. században élőknek nem ismeretlen.[4] Így valószínűleg kötetünk olvasója is tisztában van azzal, hogy a kifejezés valamilyen módon a számítógépek kultúrájára, az információs technológiára és a virtuális valóságra utal. A kifejezést azonban gyakran összekeverik, vagy szinonímaként használják az e-, a virtuális és digitális kifejezéssekkel, pedig valójában mást értünk mindegyik alatt. Érdekes felvetés továbbá, hogy miért beszélünk például virtuális, elektronikus vagy digitális bűnözés helyett a kiberbűnözésről? Valamint érdemes megvizsgálni, hogy hogyan kapcsolódnak egymáshoz ezek a hasonló ámde különböző kifejezések. Érdemes feltenni azt a kérdést is, hogy miért épp *kiber*diplomáciáról beszélünk, valamint hogy pontosan mi a különbség a kiberdiplomácia és a digitális diplomácia között. Összességében tehát fontos különbséget tenni a szavak között, amit lejjebb egy rövid áttekintésben meg is teszek.

A „kiber" előtag etimológiája az ókori görög „kormányzás" szóhoz vezethető vissza, de a napjaink modern társadalmában használt fogalmat Norbert Weiner *Kibernetika* című könyvéhez tudjuk kötni.[5] A „kiber" előtag fokozott használata, nem meglepően, követi az internet elterjedését. A 21. század elején négy fogalmat különböztetünk meg egymástól, amelyek hasonló de mégis jól elválasztható témákra utalnak:

- a *kibernetika* és a *kiber* előtag elsősorban a biztonsági kérdésekre,
- az *e- vagy elektronikus* előtagok a gazdaság különböző területeire,
- a *digitális* szó leginkább a vállalati és az állami szektorra utal, illetve itt használják, míg végül
- a *virtuális* kifejezést, amely húsz évvel ezelőtt még szinte szinonímája volt a másik háromnak, mára gyakorlatilag elhagytuk a társfogalmak közül, és inkább más, *VR – virtuális valóság* alapú eszközökre és valóságokra utalva használjuk.

Mivel a kiber előtagról és a kiber fogalmakról mint a kiberdiplomáciában leginkább elterjedtekről sok szó fog esni még a fejezetben, így itt a másik hármat mutatom be. Az „e-" az „elektronikus" szó rövidítése. Először az e-kereskedelem elterjedése révén került be a mindennapi használatba, leginkább mint az interneten alapuló kereskedelem egyik első meghatározása. A kezdeti időszakokban, például az Európai Unió (EU) lisszaboni (2000) és az Egyesült Nemzetek Szervezete (ENSZ) által szponzorált Információs Társadalom Csúcstalálkozón (World Summit on the Information Society WSIS) közzétett nyilatkozatokban is (Geneva 2003; Tunis 2005) az e- volt a leggyakrabban használt előtag. Az Információs Társadalom Csúcstalálkozókon meghatározott feladatok és javaslatok olyan cselekvési irányokat adtak meg, amelyek az e-kormányzás, az e-üzlet, az e-tanulás, az e-egészségügy, az e-foglalkoztatás, az e-mezőgazdaság és az e-tudomány területeinszerettek volna haladást elérni. Az e-diplomácia fogalmát nemzetközi szinten

[4] Jelenleg magyarul mind a kiber, mind a kíber előtagok, rövid, illetve hosszú í-vel, is elfogadott. Itt konzekvensen a kiber-t, rövid i-vel, használom.

[5] Weiner 1961.

2007 óta használjuk, amikor a svéd diplomácia felállította az első „virtuális" e-nagykövetségeket."[6] A kezdeti lelkesedés ellenére mára már az e- mint jelző egyre kisebb mértékben van jelen. Nemrégiben még az Európai Unió is elkezdett felhagyni az e-vel mint előtag használatával. Egyes értelmezések szerint ez azzal is magyarázható, hogy távolodni a próbáljon a lisszaboni menetrend kudarcától.

A digitális előtag az „1" és „0" -ra utal. A nulla és az egyes a számítógépes kódok alapjaiként, azok a számjegyek, amelyek mint bináris változók az egész internetes világ alapját képezik. A múltban a digitális előtagot, a digitális technika leírása mellett, főként a nemzetközi fejlesztési körökben használták, leginkább is a „digitális szakadék" ábrázolásaként. Az elmúlt néhány évben a digitalizálás nevű folyamat megkezdte az internet nyelvének meghódítását is, és beépült az Európai Unió által használt dokumentumokba és stratégiákba. Itt a konkrét, kódokkal leírt legközelebb álló fogalmakra gondolunk alapvetően.

Végezetül a virtuális szó leginkább az internet immateriális, nem-fizikai valóságához vagy természetéhez kapcsolódik. A virtuális valóság lehet immateriális valóság (valami, amit nem lehet megérinteni) és olyan valóság is, amely nem létezik (hamis valóság). A virtuális szó, illetve előtag, leginkább is a fent említett többértelmű jelentése miatt, ritkán jelenik meg a politikai nyelvben és a nemzetközi dokumentumokban, így a kiberdiplomácia világában is elenyésző szerepet játszik.

A „kiber" fogalom a legszélesebb kategóriát képviseli az előtagok között, és a leghasznosabb a kiberdiplomácia világában való eligazodáshoz is. Tudjuk, hogy a diplomácia az államok egymással fenntartott kapcsolatainak gyakorlata, a nemzetközi jogban meghatározott alanyok külkapcsolatainak békés módon és mindenekelőtt tárgyalásos úton történő rendezése. Itt leginkább is államokról és nemzetközi szervezetekről beszélünk. A kiberdiplomácia tehát, alapjaiban véve, a kibervilágban folytatott diplomáciaként is értelmezhető lenne, de ez természetesen bonyolultabb.

A kiberdiplomácia meghatározása

A kiberdiplomácia fogalmának hatékony megismeréséhez érdemes rövid kitérőt tenni a hagyományos diplomácia világába. Mint ismeretes, a diplomáciát folytató legfőbb szereplők az államok, valamint a nemzetközi intézmények. Az államok a nemzetközi rendszer elsődleges alanyai, amelyek lakossággal és területtel, az erőszak legitim monopóliumával, valamint belső és külső legitimitással rendelkeznek. Az államok központi szerepet játszanak mind a nemzetközi kapcsolatokban, mind a tudományági megfelelőjükben, a nemzetközi kapcsolatok elméletében is. A diplomácia a nemzeti hatalom és érdek nemzetközi kapcsolatokban való érvényesítése, békés eszközökkel.

A kiberdiplomácia fogalma, valamint pontos tudományos meghatározása még mindig vitatott. Eléggé új fogalomról van szó, amely leginkább az angolszász akadémiai világban jelenik meg, és mint a világ egyik vezető kiberhatalma, az Egyesült Államok tudományos

[6] Molnár 2019.

világában. Emellett neves egyesült királyságbéli egyetemek is foglalkoznak a kutatásával. De mindkét akadémiai világban a szakirodalom a legtöbb esetben csak érintőlegesen foglalkozik a kiberdiplomáciával, és leginkább is a kiberbiztonság és a kiberhadviselés egyik mellékvonalaként tekint rá.

Ha viszont önálló, konkrétan a kiberdiplomáciával foglalkozó cikket keresünk, akkor leginkább említésre méltó a *Kiberdiplomácia: a nemzetközi társadalom kialakítása a digitális korban* című tanulmány.[7] A szerzők azt állítják, hogy a kiberdiplomácia „növekvő fontossága ellenére továbbra is perifériás kérdés a nemzetközi kapcsolatok irodalmában", valamint kiemelik, hogy a kibernetikus események, köztük a kibertámadások a médiában sokkal nagyobb hangsúlyt kaptak, mint a kiberdiplomácia.

A fentiek alapján a kiberdiplomácia úgy definiálható, mint *egy adott állam egyedül vagy több állammal együttesen véghezvitt olyan cselekedeteinek összesége, amelyek külpolitikai célokat és érdekeket szándékoznak érvényesíteni a kibertérben, erősen támaszkodva az információ, az információkommunikáció és a számítógépek felhasználási területeire.*

Kiberdiplomácia kontra digitális diplomácia

A kiberdiplomáciát fontos elválasztani egy másik, hasonló fogalomtól, a digitális diplomáciától. Ugyan már utaltam a digitális, az „e-" a virtuális és a kiber fogalmak közötti különbségekre, de fontos megkülönböztetés, hogy a kiberdiplomácia nem egyezik a digitális vagy az e-diplomáciával. Bár hasonló részekből állnak össze, eltérő fogalmakat írnak le. A digitális diplomáciát és az e-diplomáciát viszont egymáshoz hasonló fogalomként használják, azonban mindkettő markánsan különbözik a kiberdiplomáciától.

Amíg a kiberdiplomácia a kibertérben alkotott külpolitikához köthető, a kibertér irányítására tett kísérleteket fedi le, addig a *digitális diplomácia konkrét diplomáciai cselekedetek takar a kibertérben*. Előbbire példa egy, az internet szabályozásáról szóló nemzetközi egyezmény tárgyalásához a nemzeti álláspont kidolgozása és képviselete tárgyalásos úton, míg utóbbira egy twitter üzenet, amelyen egy ország külügyminisztériuma üdvözli például Észak-Macedónia csatlakozását a NATO-hoz. Pontosabban tehát a digitális diplomácia vagy e-diplomácia az információkommunikáció technológiai eszközök és módszerek közvetlen alkalmazása a diplomácia és a külpolitika területén. A kiberdiplomácia azonban a konfliktuskezelést, a kibertér körüli megállapodásokat jelenti, és az ezzel kapcsolatos politikára utal. Ugyan a digitális és az e-diplomáciát eddig szinonímaként kezeltem, egy másik megközelítés szerint az e-diplomácia fogalmához képest a „digitális diplomácia fogalma szűkebb, alatta elsősorban a közösségi média eszközeit, a Facebookot és a Twittert értik."[8]

[7] Barrinha-Renard 2017.
[8] Molnár 2019.

A kiberdiplomácia állami megközelítései

Mint általában a politikában, a kibertér rendezésére tett javaslatokban sincs konszenzus az államok és a részes szereplők között. Nincs egyetértés továbbá abban sem, hogy a kiberteret hogyan, illetve kell-e egyáltalán, irányítani, illetve szabályozni. Ezek viszont olyan meghatározó kérdések, amelyek átfogják a kiberdiplomáciai kezdeményezéseket, és rendezésük nélkül nem, vagy csak nagyon keveset, tud a kiberdiplomáciai tér előre haladni.

Az államok, a versengés mellett, már hosszú évek óta egyeztetnek a kibertérben érvényes nemzetközi jogról és viselkedési normákról, viszont alapvető különbségek vannak az álláspontok között. Az USA, az Európai Unió, illetve a NATO és tagállamai a kibertér szabad, demokratikus jogállami és biztonságos működését alapvető értéknek és érdeknek tekintik. Ehhez csatlakoznak a hasonló értékrendű és gondolkodású országok. Az úgynevezett nyugati közösség szerint a kibertér szabadságának és biztonságának szavatolása a nemzetek, kormányzatok, a tudományos és a civil szféra közös felelősségvállalásán valósulhat meg, és a többszereplős modellt tartják fontosnak. Nyugati megközelítésben a nemzetközi jognak teljes mértékben érvényesülnie kell a kibertérben, beleértve a nemzetközi humanitárius jogot és az önvédelemhez való jogot is.

A nyugati felfogással szemben Kína, Oroszország és több fejlődő ország az államok tradicionális szuverenitásának a kibertérre történő kiterjesztését támogatja, és ellenzik a közös szerepvállalást. Ezek az államok alapvetően inkább kormányközi modell alapján képzelik el az internetszabályozást. Sok helyen eltér a véleményük a nyugati csoporttól, például ezen államok szerint a kibertérre nem lehet érvényesnek tartani a hadviselésre vonatkozó nemzetközi jogot.

Persze államok nem csupán egyedül, önmagukban tudnak kiberdiplomáciát folytatni. Különböző csoportosulások, bilaterális vagy multilaterális formációk vagy szövetségi rendszerek keretében is lehet hasonló tevékenységet folytatni, attól függően, hogy melyiknek milyen hozadékát vélik a felek felfedezni. A szabályalapú többnemzeti megközelítés egyik példájaként a NATO-tagállamok elfogadták a *Tallinni kézikönyvet*, amely a kibertérben használandó irányelveket fektet le nemzetek és más, nem nemzeti szereplők számára. A *Tallinni kézikönyv* és több, más konkrét lépés miatt a NATO-ról, illetve a tagállamairól elmondható, hogy támogatják a kibertér nemzetek felett álló szabályozását. Az SCO (a Sanghaji Együttműködési Szervezete) országai viszont alapvetően eltérő megközelítést képviselnek. Ezen országok csoportja, köztük Kína és Oroszország, a szuverenitás fontosságát hangsúlyozzák a kibertérben, és csak olyan szabályozást támogatnak, ami a nemzeti szuverenitás alatt helyezkedik el. A két megközelítés szögesen ellentmond egymásnak, emiatt a kibertérben nem pusztán kiberdiplomáciának leszünk tanúi, hanem kibertámadásoknak és, amennyiben a helyzet eszkalálódik, akár kiberháborúnak is.

A kibervilághoz kötethő fogalmak a nemzetközi kapcsolatok szakirodalmában

A kiberhez köthető előtagok, valamint a kiberdiplomácia fogalmainak pontos meghatározása után érdemes a többi, a kiberdiplomáciához köthető fogalmat is megvizsgálni. A két leginkább elterjedt fogalom a kibertér és a kiberbiztonság. A kibertér meghatározásában sincs ugyan egyetértés, de összeségben azért elmondható, hogy a „meghatározások túlnyomó többségében három értelmezéssel találkozhatunk: a kibertér egy sajátos (képzeletbeli, virtuális) környezet; a kibertér egy tartomány; a kibertér egy hálózat."[9] Nézzük továbbá, hogy mi az a kiberbiztonság! Krasznay szerint a kiberbiztonság: „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek azért, hogy a társadalmi és gazdasági folyamatok zavartalanul működhessenek, a kibertérben lévő kockázatok elfogadható szintjét hivatott biztosítani, ezáltal pedig megcélozni a kibertér megbízható környezetté alakulását."[10] Itt megemlítendő, hogy a kiberbiztonság fogalmát érdemes külön választani az információs biztonság fogalmától is, amely az informatikai rendszerek olyan állapota, amelyben a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása biztosított.

A következő fontos, vizsgálatra érdmes fogalom a kiberháború. Mint a hagyományos diplomáciát a háborútól, úgy a kiberdiplomáciát a kiberháborútól sem lehet vegytisztán és könnyedén elválasztani, sőt, a két párhuzamos fogalom között sok hasonlóságot lehet felfedezni. A kiberháború kutatásánál is kiemelten fontos kérdés természetesen az, hogy a kiberháború hagyományos értelemben vett háborúnak tekinthető-e. Mint a legtöbb tudományos vitában, ebben a viszonylag egyszerűnek tűnő kérdésben sincs egyetértés. Az egyik oldal kiáll amellett, hogy a kiberháború megfelel a hagyományos értelemben vett háború követelményeinek, míg a másik oldal szerint ez semmiképpen se igaz, és a kiberháború fogalmát új alapokra kell helyezni.

Az első oldal ékes példájaként Stone amerikai professzor szerint a kiberháború is megfelel a tradicionális értelemben vett háború fogalmának.[11] A kibervilág egy másik tudományos szaktekintélyének számító Joseph Nye is egyetért Stone-al. Nye szerint a kiberháború leghasznosabb meghatározása a következő: „olyan ellenséges cselekedetek a kibertérben, amelyek hatása legalábbis egyenértékű a jelentős kinetikus erőszakkal."[12]

Itt viszont el is értünk a kiberháború legfontosabb gyakorlati kérdéshez, amely szerint a kiberteret mint virtuális világot és az őt alátámasztó infrastruktúrát érő támadásokat valamilyen módon kezelni kell. A nehézség abban rejlik, hogy ezeket egyszerre kell tudni egyben kezelni, valamint különválasztani, mivel a kibertámadások két különválasztható hatást válthatnak ki, és két külön térben tehetnek kárt: a kibertérben és a kiberteret alátámasztó fizikai infrastruktúrában.

[9] Krasznay 2018.
[10] Krasznay 2018.
[11] Stone 2013.
[12] Nye 2017.

Amikor a kibertámadások pusztán más számítógépes rendszerek kiiktatását érik el, illetve abban okoznak kárt, például amikor egy hacker leállít egy kormányzati honlapot DDoS támadással (Distributed Denial of Service, tehát elosztott szolgáltatásmegtagadással járó támadások), akkor a helyzet egyértelmű: csak a kibertérben esik kár. Viszont egyes kibertámadásoknak konkrét kinetikus következményei is lehetnek. Ha a kibertámadás egy nukleáris reaktor vezérlőprogramját támadja meg és állítja le, akkor a nukleáris reaktorban leállás következhet be, ami akár Csernobil szintű katasztrófához is vezethet. Ebből már egyértelműen látszik, hogy a kibertámadás kifejezés a tevékenységek széles skáláját öleli fel, kezdve az egyszerű próbáktól a webhelyek megtévesztéséig, a szolgáltatásmegtagadásig, a kémkedésig és a pusztításig.

A kiberháború és a kibertámadások így alapvetően különböznek a tradicionális támadásoktól. Hasonlóképpen a hagyományos diplomáciától is valamelyest eltér a kiberdiplomácia. Két fontos különbséget kell tenni. Az első fontos különbség, hogy a kiberdiplomácia eszközei, részei, valamint egyedei alkotóelemei nem köthetőek egyértelmű földrajzi helyhez. Ez szembe megy a hagyományos diplomácia eszközeivel, ahol a territorialitás kifejezetten fontos alapeleme az interakciónak. Egy állam egy másik államban a saját képviseletét rendkívüli és meghatalmazott nagyköveteken keresztül látja el, amelyeket az 1961. évi diplomáciai kapcsolatokról szóló bécsi egyezményként ismert nemzetközi szerződés egyértelműen szabályoz. A kiberdiplomácia világában a határvonalak nem konkrétak, és gyakran fel sem lelhetők, mivel a kibertérben gyakran a kezdeményező egyén, a cselekvést lefolytató számítógép, és a végpont akár más és más kontinensen található.

A második fontos különbség a cselekvés és a cselekvést véghez vivő egyén közötti kapcsolatban található. A hagyományos diplomáciában egyértelmű a hierarchiai rend: egy küldő ország fogadó államban akkreditált nagykövete képviseli a küldő államot, és a nagykövet cselekedetei a küldő állam jóváhagyásával, úgynevezett mandátumával bírnak. A kiberdiplomáciában és az internetes világban viszont ez sokkal komplikáltabb. Itt az attribúció, vagyis a hiteles hozzárendelés gyakori hiánya komoly problémákat vet fel. A számítógépes eseményeknek ugyan vannak világos végpontjai, ahol akár fellelhető a támadás, de kiindulási pontja gyakran nem egyértelmű és könnyedén elbújtatható.

Konkrét példa az attribúciós problémra: vegyünk egy DDoS kibertámadást. A támadás végpontjai egyértelműen megállapíthatók, mivel elég megkeresni, melyek azok a webhelyek vagy website-ok, amelyek leálltak, illetve ezek melyik számítógépekhez tartoznak. De a támadás eredete sokkal összetettebb kérdés. Sok esetben lehetetlen 100% bizonyossággal meghatározni, hogy honnan indult a támadás mivel a forrás könnyen bújtatható. Szakértők a különbséget bemutatva úgy fogalmaznak, hogy míg a hagyományos világban például egy rakéta egyértelműen rendelkezik viszont-válasz-címmel (megvizsgálható a röppályából és a technikai adatokból, hogy honnan lőtték ki), addig egy számítógépes botnet általában nem rendelkezik ilyennel. A támadó azonosításához szükséges munka hónapokat vehet igénybe, és egyáltalán nem biztos, hogy a támadó azonosítása minden esetben lehetséges. Például a 2010. évi Stuxnet-támadás megkérdőjelezhetetlen attribúció kérdése mindmáig alapvetően bizonytalan. Bár

általános egyetértés van abban, hogy az Egyesült Államok és Izraeli közös művelete volt, azonban amíg a két állam ezt el nem ismeri hivatalosan, nem lehet minden kétséget kizáróan őket okolni a támadásért.

Elmondható, hogy a kiberdiplomácia olyan térben működik, amely gyökeresen eltér a hagyományos diplomácia világától. A kibertérben nincsenek földrajzi korlátozások és számos esetben gyakorlatilag nincs hiteles attribúcióra lehetőség, pedig mind a két szempont a hagyományos diplomácia elméleti és gyakorlati sarokköveit képezi. Szinte minden tudós egyetértett ezekben a különbségekben, de hogy ezeknek mekkora szerepe van, illetve hogy milyen mértékben befolyásolják a kiberdiplomáciát és annak megvalósítását, arról nincs egyetértés.

A kiberdiplomácia célja: a hatalom, reciprocitás és normák szerepe

A kiberdiplomácia meghatározása, illetve az állami szereplők feladatköre mellett fontos értelmezési kérdés, hogy milyen célt szolgál a kiberdiplomácia. Természetesen ez a kérdés is tudományos viták tárgyát képezi, viszont abból a szempontból hasznos elméleti megközelítés, hogy segít rendezni a szakirodalmat az érdeklődő részére. A kiberdiplomáciáról szóló szakirodalmat három nagy kategóriába lehet sorolni attól függően, hogy az író és a kutató a nemzetközi kapcsolatok elméletéről melyik nagy „iskola" mentén gondolkodik.

Az első csoport a kiberdiplomáciának a hatalommal való összekapcsolódását tartja a legfontosabbnak. A második nagy csoport a reciprocitást és a kölcsönösséget helyezi előtérbe, sokszor a törvényre és a jogi szerződésekre való fókuszálással. Végezetül a harmadik nagy csoport pedig a normákhoz és viselkedési mintákhoz fűződő kapcsolatokat tartja legfontosabbnak a kiberdiplomáciában. A nemzetközi kapcsolatok elméletében ezek a csoportok a realizmust, a liberalizmust és a konstruktivizmust követik le.

Így a nemzetközi kapcsolatokban a háború és béke kérdéseire is, a kibervilág rendezésére, illetve a kiberdiplomáciában is ezt a három fő megközelítési módot különböztetjük meg. A megközelítések a hatalomra, a reciprocitásra vagy a normákra helyezik a hangsúlyt, viszont kritikus kérdés lesz, hogy melyik gondolkodásmód fog az államok közötti kapcsolatokban leginkább elterjedni, és hogy sikerül-e az államoknak és a kibertérben szerepet vállaló cselekvőknek egyetértésre jutni.

A realista megközelítésnél a szerzők elsősorban úgy gondolkodnak, hogy a kiberdiplomácia pusztán kiegészítése a háborúnak. A kiberdiplomáciat a szerzők szerint leginkább a katonai erőfeszítésekkel való összefüggésben lehet megérteni. Ez a csoport a kiberdiplomáciára egyszerűen úgy tekint, mint az államok nemzeti érdekeik, saját szuverenitásuk és a túlélésük megvédése érdekében tett lépések összességére.

A kiberdiplomácia realista megközelítése olyan tradicionális témákra összpontosít, mint a katonai hatalom és a gazdasági erő. Ezek olyan gondolati elemek, amelyek máshol is jelen vannak a realista irodalomban. A hatalom szerepe ezen szerzők szerint kiemelkedően fontos a kiberdiplomácia világában, és a hatalom felhasználásának legfontosabb formái a katonai erőforrások és eszközök. A realista írók a kiberdiplomáciát az erőszak-

használat kiegészítéseként határozzák meg. Ők kutatásaik során különös tekintettel vannak a kiberelrettentés, a kibervédelem és a kiberkényszerítés fogalmaira, a kiberdiplomáciát hasonlónak tartják a nukleáris diplomáciához.

Egy másik megközelítés, a liberalizmus és a liberális megközelítés, középpontjában a reciprocitás, a kölcsönös függőség, a nemzetközi szervezetek, valamint az állami szereplők viszonossága és a jogi szerződések állnak. Ez a fajta szakirodalom a katonai erő helyett a kiberdiplomácia központi szerepét hangsúlyozza a kibertér szabályozásának és a kiberbiztonság növelésének érdekében. Itt az irodalom a liberalizmus alapvető gondolataihoz tér vissza: a kölcsönös gazdasági függőséghez, a nemzetközi szervezetek szerepéhez, valamint a demokratikus békeelmélethez.

A kiberdiplomácia megközelítéseinek harmadik és egyben utolsó nagy csoportja a nemzetközi kapcsolatok elméletének úgynevezett konstruktivista megközelítésébe sorolható. Ezek az elméleti munkák a társadalmi fogalmi konstrukciók, az identitás és a normák fontosságát hangsúlyozzák a kiberdiplomácia és a kibertér vizsgálatánál. Itt a tudományos munkák elsősorban nem magukra az internetes támadásokra vagy eseményekre összpontosítanak, hanem inkább megpróbálják kitalálni, miért fordulnak elő a támadások vagy események. A szerzők itt például arra kíváncsiak, hogy a normáknak van-e szerepe abban, hogy növekszik vagy csökken a kibertámadások gyakorisága. E megközelítés szerint a kibertérben ugyanúgy, mint a nemzetközi kapcsolatok más területein is, vannak normák, amelyek meghatározzák az egyes államok viselkedését, de a normák hatása államonként jelentősen eltér. A nem kormányzati szervezetek, a civil társadalom és az egyének ennél a megközelítésnél játsszák a legnagyobb szerepet. Ezek az írók azt állítják, hogy a normák az állami viselkedés legfontosabb mozgatórugói.

Ez a három megközelítés a kiberdiplomácia értelmezésénél nagymértékben eltér egymástól. Ez az eltérés ugyan az államok közötti viselkedés leírására utal, ugyanakkor a napi politikában is komoly szerepet játszik, mivel a kiberdiplomácia szerepét kutatjuk a kibertérben. Ha a realista megközelítés érvényesül, akkor az államok egyfajta „kiber Vadnyugat"-szerű rendszerben fognak tevékenykedni, és nemzetközi kontroll nélkül, alapvetően önerőre támaszkodva igyekeznek majd nemzeti érdekeiket érvényesíteni. A liberális megközelítés már egy másik, nemzetközi jogra és hozzá kapcsolódó intézményekre épülő kiberdiplomáciai világot feltételez: az államok jól rendezett jogi szerepek között folytatnak kiberdiplomáciát, ahol nemzetközi szerződések határolják be a szerepköröket. A vitás ügyekben nem az erő, hanem a jog, és valamilyen nemzetközi „kiberbíróság" lehet majd a mérvadó. A konstruktivista megközelítés szerint pedig alapvetően nem a jogi környezet vagy a nemzetközi szervezet megléte vagy hiánya fogja leginkább meghatározni az államok viselkedését és a kiberdiplomáciát, hanem hogy milyen viselkedésminták vagy normák terjednek el leginkább az államok között.

Egyes Államok megközelítései besorolhatók a három iskola valamelyikébe. Például az Egyesült Államok republikánus vezetés alatt realista, demokrata alatt pedig inkább liberális hozzáállást mutat. Más államok, például Oroszország, aki Kínával és a Sanghaji Együttműködési Szervezet többi tagjával együtt továbbra is támogatja egy ENSZ-alapú széles körű szerződés megkötését, de csak olyan módon, hogy ne lehessen a nemzeti

jogköröket csorbítani, konzekvensen realista. Mivel nincs egyetértés a világ nagyhatalmai között, várhatóan kiemelt szerep fog hárulni az egyetlen globális nemzetközi szervezetre, az ENSZ-re a kiberdiplomáciában.

Kiberdiplomácia és az ENSZ

Az Egyesült Nemzetek Szervezete nemzetközi szervezet, amelyet 1945-ben, a második világháború után, alapított 51 ország a nemzetközi béke és biztonság, a nemzetek közötti baráti kapcsolat fejlesztése és a társadalmi fejlődés, valamint a jobb életszínvonal és az emberi jogok elősegítése céljából.[13] Az ENSZ-nek két fő szerve játszik kiemelt szerepet a kiberdiplomáciában. Az egyik a Biztonsági Tanács, a másik pedig az ENSZ Főtitkára és az általa vezetett Nemzetközi Titkárság.[14]

Az ENSZ Biztonsági Tanácsában a kiberdiplomáciai kérdések egészen 1998-ig nyúlnak vissza. Ekkor Oroszország mint állandó ENSZ BT-tag, a testület történetében először az elektronikus és információs fegyverek betiltására nyújtott be javaslatot. A másik fő szereplő, az ENSZ főtitkára, a tagállamoktól független tevékenységet is végez. A főtitkár létrehozott egy kormányzati szakértői csoportot (UNGGE – United Nations Group of Government Experts, az Egyesült Nemzetek Kormányzati Szakértő csoportja), amely 2004 óta ülésezik, valamint jelenleg ülésezik egy OEWG (open ended working group, nyílt végű munkacsoport), amely a témát sokszor mélyrehatóan tárgyalja. Mindkét csoport létezése és működése azt jelzi, hogy bár sok rendezetlen kérdés van, az ENSZ mint fórum továbbra is megmaradt a vitás pontok rendezésére tett első kísérlet helyszínének.

Rövid bevezetés Magyarország kiberdiplomáciájába

Végezetül a fejezet nem lenne teljes legalább egy kis magyar kiberdiplomáciai kitekintés nélkül. Sokszereplős a téma, de kijelenthető, hogy a jelenleg hatályos magyar kiberdiplomácia sarokkövét a 2020-as Nemzeti Biztonsági Stratégiában találjuk. Ugyan 2012-ban már készült egy Nemzeti Biztonsági Stratégia, a körülmények, a nemzetközi rendszer és a magyar külpolitika változásai megkövetelték, hogy idén új stratégiát adjon ki a kormány. 2013-ban továbbá készült egy Nemzeti Kibervédelmi Stratégia is, de mindkettőt felülírni látszik az idén tavasszal kiadott új Nemzeti Biztonsági Stratégia. A Stratégia leginkább idevágó cikkelyei a 31-es, 32-es és a 48-as.

A 31. cikkely egyértelműen a kibervédelemmel foglalkozik, és a honvédelmi tárcához rendeli a felelősséget a magyar kormányzaton belül. Itt kibertámadások elhárításáról van szó, és a Stratégia összeköti a hibrid, valamint a kiber és kinetikus komponenseket egyszerre tartalmazó támadásokat.

Hibrid támadással szembeni ellenálló képességünket növeli a nemzet egysége, demokráciánk szilárdsága, a közös nyelv, a felgyorsított döntéshozatali képesség, valamint

[13] ENSZ 2020.
[14] Ibid.

a honvédelmi és rendvédelmi erők szoros együttműködése egymással és a releváns polgári infrastruktúrával. Az új biztonsági kihívások miatt azonban folyamatosan szükséges fejleszteni az információs és kiberhadviselés elleni védekezés rendszerét. [15]

A 32. cikkely az információs biztonságról szól, és megnevezi azt mint a kiberbiztonság egyik alapkövét.

Magyarország Kormánya mindent megtesz hazánk kiberbiztonsága érdekében, kapacitásainkat e területen is folyamatosan fejlesztjük. Tekintettel arra, hogy a kormányzati és más kulcsfontosságú infokommunikációs rendszerek elleni támadások száma növekszik és kifinomultságuk erősödik, folyamatos erőfeszítés szükséges az infokommunikációs rendszerek védelmének erősítése érdekében. Általános jelenség továbbá a felhasználók információbiztonsági tudatosságának alacsony szintje, holott a felhasználók megfelelő információbiztonsági tudatossága a kiberincidensek megelőzésének egyik kulcseleme.[16]

Végül a 48. cikkelyben találjuk meg leginkább annak az elméleti leírásnak a vonatkozó, releváns értelmezését, amelyet a fenti vonatkozásban kifejtettem. Itt a Stratégiában a kibertér mint globális közjó van feltüntetve, amiért verseny folyik. Az 5G technológiáért folyó küzdelem pedig jól mutatja a kiberdiplomáciát a gyakorlatban: hogy melyik nagyvállalat telepíti ezt a technologiát egyes országokba, például az Ericsson vagy a Huaweii, elköteleződést mutat az egyes országok között, és a nem egyeztetett vagy egyoldalú lépések komoly feszültségeket is kelthetnek a szövetségi rendszereken belül, mint például a NATO-ban.

A hatalmi vetélkedés mindinkább kiterjed a globális közjavakra is: fokozódó küzdelem folyik a nemzetközi vizek és az ott található erőforrások, az Északi-sarkvidék és a világűr ellenőrzéséért, valamint a kibertér dominanciájáért. Az emberiség technológiai szintjének rohamos fejlődésével (digitalizáció, ötödik generációs vezeték nélküli hálózat [5G], űrtechnológia stb.) folyamatosan új lehetőségek és kihívások jelennek meg, amelyek hatást gyakorolnak hazánk biztonságára. Az 5G jelentette technológia olyan forradalmi fejlesztéseket tehet lehetővé perspektivikusan, amelyek számottevő változásokat generálhatnak társadalmunk és gazdaságunk viszonylatában.[17]

Fontos még kiemelni, hogy a Nemzeti Biztonsági Stratégia szerint *Kiemelt Biztonsági Kockázatot* képeznek a „jelentős károkat okozó kibertámadások a kormányzati informatikai rendszerek, a -közigazgatás, a közműszolgáltatók, a stratégiai vállalatok, a létfontosságú infrastruktúra egyéb elemei és más, a társadalom működésében fontos szervezetek számítógépes hálózatai ellen."[18]

A stratégia mellett több szereplő foglalkozik valamilyen módon a kibertérrel és a kiberbiztonsággal Magyarországon, de a kiberdiplomáciához leginkább a Külgazdasági és Külügyminisztérium, valamint a Honvédelmi Minisztérium releváns egységei

[15] Nemzeti Biztonsági Stratégia 2020. 31. cikk:
[16] Nemzeti Biztonsági Stratégia 2020. 32. cikk:
[17] Nemzeti Biztonsági Stratégia 2020. 48. cikk:
[18] Nemzeti Biztonsági Stratégia 2020.

köthetőek. A Külgazdasági és Külügyminisztérium kibertér koordinátora a következő feladatokat látja el:

„Koordinálja a kibertérrel kapcsolatos feladatok minisztériumon belüli végrehajtását, feladatkörében képviseli a minisztériumot a Nemzeti Kiberbiztonsági Koordinációs Tanácsban, és más hazai egyeztetési fórumokon, valamint kapcsolatot tart az illetékes minisztériumokkal, egyéb szervezetekkel és a kibertérrel foglalkozó nemzetközi szervezetekkel, valamint részt vesz a kibertérrel kapcsolatos magyar álláspont kidolgozásában, és gondoskodik annak összehangolt képviseletéről a bilaterális és multilaterális kapcsolatokban, tárgyalási folyamatokban és fórumokon, és végezetül pedig segíti a kiberbiztonsággal foglalkozó magyar cégek külföldi tevékenységét."[19]

A Honvédelmi Minisztérium alatt pedig a Magyar Honvédségnek „kibervédelmi központja" jött létre 2019-ben. A HM felügyelete alatt „a kibertérben jelentkező fenyegetések elhárításához naprakész, magas színvonalú oktatásra van szükség. E képzést a katonák számára a Magyar Honvédség Kiber Képzési Központja biztosítja majd".[20] Benkő Tibor honvédelmi miniszter szerint pedig „a kibertérben alkalmazott megtévesztő információk, zavaró tényezők, blokkoló rendszerek a hibrid hadviselés révén nemcsak a műveleti feladatok végrehajtására hathatnak ki, de békeidőben az állami működésre is. Ennek oka, hogy napjainkban már minden elektronikus formában, számítógépeken keresztül működik az orvosi ellátástól a közlekedésen át egészen az adatok nyilvántartásáig. A fenyegetések elleni védekezésre fel kell készülni, ehhez pedig megfelelő oktatási és kiképzési rendszerre van szükség."[21] Itt fellelhető a két tárca közötti megközelítésbéli különbség. Míg a kibertér koordinátornál a diplomáciára helyezik a hangsúlyt, a honvédelmi tárcánál már egyértelműen fellelhetők a védelmi vonatkozású megközelítések, amelyek a tárcára és a honvédelmi meglátásokra egyaránt jellemzőek.

Felhasznált irodalom

Barrinha, André – Renard, Thomas (2017): Cyber-diplomacy: the making of an international society in the digital age. *Journal of Global Affairs*, 3(4–5), 353–364.

Barnard-Wills, David – Ashenden, Debi (2012): Securing virtual space: Cyber war, Cyber terror, and risk. *Space and Culture* 15(2), 110–123.

Betts, Richard K. (2002): The Soft Underbelly of American Primacy: Tactical Advantages of Terror. *Political Science Quarterly*, Vol. 117, No. 1. 19–36.

Buchan, Russel (2012): Cyber attacks: Unlawful uses of force or prohibited interventions? *Journal of Conflict and Security Law,* Volume 17, Issue 2, 211–227.

Clark, Richard A. – Knake, Robert K. (2010): Cyber War: The Next Threat to National Security and What to Do About It. New York, HarperCollins.

[19] 17/2018. (VI. 11.) KKM utasítás a Külgazdasági és Külügyminisztérium Szervezeti és Működési Szabályzatáról.

[20] Honvedelem.hu 2019.

[21] Honvédelem.hu 2019.

DE BRUIJN, Hans – JANSSEN, Marijn (2017): Building Cyber security Awareness: The need for evidence-based framing strategies. *Government Information Quarterly* Volume 34, Issue 1. 1–7.

DENNING, Dorothy E. (2013): Framework and principles for active Cyber defense. *Computers and Security,* Volume 40. 108–113.

Department of State of the United States. Office of the Coordinator for Cyber Issues. Forrás: www.state.gov/bureaus-offices/bureaus-and-offices-reporting-directly-to-the-secretary/office-of-the-coordinator-for-kíber-issues/ (A letöltés dátuma: 2020. 04. 01.)

DINSTEIN, Yoram (2012): The principle of distinction and Cyber war in international armed conflicts. *Journal of Conflict and Security Law,* Volume 17 Issue 2. 261–277.

ELLIOTT, David (2011): Deterring strategic Cyber attack. *IEEE Security and Privacy.* Volume 9 Issue 5. 36–40.

ENSZ. Általános Információ az ENSZről. Elérhető: www.unis.unvienna.org/unis/hu/topics/un-general.html# (A letöltés dátuma: 2020. 06. 01.)

FARWELL, James P. – ROHOZINSKI, Rafael (2011): Stuxnet and the future of cyber war. *Survival* Volume 53 Issue 1. 23–40.

GEERS, Kenneth (2010): The challenge of Cyber attack deterrence. *Computer Law and Security Review* Volume 26, Issue 3. 298–303.

HONVÉDELEM.HU (2019). Átadták a Magyar Honvédség Kiber Képzési Központját. 2019. június 13. Forrás: www.kormany.hu/hu/honvedelmi-miniszterium/hirek/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat (A letöltés dátuma: 2020. 06. 01.)

JUNIO, Timothy J. (2013): How Probable is Cyber War? Bringing IR Theory Back In to the Kíber Conflict Debate, *Journal of Strategic Studies* Volume 36, Issue 1. 125–133.

KRASZNAY Csaba (2018): A kibertér fogalma, értelmezése és fejlődése. Információbiztonság vs. kiberbiztonság.

LAWSON, Sean (2012): Putting the „war" in cyberwar: Metaphor, analogy, and Cyber security discourse in the United States. *First Monday,* Volume 17, Issue 7.

LIFF, Adam P. (2012): Cyber war: A New ‚Absolute Weapon'? The Proliferation of cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies,* Volume 35, Issue 3. 401–428.

LINDSAY, Jon R. (2015): The impact of China on Cyber security: Fiction and friction. *International Security,* Volume 39, Issue 3. 7–47.

LINDSAY, Jon R. (2015): Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity,* Volume 1, Issue 1. 53–67.

LYNN, William J. III. (2010): Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs,* Vol. 89, No. 5. 97–108.

MOLNÁR Dóra (2019): Törékeny nagyhatalmiság: a kiberbiztonság. Budapest, NKE.

MUNK, Sándor (2018): A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány*, 28 (1). 113–131.

MCGRAW, Gary (2013): Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies* Volume 36, Issue 1. 109–119.

Nemzeti Biztonsági Stratégia 2020. 1. melléklet az 1163/2020. (IV. 21.) Korm. határozathoz

Magyarország Nemzeti Biztonsági Stratégiája „Biztonságos Magyarország egy változékony világban". *Magyar Közlöny* 2020. április 21.

NYE, Joseph S. Jr. (2011): Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly* 5(4). 18–38.

NYE, Joseph S. Jr., (2016): Deterrence and Dissuasion in Cyber space. *International Security*, Vol. 41, No. 3. 44–71.

NYE, Joseph S. Jr. (2011): *The Future of Power.* New York, PublicAffairs.

Nye, Joseph S. Jr. (2018): How Will New Cybersecurity Norms Develop? The Belfer Center for Science and Internaitonal Affairs, Harvard University, March 12, 2018, Elérhető: www.belfercenter.org/publication/how-will-new-kíbersecurity-norms-develop (A letöltés dátuma: 2020. 06. 01.)

Power, Marcus (2007): Digitized virtuosity: Video war games and post-9/11 Cyber-deterrence. *Security Dialogue,* Volume 38, Issue 2. 271–288.

Stone, John (2013): Cyber War Will Take Place! *Journal of Strategic Studies,* Volume 36, Issue 1. 101–108.

Valeriano, Brandon – Maness, Ryan C. (2015): *Cyber War versus Cyber Realities: Cyber Conflict in the International System.* Oxford, Oxford University Press.

WEINER Norbert (1961): *Cybernetics: Or Control and Communication in the Animal and the Machine.* Paris, Hermann & Cie & Camb. Mass. (MIT Press) 2nd revised ed.

Nyáry Gábor

Kiberdiplomácia: hatalom, politika és technológia a geopolitika ötödik dimenziójában

Bevezetés[1]

Kiberháború, kiberbűnözés, kiberelrettentés: a szaksajtó és a közbeszéd felkapott, gyakran használt szavai és fogalmai lettek. A kibertér, ez a nehezen meghatározható, de mindenütt ott érzett közeg hovatovább az állandó konfrontáció, de legalábbis a mindig ott lebegő fenyegetés egyfajta szinonímájaként jelenik meg gondolatvilágunkban. A technicizálódó társadalmakban a konfliktusok (legyenek azok akár személyköziek, vagy a másik végletben, államok közöttiek) lassan betöltik a kiberteret. Pontosíthatunk: a kiberteret *is*. Hiszen az elmúlt két-három évtized egyik leginkább érezhető jelensége a feszültségek és összecsapások szaporodása és erősödése. Megjelent, vagyis inkább újra megjelent, egy kifejezés, amely a politológia és az újságírás világában legalább annyira közkedveltté és agyonhasználttá vált, mint a „kibertér" a technikai, informatikai szakbeszédben. Ez a „geopolitika". Képlékeny, de valahogy mindenki által „érzett" tartalmú, jelentésű kifejezés. A környezet, a földrajzi tér jelentőségét hangsúlyozza az államok életében. Arra utal, hogy a környező nagyvilágban ismét előtérbe került az érdekek leplezetlen, néha egyenesen könyörtelen érvényesítése. Majd e két kifejezés összekapaszkodott, és újabb szóösszetétel formájában lendületet kapott: beszélünk már, mert okkal beszélhetünk a „kibertér geopolitikájáról". Ebben a körbepillantásban fontos szerepet kap majd egy újkeletű pozíció (talán hivatal, vagy már lassan egyenesen önálló szakma): a kiberdiplomatáé. Mert az egyik legfontosabb mondandónk az lenne, hogy a világháló szövevényes útjait, drótjait, számítógépeit, az azokon futó programokat és persze a velük dolgozó vagy játszó embereket felölelő „kibervilág" korántsem csak a kiberharcosok, hackerek, kiberbűnözők élettere. Konfliktusok persze gyakran támadnak ebben a még kialakulófélben levő, és ezért néha rendezetlen és szabályozatlan térben. Éppen ezek megoldásán, elsimításán, szabályozásán dolgoznak a kiberdiplomácia szakemberei.

[1] A kibertérrel, a virtuális világ geopolitikai összefüggéseivel, az informatikai biztonság és a gazdaság intim kapcsolódásával rendkívül használható, jó áttekintést adó forrás áll az érdeklődők és kutatók rendelkezésére magyar nyelven is: Pintér 2016. Ugyanakkor a kibervédelem, kiberdiplomácia és az internet-gazdaság metszéspontjának egyes részkérdéseire szinte enciklopédikus segédkönyvként használható Whyte–Mazanec 2019 a későbbiekben még idézett monográfiája. A kibertér geopolitikájának, hatalmi rendszereinek, védelmi problémáinak és technológiai modernizációjának friss szemléletű elméletalkotó „mesterműve" is jó bevezetést adhat: Blount 2019.

A geopolitika beköszön a kibertérbe

A „geopolitika" napjaink egyik legtöbbet emlegetett szava, és ennek megfelelően képlékeny a jelentéstartalma és használata is.[2] Sokszor egyszerűen csak a „hatalmi politika", a „külpolitikai érdekérvényesítés" szinonímájaként használják. Hosszú időn át, a 20. század második felében, lényegében szalonképtelenné vált éppen e felfogás miatt: a szakmai közvélekedés a század első felének autoriter rendszereit megalapozó (egyik) elméletet látta benne, ezért a geopolitika koncepciója, fogalma, szóhasználata jó időre feledésbe merült.[3] Valójában használatának – a pontos jelentéstartalmaktól csaknem függetlenül – közös jellegzetessége az a felismerés, hogy a 2000-es évek eleje óta valami érezhetően megváltozott a nemzetközi kapcsolatokban: mintha addig csendben meghúzódó szereplők hirtelen a színpadra pattantak volna, hogy nagyon is aktív játékba kezdjenek.[4] És valóban: a hidegháború hosszú és külpolitikai szempontból meglehetősen világos és egyértelmű évtizedei után, az 1990-es évek elejétől a szinte meglepetésre, „ajándékba kapott" amerikai hegemónia teremtett állóvizet a külkapcsolatok világában. Ez volt az „unipoláris pillanat", az a szűk évtized, amikor az országok viszonyrendszerében lényegében egyetlen hatalom, az USA diktált, és mindenki más igazodott. A helyzet nem volt túl szép – viszont egyszerű és egyértelmű volt. A 21. század első évtizedének végére azonban már tagadhatatlan tényként látszott ennek a rendnek a felbomlása, az új, multipoláris világ egyre gyorsabb formálódása. Nem csupán Oroszország és Kína lépett (újra) a nagyhatalmi politizálás porondjára; középhatalmak, India, Törökország, az EU, sőt kisebb államok is egyre aktívabb szereplőként tűntek fel a nemzetközi küzdőtéren. Fő szabálynak a szabályok nélküliség, az igazodási pontok sokasága látszik. A nemzeti érdekérvényesítés sokszor kaotikusnak látszó, aktív korszakára mondják: visszatért a geopolitika.[5]

A földrajz bosszúja

A korábbi évtizedek elvi alapú, ideológiai szempontok alapján szerveződő nemzetközi kapcsolatait felváltotta az egyes nemzetek érdekeire koncentráló, önző" érdekérvényesítés politikája.[6] Szigorúbban véve a kifejezés arra utal, hogy a nemzetek egymás közötti

[2] A geopolitika egyik legjobban használható, sok szempontot és megközelítést felvillantó alapmunkájának továbbra is Cohen 2015 munkája tekinthető.

[3] Furcsa paradoxonként egy olyan korszakban, az ún. hidegháború időszakában, amikor a hatalmi politizálás cseppet sem „ment ki a divatból", ellenkezőleg: az egész korszakot a hatalmi szembenállás határozta meg.

[4] A kifejezés a legendás amerikai politikus, Zbigniew Brzezinski könyvcíme nyomán vált közismertté. Brzezinski 1999

[5] Kuus 2007

[6] A „pőre" nemzeti érdekeket érvényesítő külpolitikai gondolkodás legjelentősebb alakjának tekinthető amerikai Henry Kissinger hatásosan foglalja össze a világrendszer „tektonikus" átalakulását egyik fő művében: Kissinger 2016. A nemzeti érdekek *kölcsönös* felismerésén és elismerésén alapuló külpolitizálás mint a nagyhatalmi konfrontáció elkerülésének eszköze jelenik meg a volt amerikai külügyminiszter gondolkodásában. *„The Key Problem of Our Time": A Conversation with Henry Kissinger on Sino-U.S. Relations* (2018).

viszonyát, érdekérvényesítési mozgásait nagymértékben befolyásolják bizonyos hosszú távon állandó struktúrák. Elsősorban persze maga a környezet, a fizikai tér: az ország elhelyezkedése, domborzati viszonyai, vízrajza, népesedésföldrajza (benne a népesség nagysága és demográfiai mozgásai).[7] Érdemes persze elgondolkodni azon is, hogy a korábbi bő hetven év nagy ideológiái, az amerikai „szabadságeszme", majd „az emberi jogok", vagy a Szovjetunió „egyenlőség és igazságosság" ideája, „népek felszabadítása" külpolitikai narratívája mögött is alapvető nemzeti érdekek húzódtak meg; a tartós önérdek-érvényesítés értelmében felfogható „geopolitika" tehát valójában sohasem tűnt el, legfeljebb diszkréten meghúzódott a háttérben. Az igazi újdonság mostani korunkban: az érdekek immár nyílt megfogalmazása, az aktív szereplők sokasága és a nemzeti érdekérvényesítési küzdelem dimenzióinak bővülése. Ugyanakkor így már jól láthatóvá válik a „geopolitika" egy másik fontos jellegzetessége: a koncepció alapvetően látásmódot, tudományos megközelítést, vizsgálati módszert takar.[8] Olyat, ami a nemzetek közötti kapcsolódás, viszonyulás egyik (vagy éppen legfontosabb) meghatározójának tekinti a térbeliséget, illetve a fogalmat szélesebben értelmezve, a fizikai környezet tényezőit.[9] A politikai nyelvben, a közbeszédben polgárjogot nyert, gyakorta használt frappáns megfogalmazás a földrajz „bosszújáról" arra utal, hogy tévesnek bizonyultak azok a külpolitika-elméletek, amelyek – különösen az 1989–91-es esztendők, tehát az addigi kétpólusú világ hirtelen lebomlása után – úgy vélték, hogy az államok földrajzi elhelyezkedésében, fizikai adottságaiban (és ezek történeti dinamikájában) gyökerező érdekalapú külpolitizálást felváltja egy idealisztikusabb alapokon – az emberi jogok univerzális érvényesülésén, általában a jogállamiságon nyugvó – kapcsolatrendszer. A fizikai környezet hosszú távú elemei és tényezői szívósabbnak bizonyultak, és „visszatértek" a nemzetközi viszonyok alakításába.

A viszonyok és felfogások gyorsuló ütemű, jelentős átalakulására példa az Európai Unió hivatalos külpolitikai koncepciójának átformálódása. A 2019-ben hivatalba lépett új vezető testület, az Európai Bizottság nagy feltűnést keltett a nemzetközi kapcsolatok alakítására vonatkozó koncepciójával, az aktív uniós külpolitizálás elveinek megfogalmazásával. A Bizottság elnöke, Ursula von der Leyen szóhasználata

[7] A földrajzi tér erejét, meghatározó szerepét felismerő külkapcsolati felfogás egyik kiváló összefoglalóját adja az ismert amerikai külpolitikai elemző, Robert D. Kaplan *A földrajz bosszúja* című monográfiája; e fejezet fő gondolatát is innét kölcsönöztük.

[8] Szilágyi 2018 a magyar nyelven elérhető talán legjobb áttekintése a geopolitika mint tudományos diszciplina felfogásának.

[9] Élénk vita zajlott és zajlik a mai napig arról, hogy jogos-e a fizikai-földrajzi környezet ilyen *determináló* szerepét feltételezni a nemzetközi kapcsolatok alakításában. A koncepció használhatósága mellett kiállók azzal érvelnek, hogy a fizikai-földrajzi környezet hosszú távú, strukturálisan meghatározó szerepe nem azonos egy determinisztikus felfogással. A viszonyok aktuális alakításába más tényezők (illetve rövidebb élettartamú társadalmi-politikai struktúrák) is beleszólnak. A koncepció egyébként a történettudományban, a 20. század második harmadát meghatározó francia Annales iskola követőinek munkásságában kapott széles és nagy ívű társadalmi megalapozottságot. Vö. Fernand Braudel „hosszú időtartam" (longue durée) elméletével.

a „geopolitikus EU"-ról[10] meghökkenést (sőt néhol egyenesen megdöbbenést) váltott ki,[11] hiszen ez a fogalom az alapvetően a multilateralizmus elveire építő európai közösség vezető tisztviselőjétől (ráadásul éppen egy német politikus szájából[12]) egyenesen istenkáromlásnak hathatott. A politikus (aki egészen pontosan „geopolitikus Európai Bizottságot" ígért beiktatásakor) láthatóan új, dinamikusabb szerepet szánt a sokak által nehezen mozgó, erőtlen külpolitikai aktornak látszó Uniónak.[13] Az európai vezetés koncepciójának elmozdulását különösen jól jelezte az Unió másik meghatározó politikusának, Josep Borellnek e témában közreadott dolgozata, amely eloszlatott minden kételyt afelől, hogy az európai politikai beszédbe visszakerült „geopolitika" valójában hogyan értendő. Az EU külügyi és biztonságpolitikai főképviselője (azaz az Unió külügyi szervezetének irányítója, de facto „külügyminisztere"), megkerülhetetlen külpolitikai stratégia, sőt valójában külpolitikai filozófia-váltás szükségességéről beszélt. Eredetileg az EU alapvető céljaként, létrehozásának értelmeként a hatalmi politizálás eltörlése, a multilateralizmus, a nyíltság és a kölcsönösség elvein alapuló együttműködési rendszer kiépítése szerepelt. Mára azonban a világ megváltozott. Régi és új, felemelkedő hatalmak rivalizálnak egymással is az elsőségért. Borell leszögezte: Európának szemléletváltásra van szüksége. Ha a kontinens nem akar az elsőségért vetélkedő USA és Kína közé szorulva veszteségként végezni, akkor bizony „meg kell tanulnia az erő nyelvén beszélni".[14] Ennél világosabban kevesen fogalmazták meg a „geopolitikai Európai Bizottság, a geopolitikus Európa" közkeletű értelmét, jelentéstartalmát.

Kibertér: a nemzeti érdekérvényesítés 5. dimenziója

A politika és a szaktudományok sokszor elméleti vitáit félretéve, jól látható, hogy a földrajzi tér alapvető kiterjedései, a szárazföldek és vizek ősidőktől az államok közötti érdekérvényesítési küzdelmek állandó színterei. Melléjük, a 20. század első harmadától felzárkózott a levegő, majd a hidegháború korszakában az űr dimenziója is. A 21. század újdonságaként bővült ki ez a sokrétű geopolitikai világ egy újabb aspektussal, egy vadonatúj versengési területtel. A formálódó kibertér lett a geopolitikai szembenállás,

[10] Bassot 2020.

[11] Az európai szakmai-politikai eliteken belüli erős ellenkezésre több fajsúlyos megszólalás is világosan utal. Müller–Hennig 2019.

[12] A klasszikus geopolitika egyik jelentős gondolkodója, a német Friedrich Ratzel a közkeletű (ám sokak által vitatott) felfogás szerint munkásságával a náci Németország ideológiájához járulhatott hozzá.

[13] Az Unió külpolitikai teljesítményének ellentmondásosságát jól összegzi Lehne 2017. A szakmai közvélekedést azonban a legkíméletlenebb pontossággal talán maga az EU foglalja össze: „[Az EU-t] multilaterális szinten általában pozitív, de inefektív szereplőnek tekintik. Bilaterális kapcsolataiban pedig olyan aktorként érzékelik, amelyből hiányzik a koherencia." *A global actor in search of a strategy. European Union foreign policy between multilateralism and bilateralism* (2014).

[14] Borell 2020. Amihez a politikus hozzátette: Európából eddig sem az erő hiányzott, hanem a politikai akarat, hogy ezt az erőt érvényesítse a nemzetközi porondon.

érdekérvényesítés ötödik dimenziója.[15] Az informatika, a számítógépes hálózatok, mobil technológiák rohamos fejlődése szülte ezt az új „érdekmezőt", ebben az értelemben tehát tényleg ízig-vérig korunk terméke. Mint annyi fogalom, a „kibertér" is sok értelmezést, értelmezési árnyalatot takar.

Maga a kifejezés nem új keletű: egy William Gibson nevű íróhoz kötődik, aki 1982-ben kiadott novellájában használta első ízben ezt a fordulatot, egy számítógép által kreált virtuális valóságmező bemutatására. Igazi népszerűségre azonban 1984-ben tett szert, a szerző következő, *Neuromancer* című novellája révén. Azóta természetesen a kifejezés kilépett az irodalom képzeletbeli mátrixvilágából, és ma már a tudomány tereinek egyik elfogadott kifejezése. Közkeletű szakmai használatában lényegében az Internet (és hasonló technológiák) világot körbefonó, számítógépes hálózatainak szinonímájaként a leggyakoribb talán. Az Információs és Kommunikáció Technológiák (IKT) virtuális univerzumának egyfajta metaforája, ami egyre inkább kezdi felváltani az Internetre korábban elterjedt (és különösen a politikusok által előszeretettel használt) információs szupersztráda metaforát.[16] Itt érdemes kiemelni azt a mozzanatot, amely már a „sima" geopolitika térkoncepciójánál sem hagyható figyelmen kívül: a terek nem valami merev, mozdulatlan, statikus létezők, hanem ellenkezőleg: állandó mozgásban, folytonos változásban levő dinamikus viszonyrendszerek, amelyek állandó kölcsönhatásban állnak csatlakozó (társadalmi) komponenseikkel.[17]

A kibertér „térbeli" mivoltával kapcsolatban a szakirodalom nem egységes. Egyes szerzők, különösen a kiberhadviselés problematikájával foglalkozó stratégiatudományi szakértők a sokdimenziós geopolitikai közeg fokozatos (és egyre gyorsuló) virtualizálódásáról beszélnek. E szerint a hagyományos tereket a csupán átvitt értelemben létező, konkrét alakot nélkülöző tér, egyfajta „térnélküliség" váltja a geopolitika összefüggésrendszerében, éppen a kibertér, mint 5. geopolitikai dimenzió előtérbe kerülésével.[18] Olyannyira, hogy a stratégiatudományok egyik legelismertebb kortárs képviselője, az amerikai Colin Gray egyenesen „ellen-földrajzi" kiterjedésű térként definiálja, ezzel is hangsúlyozva a kibertér megfoghatatlan, képlékeny valóságát.

Másfelől viszont a kiberkomplexum technológiai aspektusaival vagy a digitalizáció társadalmi összefüggéseivel foglalkozó kutatóknál hangsúlyosan merül fel a kibertér térjellege, azaz nagyon is valóságos, fizikai térstruktúrákhoz integránsan kapcsolódó mivolta. Ebben a felfogásban a kibertérfogalom térbelisége különböző szinteken

[15] A kibertér geopolitikai jellegének egyik első megfogalmazását Szilágyi István *A geopolitika elmélete* című kiváló munkája adja.

[16] Fourkas 2004. Az így meggyökeresedett kifejezés mellett egyébként még több ilyen metafora született az IKT-jelenségkör egy-egy fontos mozzanatának köznyelvi megragadására: például közismert a digitális „könyvtár", az elektronikus „posta", vagy a virtuális „piactér", hogy a csak leggyakrabban használtakat idézzük fel.

[17] Ez az a fontos, sőt meghatározó jellegzetesség, amelyet a geopolitika fogalomrendszerének kritikusai figyelmen kívül hagynak, amikor a geopolitikai megközelítésmódot egyfajta merev (térbeli) determinizmussal vádolják.

[18] Szilágyi 2018.

jelenik meg. Szokás ezzel kapcsolatban legalább három ilyen térbeli jelentésréteget lehámozni. A fogalomnak elsőként is van egy technikai jelentésszintje, amely a kibertérnek nevezett fogalom együttes technológiai infrastruktúráját írja le. A fogalomnak van ugyanakkor egy tényleges földrajzi jelentésrétege is, amely az IKT-hálózatokat és azok csomópontjainak valóságos térbeni kiterjedését öleli fel. A fogalom ugyanakkor tartalmaz egy harmadik, társadalmi jelentésréteget is, amely az IKT-hálózatokat használó emberek térbeli szerveződéseit írja körül. A fentiekből látható tehát, hogy a kibertér, ez a sokszor virtuálisnak nevezett világ nagyon is valóságos (nem csupán metaforikusan értelmezhető) térbeliséggel rendelkezik. Kijelenthető, hogy a „kibertér" valóságos térbeli rendszer: a hálózati topológiája alapvetően függ annak térbeli rögzületeitől, és fejlődését is döntően a rendszerkörnyezet gazdasági és technológiai fejlődésének földrajza befolyásolja.

Összegezve tehát: nagyjából közös fogalmi keretként úgy tekinthetünk a kibertérre, mint az Internet, a számítástechnikai eszközök, a rajtuk futó szoftverek, sőt az őket használó, mind inkább hálózatokba szerveződő alkalmazók összességére. Alapvető jellegzetessége, hogy kezdetben merőben technikai problématerületként tűnt fel, mára azonban egyértelműen egy, a politikum által hatalmába kerített térré változott, ahol eltérő (nemzeti) érdekek, eltérő normák és eltérő értékek formálják a viszonyokat. Ma már nem sokan vonnák kétségbe, hogy ez a kibertér a geopolitikai érdekérvényesítés egyik dimenziója, éppen úgy, mint a szárazföldek, a tengerek, a levegő vagy az űr. Sőt, ma már abban is egyre nagyobb a konszenzus, hogy a nemzetek közötti érdekellentéteknek és érdekérvényesítésnek a kibertér nem csupán egyik dimenziója, hanem „a" meghatározó színtere.[19]

Geopolitikai mozgások a kibertérben

A geopolitika fogalmi rendszerének általános bemutatásánál utaltunk rá, hogy a 2010-es évtized egyértelmű fejleménye a rendszerváltásokat követő Amerika központú, unilaterális világrend felbomlása. Tudósok és politikai szakértők egyre gyakrabban említik az így kialakulóban lévő szisztémát egyfajta multipoláris világrendként.[20] Érdemes azonban hangsúlyozni, hogy a hidegháború időszakára jellemző klasszikus (egyfelől az USA, másfelől a Szovjetunió köré épülő) bipolaritás valóban nem tekinthető jellemzőnek napjainkra, és ebben az értelemben indokolt egyfajta multipoláris világrend-szerveződésről beszélni.[21] A nemzetközi tér eseményei azonban egyre

[19] Desforges 2014, továbbá a kibertér, a földrajz és a hatalmi politika modern kapcsolódási rendszereire az egyik vitathatatlanul legérdekesebb mostanában napvilágot látott munka Blount 2019 kötete.

[20] Alapos, rendszeres áttekintését adja a hatalompolitikai átrendeződés folyamatának és következményeinek az Európai Parlament kutatószolgálata által kiadott *Global Trends to 2035. Geo-politics and international power* 2017. Hasonlóan jó összefoglalót ad Dee 2015 is.

[21] Amit egy némileg cinikus, de a valóságtól néha nem túl távol álló megfogalmazással úgy jellemeznek, hogy amíg a bipoláris világban a két szembenálló nagyhatalom köré tömörült államok szövetségi rendszerei néztek egymással farkasszemet, addig a multipoláris világban inkább a „mindenki mindenki farkasa".

inkább abba az irányba fordulnak, hogy a nemzetközi kapcsolati tér meghatározó szervező erejévé a majd' három évtizede globális hegemónként vezető Egyesült Államok, és a vezető szerepért immár egyértelműen bejelentkezett Kínai Népköztársaság közötti rivalizálás válik.

Az USA és Kína közötti stratégiai jellegű geopolitikai vetélkedés (ahogy természetesen a többi nagy- és regionális hatalom közötti geopolitikai rivalizálás is) egy „megvalósítási eszközskála mentén" több különálló, de egységes rendszerbe kapcsolódó, és egyre gyakrabban formálisan is jórészt összemosódó eszközt használ a valós (vagy annak vélt) nemzeti érdekek külvilágbeli érvényesítésére. A lehetőségek tárházából még ma is gyakorta veszik elő az államok a háború (vagy talán pontosabb: a fegyveres erőszak) eszközét. Az utóbbi évtized fejleményei azonban azt mutatják, hogy már ez az előbbi pontosítás sem írja le elég hűséggel a valóságot. A kibertér „geopolitizálódásával" párhuzamosan ugyanis éppen a hagyományos fegyvereken – és az azok által előidézett „kinetikus" összecsapásokon – alapuló külpolitikai érdekérvényesítés helyébe az erőszak új – fegyvertelen de semmiképpen sem „békés" – eszközei lépnek.[22] Ez a kiberhadviselés, a kiberháborúk feljövő korszaka. A geopolitikai pozíciók megszerzésére vagy éppen azok megvédésére a megfelelő technológiai képességekkel rendelkező országok kiberhadviselési potenciálokat építenek ki.

A geopolitikai küzdelmek meghatározó szembenállásának tekinthető amerikai–kínai viszonylatban a két rivális fél mindegyike elkötelezte magát a kibertérben alkalmazható erőszakos érdekérvényesítő eszközök, rendszerek kifejlesztése, telepítése és alkalmazása mellett.[23] Szokás úgy fogalmazni, hogy ugyan kezdetben Kína és az USA más és más stratégiai keretrendszerben (Amerika alapvetően informatikai és egyéb infrastruktúráinak megóvása érdekében, tehát a védekezés céljával, míg Kína offenzív jelleggel) látott hozzá a kiberképességek kiépítéséhez, és ezért azok jellegükben is eltértek egymástól,[24] később mindkét hatalom támadó eszközökkel is felszerelt kiberarzenállal operál a nemzetközi kibertérben.[25] A 2010-es évtizedben (az előző évtizedek kezdeményezésiből kinőve) gyorsított ütemben megkezdődött a kiberhadviseléssel foglalkozó, szakosított katonai szervezetek (operatív alakulatok és irányító parancsnokságok) kiépítése mindkét egymással versengő nagyhatalomnál. A kezdeti stratégia különbségek a kapacitások kiépítésében is éreztették hatásukat: míg Kína kezdettől egységes irányítás alatt szervezte meg támadó és védekező kiberképességeit, addig az Egyesült Államok csak számos szervezeti kísérletezés nyomán, az évtized végére jutott el a hasonlóan hatékony kiberhadviselési struktúrák

[22] A téma, a nemzetközi kapcsolatok, illetve a külpolitika és a kibertér erősödő összefonódásának különösen jó áttekintését adja Choucri 2012.

[23] A kínai szándékokra és képességekre Tianjiao 2019 *Az amerikai kiberstratégia katonai komponensére* (ami nem azonos a szintén abban az évben publikált amerikai Nemzeti Kiber Stratégiával!) *US Department of Defense Cyber Strategy 2018* (2018).

[24] Domingo 2016.

[25] Azaz, az amerikai kiberstratégiában is (annak radikális átszabása nyomán) megjelent az infrastruktúra-védelem prioritása mellett a kibertérben biztosítandó katonai erőfölény megszerzésének célja is.

kialakításáig.[26] A kibertérben zajló katonai akciókról – azok jellegénél fogva – kevés megbízható információ lelhető fel a szabadon hozzáférhető (nyílt) irodalomban. Érdekességként megemlíthetjük, hogy a kibertérben való hadviselési műveletek jóval régebbiek, mint azt gondolhatnánk: az első (nyilvánosságra került) ilyen akció a hidegháború időszakába vezet vissza, a szovjet Transz-Szibériai gázvezeték vezérlő rendszerei elleni kiberműveletig.[27] Jellemző szakmai vélekedésnek látszik ugyanakkor, hogy az ezredfordulótól sokasodó katonai akciókban a kínai kiberhadviselési alakulatok – miközben komoly, különösen kinetikus jellegű károkat nem okoztak – általában jól fedték fel az ellenfelek (elsősorban az USA) digitális hálózatainak, rendszereinek sérülékenységeit. Erre utaltak a 2010-es évtizedben sűrűsödő kínai támadások amerikai kormányzati rendszerek ellen, amikor a cél többnyire érzékeny információk megszerzése volt. [28]

Az államok közötti kiberkonfliktusok (incidensek) egyébként négy fő kategóriába sorolhatók: az első, a már említett információszerző műveletek csoportja. Célozhatják ugyanakkor a kiberakciók az ellenfél hálózatainak, rendszereinek megzavarását, lassítását, bénítását, elpusztítását. A kibertérben folytatott akciók szolgálhatják valamilyen, a szokásos katonai környezetben történő akció támogatását. És végül a kibertámadások célja lehet az ellenfél információs környezetének megzavarása, manipulálása.[29]

Az elmúlt évtizedek kiberincidenseinek kronológiája, és különösen a két versengő nagyhatalom kibertérbeli rivalizálásai alapján a kibervilágnak mint geopolitikai „hadszíntérnek" a következő jellegzetességei látszanak kirajzolódni. A proliferáció (a kiberhadviselésre alkalmas informatikai eszközök és eljárások elterjedése) nehezen látszik megállíthatónak. Ennek nyomán a (roppant hatékony, akár stratégiai csapásmérésre is alkalmas) kiberhadviselési képességek gyors ütemben terjednek majd a közepes hatalmak, de akár a kevésbé jelentős hatalmi szereplők körében is. Ugyanakkor azonban továbbra is a nagyhatalmak dominálják majd a kiberteret (is), mivel komplex, bonyolult támadások kivitelezésére továbbra is csak komoly technológiai háttérrel rendelkező országok képesek. Végül, különösen nyugtalanító fejleményként a szakemberek elképzelhetőnek tartják, hogy a kibertámadások, a csapások-ellencsapások eszkalálódásával, valóságos („kinetikus") károkozássá fajulhatnak el.[30]

[26] .Domingo 2016, 162. Míg Kína kezdettől a Kínai Népi Felszabadító Hadsereg vezérkarának Harmadik- és Negyedik Igazgatósága alá rendelve – egységes parancsnoki rendszerbe szervezve – építette kiberkapacitásait, addig az USA csupán a 2010-es évtized végére, az US Cyber Command (USCYBERCOM) felállításával érte el a kínaiakéhoz hasonló integrált vezetési és irányítási szervezetet.

[27] Az akcióra 1982-ben került sor, és állítólag a CIA állt a hadművelet hátterében, ami egy digitális kártevővel fertőzött szoftver révén tette tönkre a rendszer vezérlését. A beavatkozás egyébként kinetikus hatásokkal járt: kolosszális méretű gázrobbanást idézve elő. Whyte–Mazanec 2019.

[28] 2003 és 2012 között legalább hat jelentősebb – amerikai kormányzati célpontok elleni –- támadást írnak a Kínai Népköztársaság számlájára, amiből kettő különösen veszélyesnek bizonyult. 2005: Titan Rat hadművelet, az amerikai Hadügyminisztérium, Külügyminisztérium és Belbiztonsági Minisztérium rendszerei ellen. 2009: Shady Rat hadművelet a Lockheed Martin, Northrop és BAE hadiipari beszállítók rendszerei ellen. A cél mindenhol titkos információk megszerzése volt. Domingo 2016, 162.

[29] Whyte–Mazanec 2019, 100.

[30] Domingo 2016, 166.

Diplomáciától a kiberdiplomáciáig

A geopolitika általános fogalmairól és kereteiről szólva említettük: a földrajz, domborzat, demográfia, történelem dinamikus rendszert alkotó terében létező államok vélt vagy valós nemzeti érdekeiket igyekeznek érvényesíteni. Néha (nem is olyan ritkán) egymás rovására, máskor egymással együttműködésben. Az előző fejezetrészben azt villantottuk fel, hogy hogyan használják az államok (egy speciális dimenzióban, az úgynevezett kibertérben) az érdekeik érvényesítésére rendelkezésre álló *egyik* eszközkészletet: az erőszakot. A hangsúly itt most azon van, hogy ez az *egyik* lehetséges eszközrendszer. A paletta (vagy inkább egyfajta eszköz-skála) másik végén egy *másik*, szintén jól ismert eszközt találunk, a diplomáciát. A külpolitikát tehát sajátos cselekvési terepnek foghatjuk fel: egy állam sajátos nemzeti érdekeinek, értékeinek, céljainak érvényesítése, méghozzá egy (többnyire bonyolult) kapcsolatrendszerben. A külpolitika ugyanis mindig csak viszonyként értelmezhető: más, hasonló államokkal való interakcióban. A diplomácia tehát, fogalmaztuk meg kicsit magasabb szinten, a külpolitika érvényre juttatásának másik lehetséges eszközcsoportja. Olyan tevékenység, amely sajátos funkciókkal és hasonlóan egyedi eljárásokkal rendelkezik. A hadviselésétől jócskán elütő eszközkészletét, jellemzően a tárgyalás és a megegyezés alkotják. A kibertér mint geopolitikai struktúra vonatkozásában pedig sajátos válfaja, a kiberdiplomácia kap egyre inkább teret. Bizonyos értelemben azonban, már maga a kifejezés is okozhat némi fejtörést a szemlélőnek.

A terminológia őserdejében

Ha az államigazgatás digitalizációja, úgy általában, a fogalmi tisztázatlanságok jellegzetes terepe ma még, akkor ez végképp igaz a diplomáciával kapcsolatos elnevezési helyzetre. A nemzetközi szakmai közbeszédben egyelőre szinte átláthatatlan, kaotikus örvénylésben kavarognak a külszolgálatok digitalizálását leírni kívánó konstrukciók: „kiberdiplomácia", „e-diplomácia", hogy a korábban leggyakoribb összetételeket idézzük, de ott van még az elmúlt fél évtized különösen kedvelt megfogalmazása, a „Twitter-diplomácia", más néven „közösségi média diplomácia", vagy „Facebook-diplomácia" elnevezése is. A sor pedig korántsem ért véget. Felbukkant már az „algoritmikus diplomácia" összetétel is, aztán gyakorta találkozhatunk a „techno diplomácia" fogalmával is, de bizonyos összefüggésekben előjön az „adat diplomácia" szóösszetétel is. És persze létezik a „digitális diplomácia" kifejezés is, amely lassan, de biztosan kezd általános érvényű használatot kivívni magának.[31]

A fogalomhasználat áttekintése és elemzése nyomán a következő főbb megállapításokat tehetjük:

[31] A diplomácia legutóbbi évtizedekben felgyorsuló fejlődésének problémáit lásd Clüver Ashbrook 2014. A téma talán legelismertebb szakértője az Oxfordban tanító román tudós, Corneliu Bjola írásai megkerülhetetlenek a technicizálódó külkapcsolatok és általában a 21. századi diplomácia tanulmányozásához. Bjola é. n., valamint Bjola 2018.

– A diplomáciai, nemzetközi kapcsolatokhoz kötődő IKT-fejlesztések leírására használt fogalomrendszer különböző elemei, az esetek jelentős többségében, csupán szinonimaként szerepelnek a szakmai közbeszédben is.
– Ebben a használati módban a kifejezések sokszor nyelvi divatciklusok szerint váltják, követik egymást (anélkül, hogy a kifejezések váltása mögött bármiféle komoly szemantikai szándék állna).

Ugyanakkor történtek már kezdeti lépések a fogalmak szisztematikus elemzésére, egy általánosan használható fogalmi háló kialakítására (a nyelvi-elméleti alapvetések általánossá válásának azonban továbbra sem lehetünk tanúi a szakirodalomban, még kevésbé a nyilvános közbeszédben).[32]

Szűkebb témánk, a kiberdiplomácia ismertetése előtt érdemes – a nemzetközi szakmai gondolkodás eredményeit figyelembe véve – a terminológia rendszerszerű tisztázására kísérletet tenni. Mielőtt azonban ezt röviden felvázoljuk, mindenképpen fontosnak tartjuk még egy további fogalmi kitérő bejárását is.

A diplomácia értelmezése és átértelmezése

Talán meglepő, de a külügyek IKT-fejlesztései témájában a nemzetközi szakmai közbeszédben szinte alig merül fel magának a diplomáciának a definíciós igénye. Miközben ezt tehát látszólag mindenki magától értetődőnek veszi, mi azt gondoljuk, hogy érdemes a jelenség tartalmának alaposabb vizsgálata. Ez szolgáltatja ugyanis azt a kontextust, amelyben a digitalizáció folyamatai, eszközei, megoldásai egyáltalán értelmezhetővé válnak. A szakma külföldi művelői általában így summáznak: „a digitális diplomácia vagy e-diplomácia az a terület, ahol a korszerű IKT-eszközrendszert mozgósítják egy állam külpolitikai céljainak szolgálatára".[33] Összefoglalónak megteszi, de mindenképpen érdemes egy kicsit a tartalmi mélységekbe is bepillantani. Meggyőződésünk, hogy a külügyek digitalizációját vizsgálva semmi sem visz minket közelebb a jelenségek megértéséhez, mint a „diplomácia" funkcionális vizsgálata. Ez a szemrevételezés ad ugyanis választ a hogyanokra és a holokra is. Hogyan (illetve pontosan melyik résztémában) szolgálja a diplomácia szervezete és folyamatrendszere egy állam külpolitikai céljainak érvényesítését? A megközelítés azért is érdekes és fontos, mert ezen a ponton esetlegességekről aligha lehet szó.[34] Az egyes államok diplomáciai testületeinek munkáját

[32] A diplomácia IKT-alapú átalakulásának fogalmi kereteivel legtöbbet két kiemelkedő szakmai műhelyhez köthető kutatók foglalkoztak. Kiemelkedő szerepet játszik az Oxford Digital Diplomacy Research Group. A másik fontos elméleti-fogalmi tisztázó munkát végző szakmai műhely a Holland Külügyminisztérium háttérintézete, a híres Clingendael. Vö.: Bjola 2015, 71–89. Továbbá Melissen et al. é. n. 27–51.

[33] A fiatal generáció legkiemelkedőbb kutatóegyénisége, a Bjola professzor mellett Oxfordban dolgozó izraeli Ilan Manor érdeme a szakterület definíciós tisztázására tett első erőfeszítés. Manor 2016 és Manor 2017.

[34] A modern diplomácia funkcióira, szervezetrendszerére, működési formáira, fontosabb problématerületeire ad jó áttekintést Barston 2013 munkája.

ugyanis, ilyen funkcionális megközelítésben, egyenesen egy nemzetközi megállapodás rögzíti és részletezi:

– képviseleti funkció,
– információs funkció (tájékoztatás, illetve tájékozódás),
– kapcsolatépítési funkció,
– tárgyalási funkció,
– állampolgári érdekképviseleti (konzuli) funkció.[35]

Úgy gondoljuk: ezt a felosztást, működési tartalmat kell szem előtt tartani ahhoz, hogy értelmezni tudjuk a külügyek terén megvalósuló IKT-fejlesztések pontos szerepét és valóságos súlyát.[36]

Még egy fogalmi kérdés van, amelyre mindenképpen ki kell térnünk. Gyakorta kerül elénk, a köznapi szóhasználatban és a hivatali nyelvben is, a „közdiplomácia" fogalma. Úgy véljük, kulcsfogalom ez – s így különösen zavaró, hogy némileg félreértett módon használják. 19. századi előzmények után 1965-től jelölik ezzel az angolul „public diplomacy"-nak mondott szóösszetétellel azt az átalakulást, ami a modern diplomáciatörténet legnagyobb változását hozta.[37] Az eredetileg államok (vagy azok hivatalos szereplői) közötti kapcsolatokra szorítkozó diplomácia a 20. század drámai társadalmi-politikai átalakulásai nyomán váltott paradigmát: fokozatosan az államok (vagy azok hivatalos szereplői) és más államok közösségei (szervezetei, de akár egyénei) közötti kapcsolatok váltak a diplomáciai működés meghatározó mozzanatává. Ez az átalakulás mindennél fontosabb az államigazgatás e területének digitális transzformációja szempontjából is: a két folyamat kéz a kézben jár. Egymás nélkül elképzelhetetlenek, sőt bizonyos mértékig érthetetlenek is. Éppen ezért a szakmai tisztánlátást is nehezíti, hogy ma még a „közdiplomácia" a külügyminisztériumokon belül egy részterületnek számít, mintha a public diplomacy a diplomáciai működésnek egy lehetséges válfaja, szakmai terepe lenne csupán, nem pedig az egész ágazat legújabb kori transzformációjának fémjele.[38]

Értelmezési keretrendszer

A diplomácia digitalizációs jelenségeivel kapcsolatban a fogalmi rendszer tisztázására (akár egyfajta szakmai „munkanyelv" elemeiként) egy áttekinthető, egyszerűsítő rendszerezést javasolunk. Alapvetően négy fogalmat ajánlunk megtartásra, azzal a megkö-

[35] Az úgynevezett Bécsi Diplomáciai Szerződés (a diplomáciai kapcsolatokról szóló 1961. évi bécsi szerződés). Vö. Bába–Séringer 2018, 71–75. és 110.

[36] A diplomáciai tevékenységeknek ez a klasszikus funkcionális keresztmetszete az erőteljes digitalizáció korszakában is érvényesnek tekinthető, és a szakma elemzésének alapvető kiindulási pontját jelenti. Rana 2011.

[37] Vő. *Public diplomacy stratégiák* é. n., 8.

[38] A digitális diplomácia eszközeinek és eljárásainak evolúciójára lásd *History of Digital Diplomacy and Main Milestones* é. n.

téssel, hogy tulajdonképpen három szerkezettel is leírható valamennyi fontos jelenség ezen a szakmai területen.

Az egyik legfontosabb fogalmi tisztázás arra vonatkozik, hogy a digitális diplomácia alapvetően két elkülönülő aspektust ölel fel (nagyon hasonlóan a digitális államigazgatás fogalmának kettős jelentéséhez). E szerint a „digitális diplomácia" egyfelől a digitális térre vonatkozó diplomácia, másfelől a diplomácia digitalizált formája. Ez a legelső, legfontosabb kettősség. A tisztánlátás kedvéért mi a továbbiakban az előbbi aspektust (tehát az online terek, működések és szereplők szabályozásával kapcsolatos) diplomáciai, államközi tevékenységeket fogjuk „kiberdiplomáciának" nevezni. A „digitális diplomácia" fogalmat pedig megőrizzük a diplomáciai működés IKT-alapú transzformációja jelölésére.

1. táblázat: A digitális diplomácia javasolt fogalmi keretrendszere[39]

Fogalom		Tartalma
(magyarul)	(angolul)	
kiberdiplomácia	cyber diplomacy	A kibertérre, az online jelenségekre, a nagy globális technológiai cégekre vonatkozó nemzetközi szabályozó és irányító tevékenységekre vonatkozó államok közötti (diplomáciai) tevékenységek.
techno diplomácia	techno diplomacy	A kibertérre, az online jelenségekre, elsősorban a nagy globális technológiai cégekre vonatkozó szabályozó és irányító tevékenységek. Államok és globális technológiai cégek közötti kapcsolat.
e-diplomácia	e-diplomacy	A diplomácia digitalizálása a hagyományos működések gyökeres átalakítása nélkül.
digitális diplomácia	digital diplomacy	A diplomácia hagyományos folyamatainak gyökeres („transzformatív") átalakítása az IKT-technológiák következtében.

Forrás: a szerző szerkesztése

Használatra javasoljuk még a „techno diplomácia" kifejezést, amely nagyon hasonló jelenségre vonatkozik, mint a kiberdiplomácia, ám egy fontos különbséggel: itt államok lépnek interakcióba kvázi államszerűen fellépő gigantikus magáncégekkel. A jelenség még ritkaság, de erősen terjed.[40] Továbbá használhatónak tartjuk az e-diplomácia kifejezést, elsősorban a diplomáciai szervezetek „üzemszerű" működésének korszerű IKT-eszközökkel történő támogatására, modernizálására. Itt a kulcsmozzanat az, hogy a digitális eszközök beállítása nem hozza maga után a támogatott hagyományos diplomáciai működések, folyamatok gyökeres átalakulását.

Kiberdiplomácia: kialakulás, tartalmak, fejlődési irányok

A kiberdiplomácia végső soron nem más, mint a diplomácia erőforrásainak, eljárásainak felhasználása a nemzeti érdekek, értékek és célok érvényesítésére, méghozzá egy spe-

[39] Nyáry 2019, 78.

[40] Képviselői, motorjai az úgynevezett techno diplomaták, akiknek őstípusát a dán Casper Klynge képviseli, akit országa külügyminisztériuma 2017-ben nevezett ki erre a posztra, és akit nem valamely nemzetállam kormányánál akkreditáltak, hanem a Szilícium-völgyben.

ciális közegben vagy dimenzióban: nevezetesen a kibertérben. Érdemes megemlíteni, hogy amíg egy ország külpolitikájának fő vonásait valamilyen általános stratégiai dokumentum (nemzetstratégia, nemzeti biztonsági stratégia, védelmi stratégia, külpolitikai stratégia) határozza meg, addig az országok kibertérben érvényesítendő sajátos érdekeit, értékeit és céljait egy speciális stratégiai anyag, az úgynevezett kiberstratégia (vagy kiberbiztonsági stratégia) tartalmazza. A kiberdiplomácia működési terepe jó néhány különálló ügyterületet, speciális témát felölelhet. A legfontosabb, szinte folyamatosan terítéken levő kérdések a kiberbiztonság, a kiberbűnözés problémája. Ugyancsak fontos, állandó ügy a bizalomépítés kulcsfontosságú kérdése (mint még látni fogjuk, a diplomácia, a békés kapcsolatrendezés e fontos összetevője a kibertér sajátos viszonyai közepette csak jelentősen korlátozott formában jelenhet meg). Fontos tárgyalási terület az Internet szabadságának kérdése, illetve (az előző szemponttal szoros összefüggésben) egyre nagyobb súllyal jelenik meg ma már a nemzetek közötti viszonyrendszerben a kiberszuverenitás kérdése is.

Szeretnénk hangsúlyozni: a „kiberdiplomácia" nem valami metafora csupán, hanem valóságos külkapcsolati terület és államközi interakciós terep. A kiberdiplomáciát valóságos diplomaták művelik, formáját tekintve pedig – ahogy a diplomácia „hétköznapi", klasszikus válfaja is – felölelhet bilaterális viszonyt (mint például az USA és Kína között 2015-ben kötött kiberbiztonsági megállapodás), illetve a nemzetközi rendezések multilaterális formáját is (például jellemzően az ENSZ általános vagy szakosított keretrendszerén belül).[41]

A kiberdiplomácia mint önálló, de legalábbis jól elkülönülő diplomáciai terep és tevékenység, az új évezred első évtizedének a vége felé jelenik meg.[42] A kibertérben meghatározó szerepet játszó (vagy játszani kívánó) hatalmak egymás után rukkolnak elő a kibertérre vonatkozó stratégiai dokumentumaikkal, ahogy egyre nyilvánvalóbbá kezd válni a kiberdomén geopolitikai értelemben meghatározó szerepe. Az USA 2009-ben publikálta a *Kibertér Politikai Áttekintés (Cyberspace Policy Review)*[43] című dokumentumot; ugyanabban az évben jelent meg a brit *Kiberbiztonsági Stratégia (Cybersecurity Strategy)*, illetve a rákövetkező évben Kína is előállt a *Fehérkönyv a Kínai Internetről (White Paper on the Internet in China)* című stratégiai dokumentummal. Ezek a dokumentumok kivétel nélkül a kiberbiztonság belföldi aspektusaira fókuszáltak (kibervédelmi kapacitások kiépítése, a kibervédelemmel kapcsolatos kormányzati koordináció erősítése), és a téma nemzetközi összefüggései legfeljebb csak érintőlegesen kerültek említésre. Ezekkel a fejleményekkel párhuzamosan azonban multilaterális keretek között is megindultak az első tapogatózások a kibertér sajátos problémáinak feltárására, illetve a terület nemzetközi szabályozásának előkészítésére (lásd lejjebb).[44]

[41] A kiberdiplomácia egyik legérdekesebb szemléletmódú bemutatását a digitális diplomácia kutatási terület egyik legjelesebb kutatójának, Shaun Riordannak köszönhetjük. Riordan 2019.

[42] Barrinha–Renard 2017, 358.

[43] A nemzeti kiberstratégiák fejlődése szempontjából az egyik legfontosabb ösztönző és egyben minta az amerikai kormányzat úttörő jellegű dokumentuma volt. Vö.: *Cyberspace Policy Review* é. n.

[44] A téma áttekintésére haszonnal forgatható Berzsenyi–Krasznay 2019.

A szorosan vett kiberdiplomácia tevékenységet, illetve gyakorlatot a 2010-es évtized legelejére datálhatjuk. Ekkor jelent meg 2011-ben az Egyesült Államok kormányának a *Kibertér Nemzetközi Stratégiája (International Strategy for Cyberspace)* című korszakos dokumentuma. Korszakos azért, mivel ez az első olyan kormányzati dokumentum, amely koherens módon, önálló tématerületként tárgyalja a kibertér problematikájának nemzetközi összefüggéseit.[45] A stratégia azonosít néhány olyan problématerületet, amellyel kapcsolatban a nemzetközi szabályozás kialakítása kívánatos lehet: gazdaság, hálózatvédelem, rendvédelem, hadügyek, Internetkormányzás, nemzetközi fejlesztés politika és az Internet szabadsága. A fenti problémákkal való foglalkozásra első ízben jelöli meg (a katonai és a fejlesztéspolitikai eszközökkel együttesen) a diplomáciát mint a kibertérrel kapcsolatos kérdések megoldásának lehetséges eszközét. A dokumentum, az irányelvek lefektetésével párhuzamosan, gondoskodik a megvalósítási intézményrendszer felállításáról is: az USA Külügyminisztériumán belül megalakult a Kibertérügyi Koordinátor Hivatala (Office of the Coordinator for Cyber Issues).[46]

Miközben a 2010-es évtized folyamán egyre több ország dolgozott ki és fogadott el a nemzeti kiberstratégiájára vonatkozó dokumentumot, a fenti amerikai kezdeményezéshez hasonló, kifejezetten a kibertér nemzetközi aspektusaira fókuszáló kormányzati dokumentumot csak elvétve szültek ezek az évek. A kivételek között szerepel a japán kormány által 2013-ban elfogadott *Nemzetközi Kiberbiztonsági Együttműködési Stratégia (International Strategy on Cybersecurity Cooperation)*.[47] Szintén a fontos mérföldkövek közé számíthatjuk az EU Tanácsa által 2015-ben elfogadott *Európai Tanácsi Következtetést a Kiberdiplomáciáról (Council Conclusions on Cyber Diplomacy),* amely első ízben használta – hivatalos dokumentumban – a „kiberdiplomácia" kifejezést az Unió intézményrendszerében. Az elsősorban nemzeti fókuszú *Francia Nemzeti Digitális Biztonsági Stratégiában (French National Digital Security Strategy)* külön fejezet foglalkozik a kibertér nemzetközi együttműködési kérdéseivel.[48] A stratégiai tervezéssel párhuzamosan több országban is felállítottak, általában a külügyminisztérium keretén belül, a kiberdiplomácia kérdéseire szakosodott szervezeti egységet (például Németországban, Belgiumban). Az önálló kiber-részleg felállítása mögött az a felismerés húzódott, hogy a külügyi tárcákon belül korábban sokfelé elaprózva, több ügyosztályhoz is hozzárendelve kezelték a kibertér egyes részterületeihez kapcsolódó problémákat, ami a koordináció hiányához és kevéssé hatékony működéshez vezetett.[49]

[45] *International Strategy for Cyberspace* 2011.
[46] *Office of the Coordinator of Cyber Issues* (é. n.).
[47] Barrinha–Renard 2017, 359.
[48] *French National Digital Security Strategy* 2015.
[49] *French National Digital Security Strategy* 2015. és Barston 2013, 112.

A kibertér szabályozása és igazgatása (cyber governance)

A kibertér kihívásai, szabályozási keretek és kezdeményezések

A kibertérhez közvetlenül vagy áttételesen kapcsolódó problémákat szemügyre véve jól érzékelhető, hogy ennek a „geopolitikai dimenziónak" van egy különös (a hatalmi viszonyok érvényesülésére szolgáló többi térelemre – a szárazföldre, a vízre, a levegőre és az űrre – nem mindig jellemző) sajátossága: szinte hívogatja a diplomáciát mint a kérdések rendezésének célszerű és kívánatos eszközét. Talán furcsán hangzik ez, hiszen a szakmai közbeszédben (hogy a politikát és a közvéleményt már ne is említsük) az erőszak (a kibertámadás) jelenik meg általában a kibertérbeli államközi interakciók bonyolítására szolgáló eszközként. Pedig a kiberdomén néhány jellegzetessége miatt igenis kívánatos terepnek számít a békés tárgyaláson, egyezkedésen, kölcsönös megállapodáson alapuló diplomáciai rendezések számára. Nézzünk ezek közül legalább néhányat![50]

Elsőként érdemes mindjárt előrebocsátani a korábban már megismert, de fontos alapelvet: a kiberdomén valóságos globális „tér". Olyan, ami egyszerre összeköti a nemzeteket, ugyanakkor természetesen a közöttük való súrlódásoknak is gyakori terepe. A kiberteret egyfajta „globális közlegelőnek" (global commons) szokták tekinteni.[51] Azaz olyan nemzetközi vagy még inkább nemzetek feletti erőforrásnak tekinthetjük, amilyen például a világtenger vagy a légkör, illetve maga a világűr is. Az ilyen közlegelők igazgatása rendszerint óhatatlanul felbukkanó dilemmával néz szembe. A közös és osztatlan erőforrást használó szereplők (államok) egy része abban érdekelt, hogy a közösen használt erőforrásra vonatkozóan éppen csak minimális nemzetközi szabályozás létezzen; olyan, ami a szabad hozzáférést, akadálytalan felhasználást és kiaknázást nem korlátozza lényegesen. Ezzel ellentétesen azonban, a hatalmi rivalizálást a geopolitika valamennyi (általuk elérhető) dimenziójára kiterjeszteni akaró hatalmak abban érdekeltek, hogy sajátos vízióikat, értékeiket és érdekeiket maradéktalanul kivetíthessék a hálózatos térbeli közlegelőre is. Ez a helyzet, a benne feszülő ellentétek miatt, fontos terepet kínál az egyeztetés, az érdekek békés összehangolása szakértőinek számító diplomaták számára.

A kibertér másik jellegzetessége, ami az erőszakos eszközökkel szemben inkább a diplomácia békés eszköztárának bevetését teszi indokolttá, az úgynevezett attribúció közmondásos nehézsége ebben a közegben. Röviden tehát: a kibertér struktúrája, működése folytán nehéz egyértelműen azonosítani az egyes kibertámadások elkövetőit.[52] Ez jelentősen hozzájárul a közbizalom aláásásához, az agresszív viselkedési normák bátorításához, ami végső soron egyik közlegelő használónak sem érdeke.[53]

[50] A kibertér szabályozására, irányítására vonatkozó nemzetközi koncepciók és törekvések áttekintését adja Jaywardane 2015.

[51] Kumar 2015.

[52] Legalábbis a hivatalos álláspont szerint. A kibervédelemmel foglalkozó titkosszolgálati szakemberek egy része ugyanakkor – háttérbeszélgetések során – állítja: a jelentős kiberkapacitásokkal és tapasztalattal rendelkező hatalmak igen jó pontossággal tudják azonosítani az online terekben végrehajtott támadó akciók tényleges kiindulási forrásait.

[53] Barrinha–Renard 2017, 357.

További jellegzetesség (és az előző pontban említett sajátosság tulajdonképpen így nyer értelmet), hogy a kibertérben nem (vagy csak elenyésző mértékben) működik a klaszszikus geopolitikai konfrontációs helyzetek egyik legfontosabb eleme: az elrettentés. A kibertérben végrehajtott erőszakos akciók jellegüknél fogva rejtve maradnak, vagy a valódi elkövető kiléte marad homályban. Ennek következtében nem tudják betölteni az egyedi erőszakos (fegyveres) állami akciók egyik legfontosabb funkcióját: azt tudniillik, hogy a potenciális ellenfelet elriasszák az erőszakhoz való folyamodástól. A kibertér ezen sajátosságai tehát abba az irányba hatnak, hogy az erőszakos akciók – más geopolitikai dimenziókkal, potenciális csataterekkel összevetve – kevésbé vonzó alternatívát kínáljanak az államközi viszonyok diplomáciai rendezése helyett.

Globális normák, szabályozási törekvések

Feljebb már említettük, hogy az első kormányzati kiberstratégiai dokumentumok kidolgozásával lényegében egy időben multilaterális keretek között is megindultak a munkálatok a kibertér sajátos problémáinak feltárására, illetve a terület nemzetközi szabályozásának előkészítésére. Ebben az összefüggésben különösen fontosak voltak az ENSZ Kormányzati Szakértői Csoportjainak[54] ülései 2010-től kezdve, amelyek azt tűzték ki célul, hogy a nemzetközi közösség összefogásával a kibertámadások fenyegetéseinek csökkentésére vonatkozó, illetve általánosságban véve a felelősségteljes állami magatartás önkéntes normáit kidolgozzák a kibertér vonatkozásában. A csoport, aminek felállításáról egy jóval korábban Oroszország által beterjesztett javaslat[55] alapján döntött a Világszervezet, olyan munkaterepet nyitott az egymással rivalizáló nagyhatalmak számára, ahol azok megpróbálhattak valamiféle találkozási pontokat kialakítani, elsősorban a területen égetően szükséges bizalomerősítés szférájában. A munkaszervezetben a nagyhatalmak képviselői kaptak helyet, és a hatalmi rivalizálások végül erősen rányomták bélyegüket a csoport tevékenységére.

A kibertér problémáinak feltérképezésére, a követendő normarendszerek kidolgozására a Világszervezet egy másik kezdeményezést is útjára indított. Részben a UN GGE csoport tapasztalatai alapján, tanulva annak relatív sikertelenségéből (a szervezet nem volt képes munkáját a szokásos jelentés formájában összegezni), egyébként ismét orosz kezdeményezésre, 2017-ben az ENSZ egy Nyílt Végű Munkacsoport felállításáról határozott. A valamennyi tagállam számára nyitott formátumtól azt várták, hogy a közös szabályrendszerek kidolgozásában képes lesz majd bevonni az ENSZ olyan tagjait is, amelyek a korábban felállított Kormányzati Szakértői Csoportból óhatatlanul kimaradtak.[56]

[54] UN Group of Governmental Experts (UN GGE). A multilaterális szabályozási törekvések jó összefoglalóját adja közre Tikk–Kertunnen 2018.

[55] Az ENSZ Közgyűlés 66/24 sz., 2011-ben elfogadott határozata. Barrinha–Renard 2017, 359.

[56] Ruhl et al. 2020, 7.

A multilaterális szinten történő egyeztetések, normakidolgozások területén említésre méltó kezdeményezés volt még az úgynevezett Kibertér Stabilitási Globális Bizottság (Global Commission on the Stability of Cyberspace), amit két magán kutatóintézet (think tank) hívott életre 2019 novemberében. A cél az volt, hogy széles körből merítve a résztvevőket, a kormányzat mellett a tudományos élet, az ipar és a civil világ képviselőit is bevonja a kibertér nemzetközi normáinak kialakítását célzó közös gondolkodásba. A testület által közreadott *Szingapúri Normacsomag* című dokumentumban foglalt ajánlások végül bekerültek egy másik nemzetközi szabályalkotó grémium, az úgynevezett Párizsi Felhívás dokumentumai közé is.[57]

Az ugyancsak 2019 novemberében életre hívott Párizsi Felhívás[58] (Paris Call for Trust and Security in Cyberspace) a francia kormányzat kezdeményezése, amely mögé a Microsoft vállalat is beállt főtámogatónak. Aláírói (több mint ezer különféle kormányzati és magánszervezet, tudományos és szakmai entitás) kilenc önkéntesen vállalt norma mellett tették le a voksukat. Az alapelvek (amelyek között hangsúlyosan szerepel az egyének és a kritikus infrastruktúrák védelme, az Internet nyilvános magjának védelme, valamint az online választói folyamatok kiemelt védelme) a korábbi megelőző multilaterális egyeztetések eredményeire építettek.[59]

Végezetül érdemes röviden megemlíteni az EU szerepét, törekvéseit.[60] Az Unió 2016-ban elfogadott alapvető biztonságpolitikai dokumentuma a tagállamokra leselkedő veszélyek között kiemelt helyen említi a kibertér fenyegetéseit.[61] A dokumentum leszögezi: az EU-nak a jövő felé tekintő kiberszereplővé kell válnia a kiberdiplomácia terén.[62] Az Unió koncepciójában – miközben a szervezet egyértelműen tudatában van a kiberdomén veszélyeztetettségének rohamos növekedésével – a kiberbűnözéssel, kiberkárokozással szembeni küzdelemben egyértelműen a kiberdiplomácia jelenik meg központi pillérként.

Kitekintés

Változnak az idők – és a jelek szerint velük változnak a „terek" is. Tanulmányunk elején igyekeztünk végigkövetni az utat, amelynek során a földgolyó országainak egymáshoz való kapcsolódási hálója, a manapság ismét sokat emlegetett világrend fokozatosan átalakult: a második világháború nem csupán emberéletekben és anyagi értékekben okozott rettenetes pusztítást, de egyben a hatalmi viszonyokat is drámaian átszabta, megágyazva egy olyan kétpólusú berendezkedésnek, ahol a világban csupán két óriás számított, az USA és a Szovjetunió. A hidegháború végével, az 1990-as évek

[57] Ruhl et al. 2020, 7.
[58] Ruhl et al. 2020, 7.
[59] *Paris Call for Trust and Security in Cyberspace,* továbbá Ruhl et al. 2020. 7.
[60] Az Európai Unió kiberbiztonsági politikáival a könyv külön fejezete foglalkozik részletesen.
[61] Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy 2016, 22.
[62] Latici 2019.

legelejére, a riválisnagyhatalom és maga köré épített blokkjának felbomlása nyomán Amerika hirtelen egyedül maradt a hatalom porondján. Ez volt a szakértők által említett „unipoláris pillanat", amikor a világ a liberális demokráciák élén álló USA vezetésével egypólusúvá alakult. A megnevezés találó, mert mára jól látszik, hogy ez a hatalmi konstrukció – történelmi léptékkel mérve – valóban csupán egy pillanatig tartott. A 2000-es évek első évtizedétől, régi és új hatalmak bejelentkezésével és emelkedésével fokozatosan látszik kiépülni egy újabb, immár multipoláris világrend. Olyan hatalmi konstrukció, ahol helyi-regionális és természetesen világhatalmi ambíciókkal rendelkező államok egész sora alkot erőközpontokat, egymást sokszor keresztülszelő hatalmi hálókat. A hálómetafora használata kétszeresen is indokoltnak látszik. A hatalmi erőegyensúlyban, geopolitikai viszonyrendszerben ugyanis egyre meghatározóbbá válik a kibertér dimenziója.[63] Az a számítógépes rendszerekből, szoftverekből és azokat használó emberekből a világháló révén összefont struktúra tehát, amit röviden kibertérnek nevezünk. Jól látható már az állami kiberképességek erőkompenzáló funkciója: kicsi (tehát a szokványos hatalomdefiníciók szerint meghatározó szerepre alkalmatlan) országok is, hálózatos technológiai kapacitásaik kiépítésével olyan világpolitikai szereplőkké válnak, amelyekkel számolni kell.[64]

Ez az egyszerre virtuális és ugyanakkor kézzelfoghatóan valóságos tér maga is változóban van. Éppen azért, mert a geopolitikai átrendeződések visszahatnak erre az egyre fontosabb vetélkedési területre is. A kiberteret születésekor, létrejötte pillanatától a nyugati világ elvei és koncepciói formálták.[65] Liberális elvek szerint szerveződött, nyugati technológiák és intézmények dominálták. Ahogy a világ változik, jól láthatóan változni kezdett ez a tér is. A multipoláris világrend feltörekvői bejelentkeztek a kibervalóság „átvételére" is, de legalább a korábbi nyugati (amerikai) monopolhelyzet felszámolására. Ami a szemünk előtt formálódik tehát, az egy sokkal kevésbé nyugatos, és sokkal inkább „poszt-liberális" kibervilág.[66] Ebben az átalakulásban, a kibertér drámai átrajzolásában egyre meghatározóbb szerepet kapnak a kiberdiplomaták. Ezeken a vidékeken, amelyek korábban az informatikusok, számítástechnikai mérnökök, hálózattudósok felségterületének számítottak, ma már egyre inkább a külkapcsolat-építés hivatásosai mozognak otthonosan. Szakdiplomaták – akik ugyanakkor eligazodnak a modern kibervilág technológiai, jogi és etikai kérdéseiben is.

[63] Barrinha–Renard 2020a, 756.

[64] Barrinha–Renard 2020a. A legismertebb példa a kis nemzetek ilyen „erejükön felüli" pozícionálására, köszönhetően a kiberképességeik színvonalának és nagyságának: Szingapúr és különösen Észtország esete.

[65] A nyugati világban (elsősorban az Egyesült Államokban) születtek a számítástechnika jelentős technológiai fejlesztései, az eszközöktől a szoftvereken át az ott megálmodott Világhálóig. Ezt az előnyt, monopolhelyzetet erősítette tovább az iparág (kezdve a számítástechnikai ipartól az internetes iparokig, közösségi hálózati szolgáltatásokig) szinte teljes Amerika-központúsága (amihez a szintén a nyugati szövetséghez tartozó Japán, Dél-Korea, illetve skandináv államok adtak további koncentráló erőt).

[66] Barrinha–Renard 2020b.

Felhasznált irodalom

A global actor in search of a strategy. European Union foreign policy between multilateralism and bilateralism (2014). Brussels, European Union.

Bába Iván – Sáringer János (2018): *Diplomáciai lexikon. A nemzetközi kapcsolatok kézikönyve.* Budapest, Éghajlat.

Barrinha, André – Renard, Thomas (2017): Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, 3:4–5, 353–364.

Barrinha, André – Renard, Thomas (2020a): Power and Diplomacy in the Post-Liberal Cyberspace. *International Affairs*, vol. 96, Issue 3, May 2020, 749–766.

Barrinha, André – Renard, Thomas (2020b): *The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyberspace.* Forrás: www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace (A letöltés dátuma: 2020. 06. 16.)

Barston, Ronald Peter (2013): *Modern Diplomacy.* New York, Routledge.

Bassot, Etienne (2020): *The von der Leyen Commission's priorities for 2019–2024*. Forrás: www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)646148 (A letöltés dátuma: 2020. 06. 08.)

Berzsenyi Dániel – Krasznay Csaba (2019): *Nemzetközi kapcsolatok a kibertérben*. Budapest, Nemzeti Közszolgálati Egyetem.

Bjola, Corneliu (2015): *Digital Diplomacy.* London-New York, Routledge.

Bjola, Corneliu (2018): Digital Diplomacy 2.0. Trends and Counter-Trends. *Revista Mexicana de Política Exterior*, 2018. 35–52.

Bjola, Corneliu (é. n.): *Digital Diplomacy: From Tactics to Strategy*. Forrás: www.americanacademy.de/digital-diplomacy-tactics-strategy/ (A letöltés dátuma: 2020. 02. 09.)

Blount, P. J. (2019): *Reprogramming the World. Cyberspace and the Geography of Global Order.* Bristol, E-International Relations Publishing.

Borell, Josep (2020): *HR/VP Josep Borell: Embracing 'Geopolitical' Europe's Power.* Forrás: www.eubulletin.com/10653-hr-vp-josep-borrell-embracing-geopolitical-europes-power.html (A letöltés dátuma: 2020. 04. 22.)

Brzezinski, Zbigniew (1999): *A nagy sakktábla*. Budapest, Európa Könyvkiadó.

Choucri, Nazil (2012): *Cyberpolitics in International Relations.* Cambridge, MIT Press.

Clüver Ashbrook, Cathryn (2014): *21st Century Diplomacy.* Forrás:www.belfercenter.org/publication/21st-century-diplomacy (A letöltés dátuma: 2020. 02. 14.)

Cohen, Saul Bernard (2015): *Geopolitics: The Geography of International Relations.* Lanham, Rowman and Littlefield.

Cyberspace Policy Review (é. n.). Forrás: https://fas.org/irp/eprint/cyber-review.pdf (A letöltés dátuma: 2020. 02. 27.)

Desforges, Alix (2014): Representations of Cyberspace: A Geopolitical Tool. *Hérodote*, 2014/1 (No. 152–153) 67–81.

Dee, Megan (2015): *The European Union in a Multipolar World. World Trade, Global Governance and the Case of the WTO.* London, Palgrave MacMillan.

Domingo, Francis C. (2016): Conquering a new domain: Explaining great power competition in cyberspace. *Comparative Strategy*, 35(2). 154–168.

Fourkas, Vassilys (2004): What is 'cyberspace'? *Media Development* 2004/3 6–7.

Global Trends to 2035. Geo-politics and international power (2017). Brussels, European Parliamentary Research Service.

History of Digital Diplomacy and Main Milestones (é. n.). Forrás: http://diplomacydata.com/history-of-digital-diplomacy-and-main-milestones/ (A letöltés dátuma: 2019. 05. 20.)

Jaywardane, Sash (2015): *Cyber Governance: Challenges, Solutions and Lessons for Effective Global Governance.* The Hague, The Hague Institute for Global Justice.

Kaplan, Robert D. (2019): *A földrajz bosszúja.* Budapest, Antall József Tudásközpont.

Kissinger, Henry (2016): *Világrend*. Budapest, Antall József Tudásközpont.

Kumar, Davinder (2015): Securing cyberspace: A Global Commons. *Indian Defense Review*, vol. 30(2). Forrás: www.indiandefencereview.com/news/securing-cyberspace-a-global-commons/ (A letöltés dátuma: 2020. 05. 24.)

Kuus, Merje (2007): *Geopolitics Reframed. Security and Identity in Europe's Eastern Enlargement.* New York, Palgrave MacMillan.

Latici, Tania (2019): *Cyber: How big is the threat?* Forrás: www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2019)637980 (A letöltés dátuma: 2020. 05. 20.)

Lehne, Stefan (2017): *Is There Hope for EU Foreign Policy?* Brussels, Carnegie Endowment.

Manor, Illan (2016): *What is Digital Diplomacy, and how is it Practiced around the World?* Forrás: www.researchgate.net/publication/310952363_What_is_Digital_Diplomacy_and_how_is_it_Practiced_around_the_World_A_brief_introduction/link/583b591708ae3a74b4a06b2f/download (A letöltés dátuma: 2020. 06. 08.)

Manor, Illan (2017): *Exploring Digital Diplomacy. Toward Clarification of a Fractured Terminology.* Forrás: https://digdipblog.com/countries-on-twitter-and-facebook/ (A letöltés dátuma: 2020. 06. 08.)

Melissen, Jan et al. (é. n.): *Diplomacy in the Digital Age*. The Hague, Clingendael.

Müller-Hennig, Marius (2019): *A truly geopolitical EU Commission? Rather than playing geopolitical games itself, von der Leyen's Commission should be critical of the very notion of geopolitics.* Forrás: www.ips-journal.eu/regions/europe/article/show/a-truly-geopolitical-eu-commission-3918/ (A letöltés dátuma: 2020. 05. 06.)

Nyáry, Gábor (2019): A digitális állam a külpolitikai térben. A Twittertől az adattudományig. Új Magyar Közigazgatás, 12. évf., 2. sz. 75–82.

Office of the Coordinator of Cyber Issues (é. n.). Forrás: www.state.gov/bureaus-offices/bureaus-and-offices-reporting-directly-to-the-secretary/office-of-the-coordinator-for-cyber-issues/ (A letöltés dátuma: 2020. 06. 08.)

Paris Call for Trust and Security in Cyberspace (2018). Forrás: https://pariscall.international/en/call (A letöltés dátuma: 2020. 06. 08.)

Pintér István szerk. (2016): *Műhelymunkák. A virtuális tér geopolitikája. 2016/1* Budapest, Geopolitikai Tanács Közhasznú Alapítvány.

Public diplomacy stratégiák. (é. n.). Budapest, Századvég Politikai Iskola Alapítvány.

Rana, Kishan. S. (2011): *21st Century Diplomacy. A Practicioner's Guide*. London–New York, The Continuum International.

Riordan, Shaun (2019): *Cyberdiplomacy. Managing Security and Governance Online.* Cambridge, Polity Press.

Ruhl, Christian (2020): *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at Crossroads.* Washington, Carnegie Endowmwent.

Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy (2016).

Szilágyi István (2018): *A geopolitika elmélete.* Budapest, Pallas Athéné Könyvkiadó.

„The Key Problem of Our Time": A Conversation with Henry Kissinger on Sino-U.S. Relations (2018). Forrás: www.wilsoncenter.org/article/the-key-problem-our-time-conversation-henry-kissinger-sino-us-relations (A letöltés dátuma: 2020. 06. 08.)

Tianjiao, Jiang (2019): From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar. *Chinese Journal of International Review* vol. 1, no. 2. 1–23.

Tikk, Eneken – Kerttunen, Mika (2018): *Parabasis. Cyber diplomacy in Stalemate.* Oslo, Norwegian Institute of International Affairs.

US Department of Defense Cyber Strategy 2018 (2018). Forrás: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (A letöltés dátuma: 2020. 06. 08.)

Whyte, Christopher – Mazanec, Brian (2019): *Understanding Cyber Warfare: Politics, Policy and Strategy.* New York, Routledge.

VÁKÁT OLDAL

Molnár Anna

A kiberdiplomácia fejlődése az Európai Unióban

Bevezetés

Noha az Európai Unió (a továbbiakban: EU) már a kilencvenes évek második felétől megkezdte a számítástechnikával és az elektronikus kommunikációval kapcsolatos tevékenységeinek fejlesztését, az átfogó megközelítésre építő kiberbiztonsági szakpolitikai keret- és intézményrendszer kiépítése valójában csak az elmúlt évtizedben kezdődött el. Az egyénekkel, vállalatokkal és a kritikus infrastruktúrákkal szembeni növekvő számú kibertámadások egyre inkább felhívták a figyelmet a kibertérrel kapcsolatos fenyegetésekre és kockázatokra. Tekintettel arra, hogy a számítógépes bűnözés nem ismeri a nemzeti határokat, e területen is szükségessé vált az uniós szintű együttműködés feltételrendszerének kiépítése. Ezt a folyamatot jogi intézkedések elfogadása (például az információs rendszerek elleni támadásokról szóló 2005. évi tanácsi kerethatározat), és új intézményi struktúrák létrehozása (például az Európai Hálózat- és Információbiztonsági Ügynökség – ENISA 2004-ben és a Europolban a számítástechnikai bűnözéssel foglalkozó európai központ, az EC3 létrehozása 2013-ban) jelezte.[67] E tanulmány célja, hogy átfogó képet nyújtson az EU kiberdiplomáciával összefüggő intézményi struktúrákról és stratégiai keretekről.

2007 után az észt magán- és közintézmények, illetve infrastruktúra ellen elkövetett orosz eredetű elosztott szolgáltatásmegtagadással járó támadásokat (DDoS) követően az EU egyre nagyobb hangsúlyt fektetett az információ- és hálózatbiztonság megerősítésére. Napjainkra a kibertér a nemzetközi kapcsolatok kiemelt területévé vált, és az uniós külpolitika szerves részét képezik a kiberdiplomáciával kapcsolatos területek. Az Európai Unió is megkezdte a kiberdiplomáciával és a kibervédelemmel összefüggő eszköz- és intézményrendszerének kiépítését.

Az uniós intézmények és infrastruktúra elleni egyre célzottabb és nagyszabású kibertámadások arra késztették a döntéselőkészítőket és döntéshozókat, hogy a hatáskörükbe tartozó főbb tevékenységek mindegyikére kiterjedő átfogó kiberbiztonsági politikát fejlesszenek. Az EU-ról szóló szerződés 3. cikke sorolja fel az Unió céljait és tevékenységeinek főbb területeit. Ezek közül kiemelhető az egységes piac megvalósítása, a szabadság, biztonság és jog térségének kialakítása és a közös kül- és biztonságpolitika megvalósítása. A 2010-es évektől megkezdődött a kiberbiztonsággal és kibervédelemmel összefüggő többszintű kormányzás uniós szintű eszköz- és intézményrendszerének a kiépülése.[68] Ennek fontos elemeként a kiberdiplomáciával összefüggő tevékenységek elsősorban a közös kül- és biztonságpolitikát, és annak szerves részét képező közös biz-

[67] Carrapico–Barrinha 2018.
[68] Christou 2018, 1–2.

tonság- és védelempolitika területeit érintik, de a közös piaccal és a szabadság, biztonság és jog térségének kialakításával összefüggő kiberbiztonsági kérdések nemzetközi szintű képviselete is ide tartozik.

Számos, az EU kiberbiztonságát és kiberdiplomáciáját befolyásoló tényező, mint például az egyre nagyobb számban jelentkező kiberfenyegetések és kibertámadások között megemlíthetjük az Egyesült Királyság kilépését az EU-ból. Noha a Brexit valószínűsíthetően e területen is negatív hatást gyakorol, az EU és az EK közötti kölcsönös egymásrautaltság a szoros kapcsolatok fenntartását fogja eredményezni.[69]

Kiberdiplomácia

A kiberdiplomácia fogalmára számos definíció található a szakirodalomban. Ezek közül megemlíthetjük André Barrinha és Thomas Renard meghatározását, amely szerint a kiberdiplomácia a kibertérrel összefüggő diplomácia, vagyis diplomáciai erőforrások felhasználása és diplomáciai feladatok ellátása a kibertérrel kapcsolatos ügyek és a nemzeti érdekek biztosítása érdekében. Az ezzel összefüggő érdekeket és célokat a kiberbiztonsági stratégiák fektetik le. A kiberdiplomácia napirendjén szereplő legfontosabb kérdések között megemlíthetjük a kiberbiztonság, a kiberbűnözés, a bizalomépítés, az internet szabadsága és az internet irányítása területeit. A kiberdiplomácia legfontosabb szereplői közé a hagyományos diplomaták, illetve az e szakpolitikai területen meghatározó szerepet játszó különböző intézmények, testületek és ügynökségek képviselői tartoznak.[70] Mivel napjainkban a kibertérben egyre gyakoribbak az egyes szereplők és, ebből következően, a nagyhatalmak közötti feszültségek, egyre nagyobb szükség van az ilyen típusú konfliktusok rendezését célzó nemzetközi tárgyalások folytatására és megállapodások kötésére. Az elmúlt évtizedekben az EU nem csupán a saját tagállamai közötti integrációs folyamat mélyülése következtében, hanem a kiberbiztonsággal és kibervédelemmel összefüggő nemzetközi viták rendezése érdekében is egyre aktívabb szerepet töltött be.[71]

Noha az IKT (információ- és kommunikációtechnológiai) eszközök használata egyre elterjedtebb a külügyi igazgatási szintek különböző szereplői körében, a kiberdiplomácia és az e-diplomácia – amelyet elektronikus vagy digitális diplomáciának is nevezünk – két különböző fogalomként határozható meg. Annak ellenére, hogy a két fogalom használata sokszor keveredik, esetenként egymás szinonímáiként is használják azokat, a két fogalom között jelentős különbség van. A legfőbb különbséget abban határozhatjuk meg, hogy az e-diplomácia kizárólag a digitális eszközök használatát jelenti a diplomaták, a külügyi alkalmazottak és külügyminiszterek által. Tom Fletcher szerint az e-diplomácia hivatalosan 1994-ben született, amikor a svéd külügyminiszter, Carl Bildt elküldte első hivatalos diplomáciai e-mail-jét Bill Clintonnak. A svéd diplomata így gratulált

[69] Stevens–O'Brien 2019.
[70] Barrinha–Renard 2017, 3.
[71] Renard 2018.

az amerikai elnöknek a Vietnámmal szemben alkalmazott embargó megszüntetésének alkalmával.[72] Ezzel szemben Smith és Sutherland a kiberdiplomácia kifejezést az egyre intenzívebb, a digitális eszközök segítségével megvalósuló diplomáciai tevékenységek meghatározásaként is használják.[73]

Az uniós kiberdiplomácia fejlődése

Stratégiai keretek

A 2000-es évektől egyre több uniós dokumentum foglalkozott a kiberbiztonság szerteágazó kérdésével. Az első átfogó kiberbiztonsági stratégia kidolgozására 2013-ban került sor, az új dokumentum a *Nyílt, megbízható és biztonságos kibertér* címet viselte".[74] A stratégia elkészítésében az EU külügyi és biztonságpolitikai főképviselője, Chatherine Ashton irányításával az Európai Külügyi Szolgálat és az Európai Bizottság is együttműködött. E dokumentum említette először az EU nemzetközi kiberbiztonsági politikáját és kibervédelmi céljait. A NATO hasonló stratégiáival összehasonlítva (2008, 2011) az uniós dokumentum nem csupán a saját informatikai hálózatának védelmére szorítkozott, hanem szinte minden uniós kompetenciába tartozó területre kiterjedt.[75]

A 2013-as stratégia az EU nemzetközi kiberpolitikájával kapcsolatos céljait is meghatározta. Az új szakpolitika a szabad és nyitott internet védelme mellett célul tűzte ki a felelősségteljes állami magatartás nemzetközi jogi normáinak és a bizalomépítő intézkedések előmozdítását a kibertérben és az EU stratégiai partnereivel történő együttműködés javítását. Az uniós kiberdiplomácia részeként tárgyalások kezdődtek az Egyesült Államokkal, Kínával, Japánnal, Dél-Koreával, Indiával és Brazíliával. A résztvevő felek a tárgyalások során többek között érintették a kibertérben zajló nemzetközi biztonság, az ellenálló képesség, a kiberbűnözés, az internet szabályozása és a kiberbiztonsági előírások területeit.

Kiberdiplomácia

2015-ben fontos mérföldkő volt az EU kollektív erőfeszítéseinek elősegítése érdekében a kiberdiplomáciáról szóló tanácsi következtetések elfogadása.[76] Barrinha és Renard szerint ez volt az első olyan hivatalos kormányzati dokumentum, amely a kiberdiplomácia kifejezést használta.[77] 2015-től – a tanácsi következtetésekkel és az általános külpolitikai célokkal összhangban – az EU a kiberdiplomácia területén is elő kívánta mozdítani és védeni az emberi jogokat.

[72] Barrinha – Renard 2017, 4.
[73] Smith–Sutherland 2002, 155.
[74] Európai Bizottság 2013.
[75] Rehrl 2018, 18.
[76] Rehrl 2018, 23; Cavelty 2018, 10.
[77] Barrinha–Renard 2017, 7..

A kiberdiplomácia „az Unió alapvető értékein, vagyis a demokrácián, az emberi jogokon és a jogállamiságon, ezen belül a véleménynyilvánítás szabadságához való jogon, az információhoz való hozzáférés szabadságán és a magánélethez való jogon alapul. Az Unió célja annak biztosítása, hogy ne lehessen az internet nyújtotta lehetőségekkel visszaélni gyűlöletkeltés és erőszakra való felbujtás céljával, valamint hogy az internet – az alapvető szabadságok teljes tiszteletben tartásával – továbbra is a szabad véleménynyilvánítás fóruma maradjon a jog maradéktalan betartása mellett. A célok között megjelenik a nemek közötti egyenlőséget is figyelembe vevő kiberpolitika előmozdítása. Az EU ösztönzi az európai növekedést, jólétet és versenyképességet, valamint védi a legfontosabb uniós értékeket, többek között a kiberbiztonság erősítése és a számítástechnikai bűnözés elleni küzdelem terén folytatott együttműködés javítása révén. Az uniós diplomáciai és jogi eszközök igénybevétele révén hozzájárul a kiberbiztonságot fenyegető veszélyek mérsékléséhez, a konfliktusmegelőzéshez és a stabilitás növekedéséhez a nemzetközi kapcsolatok terén. Mindemellett segíti az internet irányítására vonatkozó többérdekeltes modell erősítésére irányuló erőfeszítéseket. Az EU ösztönzi a nyitott és virágzó társadalmak kialakulását harmadik országokban olyan kiberkapacitás-építési és -fejlesztési intézkedéseken keresztül, amelyek hozzájárulnak a véleménynyilvánítás és az információhoz való hozzáférés szabadságához való jog előmozdításához és védelméhez, és amelyek lehetővé teszik a polgárok számára, hogy teljes mértékben a javukra fordítsák a kibertér társadalmi, kulturális és gazdasági előnyeit, többek között a digitális infrastruktúrák biztonságosságának fokozása révén. Az Európai Unió célja, hogy előmozdítsa a felelősség megosztását az érintett érdekelt felek között, többek között a köz- és a magánszektor, valamint a kutató- és tudományos intézetek között a kibertérrel kapcsolatban folytatandó együttműködés révén."[78]

Kiberbiztonság és a digitális egységes piac

A 2010-es években az európai gazdaságok egyre szélesebb körű digitalizációja sürgette a biztonságos kibertér támogatását célzó uniós szintű stratégiák és intézkedések kidolgozását. A 2015-ös digitális egységes piaci stratégia a gazdaság digitalizációjával összefüggő kérdések mellett a kibertér biztonságát, azaz a kritikus infrastruktúra és a hálózatok védelmét is hangsúlyozta.[79] A 2015-ös uniós belső biztonsági stratégia és a hibrid fenyegetések elleni fellépést szorgalmazó európai bizottsági és külügyi szolgálati dokumentum is stratégiai irányelveket fogalmazott meg a kiberbűnözéssel és a kiberbiztonsággal kapcsolatban.[80] Az Unió 2016-ban meghozta az első kiberbiztonságra vonatkozó uniós jogi aktust, a hálózati és információs rendszerek biztonságáról szóló (EU) irányelvet (NIS).[81]

[78] Európai Unió Tanácsa 2015.
[79] Európai Bizottság 2015.
[80] Christou 2018, 2.
[81] Európai Parlament és a Tanács (EU) 2016/1148 irányelve.

Kiberdiplomáciai eszköztár

Az Európai Unión belüli, kiberbiztonsággal összefüggő szakpolitikai területek mélyülése következtében az e területekkel összefüggő érdekeket képviselő diplomáciai eszköztár megerősítése is szükségessé vált. Az Unió politikai, biztonsági és gazdasági érdekeinek átfogó védelme érdekében, 2017-ben az EU Tanácsa megállapodott arról, hogy kidolgozza az állami és nem állami szereplők részéről mutatkozó rossz szándékú és tudatos kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretét, az úgynevezett kiberdiplomáciai eszköztárat (EU Cyberdiplomacy Toolbox). Az új eszköztár az EU közös kül- és biztonságpolitikai eszköztárára támaszkodik. A tanácsi döntéssel összhangban azon információs és kommunikációs technológiák (IKT) felhasználásával végrehajtott tevékenységekkel szemben, amelyek kimeríthetik a nemzetközi jogot sértő cselekmény fogalmát, az EU kész a közös kül- és biztonságpolitikai intézkedésekkel, ideértve a korlátozó intézkedéseket is, fellépni.[82]

Az EU kiberdiplomáciai megközelítésével összhangban a közös intézkedések elősegítik a konfliktusmegelőzést, a kiberbiztonságot fenyegető veszélyek mérséklését, és a stabilitás növekedését a nemzetközi kapcsolatok terén. A Tanács célul tűzte ki, hogy a közös uniós diplomáciai intézkedések kerete segíti az együttműködést, előmozdítja a veszélyek csökkentését, valamint hatással lesz a potenciális támadók magatartására. Döntés született arról is, hogy ezekben az esetekben teljes körűen alkalmazni fogják a közös kül- és biztonságpolitika területéhez tartozó intézkedéseket, beleértve a korlátozó, esetleg szankciós intézkedéseket is. Az alkalmazott intézkedéseknek – a nemzetközi joggal összhangban – arányosnak kell lenniük a rossz szándékú „kibertevékenység hatókörével, léptékével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásaival." Az EU egyúttal megerősítette, hogy „elkötelezett a kibertérben folyó nemzetközi viták békés úton történő rendezése mellett." Ezzel összefüggésben minden erőfeszítése arra irányul, hogy hozzájáruljon a kibertér biztonságához és stabilitásához, illetve hogy csökkentse az IKT használatából eredő félreértések, konfliktusok kialakulásának és terjedésének kockázatát.[83]

A Politikai és Biztonsági Bizottság 2017. október 11-én a kiberdiplomáciai eszköztárra vonatkozóan végrehajtási iránymutatásokat fogadott el. A dokumentum a kiberdiplomáciai eszköztáron belül öt intézkedéskategóriát sorolt fel: 1) a megelőző intézkedéseket, 2) az együttműködési intézkedéseket, 3) a stabilitást szolgáló intézkedéseket, 4) a korlátozó intézkedéseket és 5) a lehetséges uniós támogatást a tagállamok jogszerű válaszaihoz. A dokumentum tartalmazza ezen intézkedések bevezetésére vonatkozó eljárást is.[84]

A megelőző intézkedések közé sorolhatjuk az EU által támogatott bizalomépítő intézkedéseket, az uniós politikákkal kapcsolatos tudatosság fejlesztését és az EU támogatását a kiberterületen megvalósuló kapacitásépítés érdekében a harmadik országokban. Az együttműködési intézkedések tartalmazzák az EU által vezetett politikai és tematikus

[82] Európai Unió Tanácsa 2017a.
[83] Európai Unió Tanácsa 2017a.
[84] Council of the European Union 2017a; Tanács (KKBP) 2019/797 határozata.

párbeszédeket vagy az EU küldöttségeinek részvételével folytatott diplomáciai lépéseket. A stabilitást szolgáló intézkedések közé a főképviselő vagy az EU Tanácsa nevében tett nyilatkozatok, a tanácsi következtetések vonatkozó részei, az uniós küldöttségek diplomáciai lépései és az EU által vezetett politikai és tematikus párbeszédek révén megfogalmazott jelzések tartoznak. A korlátozó intézkedések magukban foglalhatnak többek között utazási tilalmakat, fegyverembargót, pénzeszközök vagy gazdasági források befagyasztását. A lehetséges uniós támogatások között a dokumentum a lisszaboni szerződés kölcsönös segítségnyújtási klauzuláját (42.7 cikk) is megemlíti.[85]

Közös biztonság- és védelempolitika

2017-ben a globális stratégia végrehajtásával megkezdődött az európai védelmi együttműködés elmélyítését szolgáló kezdeményezések gyakorlati megvalósítása: így az állandó strukturált együttműködés (PESCO) alkalmazása, a védelmi kiadások koordinált éves felülvizsgálata (Co-ordinated Annual Review on Defence, CARD), a Katonai Tervezési és Végrehajtási Szolgálat (MPCC) létrehozása, illetve az Európai Bizottság által készített európai védelmi cselekvési terv (European Defence Action Plan, EDAP) alapján az Európai Védelmi Alap (EDF) felállításának előkészítése. Az Európai Védelmi Alap létrehozásával kapcsolatos tervek is kiemelt prioritásként tekintettek a kibervédelemi intézkedések és a kiberbiztonsággal kapcsolatos uniós kezdeményezések és így az Unió különböző szakpolitikái közötti szinergiák támogatására.[86]

2016-tól kiemelt szerepet kapott a védelmi területen történő állandó strukturált együttműködés (Permanent Structured Cooperation – PESCO) megvalósítása. A 2017-től induló összesen 47 PESCO projekt közül nyolc a kibertér kérdésköréhez kapcsolódik:

- a biztonságos európai szoftverirányítású rádió (European Secure Software defined Radio – ESSOR);
- a kiberfenyegetésekre és kiberbiztonsági eseményekre való reagálással kapcsolatos információmegosztási platform (Cyber Threats and Incident Response Information Sharing Platform);
- kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok, valamint kölcsönös segítségnyújtás a kiberbiztonság területén (Cyber Rapid Response Teams and Mutual Assistance in Cyber Security);
- stratégiai vezetési és irányítási (C2) rendszer a KBVP-missziók és -műveletek vonatkozásában (Strategic Command and Control (C2) Systems for CSDP Missions and Operations);
- európai magaslégköri léghajó-platform – kitartó hírszerzési, megfigyelési és felderítési képesség (European High Atmosphere Airship Platform (EHAAP) – Persistent Intelligence, Surveillance and Reconnaissance (ISR) Capability);

[85] Council of the European Union 2017a.
[86] Javaslat az Európai Parlament és a Tanács rendelete 2018.

– egyetlen, taktikai vezetési és vezetés-irányítási (C2) állomás a bevethető különleges műveleti egységek számára a kisebb együttes műveletekben (One Deployable Special Operations Forces [SOF] Tactical Command and Control [C2] Command Post [CP] for Small Joint Operations [SJO] – [SOCC] for SJO).[87]

Kibervédelmi szakpolitikai keret

A 2018-as kibervédelmi szakpolitikai keret szerint a korábbi évek eseményei még inkább rávilágítottak arra a tényre, hogy a nemzetközi közösségnek együtt kell működnie a konfliktusok megelőzése és a kibertér stabilitásának erősítése érdekében. „Az EU más nemzetközi szervezetekkel, elsősorban az ENSZ-szel (Egyesült Nemzetek Szervezete), az EBESZ-szel (Európai Biztonsági és Együttműködési Szevezet) és az ASEAN (Délkelet-ázsiai Nemzetek Szövetsége – Association of Southeast Asian Nation) regionális fórummal együtt elő kívánja mozdítani egy olyan, a konfliktusmegelőzésre, az együttműködésre és a kibertér stabilitásának erősítésére vonatkozó stratégiai keretet, amely magában foglalja a következőket: a nemzetközi jognak és különösen az ENSZ Alapokmányának teljes körű alkalmazása a kibertérben; a kibertérben tanúsított felelősségteljes állami magatartásra vonatkozó egyetemes, nem kötelező erejű normák, szabályok és elvek tiszteletben tartása; regionális bizalomépítő intézkedések kidolgozása és végrehajtása. Ezt a törekvést az uniós kibervédelmi szakpolitikai keretnek is támogatnia kell."[88]

Korlátozó intézkedések

2019-ben az EU jelentős előrehaladást ért el a rossz szándékú kibertevékenységekkel szembeni közös uniós kiberdiplomáciai eszköztár működőképessé és hatékonnyá tétele érdekében. Az Európai Tanács 2018. júniusi és 2018. októberi következtetéseiben megfogalmazott célok elérése érdekében olyan uniós korlátozó intézkedések bevezetéséről döntött, amelyek segítik a kibertámadásokkal kapcsolatos reagálási és elrettentési képesség javítását. 2019. május 17-én döntés született az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló KKBP-határozatról[89] és a tanácsi rendeletről[90]. A határozat a rossz szándékú és szándékos kibertevékenységekkel szembeni közös uniós korlátozó intézkedések alkalmazhatóságáról döntött, a rendelet pedig a jelentős hatású kibertámadások esetén szankciók alkalmazását teszi lehetővé az EU részéről.

Az új jogi keret így már lehetővé tette az EU számára, hogy szankciókat is kivethessen (például eszközök befagyasztása, utazási tilalom) az Unióra vagy a tagállamaira külső fenyegetést jelentő kibertámadásoktól való elrettentés, valamint az azokra való

[87] PESCO 2020.
[88] Európai Unió Tanácsa 2018, 8.
[89] Tanács (KKBP) 2019/797 határozata.
[90] Tanács (EU) 2019/796 rendelete.

reagálás érdekében.[91] A szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük (A Tanács [EU] 2019/796 rendelete 15. cikk).

„Az EU az alábbi elvek alapján fogja folytatni a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretének kidolgozását:

- védeni kell az EU, az uniós tagállamok és az uniós polgárok sértetlenségét és biztonságát;
- figyelembe kell venni az érintett állammal fennálló uniós külkapcsolatok tágabb összefüggéseit;
- biztosítani kell a KKBP-célkitűzések elérését, az Európai Unióról szóló szerződésben foglaltakkal és az e célkitűzések elérése érdekében meghatározott megfelelő eljárásokkal összhangban;
- az intézkedéseknek a tagállamok által közösen kialakított helyzetismereten kell alapulniuk, és meg kell felelniük az adott helyzet támasztotta igényeknek;
- az intézkedéseknek arányosnak kell lenniük a kibertevékenység hatókörével, léptékével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásaival;
- tiszteletben kell tartani az alkalmazandó nemzetközi jogot és nem szabad alapvető jogokat és szabadságokat sérteni."[92]

Az EU–NATO együttműködés

A lisszaboni szerződés hatálybalépését követően, és az uniós diplomáciai intézményrendszer, a képességek és hatáskörök bővülésének köszönhetően az EU nemzetközi jelenléte és szerepe folyamatosan erősödött. Az Európai Unió a hagyományos normatív szerepén túl a kiberdiplomácia területén megvalósított stratégiai partnerségi kapcsolatok kialakításában is érdekeltté vált. E bilaterális kapcsolatok jelentős szerepet játszanak a multilaterális együttműködési formák megerősítésében.[93] Napjainkban az együttműködésen alapuló, a nyugati inspirációjú multilaterális keretekre épülő nemzetközi rendszer szétfeszülni látszik. Mivel a kibertérben is új regionális és globális hatalmak felemelkedése várható, az EU továbbra is a multilaterális együttműködési formák fenntartásában és megerősítésében érdekelt.

A 2015-ös kiberdiplomáciáról szóló tanácsi következtetésekkel összhangban az EU a legfontosabb partnerekkel és a nemzetközi szervezetekkel stratégiai együttműködést kíván kialakítani, és hangsúlyozza, hogy a kibertérrel kapcsolatos kérdésekben hozott szakpolitikai döntések többsége szükségessé teszi az aktív nemzetközi párbeszédet, együttműködést és koordinációt.[94] Mindezzel összefüggésben a NATO-val kiépített kapcsolatok jelentősége is fokozatosan növekedett.

[91] Európai Bizottság 2019, 9.
[92] Európai Unió Tanácsa 2017b.
[93] Renard 2018, 5.
[94] Európai Unió Tanácsa 2015.

Az EU és a NATO közötti együttműködés területén kialakított folyamat valódi lendületet 2016-tól kapott. Az EU globális stratégiájának elfogadását követő végrehajtási folyamatban a két nemzetközi biztonsági szervezet között a kiberbiztonság és kibervédelem területén egyre intenzívebb kapcsolat jött létre.[95] A globális stratégia hangsúlyozza, hogy míg a NATO a kollektív védelem elsődleges keretét biztosítja a legtöbb tagállam számára, addig az EU elsősorban az olyan belső és külső kihívásokkal szemben kíván fellépni, mint a terrorizmus, a hibrid fenyegetések, a kiber- és energiabiztonság, a szervezett bűnözés és a külső határok igazgatása.

2016. július 8-án a NATO-csúcson Varsóban az EU részéről az Európai Tanács elnöke és az Európai Bizottság elnöke, illetve a NATO főtitkára együttes nyilatkozatot írt alá az EU és a NATO közötti együttműködésről. A nyilatkozat aláírását követően a két szervezet közötti együttműködés új lendületet kapott, és kiterjed a hibrid fenyegetések elleni küzdelemre; a kiberbiztonság és -védelem területeire is.[96] Az együttes nyilatkozat konkrét célkitűzéseket fogalmazott meg a kibervédelmi együttműködés előmozdítása érdekében: megerősíteni a kibervédelemi interoperabilitást a missziók és műveletek során; az együttműködés erősítése a képzéseken és a gyakorlatokon; a kibervédelmi kutatásokkal és technológiai innovációval kapcsolatos együttműködés előmozdítása; valamint a kibernetikus szempontok beépítése a válságkezelésbe.[97]

2016 februárjában, az EU és a NATO képviselői aláírták az EU hálózatbiztonsági vészhelyzeteket elhárító csoportja (Computer Emergency Response Teams – CERT) és a NATO hálózatbiztonsági incidenskezelő csoportja (NATO's Computer Incident Response Capability – NCIRC) közötti technikai megállapodást. A megállapodás célja a technikai információk megosztásának megkönnyítése a számítógépes események megelőzése érdekében, illetve a kiberbiztonsági események felderítése és az azokra való reagálás erősítése mindkét szervezetben. Az e területeken megvalósuló tevékenységek mind a mai napig a két szervezet közötti együttműködés alapját képezik.

Az együttműködés másik legfontosabb eredménye, hogy – finn kezdeményezésre, de az EU és a NATO támogatásával – 2017-ben Helsinkiben létrejöhetett a Hibrid Fenyegetések Elleni Kiválósági Központ (European Centre of Excellence for Countering Hybrid Threats), amelynek feladata az elsősorban Oroszország felől érkező kiberbiztonsági kihívások, a dezinformációs műveletek és a stratégiai kommunikáció elemzése, valamint a kihívásokra hatékony és közösen koordinált válaszok kidolgozása.[98] Az új központ felállítása lehetőséget biztosított az Észak-atlanti Tanács és az uniós Politikai és Biztonsági Bizottság közötti informális találkozók megszervezésére, és így a hibrid fenyegetéssel szembeni koordinált fellépés kidolgozására.[99]

A 2017. novemberi második előrehaladási jelentésben első helyen szerepelt az új központ felállítása. A jelentés emellett kiemelte a tengerbiztonsági, valamint a kiberbizton-

[95] Európai Külügyi Szolgálat 2016.
[96] Európai Unió Tanácsa 2016.
[97] Council of the European Union 2016.
[98] Hybrid CoE n. é. a.
[99] Hybrid CoE 2018.

sági és a védelmi fejlesztés területeken elért eredményeket, illetve ezek közül a képzések és gyakorlatok területén megvalósuló együttműködések fontosságát. A NATO-alkalmazottak például részt vehettek az uniós ügynökség, az ENISMA (European Union Agency for Cybersecurity, Európai Uniós Kiberbiztonsági Ügynökség, a továbbiakban: ENISMA) kiberbiztonsági gyakorlatán. A fejlesztési duplikációk elkerülése érdekében folyamatossá vált az együttműködés.[100]

Az önállóan működő központ munkájába 2020 májusáig Ausztria, Ciprus, a Cseh Köztársaság, Dánia, az Egyesült Királyság, Észtország, Finnország, Franciaország, Görögország, Hollandia, Kanada, Lengyelország, Lettország, Litvánia, Luxemburg, Magyarország, Montenegró, Németország, Norvégia, Olaszország, Portugália, Románia, Szlovénia, Spanyolország, Svédország, Törökország és az USA kapcsolódott be. Fontos megjegyezni, hogy az új együttműködési forma a semleges EU-tagállamok (Ausztria, Finnország és Svédország), illetve a nem uniós NATO-tagok (USA, Kanada és Norvégia) számára is lehetővé tette a csatlakozást. A meglévő ellentétek következtében kezdetben Ciprus és Törökország nem vett részt a megvalósításban.[101]

2017-ben és 2018-ban a NATO és az Európai Unió párhuzamos és összehangolt gyakorlatokat folytattak egy hibrid forgatókönyvre reagálva, annak érdekében, hogy javítsák az EU válaszadási képességét a hibrid fenyegetés esetén, és tovább fejlesszék az EU és a NATO közötti együttműködést. 2017-ben NATO-irányítással, 2018-ban pedig az Unió vezetésével hajtották végre a gyakorlatokat. A 2018-as „EU-HEX-ML 18 (PACE)" gyakorlat jelentősen segítette a szervezetek személyi állományai közötti együttműködést.[102] 2019-ben a jól bevált gyakorlat folytatódott, és a NATO CMX 19 gyakorlat is kiterjedt a személyi állományok közötti együttműködésre az EU intézményeivel (EKSZ, EK és a Tanács).[103]

Következtetések

Az EU döntéshozói kezdetben elsősorban gazdasági kérdésként tekintettek a digitalizációval és az IKT-eszközök használatával kapcsolatos kérdéskörre. A 2010-es évek elejétől azonban megkezdődött e terület biztonságiasításának folyamata, amelyben mérföldkőnek a 2013-as kiberbiztonsági stratégia tekinthető.[104]

Mivel az IKT-eszközök használata az élet minden területére kiterjed, így nem véletlen, hogy napjainkban a kibertér a nemzetközi kapcsolatok kiemelt területévé vált. A nagyhatalmakhoz hasonlóan az uniós külpolitika szerves részét képezik a kiberdiplomáciával kapcsolatos területek. Az elmúlt évtizedekben az ENSZ, a NATO vagy akár az EBESZ hasonló törekvéseivel párhuzamosan az Európai Unió is megkezdte a kiberdiplomáciával és a kibervédelemmel összefüggő eszköz- és intézményrendszerének kiépítését.

[100] Council of the European Union 2017b.
[101] Hybrid CoE n. é. b.
[102] European External Action Service 2018.
[103] Allison 2019.
[104] Christou 2018, 13.

Nemzetközi szinten az EU a kibertérben a konfliktusmegelőzés és a stabilitás érdekében a speciálisan alkalmazandó nemzetközi jog, különösen az ENSZ Alapokmánya és a nemzetközi humanitárius jog szigorú alkalmazását, és a felelősségteljes állami magatartás nem kötelező érvényű egyetemes számítógépes normáinak, szabályainak és alapelveinek teljes végrehajtását határozta meg legfőbb stratégiai céljai között.[105]

Felhasznált irodalom

Allison, George (2019): NATO conducts Crisis Management exercise. *UK Defence Journal*. Elérhető: https://ukdefencejournal.org.uk/nato-conducts-crisis-management-exercise/ (A letöltés dátuma: 2020. 06.13.)

Az Európai Unió Tanácsa (2015): A Tanács következtetései a kiberdiplomáciáról, Brüsszel, 2015. február 11. Elérhető: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf (A letöltés dátuma: 2020. 06.13.)

Barrinha, André – Renard, Thomas (2017): Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, 3. Issue 4–5. 1–13.

Carrapico, Helena – Barrinha, Andre (2018): European Union cyber security as an emerging research and policy field. *European Politics and Society*, 19:3, 299–303.

Cavelty, Myriam Dunn (2018): Europe's cyber-power. *European Politics and Society*, Volume 19, Issue 3. 1–17.

Christou, George (2018): The collective securitisation of cyberspace in the European Union. *West European Politics* 1–24.

Council of the European Union (2016): *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation*. Elérhető: www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf (A letöltés dátuma: 2020. 06. 13.)

Council of the European Union (2017a): *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – approval of the final text, Brussels, 9 October 2017 (OR. en)*. Elérhető: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf (A letöltés dátuma: 2020. 06.13.)

Council of the European Union (2017b): *Second progress report on the implementation of the common set of proposals endorsed by NATO and EU.* Elérhető: www.consilium.europa.eu/media/35577/report-ue-nato-layout-en.pdf (A letöltés dátuma: 2020. 06. 13.)

Európai Bizottság (2013): *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér JOIN/2013/01 final.* Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52013JC0001 (A letöltés dátuma: 2020. 06. 13.)

Európai Bizottság (2015): *Európai digitális egységes piaci stratégia. Brüsszel, 2015.5.6. COM(2015) 192 final.* Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52015DC0192&from=HU (A letöltés dátuma: 2020. 06. 13.)

Európai Bizottság (2019*): Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról, közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Brüsszel, 2019.6.14. JOIN (2019) 12 final*. Elérhető:

[105] Rehrl 2018, 25.

https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52019JC0012&from=EN (A letöltés dátuma: 2020. 05. 13.)

Európai Külügyi Szolgálat (2016): *Közös jövőkép, közös fellépés: Erősebb Európa Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan*. Elérhető: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_hu_.pdf (A letöltés dátuma: 2020. 05. 13.)

Európai Parlament és a Tanács (EU) 2016/1148 irányelve: *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).*

Európai Unió Tanácsa (2016): *EU–NATO együttműködés: A Tanács következtetéseket fogadott el az együttes nyilatkozat végrehajtása céljából*. Elérhető: www.consilium.europa.eu/hu/press/press-releases/2016/12/06/eu-nato-joint-declaration/ (A letöltés dátuma: 2020. 05. 13.)

Európai Unió Tanácsa (2017a): *Informatikai támadások: az EU készen áll az ellenintézkedésekre, ideértve a szankciókat is.* Elérhető: www.consilium.europa.eu/hu/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/ (A letöltés dátuma: 2020. 05. 13.)

Európai Unió Tanácsa (2017b): *Tervezet – a Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („Kiberdiplomáciai eszköztár"), Brüsszel, 2017. június 7. (OR. en)*. Elérhető: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/hu/pdf (A letöltés dátuma: 2020. 05. 13.)

Európai Unió Tanácsa (2018): *Uniós kibervédelmi szakpolitikai keret, (2018. évi naprakésszé tett változat), Brüsszel, 2018. november 19. (OR. en) 14413/18*. Elérhető: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf (A letöltés dátuma: 2020. 05. 13.)

European External Action Service (2018): *Crisis preparedness: EU launches civil-military crisis management exercise, Bruxelles, 16/11/2018 – 15:25, UNIQUE ID: 181116_7*. Elérhető: https://eeas.europa.eu/headquarters/headquarters-Homepage/53926/crisis-preparedness-eu-launches-civil-military-crisis-management-exercise_en (A letöltés dátuma: 2020. 05. 13.)

Hybrid CoE (2018): *Hybrid CoE Supports Informal NAC-PSC Discussion, September 28, 2018.* Elérhető: www.hybridcoe.fi/news/hybrid-coe-supports-informal-nac-psc-discussion/ (A letöltés dátuma: 2020. 03. 13.)

Hybrid CoE (n. é. a): *European Centre of Excellence for Countering Hybrid Threats.* Elérhető: www.hybridcoe.fi/ (A letöltés dátuma: 2020. 03. 13.)

Hybrid CoE (n. é. b): *European Centre of Excellence for Countering Hybrid Threats. What is Hyrid CoE?* Elérhető: www.hybridcoe.fi/what-is-hybridcoe/ (A letöltés dátuma: 2020. 03. 13.)

Javaslat az Európai Parlament és a Tanács rendelete (2018): *Javaslat az Európai Parlament és a Tanács rendelete, az Európai Védelmi Alap létrehozásáról Brüsszel, COM(2018) 476, 2018/0254(COD)*. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52018PC0476 (A letöltés dátuma: 2020. 03. 13.)

PESCO (2020): PESCO Projects. Elérhető: https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/ (A letöltés dátuma: 2020. 03. 13.)

Rehrl, Jochen ed. (2018): *Handbook on cyber security. The Common Security and Defence Policy of the European Union*. Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria. Elérhető: https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1 18 p (A letöltés dátuma: 2020. 03. 13.)

Renard, Thomas (2018): EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*, Volume 19, Issue 3. 321–337.

Smith, Gordon – Sutherland, Allen (2002): The New Diplomacy: Real-Time Implications and Applications. In Potter, Evan H. ed.: *Cyber-diplomacy: managing foreign policy in the twentyfirst century*. Quebec, McGill-Queen's University Press. 151–177.

Stevens, Tim – O'Brien, Kevin (2019): Brexit and Cyber Security. *The RUSI Journal*, 164(3). 22–30.

Tanács (EU) 2019/796 rendelete: *A Tanács (EU) 2019/796 rendelete, (2019. május 17.), az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről*. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.HUN&toc=OJ:L:2019:129I:TOC (A letöltés dátuma: 2020. 04. 14.)

Tanács (KKBP) 2019/797 határozata (2019. május 17.): *az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről.* Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019D0797&from=EN (A letöltés dátuma: 2020. 04. 14.)

VÁKÁT OLDAL

Molnár Dóra

Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon

A világ domináns hatalmai meghatározó szerepet játszanak a biztonság valamennyi területének formálásában, s nincs ez másképp a kiberbiztonságot illetően sem. Jelenleg azonban nincs olyan átfogó nemzetközi egyezmény, amely az államok kibertérben tanúsítandó magatartási szabályait rögzítené és a kibertér használatát érintő kérdéseket szabályozná. Bár kétség kívül hatalmas diplomáciai siker volna egy nemzetközi kiberegyezmény megalkotása, kérdés, hogy egyáltalán szükséges-e? A szakértők egy csoportja úgy véli, hogy erre nem fog sor kerülni a gyors technológiai változások okozta újabb és újabb kihívások, valamint az egyezményben foglaltak betartásának ellenőrzési nehézségei okán. Helyette az informális együttműködést és a stratégiai elrettentést tartják járható útnak. A szakértők másik csoportja viszont kitart egy nemzetközi egyezmény megalkotásának szükségessége mellett, és sikeres példaként említi a 20. századi fegyverzetkorlátozási megállapodásokat. Egy nemzetközi kiberrezsim ugyanis lehetőséget teremtene az államoknak a fő kérdések megvitatására, és hozzá tudna járulni a hatékony kiberelrettentéshez.

A kiberrezsim ellen számos érv hozható fel.[1] Az egyik, hogy lehetetlen beépíteni monitoring és kényszerítő mechanizmusokat a kiberfegyverek tulajdonságai miatt. Ugyanis az ellenőrzésnek még a fegyverek fejlesztésének időszakában meg kellene kezdődnie, és nem magát a fegyverhasználatot kellene ellenőrizni.[2] További ellenérvek a tárgyalási időszak hosszúsága, a gyors technológiai változásokhoz való alkalmazkodóképesség hiánya, valamint az, hogy korai volna még egy ilyen egyezmény megalkotása. Az egyezmények ugyanis azt követően szoktak köttetni, hogy az adott technológiákat már használták. Ezen kívül egy ilyen egyezménynek csak az igazán elkötelezett államok válnának részeseivé és még számukra is egyfajta kényszerítést jelentene a részvétel.

Elképzelhető, hogy a nemzetközi kiberrezsim lazább szabályozási struktúrák kialakítása mentén is felépíthető lehet. Ez esetben a *bizalomépítő intézkedéseknek* lehet központi szerepe, amelyet az EBESZ és az ASEAN[3] elmúlt évtizedes gyakorlata is bizonyít.

2009-től, miután az Obama-adminisztráció bejelentette új nemzetközi kiberpolitikáját, az Egyesült Államok vált az EBESZ kiberagendája vezető államává. A szervezet kibertevékenységének és a stratégiai kiberbiztonsági párbeszéd alapjait 2010 júniusában rakták le a Biztonsági Együttműködési Fórum és az Állandó Tanács közös találkozóján.

[1] Nabeel 2018.

[2] Minderre Eilstrup-Sangiovanni az exante és ex-post kifejezéseket használja. Lásd Eilstrup-Sangiovanni 2018.

[3] Az ASEAN esetében a Regionális Fórum (ASEAN Regional Forum) keretein belül tárgyalják a kérdéskört.

Az Egyesült Államok már ekkor javaslatot tett az állami viselkedési normák tárgyalására, majd egy évvel később a bizalomépítő intézkedések formálására. Ezzel párhuzamosan az Egyesült Államok és Oroszország tárgyalásokat folytatott a kiber bizalomépítő intézkedések kezdeti körét illetően,[4] majd 2013-ban mindezt egyezségben is rögzítették. A megállapodás lényegi elemei a következők:[5]

– a CERT-tek között kommunikációs csatornák létrehozása és információmegosztási megállapodások megkötése a kritikus információs rendszerek védelme érdekében;
– az országok nukleáris kockázatcsökkentési központjai közötti közvetlen kommunikációs csatorna használatának engedélyezése (az Egyesült Államok washingtoni Külügyminisztériuma és Oroszország moszkvai Védelmi Minisztériuma között);
– közvetlen biztonságos telefonösszeköttetés megteremtése az amerikai kiberbiztonsági koordinátor és az orosz Biztonsági Tanács főtitkárhelyettese között, valamint
– egy hónapon belül egy kétoldalú munkacsoport felállítása az infokommunikációs technológiára leselkedő veszélyekre.

Az EBESZ keretein belül kialakítandó lépések körét illetően az egyes államok különböző javaslatokkal álltak elő. Németország a bizalomépítő intézkedések két nagy csoportját különböztette meg: az átláthatósággal és a stabilitással összefüggő intézkedések körét. Míg az előbbi körébe tartozott a kockázatok csökkentése és az információcsere (az alkalmazandó nemzetközi jog, az szervezeti struktúrák, a stratégiák és a partnerek vonatkozásában), addig az utóbbi körben a közös kibergyakorlatokat, valamint a válságkommunikációs csatornák és a CERT-ek felállítását nevesítették.[6]

Oroszország szélesebb körű listát készített. A 2011-ben kiadott, az *Orosz Föderáció fegyveres erejének információs térben való tevékenységére vonatkozó fogalmi kérdések* (Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space) című dokumentum alapján a fegyveres erők feladata az információs tér katonai alkalmazására vonatkozó bizalomépítő intézkedések körének meghatározása, majd 2012-ben újabb dokumentumban tovább részletezte az intézkedések körét. Ezek közt szerepel a nemzeti szabályok harmonizálása, egy nemzetközileg elfogadott információbiztonsági terminológiarendszer kidolgozása, valamint a rendőri szervek közötti nemzetközi együttműködés szervezeti kereteinek megteremtése.[7]

Mindezek komoly erőfeszítések a nemzetközi közösség részéről, azonban nem szabad megfeledkezni arról, hogy egy nemzetközi kiberrezsim is csak akkor lehet sikeres, ha az államok minél szélesebb köre vesz benne részt. A kiberbiztonság vezető államainak részvétele elengedhetetlenül szükséges, jelenleg azonban még komoly csatározások zajlanak a nyugati világ és a Kína vezette feltörekvő államok között a rezsim legalapvetőbb kérdéseit illetően is. Elég, ha arra gondolunk, hogy 2018 novemberében több mint 50

[4] Ziolkowski 2013.
[5] *Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building* 2013.
[6] *Cyber security: confidence and security-building measures (CSBMs).*
[7] Fedosov 2012.

állam (valamint 130 magánvállalat és 90 tudományos testület) aláírta a kiberhadviselés szabályai megalkotásának szükségességéről szóló nemzetközi kiberbiztonsági paktumot, azonban az Egyesült Államok, Kína, Oroszország, Észak-Korea, Izrael, Irán, Ausztrália és Szaúd-Arábia, valamint a Huawei és a ZTE[8] nem voltak az aláírók között.[9] Jelen tanulmány célja, hogy bemutassa, mit jelentenek a gyakorlatban a kiberdiplomáciai manőverek az egyes országok vonatkozásában. A tanulmány a három vezető kiber-világhatalom, az Egyesült Államok, Kína és Oroszország főbb kiberdiplomáciai lépéseit elemzi, majd a következő fejezetben kitér az Öreg Kontinens vezető államainak ezirányú lépéseire is.

Az Egyesült Államok mint kiberdiplomáciai óriás

Az Egyesült Államok kiberdiplomáciáját bemutató rész rövidebb a további két országot ismertető részhez képest. Ennek indoka egyrészt, hogy a másik két állam tárgyalása kapcsán számos, az amerikai kiberpolitikával kapcsolatos kérdést érintek, másrészt pedig az amerikai kiberdiplomácia olyan kiterjedt elméleti háttérrel rendelkezik, és olyan széleskörű a gyakorlat, hogy annak részletes bemutatása meghaladná jelen fejezet terjedelmi korlátait. Ezért a hivatalosan 2009-ben útjára indított amerikai kiberdiplomáciai folyamatoknak csak a legfontosabb állomásait foglalom össze.[10]

Az amerikai kiberdiplomácia sarokkövét a 2011 májusában az ország *kibertérre vonatkozó nemzetközi stratégiájának*[11] elfogadása jelentette. A stratégia kiadásával az Egyesült Államok a kiberdiplomácia kérdését szilárd alapokra helyezte, és felállította a szervezeti struktúrát is. A dokumentum maga is definiálja a kiberdiplomácia fogalmát: felöleli az amerikai érdekek széles spektrumát a kibertérben – ez nemcsak a kiberbiztonságot és az internetszabadságot foglalja magában, hanem az internetkormányzást, valamint az internet, az innováció és a gazdasági növekedés katonai célú használatát is. A Külügyminisztériumban létrehozták a Kiberkoordinátori Hivatalt (Office of the Coordinator for Cyber Issues), amelynek első (és egyben utolsó) vezetője Christopher Painter lett. A kiberdiplomácia az amerikai kül- és nemzetbiztonsági politika kritikus komponensévé vált. A Hivatal hat és fél éves működése alatt számos két- és többoldalú partneri kapcsolatot épített ki, és világszerte tárgyalt formálisan vagy informális módon a kiberkérdések széles körét érintve.[12] Több szakértői javaslat is napvilágot látott a további kiberdiplomáciai építkezés szükségességéről, ám a Trump-adminisztráció

[8] A Huawei és a ZTE Kína két legnagyobb távközlési cége, egyúttal a világ vezető információs és kommunikációs technológiai vállalatai.

[9] *UK and 50 nations sign cyber security pact* 2018.

[10] A digitalizáció az Egyesült Államok közigazgatásában hosszú múltra tekint vissza, de igazi fordulópontot e tekintetben is a 2001. évi terrortámadás jelentett. A Külügyminisztériumban 2003-ra készült el az első átfogó koncepció az e-diplomácia fejlesztésére, amelyet további fejlesztések és számos előrelépés követett. Részletesebben lásd Nyáry 2019.

[11] *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World* 2011.

[12] Painter 2018.

másképp vélekedett e kérdés jövőjéről, és Tillerson külügyminiszter a Hivatal megszüntetéséről (és az alkalmazottaknak a minisztérium Gazdasági és Üzleti Ügyek Irodájában történő áthelyezéséről) döntött. Ezzel hatalmas űr keletkezett, amelyet egy 2017. májusi elnöki rendelettel[13] elrendelt új kiberstratégia megalkotásával kívántak betölteni, annak elmaradása azonban további bizonytalanságokhoz vezetett a diplomáciai testületek körében. A kiberdiplomáciai törvényre vonatkozó, kétpárti egyetértést tükröző javaslatot 2017 szeptemberében terjesztették elő a Képviselőházban, majd a hosszas jogalkotási folyamat végül 2019. január 24-én zárult le. Az elfogadott törvényben az ország hozzá kíván járulni egy nyitott, interoperábilis, megbízható, korlátlan és biztonságos internethez, amelyet a többszereplős (multi-stakeholder) modell alapján kormányoznak. Az Egyesült Államok tehát továbbra is kitart a multilaterális megközelítés elvetésében, szembe helyezkedve ezzel a Kína és Oroszország vezette másik táborral. A stratégia mindezt tovább tetézi azzal, hogy olyan országokat és csoportokat nevesít, amelyek fenyegetést jelentenek a kibertérben: első helyen Oroszország, majd Kína, Irán és Észak-Korea, a terrorista, valamint a bűnözői csoportok állnak. A dokumentum ugyanakkor kiemeli a kétoldalú kapcsolatok fontosságát, és nevesíti a 2014 és 2018 között megkötött bilaterális kiberszerződéseket.[14] A szervezeti téren keletkezett anomália helyreállítására új központi kiberszervként fel kell állítani a Nemzetközi Kiberpolitikai Hivatalt (Office of International Cyberspace Policy), amelyet az elnök által kinevezett kibernagykövet fog irányítani.

A folytatást illetően annyi bizonyos volt, hogy nem lesz elégséges egy új stratégia megalkotása és egy új hivatal felállítása az országot a kibertérben érő konfrontációk és dilemmák megválaszolására, a részletkérdések kidolgozása azonban még várat magára. Ha az Egyesült Államok sikereket kíván elérni e téren is, a nyílt konfrontáció mindenképp kerülendő mind Kínával, mind Oroszországgal; ezen államokkal konzisztens politikát kell folytatni, amelyet kommunikálni kell a szövetségesek és világ más államai felé is. A megoldás az lehet, ha az Egyesült Államoknak sikerül rábírnia az európai, az afrikai, dél-amerikai, és a közép-, dél-, dél-kelet ázsiai államokat, hogy válasszanak néhány vezető államot a térségükből – ellensúlyozva ezzel a kínai és orosz dominanciát.[15]

Kína és a kiberdiplomácia: egy újabb sikertörténet?

Nem túlzás azt állítani, hogy Kína a diplomácia területén is átvette a vezető szerepet. Ezt jelzi a diplomáciai hálózat kiterjedtsége, amely egyúttal a globális befolyás fokmérője is. 2019-re Kína 276 diplomáciai állomáshellyel rendelkezett világszerte, megelőzve ezzel az addig vezető Egyesült Államokat is, amelynek „csak" 273 kirendeltsége van.[16]

[13] *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructur.* 2017.

[14] Az országok között szerepel többek között Kína, Japán, az Egyesült Királyság, Franciaország, Izrael, Dél-Korea és Ausztrália.

[15] Chapman 2019.

[16] Bley 2019.

Ez a nagyhatalmi versengésnek is fordulópontja lehet, mert Kína minden bizonnyal készen áll arra, hogy globális erejét ténylegesen is alkalmazza. Egyes vélemények szerint Kína már nem pusztán kibernagyhatalom, hanem az elmúlt pár évben *kiber szuperhatalommá nőtte ki magát*.[17] Mindez nem lehet véletlen, ha a kínai elnök 2016-ban elhangzott szavaira tekintünk: kiberbiztonság nélkül nincs nemzeti biztonság, és informatizáció nélkül nincs modernizáció.[18]

A diplomáciai lépések megalapozását a 2017 márciusában kiadott *Együttműködés a kibertérben nemzetközi stratégia* (International Strategy of Cooperation on Cyberspace)[19] című új kiberbiztonsági dokumentum képezi. A stratégia már nevében is azt sugallja, hogy Kína a kibertérbeli konfliktusok megoldását elsősorban az együttműködésre építve, békés eszközök használatával képzeli el – s e körben kiemelt szerepe van a kiberdiplomáciának.

A stratégia rögzíti, hogy a kibertér jövője valamennyi ország kezében van, s bár nő a digitális szakadék az egyes országok és régiók közt, a nemzetközi közösségnek mégis egységes egészként kell együttműködnie a kölcsönös tisztelet és a kölcsönös megértés szellemében, hogy az internet világának szuverenitása biztosítva legyen. S itt eljutunk a kulcsfogalomig, a szuverenitás fogalmához. A szuverenitás a négy alapelv egyikeként jelenik meg a dokumentumban (a béke, a megosztott kormányzás és a megosztott előnyök mellett), s ezzel összefüggésben az internet szuverenitásának fontossága áthatja a stratégia egészét – nem meglepő módon, hiszen Kína esetében egy demokratikusnak látszó köntösbe bújt autoriter rezsimmel állunk szemben, így nem véletlen, hogy a be nem avatkozás elve mint egyik elsődleges vezérlő elv van jelen. A stratégia definiálja az internet-szuverenitás (vagy kiberszuverenitás) fogalmát is: az államoknak tiszteletben kell tartaniuk egymás jogát, hogy maguk válasszák meg a kiberfejlődés útját, a kiberszabályozás modelljét és az internetre vonatkozó politikájukat, és biztosítani kell, hogy egyenlő mértékben részt vehessenek a nemzetközi kibertér kormányzásában. Egyik állam sem törhet kiberhegemóniára, nem avatkozhat be más állam belügyeibe, és nem támogathat olyan kibertevékenységet, amely más állam nemzetbiztonságát aláássa. A szuverenitás kérdésköre a stratégiai célok közt is előkerül, mégpedig az első helyen mint a „szuverenitás és a biztonság garantálása". Az ország kiemelten a békés eszközök igénybevételével képzeli el ezen stratégiai céljának elérését, és célja annak elkerülése, hogy a kibertér új hadszíntérré váljon. Ennek némiképp ellentmond, de ugyanakkor nem véletlen, hogy Kína a védelmi kiberképességeit a továbbiakban is fejleszteni (és minden bizonnyal használni is) fogja, és a hadseregnek fontos szerepet szán a kibertéri feladatok ellátásában. Tervezi önálló kibererő létrehozását is.

A stratégiai célok közül kiemelem a másodikként nevesített nemzetközi szabályrendszer megalkotását, valamint a harmadikként szereplő tisztességes internetkormányzás kérdéskörét. Az előbbi vonatkozásában Kína kiáll amellett, hogy az ENSZ keretein belül

[17] Segal 2018.
[18] *Xi Jinping gives speech at Cybersecurity and Informatization World Conference* 2016.
[19] *International Strategy of Cooperation on Cyberspace* 2017.

létre kell hozni egy egyetemlegesen elfogadott nemzetközi szabály- és magatartási normarendszert, amely az államok kibertérbeli magatartásának kereteit rögzíti. Az utóbbival összefüggésben pedig úgy fogalmaz a stratégia, hogy egy „multilaterális, demokratikus és transzparens" globális internetkormányzásra van szükség, amely az egyenlő részvétel és a közös döntéshozatal elvére épül. A multilaterális jelző kiemelést érdemel, ugyanis ez jelenti az egyik fő nézeteltérést a nyugati hatalmakkal, akik az internetkormányzás többszereplős (multi-stakeholder) modelljét kívánják megvalósítani.

A kínai külpolitikának három fő célja van: csökkenteni a fenyegetést, amelyet az internet és az információáramlás jelenthet a belső stabilitásra és a rendszer legitimációjára; oly módon formálni a kiberteret, hogy az ország politikai, katonai és gazdasági befolyása növekedjen; valamint ellensúlyozni az amerikai túlsúlyt, Kína mozgásterének növelése mellett.[20] Ebbe a célrendszerbe illeszkednek az ország kiberdiplomáciai lépései is. Kína Hszi Csin-Ping elnöksége alatt változtatott korábbi reaktív és védekező kiberpolitikáján, és az aktív kiberdiplomácia alkalmazása mellett döntve igen rövid idő alatt építette ki kiberdiplomáciai csatornáit, amelyeket nagyon eredményesen használ céljai eléréséhez. A kiberbiztonság Peking számára egyszerre képes biztosítani a terrorizmus jelentette fenyegetés ellensúlyozását, a regionális befolyás garantálását és a kétoldalú kapcsolatainak építését az olyan fontos partnerállamokkal, mint az Egyesült Államok. Kína 2014-ben rendezte meg az első wuzheni Internet Világkonferenciát. Akkor Kína elnöke mindössze egy üdvözlő üzenetet küldött a rendezvény résztvevőinek. Egy évvel később Hszi Csin-Ping személyesen vett részt a konferencián és mondott beszédet, jelezve ezzel a kiberbiztonsági kérdések megnövekedett fontosságát Kína számára. A kínai elnök beszédének középpontjában az internetszuverenitás kérdése mellett a globális internetkormányzás kérdésköre, azon belül is a multilateralitás propagálása állt. Nem kis diplomáciai gesztusnak számított, hogy Medvegyev orosz elnök konferenciabeszédében azonnal reagált a kínai elnök szavaira és támogatásáról biztosította őt.[21] A két ország egyébiránt igen jelentős sikert tudhatott magáénak már a konferenciát megelőző napon, amikor sikeres lobbi tevékenységüknek köszönhetően a 70/125. sz. ENSZ közgyűlési határozat szövegébe bekerült a multilaterális kifejezés – kiváltva ezzel a nyugati világ ellenérzését.[22]

A kínai kiberdiplomácia a belügyekbe való be nem avatkozás alapelvének és az egyenlő részvétel elvének elismerésében, a kapacitásépítés és fejlesztési támogatás fontosságában, valamint az ENSZ és más nemzetközi intézmények támogatásában gyökerezik. Mindezek eredője pedig a kiberszuverenitás vagy internetszuverenitás kérdése, amely központi kérdés a kiberdiplomácia kezdeteitől fogva. Kína az internet világára kétélű kardként tekint: mint elengedhetetlen elem a gazdasági fejlődés és a kormányzás biztosításához, de ugyanakkor a belső stabilitás és a rendszer legitimációjára nézve fenyegetés. Az ország elsősorban az országon belüli cenzúra segítségével szándékozik megadni a válaszokat (lásd Great Firewall), de hangsúlyozza a nemzetközi együttműködés fontosságát is.

[20] Segal 2017.
[21] Bandurski 2015.
[22] *70/125. sz. ENSZ közgyűlési határozat.*

A kínai kiberdiplomáciai erőfeszítések között évek óta kiemelt helyen szerepel az internetforrások egyenlőtlen elosztása elleni fellépés és ezzel összefüggésben az IANA[23] feletti erős amerikai ellenőrzés és az ICANN[24] megreformálásának kívánalma. Ugyanis a világ 13 gyökérszerveréből 10 az Egyesült Államokban található, és az IANA is az ICANN és az amerikai Kereskedelmi Minisztérium között köttetett szerződés eredményeként jött létre.[25] Ezért sem meglepő, hogy az amerikai dominancia letörése érdekében Kína multilaterális internetkormányzás megvalósítását támogatja.

A kiberkérdések egyre fontosabb helyet kapnak Kína *kétoldalú és regionális kapcsolataiban* is. Peking a kiberbiztonságot egyrészt a regionális pozíciója erősítéséhez, másrészt a regionális és fejlődő országok körében vezető pozíciójának biztosítására használja fel. *Kiemelt kétoldalú kapcsolatokat ápol az Egyesült Államokkal*, azonban a kiberkérdéseket illetően meglehetősen változékonyan alakult a két nagyhatalom kapcsolata. A kétoldalú kapcsolatok erősítését kezdetben az Egyesült Államok forszírozta, a párbeszéd azonban leginkább gazdasági kérdésekre korlátozódott – részben annak köszönhetően, hogy a kínai diplomaták a külügyminisztérium állományából érkeztek és nem rendelkeztek kiber szakértelemmel. Az Egyesült Államok egyre keményebb hangot ütött meg, és 2013 júniusában, amikor a két ország vezetői Kaliforniában találkoztak, Obama arra figyelmeztette a kínai elnököt, hogy a kiberkémkedés súlyosan árt a kétoldalú kapcsolataiknak. Nem sokkal ezután robbant ki a Snowden-ügy, az Egyesült Államok pedig öt kínai hekker ellen emelt vádat – mire Kína válasza a kétoldalú tárgyalások befagyasztása volt. Ebben az időszakban mindkét fél részéről két nagy kutatóintézet készített éves jelentéseket a kiberbiztonság aktuális helyzetről (az amerikai CSIS és a kínai CICIR)[26]. A kapcsolatok konszolidálásra csak azt követően került sor, hogy a kínai hekkerek elleni vádakat elejtették. 2015 szeptemberében Hszi elnök hivatalos látogatásra érkezett Washingtonba, ahol a kétnapos tárgyalás eredményeként a két nagyhatalom korszakos jelentőségű bilaterális egyezményt írt alá, amely külön rendelkezik a kiberbiztonság kérdéseiről is. Az egyezmény aláírása azért is fontos lépés volt, mert a kiberkapcsolatok alakításának is mintájaként szolgált az Egyesült Királyság, Németország és más nyugati államok esetében.

A 2015. szeptember 25-én aláírt kétoldalú megállapodás rögzíti,[27] hogy időben választ kell adni információ vagy segítségkérésre vonatkozó megkeresésekre, ha az rosszindulatú kibertevékenységekkel kapcsolatos. A felek kötelesek együttműködni a kiberbűncselekmények felderítésében és elektronikus bizonyítékok gyűjtésében, valamint naprakész adatokat szolgáltatnak a nyomozás állásáról és eredményéről. Kötelezettséget vállalnak arra is, hogy egyik kormány sem folytat vagy támogat a szellemi tulajdon eltulajdonlására irányuló kibertérbeli tevékenységet. Mindkét fél támogatja az államok kibertérben

[23] Internet Assigned Numbers Authority.
[24] International Corporation for Assigned Names and Numbers.
[25] Swaine 2013.
[26] CSIS – Center for Strategic and International Studies; CICIR – China Institute of Contemporary International Relations.
[27] *Fact sheet: President Xi Jinping's State Visit to the United States* 2015.

való magatartási szabályainak lefektetését, amely kérdéskört egy felállítandó szakértői csoport fog tüzetesebben megvizsgálni. Végezetül külön együttműködési mechanizmust is felállítanak a kiberbűnözéssel kapcsolatos kérdések megvitatására. A „magas szintű közös párbeszéd" elnevezésű csoport évente kétszer ül össze tanácskozási céllal.[28]

Az egyezmény utáni időszakban a két ország egymás ellen folytatott kiberkémkedési tevékenysége alacsonyabb szintre csökkent, azonban nem kizárt az újbóli növekedés – s ez az amerikai–kínai kétoldalú kapcsolatok első számú prioritásává emelheti a kiberbiztonságot. Ennek valószínűsége azonban csekély, ugyanakkor vannak olyan alapvető kérdések, amelyekben gyökeresen eltér a két nagyhatalom álláspontja. Ilyen a kibertér militarizációjának, a nemzetközi jog kiberhadviselésre való alkalmazhatóságának kérdése, valamint a kiberkémkedés legitim mértékének és céljának megítélése. Márpedig ez a feszültség óhatatlanul magában rejti egy esetleges súlyosabb konfliktus kialakulásának veszélyét is. Egy ilyen konfliktus megelőzésére a kibertérbeli viszonyokra is alkalmazni lehetne a fegyverzetkorlátozás logikáját és célrendszerét – annak ellenére, hogy a fegyverzetkorlátozási mechanizmusok a hidegháború időszakában a nukleáris arzenálra vonatkoztak és alapvetően különböznek[29] a kibertérbeli viszonyoktól.[30] Ha azonban a Trump-adminisztráció vagy Amerikai jövőbeli vezetésének egyirányú és egyoldalú diplomáciai lépései a jövőben is folytatódnak, további feszültségek várhatók a két ország viszonyában.[31]

A kétoldalú kapcsolatok közt mindenképpen ki kell térni az *kínai–orosz kapcsolatokra* is. A két ország 2015 májusában 32 kétoldalú megállapodást írt alá – köztük egy együttműködési megállapodást a nemzetközi információs biztonságról.[32] Ebben kötelezettséget vállalnak arra, hogy egymás ellen nem indítanak hekkertámadásokat, és elítélik a belpolitika destabilizálására irányuló, interneten keresztül tett kísérleteket. Ez utóbbi a megállapodás újnak tekinthető a Shanghai Együttműködési Szervezet égisze alatt már megkötött egyezményekhez képest. További előrelépés a konkrét intézkedések nevesítése, mint a kontaktpontok felállítása, vagy közös tudományos kiberprojektek futtatása.

A kétoldalú kapcsolatok között említést kell tenni az Európai Unióval 2012-ben kialakított partneri viszonyról is. A minden évben megrendezett EU–Kína csúcs keretében rendszeresen ülésezik az EU–Kína-kibercsoport is, amely lényegében az Unió kínai kiberbiztonsági politikával kapcsolatos aggodalmai kifejezésének és az internetkormányzással kapcsolatos megbeszélések fóruma lett.[33] A munkacso-

[28] Renard 2015.

[29] A kiberképességek kettős felhasználásúak és leginkább láthatatlanok, a kibertér legfőbb szereplői a magánszektor entitásai (szemben a nukleáris hatalmakkal mint államokkal), a kibertérbeli kötelezettségvállalások ellenőrzése lényegében lehetetlen, valamint a kiberfegyverek kiválóan alkalmasak lokalizált és múló hatás elérésére.

[30] Levite–Jinghua 2019.

[31] Erről részletesebben lásd Dollar–Hass–Bader 2019.

[32] Roth 2015.

[33] Pawlak 2015.

port 2020. január 13-án tartotta hetedik ülését Kínában, ahol jelentős eredményként értékelték a gyakorlati együttműködés kiterjesztését és a kétoldalú átfogó stratégiai partnerség elmélyítését.[34] Kína az európai államok közül az Egyesült Királysággal is évente tárgyal kiberkérdésekről a kétoldalú partnerség keretében, megvitatva főként a kiberbűnözési kérdéseket.

Kína diplomáciai agendájának centrumában minden bizonnyal továbbra is a kiberszuverenitás kérdése fog állni, és kibertérbeli pozícióját a gazdasági eszközök segítségével fogja javítani. Már most is a kínai kiberdiplomácia egyik speciális, ugyanakkor igen fejlett területe a *kereskedelmi és befektetéspolitika*, amelyeket gazdasági és indirekt politikai eszközökként használ. Azáltal, hogy új piacokat nyit szerte a világban, új támogatókat szerez a kínai külpolitikának és egyúttal a kínai kiberpolitikának, valamint a kibernormák elfogadtatásának. A befektetés azonban nem mindig közvetlen módon konvertálható politikai befolyássá, az gyakran indirekt formában jelenik meg. A közvetlen befolyásra példa lehet a Huawei afrikai piacra lépése. 2005-ben Nigéria fővárosában a Huawei iskolát nyitott, öt évvel később pedig már 50 afrikai országban működött, ellátva 300 millió afrikai felhasználót. Másik jó példa a One Belt, One Road (OBOR) kezdeményezés. Ez két elemből tevődik össze: az egyik a Selyemút gazdasági öve, amely Kínát a Perzsa-öbölben, a mediterrán térséggel és az Indiai-óceán térségével köti össze, míg a másik, a 21. századi tengeri selyemút, amely a régió vízi útjait köti össze. Ehhez kapcsolódóan tervezik egy „információs selyemút" kiépítését is, amely eredendően határokat átszelő optikai kábelek lefektetését és más kommunikációs hálózatok létrehozását jelentette.[35] A tervezett optikai kábel, amely Kínát 48 afrikai országgal köti össze 200 000 km hosszú, a kiépítés tervezett költsége pedig 173 milliárd.[36] A terv azonban 2019 novemberében kiegészült, és már nemcsak a kábelrengeteget kívánják lefektetni, hanem hálózati eszközök és szoftverek is részét fogják képezni, valamint okos portokat is kiépítenek a jövő menedzsmentstruktúráinak támogatására.[37]

A kínai kiberpolitika és diplomácia alakulását a következő időszakban két külső tényező fogja meghatározni. Az egyik az Egyesült Államokban zajló folyamatok. Ha az ország elsősorban a belső problémáira fog koncentrálni, az lehetőséget jelent Kína számára, hogy nagyobb szerepet játsszon a kibertérbeli szabályok megalkotásában. A másik a kiberbiztonsági környezet alakulása, amely a jelenlegi tendenciák alapján egyre veszélyesebbé válik, és félő, hogy bekövetkezik a „kibertér militarizációja".[38] A fontolva haladás ősi kínai elvét azonban aligha fogja Kína feladni, és megfontolt politikai-gazdasági lépéseinek legfőbb terepe továbbra is a diplomácia marad a kibertér vonatkozásában is.

[34] *The 7th China-EU Cyber Taskforce was Held in Beijing* 2020.

[35] A terv sarokpontjait 2016-ban rögzítették, és megvalósítását 2018-ra tervezték, de a tényleges kiépülés még várat magára.

[36] Chinese Firm Hopes to Wire Continent with Same Strategy that Boosted Internet Access Across China 2017.

[37] *China's Digital Silk Road (DSR): The new frontier in the Digital Arms Race* 2020.

[38] DSR 2020, 2.

Oroszország és a kiberdiplomácia

Az orosz kiberpotenciál az egyik legnagyobb és technológiailag legfejlettebb a világon, karöltve az amerikaival és a kínaival. Az elmúlt években azonban az ország e képességeit többször is támadó szándékkal használta fel – ahogyan az történt Észtország vagy Georgia esetében, de még az Egyesült Államokkal szemben is. Oroszország a kiberkonfliktusokat kényszerítő eszközként használja, a Nagy Stratégia részeként az ellenséggel szemben, hogy vágyott céljait elérje. Ezek az akciók azonban a poszt-szovjet régió határait csak a legritkább esetben lépik át – a kérdés, hogy miért? A válasz abban rejlik, hogy Oroszország nemzeti érdekei és céljai is elsősorban a poszt-szovjet térségre fókuszálnak, a globális színpad ehhez képest csak másodlagos – s nincs ez másképp a kibertér vonatkozásában sem.

A kiberinterakciókat vizsgálva[39] szembetűnő, hogy Oroszország messze az utolsó helyen áll, míg az Egyesült Államok és Kína toronymagasan vezet. Ebből az következik, hogy a kiberdiplomácia jelentőségét Oroszország alulértékeli, és nem a diplomácia eszközrendszere segítségével kívánja a kibertérbeli konfliktusokat rendezni, hanem sokkal inkább a kiber(támadó) képességei használatával.[40] Ennek okát a „végrehajtói körnél" kell keresni. Míg nyugaton a civil társadalom számos intézménye a soft power letéteményese, addig Oroszország esetében az az állami kontroll alatt lévő média által támogatott állami szervek kizárólagos joga. Ezért nem meglepő, hogy az orosz külpolitikai eszközök tárháza közt a kiberdiplomáciai eszközök nem az első helyen szerepelnek.[41]

Azonban ez nem volt mindig így. A 2000-es évek elején Oroszország még aktívan részt vett a multilaterális és regionális kibertanácskozásokon, mivel azonban ezen erőfeszítései nem hozták meg a kívánt eredményt, a diplomáciai lépések helyét egyre inkább a támadó jellegű kiberfellépések vették át. Ugyanis Oroszország a kiberhatalmára mint a Nagy Stratégia szerves részére tekint, és azt politikai céljai elérése érdekében kívánja használni – összhangban a clausewitz-i gondolattal: a háború a politika folytatása más eszközökkel.[42]

Ami a kezdeti időszakot illeti, Oroszország diplomáciai lépéseinek célja a konfliktusok és az államok közötti kiberfegyverkezési verseny megelőzése volt. Ennek jele volt az 1999-ban orosz kezdeményezésre elfogadott 53/70. sz. ENSZ közgyűlési határozat *Fejlődés az információ és a távközlés területén a nemzetközi biztonsággal összefüggésben*[43] címmel. Igor Ivanov orosz külügyminiszter már ekkor felhívta az államok figyelmét a kibertér militarizációjának veszélyére, hangsúlyozva a kiberfegyverek esetleges ártó hatásait is.[44] Mindez azonban még nem talált teljes megértésre az államok részéről

[39] Brandon–Maness 2014.
[40] Ezzel szemben áll az Egyesült Államok, amelynek lehetősége lett volna a fejlett kiberképességei bevetésére az iraki, az afganisztáni vagy akár a líbiai konfliktus során, azt mégsem tette.
[41] McNabb 2016.
[42] Wirtz 2015.
[43] *UN General Assembly, Resolution A/RES/53/70.*
[44] Dam–Owens 2009.

(részben azért, mert akkor még alacsony, 250 000 fő körüli volt az internetethasználók száma). Az orosz diplomáciai erőfeszítések azonban folytatódtak, és *A kiberbiztonság globális kultúrájának megteremtése és a kritikus információs infrastruktúrák védelmére tett nemzeti erőfeszítések áttekintése* című, 2009-ben elfogadott ENSZ közgyűlési határozatban nyertek formát.[45] Mivel azonban a határozat nem volt kötelező érvényű, az abban foglaltak gyakorlati megvalósítása elmaradt.

Oroszország továbbra is az *ENSZ-rendszer keretein belül* kereste a diplomáciai megoldásokat, és üdvözölte az ENSZ Kormányzati Szakértői Csoport (UN Group of Governmental Experts – GGE) 2004-ben történt megalakítását. Ekkora azonban már az orosz kiberdiplomácia célja megváltozott, és a megelőzés helyett a szabályozás vált elsődlegessé. Ennek oka, hogy eddigre már számos ország (köztük Oroszország is) aktívan fejlesztette kiberképességeit. Az első eredményekig azonban egészen 2014-ig kellett várni, amikor a Szakértői Csoport jelentésében rögzítette, hogy a nemzetközi jog – s különösen az ENSZ Alapokmánya – alkalmazandó a kibertérben is.[46] A kormányzati munka ezt követően folytatódott, és a csoport 2015. évi jelentése már egy kormányzati kibermagatartási kódex megalkotásának alapjait is letette, azonban a folyamatok ezt követően elakadtak.

Ezzel párhuzamosan Oroszország a *regionális kapcsolatain* keresztül is forszírozta a kódex megalkotásának szükségességét. 2011-ben a Shanghai Együttműködési Szervezet nevében három országgal együtt nyújtott be erre vonatkozó javaslatot az ENSZ-nek, majd szintén 2011-ben megalkotta a Nemzetközi Információbiztonsági Konvenció tervezetét.[47] Mindkét dokumentum hangsúlyozza az állami szuverenitás és területi integritás elvét a kibertér vonatkozásában. Az orosz akaratot ezen kívül sikerült érvényesíteni a Kollektív Biztonsági Szerződés Szervezetében és a BRICS államok között is, elfogadva határozatokat és felállítva munkacsoportokat.

Végezetül az orosz diplomácia a *kétoldalú partneri kapcsolatok* segítségével is igyekezett a kibertér szabályozását elérni. A világ első kétoldalú kiberegyezménye Oroszország és az Egyesült Államok között köttetett meg 2013-ban. A siker azonban nem egyértelmű, mert az egyezmény csak az együttműködés technikai kérdéseire szorítkozott. Rögzítette a nemzeti CERT-ek közötti információcsere és egy kiber forró drót létrehozásának szükségességét. Az oroszokban élt a remény, hogy sor kerülhet egy szélesebb körű orosz–amerikai egyezmény aláírására is, de az ukrán konfliktus miatt a tárgyalási folyamat megakadt, majd 2017-ben, amikor Oroszország ismételten próbálkozott egy, a veszélyes katonai tevékenységekről szóló egyezmény megalkotásával, attól az amerikai fél az aláírás előtti napon elállt – vélhetően a 2016-os elnökválasztásba történt orosz beavatkozásról kiderült fejlemények miatt.[48] Az első kiberegyezményen túl Oroszor-

[45] *UN General Assembly, A/RES/64/211.*

[46] *UN General Assembly, A/68/98.*

[47] A dokumentumok megalkotásában szerepet játszhatott az, hogy az internet ereje minden állam számára nyilvánvalóvá vált az arab tavasz eseményei tükrében, és Oroszország szerette volna elkerülni az orosz politikai rendszer kívülről történő manipulálását.

[48] Popescu–Secrieru 2018.

ság már több országgal is kötött hasonló megállapodást, így például Kínával, Indiával, Dél-Afrikával, Fehéroroszországgal vagy Kubával, és további egyezmények megkötését tervezi Franciaországgal, Németországgal, Izraellel, Japánnal és Dél-Koreával.

Oroszország már 20 évvel ezelőtt rögzítette kiberstratégiájában a kibertér nemzetközi szabályozásának szükségességét, és – Kínával, valamint a CSTO többi tagállamával együtt – a mai napig kitart a kibertérre vonatkozó magatartási szabályok, valamint a szuverenitás és a belügyekbe való be nem avatkozás kibertérben való alkalmazandósága mellett. Ellentétben a Nyugattal – élén az Egyesült Államokkal –, amely korábban mindezt ellenezte, az utóbbi időben azonban a szabályok szükségességének elismerésére egyre nagyobb hajlandóságot mutat. A két tábor közötti szakadék igen negatívan hat az orosz–amerikai, illetve orosz–európai kapcsolatokra is, amely következményeként egyre kisebb az esély a globális egyetértésre – még ha maga az ENSZ főtitkára a szabályrendszer megalkotásának szükségessége mellett is foglal állást.[49]

Összegzés

Az egyes államok kiberbiztonsági helyzetének összehasonlítására több mutató is létezik. Ezek közül az ENSZ Nemzetközi Távközlési Egyesülete által jegyzett Globális kiberbiztonsági indexet emelem ki, amely öt mutató mentén hasonlítja össze az államokat. Az ötödik mutató az együttműködés, amely keretében többek között a két- és többoldalú együttműködési keretek, valamint a nemzetközi szervezetekben lévő tagság jelentik a fokmérőt. Az index összesített értékelése alapján az Egyesült Államok a 2., Oroszország a 26., Kína pedig a 27. helyen szerepel a világranglistán.[50] Látható, hogy a három vizsgált ország közül egyértelműen kitűnik az Egyesült Államok, amely valóban kiberdiplomáciai nagyhatalomnak számít. Kína esetében a mutató által tükrözött relatív lemaradás annak köszönhető, hogy az ország csak az utóbbi években kezdett aktív kiberdiplomáciába, és a kezdeti lépések hatásai még nem köszönnek vissza az index számaiban. Oroszország esetében nem meglepő az eredmény, mivel az oroszok a szerteágazó kapcsolatrendszerüket nem feltétlenül a kiberbiztonság területén kívánják használni. Ugyanakkor valamennyi ország esetén elmondható, hogy az együttműködési mutató alacsonynak mondható, ezért várható, hogy a kiberdiplomácia területe a jövőben jelentős fejlődést fog mutatni.

Felhasznált irodalom

53/70. sz. ENSZ közgyűlési határozat. „Developments in the Field of Information and Telecommunications in the Context of International Security”, 1999. január 4. Forrás: https://undocs.org/A/RES/53/70 (A letöltés ideje: 2020. 04. 15.)

64/211. sz. ENSZ közgyűlési határozat. „Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures”, 2009. december 11. Forrás: www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211 (A letöltés dátuma: 2020. 04. 06.)

[49] *US Chief Calls for Regulatory Scheme for Cyberwarfare* 2018.
[50] *Global Cybersecurity Index 2018* 2019.

68/98. sz. ENSZ közgyűlési határozat. „Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.", 2013. június 24. Forrás: www.un.org/ga/search/view_doc.asp?symbol=A/68/98 (A letöltés dátuma: 2020. 04. 06.)

70/125. sz. ENSZ közgyűlési határozat. Outcome document of the high-level meeting of the Genereal Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society. 2015. december 16. Forrás: https://publicadministration.un.org/wsis10/ (A letöltés dátuma: 2020. 04. 09.)

Bandurski, David (2015): *China's cyber-diplomacy*. 2015. december 21. Forrás: http://chinamediaproject.org/2015/12/21/chinas-cyber-diplomacy/ (A letöltés dátuma: 2020. 04. 09.)

Bley, Bonnie (2019): *The New Geography of Global Diplomacy. China Advances as the United States Retreats.* 2019. november 27. Forrás: www.foreignaffairs.com/articles/china/2019-11-27/new-geography-global-diplomacy (A letöltés dátuma: 2020. 04. 08.)

Brandon, Valeriano – Maness, Ryan C. (2014): The Dynamics of Cyber Conflict between Rival Antagonists, 2001–2011. *Journal of Peace Research* 51(3). 347–360. Forrás: www.researchgate.net/publication/256046745_The_Dynamics_of_Cyber_Conflict_between_Rival_Antagonists_2001-2011 (A letöltés dátuma: 2020. 04. 20.)

Chapman, Justin (2019): *Threats and Opportunities of Cyber Diplomacy at PolicyWest.* 2019. december 24. Forrás: www.pacificcouncil.org/newsroom/threats-and-opportunities-cyber-diplomacy-policywest (A letöltés dátuma: 2020. 04. 13.)

China's Digital Silk Road (DSR): The new frontier in the Digital Arms Race. 2020. 02. 19. Forrás: www.silkroadbriefing.com/news/2020/02/19/chinas-digital-silk-road-dsr-new-frontier-digital-arms-race/ (A letöltés dátuma: 2020. 04. 20.)

Chinese Firm Hopes to Wire Continent with Same Strategy that Boosted Internet Access Across China. *Global Times*, 2017. március 13. Forrás: www.globaltimes.cn/content/1037500.shtml (A letöltés dátuma: 2020. 04. 08.)

Conflict between Rival Antagonists, 2001–2011. *Journal of Peace Research* 51(3). 347–360. Forrás: www.researchgate.net/publication/256046745_The_Dynamics_of_Cyber_Conflict_between_Rival_Antagonists_2001-2011 (A letöltés dátuma: 2020. 04. 10.)

Cyber security: confidence and security-building measures (CSBMs). Federal Foreign Office website. Forrás: www.auswaertiges-amt.de/EN/Aussenpolitik/Friedenspolitik/Abruestung_/KonvRueKontrolle/VN-Konventionelle-Abruestung-Ruestungskontrolle_node.html (A letöltés dátuma: 2020. 04. 10.)

Dam, Kenneth W. – Owens, William (2009): *Technology, Policy, Law and Ethics Regarding U.S. Acquizition and Use of Cyberattack Capabilities*. Committee on Offensive Information Warfare, National Research Council. Forrás: https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2013/01/NRC-Report.pdf (A letöltés dátuma: 2020. 04. 15.)

Dollar, David – Hass, Ryan – Bader, Jeffrey A. (2019*): Assessing U.S.-China relations 2 years into the Trump presidency.* 2019. január 15. Forrás: www.brookings.edu/blog/order-from-chaos/2019/01/15/assessing-u-s-china-relations-2-years-into-the-trump-presidency/ (A letöltés dátuma: 2020. 04. 08.)

Eilstrup-Sangiovanni, Mette (2018): Why the World Needs an Internationa Cyberwar Convention. *Philosophy&Technology* 30, no. 3. 399.

Fact sheet: President Xi Jinping's State Visit to the United States. The White House, Office of the Press Secretary, 2015. szeptember 25. Forrás: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (A letöltés dátuma: 2020. 04. 08.)

Fedosov, Sergey (2012): *Statement by the Russian participant at the UNIDIR Cyber Security Conference 'What does a Stable Cyber Environment Look Like?* Geneva, UNIDIR. 8–9 November 2012 Forrás: www.unidir.ch/files/conferences/pdfs/pdf-conf1922.pdf (A letöltés dátuma: 2020. 04. 10.)

Global Cybersecurity Index 2018. UN ITU, Geneva, 2019. Forrás: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (A letöltés ideje: 2020. 04. 20.)

International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. United States, 2011. május. Forrás: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf (A letöltés dátuma: 2020. 04. 13.)

International Strategy of Cooperation on Cyberspace. A Kínai Népköztársaság Külügyminisztériuma, 2017. március 1. Forrás: www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml (A letöltés dátuma: 2020. 04. 08.)

Levite, Ariel (Eli) – Jinghua, Lyu (2019): *Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation.* 2019. január 24. Forrás: https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213 (A letöltés dátuma: 2020. 04. 08.)

Maness, Ryan C. – Valeriano, Brandon (2015): *Russia's Coercive Diplomacy. Energy, Cyber and Maritime Policy as New Sources of Power.* Palgrave Macmillan.

McNabb, David E. (2016): *Vladimir Putin and Russia's Imperial Revival.* CRC Press.

Nabeel, Fahrad (2018): International Cyber Regime: A Comparative Analysis of the US-China-Russia Approaches. *Strategem* Vol. 1, No. 2, December 2018. 8–27. Forrás: www.academia.edu/38296708/International_Cyber_Regime_A_Comparative_Analysis_of_the_US-China-Russia_Approaches (A letöltés dátuma: 2020. 04. 08.)

Nyáry, Gábor (2019): A digitális állam a külpolitikai térben. A Twittertől az adattudományig. Új Magyar Közigazgatás 12. évf., 2. szám, 75–82. Forrás: www.kozszov.org.hu/dokumentumok/UMK_2019/2/08_Ekozig_Digitalis_allam.pdf (A letöltés dátuma: 2020. 04. 12.)

Painter, Christopher (2018): The rise of the internet and cyber technologies constitutes one of the central foriegn policy issues of the 21st century. *The Foreign Service Journal*, 2018. június Forrás: www.afsa.org/diplomacy-cyberspace (A letöltés dátuma: 2020. 04. 13.)

Pawlak, Patryk (2015): Cyber Diplomacy: EU Dialogue with Third Countries. *European Parliament Think Tank,* 2015. június 29. Forrás: www.europarl.europa.eu/RegData/etudes/BRIE/2015/564374/EPRS_BRI(2015)564374_EN.pdf (A letöltés dátuma: 2020. 04. 08.)

Popescu, Nicu – Secrieru, Stanislav eds. (2018): Hacks, leaks and disruptions. Russian cyber strategy. *Chaillot Papers* No. 148., 2018. október, European Union Institute for Security Studies. Forrás: www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf (A letöltés dátuma: 2020. 04. 06.)

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 2017. május 11. Forrás: www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (A letöltés dátuma: 2020. 04. 13.)

Renard, Thomas (2015): *US–China cybersecurity agreement: a good case of cyber diplomacy.* 2015. október 1. Forrás: www.egmontinstitute.be/us-china-cybersecurity-agreement-a-good-case-of-cyber-diplomacy/ (A letöltés dátuma: 2020. 04. 08.)

Roth, Andrew (2015): Russia and China Sign Cooperation Pacts. *The New York Times,* 2015. május 8. Forrás: www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0 (A letöltés dátuma: 2020. 04. 08.)

Segal, Adam (2017): Chinese Cyber Diplomacy in a New Era of Uncertainty. A Hoover Institute essay. *Aegis Paper Series* No. 1703. Forrás: www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf (A letöltés dátuma: 2020. 04. 07.)

Segal, Adam (2018): *Year in Review: Chinese Cyber Sovereignity in Action*. 2018. január 8. Forrás: www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action (A letöltés dátuma: 2020. 04. 08.)

Swaine, Michael D. (2013): Chinese View on Cybersecurity in Foreign Relations. *China Leadership Monitor*, No. 42. Forrás: https://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf (A letöltés dátuma: 2020. 04. 07.)

The 7th China-EU Cyber Taskforce was Held in Beijing. 2020. január 13. Forrás: www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/jkxw_665234/t1731937.shtml (A letöltés dátuma: 2020. 04. 08.)

The White House: *Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building* (17 June 2013) Forrás: www.whitehouse.gov/the-pressoffice/2013/06/17/joint-statement-on-a-new-field-of-cooperation-in-confidence-building (A letöltés dátuma: 2020. 04. 10.)

UK and 50 nations sign cyber security pact. 2018. november 13. Forrás: www.itproportal.com/news/uk-and-50-nations-sign-cyber-security-pact/ (A letöltés dátuma: 2020. 04. 16.)

US Chief Calls for Regulatory Scheme for Cyberwarfare. (2018) *Radio Free Europe/Radio Liberty*, 2018. február 19. Forrás: www.rferl.org/a/un-guterres-calls-for-cyberwarfare-rules/29049069.html (2020. 04. 06.)

Wirtz, James J. (2015): Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. In GEERS, Keneth: *Cyber War in Perspective: Russian Agression Against Ukraine*. Tallinn, NATO CCD COE Publications. Forrás: https://ccdcoe.org/uploads/2018/10/Ch03_CyberWarinPerspective_Wirtz.pdf (A letöltés dátuma: 2020. 04. 10.)

Xi Jinping gives speech at Cybersecurity and Informatization World Conference. 2016. április 19. Forrás: https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/ (A letöltés dátuma: 2020. 04. 08.)

Ziolkowski, Katharina ed. (2013): *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, Tallinn, NATO CCDCOE Publication.

VÁKÁT OLDAL

Molnár Dóra

Európai kiberdiplomáciai helyzetkép – Franciaország, az Egyesült Királyság és Németország

Az előző fejezet folytatásaként e fejezet a három vezető európai állam, Franciaország, az Egyesült Királyság és Németország kiberdiplomáciájának alapvető elméleti és gyakorlati kérdéseit mutatja be.

Franciaország mint kiberdiplomáciai nagyhatalom

Talán nem túlzás azt állítani, hogy Franciaország évszázadok óta a diplomácia fellegvára, és a franciák a „soft" eszközök alkalmazásának nagymesterei a politikában. Az ország erejét globális szerepvállalása adja, amelyhez a kiterjedt diplomáciai hálózata szolgál alapul: páratlanul széleskörű tagsággal bír multilaterális és nemzetközi szervezetekben, külföldi kulturális misszióinak száma a legmagasabb, és az 5. legnagyobb segélyező állam.[1] Ezért nem meglepő, hogy a francia politika előszeretettel és hatékonyan használja a diplomácia eszköztárát a kibertérben is – olyannyira, hogy európai szinten első e téren. Ez indokolja, hogy az európai országok vizsgálatát Franciaországgal kezdem, még ha kiberhatalmi potenciál terén van más európai állam, amely megelőzi az országot.

Már az első, 2011-ben kiadott, *Az információs rendszerek védelme és biztonsága: Franciaország stratégiája* című kiberstratégiában megjelenik a kibertérbeli nemzetközi együttműködés szükségessége mint a szükséges cselekvési területek egyike.[2] Ezt a 2012-ben elfogadott 681. számú szenátusi információs jelentés konkretizálja azáltal, hogy a tíz prioritás egyikeként hangsúlyozza a bilaterális kapcsolatok fontosságát, közös akciókat sürget az Észak-atlanti Együttműködés Szervezetével (a továbbiakban: NATO) és az Európai Unióval (a továbbiakban: EU), párbeszédet Kínával és Oroszországgal, valamint támogatja a nemzetközi bizalomépítő intézkedések elfogadását.[3] A 2013-ban kiadott Fehér Könyv kiemeli, hogy a kibertámadások kivédése érdekében „globális kormányzati megközelítést" kell alkalmazni, amely részeként Franciaország épít diplomáciai, jogi és politikai eszközeire.[4]

Az ország kiberstratégiáját 2015-ben adták ki *A digitális biztonság nemzeti stratégiája* címmel.[5] A stratégia öt fő célkitűzést rögzít, amelyek közül az ötödik az *Európa, digitális stratégiai autonómia, a kibertér stabilitása* címet viseli. Franciaország Európa digitális

[1] *La diplomatie française* à *l'*ère *numérique* 2019.

[2] *Défense et sécurité des systèmes d'information: Stratégie de la France* 2011.

[3] *Rapport d'Information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense* 2012.

[4] *Livre Blanc. Défense et sécurité nationale 2013.*

[5] *La stratégie nationale pour la sécurité de la numérique 2015.*

transzformációjában szövetségesi kapcsolatain keresztül kíván részt venni, három főbb módon: az európai stratégia megalkotására vonatkozó menetrend megfogalmazásával közösen más uniós, önkéntesen résztvevő államok, a nemzetközi kibermegbeszéléseken való francia jelenlét és befolyás erősítésével, valamint a kiberkapacitások építésében más államok támogatásával, hozzájárulva ezzel a kibertér globális stabilitásához. A stratégia értelmében a befolyásnövelés fő színterei a nemzetközi szervezetek közül az Egyesült Nemzetek Szervezete (a továbbiakban: ENSZ) és az Európai Biztonsági és Együttműködési Szervezet (a továbbiakban: EBESZ), a bilaterális kapcsolatok miniszteri szintű diplomáciai párbeszéd keretében, valamint a politikai döntéshozók és a tudományos élet szereplői részvételével megrendezett informális nemzetközi fórumokon való aktív jelenlét. A stratégiában foglaltak végrehajtására centralizálták a kiberdiplomácia területét, és 2015-ben a Külügyminisztériumban felállították a kiberdiplomácia és digitális gazdaság nagyköveti pozícióját.[6]

A 2015-ös stratégia elfogadása óta a nemzetközi környezet jelentősen megváltozott. Elég, ha a Charlie Hebdo elleni terrortámadást követő vagy a TV5 televíziócsatorna elleni kibertámadás-sorozatokra gondolunk. Az események új megvilágításba helyezték a kiberbiztonság kérdéskörét Franciaországban is, és az országot aktívabb és erőteljesebb nemzeti és nemzetközi fellépésre sarkallták.

Az új megközelítést tükrözi a *Támadó kiberműveletek doktrínája*, amelyet 2018. január 18-án publikáltak, mintegy három héttel megelőzve a *Kibervédelmi stratégiai áttekintés* kiadását. A dokumentumban Franciaország nyíltan ír arról, hogy katonai tevékenységének részét képezik a kiberkapacitások, amelyeket szükség esetén kész bevetni. Ez mindenképpen fordulópontot jelez a francia kiberpolitikában, amelyet ezidáig a diszkrét diplomáciai lépések megtétele jellemzett: még olyan nyilvánvaló kiberkonfliktusok esetén, mint az oroszok által szponzorált, a haditengerészet olajutánpótlás csatornáinak kiderítését célzó kibertámadás kapcsán sem lépett fel Franciaország támadó retorikával, hanem a párbeszéd eszközéhez nyúlva igyekezett a feszültséget csillapítani.[7]

A 2018. február 8-án *Kibervédelmi stratégiai áttekintés* címmel adták ki a legújabb kiberdokumentumot, amely az ország kibervédelmi ambícióinak összefoglaló hivatalos anyaga.[8] A kibervédelem fehér könyvének is nevezett dokumentum több fejezetben is kitér az egyes kiberdiplomáciai lépések szükségességére, és rögzíti Franciaország adott kérdéssel kapcsolatos álláspontját. Önálló fejezet szól a kibertér szabályozásáról szóló nemzetközi tárgyalásokról, kiemelve az ENSZ és a Kormányzati Szakértők Csoport (Group of Governmental Experts, a továbbiakban: GGE) szerepét és elért eredményeit 2013-tól kezdődően. Franciaország a 2016–2017-es ülésszakon önálló javaslattal állt elő a visszatámadás tilalmának mélyebb szabályozását illetően, amely javaslatot bár támogattak a részvevő államok, de a tárgyalások megakadtak a nemzetközi jog alkal-

[6] A tisztséget, amelyet 2017. november 22-e óta digitális nagykövetnek neveznek, David Martinon töltötte be.

[7] Laudrain 2019.

[8] *La Revue Stratégique de Cyberdéfense* 2018.

mazásának módjával kapcsolatos eltérő nézetek miatt. Egy másik fejezet azt mutatja be, hogy az ország a kibertérben hogyan lép fel nemzetközi szinten. A kiberkonfliktusok megelőzése érdekében támogatja a párbeszédet és az együttműködést a szövetségeseivel, a kibertér szabályozását sürgeti, és célja, hogy az európai biztonság és autonómia a kibertérben is biztosítva legyen. A bilaterális kapcsolatai közül kiemeli az Egyesült Államokkal,[9] Kínával, Indiával,[10] Brazíliával és Japánnal fennálló kiberkapcsolatait, hozzátéve, hogy a nyugati szövetségeseivel továbbra is mély kapcsolatokat fog ápolni, de egyre nagyobb hangsúlyt helyez a szubszaharai térségre, ahol kapcsolatok kiépítését sürgeti a frankofón államokkal. Az európai kiberkapcsolatokat három kérdéskör mentén kell rendezni: a technikai, a szabályozási és a kapacitási kérdések azok, amelyekben szükséges a közös alapok megfogalmazása és azok elfogadása. Mind a bilaterális, mind az európai kapcsolatok szempontjából kiemelt helyet foglal el a francia–német kapcsolatrendszer. A két ország közötti együttműködés igen intenzív és kiterjedt, amelyet az eddig kiadott két közös jelentés is alátámaszt.[11] Végezetül pedig a dokumentumban foglaltak értelmében szükséges egy cselekvési doktrína elfogadása, amely olyan alapvető kérdéseket rögzít, mint a kibertámadások osztályozásának rendszere és a kiberincidensekre adandó válaszlehetőségek köre. A kibertér szabályozásának globális rendszerét csak olyan alapelvek mentén lehet megvalósítani, mint a megelőzés, az együttműködés és a stabilitás.

A „támadóbb" szellemű hozzáállás ellenére a francia politikában minden bizonnyal a jövőben is meghatározó szerepet fognak játszani a diplomáciai lépések. Nem véletlen, hogy a különböző nemzetközi szervezetekben Franciaország az egyik legaktívabb tagállam, amikor kiberbiztonsággal kapcsolatos kérdések merülnek fel. Nemcsak az ENSZ-ben – ahogyan a GGE kapcsán arról fentebb már szó esett – hanem a NATO-ban, G7-ben és az EBESZ-ben is.[12] Ez utóbbi szervezetnél Franciaország igen jelentős szerepet játszott a kiberbiztonsággal kapcsolatos bizalomerősítő intézkedés két csomagjának elfogadásában. A G7-ben való francia részvétellel kapcsolatban kiemelem a 2019. április 5–6-án Dinard francia kisvárosban megrendezett találkozót, ahol elfogadták az úgynevezett Dinard deklarációt a kiberszabályok kezdeményezéséről.[13] Ebben üdvözölték az ENSZ közgyűlésének támogató hozzáállását a nemzetközi jog kibertérben való alkalmazhatóságáról, és megerősítették szándékukat egy nyitott, biztonságos, stabil, hozzáférhető

[9] A francia–amerikai kiberdialógus harmadik állomását 2020. január 22-én, Párizsban rendezték meg. A találkozó központi témája a nemzetközi jog kibertérre történő alkalmazhatósága volt. Lásd *Troisième dialogue stratégique France-États-Unis en matière de cybersécurité* 2020.

[10] Az Indiai–Francia Bilaterális Kiberdialógust 2019. június 20-án harmadik alkalommal rendezték meg, megvitatva elsősorban a kibernormákkal kapcsolatos kérdéseket. Jól jelzi a kétoldalú kiberkapcsolatok fontosságát, hogy India meghívást kapott a 2019-es G7 csúcsra az elnöki tisztet 2019-ben betöltő Franciaországtól. Lásd *Indo–French Bilateral Cyber Dialogue (Paris, 20 June 2019)* 2019.

[11] *ANSSI/BSI Common situational picture* 2018, *Second Edition of the Franco–German Common Situational Picture* 2019.

[12] *La France et la cybersécurité.* é. n.

[13] *Dinard Declaration on the Cyber Norm Initiative* 2019.

és békés kibertér támogatása iránt. Egyúttal megerősítették szándékukat egy Kiberszabályozási kezdeményezés (Cyber Norm Initiative – CNI) megfogalmazására, amelyet 2019. augusztus 26-án öntöttek formába tíz, a kibertérben alkalmazandó alapvető szabály megfogalmazásával.[14] Mindez jól illeszkedik a francia soft politika sikertörténetébe, bár hozzá kell tenni, hogy nem volt előzmények nélküli egy ilyen kezdeményezés elfogadása. 2018. november 12. és 14. között ugyanis az UNESCO párizsi székháza adott otthont az Internetkormányzási Fórum (Internet Governance Forum) éves, tizenharmadik ülésének, ahol Emmanuel Macron francia elnök maga jelentette be a *Párizsi felhívást* a bizalom és biztonság kibertérben való megteremtésére.[15] A felhívásban foglaltak széleskörű elfogadását jól jelzi, hogy azt azonnal több mint 500 entitás (állam, szervezet és vállalat) támogatta.[16] A kép teljességéhez azonban az is hozzátartozik, hogy a három „nagy" kiberállam mindegyike visszautasította a kezdeményezést, megtorpedózva ezzel annak globális elfogadhatóságát. A felhívással és a számos hasonló kezdeményezéssel Franciaország célja, hogy az országot kibernagyhatalomként tartsák számon világszerte. Talán ez a cél vezérelte az országot 2019. szeptember 9-én is, amikor a francia Védelmi Minisztérium hivatalos dokumentumban rögzítette véleményét arról, hogy a nemzetközi jog Franciaország szerint miként alkalmazható a kibertérben,[17] – ezzel is úttörő kiberdiplomáciai szerepet vállalva.

Németország

Bár Németország 2004-től aktívan részt vett az ENSZ kiberbiztonsági tanácskozásain és más két- és többoldalú fórumokon, az együttműködés a technikai kérdésekre korlátozódott. Az első, 2011. évi német kiberbiztonsági stratégia megemlítette ugyan a kiberbiztonság nemzetközi és diplomáciai dimenzióit, egészen a Snowden-ügyig azonban Németország nem játszott különösebb szerepet a kiberporondon. Csak ezt követően kezdeményezte Angela Merkel német kancellár érintettsége okán Németország – Brazíliával karöltve – az ENSZ-ben a magánélethez való jog védelméről és sérthetetlenségéről szóló határozat elfogadását a digitális kor vonatkozásában, amely eredményeképp 2013. december 18-án megszületett a 68/167. sz. közgyűlési határozat. Ez Németország jelentős kiberdiplomáciai sikere volt, különösen úgy, hogy a dél-amerikai támogatással globális szintre sikerült emelnie e kérdéskört. Innentől kezdve Németország a kiberdiplomácia aktív támogatójává vált. 2016-ban az EBESZ német elnöksége alatt fogadták el a kibertérbeli bizalomerősítő intézkedések második csomagját, majd 2016–17-ben Németország diplomáciai képviselői elnököltek a UN GGE-n is.

[14] *Inititative pour des normes dans le cyberespace. Synthese des enseignements tirés et des bonnes pratiques* 2019.
[15] *Appel de Paris pour la confiance et la sécurité dans le cyberespace* 2018.
[16] *Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans la cyberespace* 2018.
[17] Rogusky 2019.

Az egyre aktívabb német fellépés alapjai az ország *kiberbiztonsági stratégiájában* keresendők. 2016-ban adták ki az ország második kiberstratégiáját.[18] A dokumentum már kiemelten kezeli az együttműködés fontosságát, amely azonban nem korlátozódhat nemzeti keretek közé, hanem összeurópai, sőt világszintű együttműködési csatornákat kell kialakítani. A stratégia négy cselekvési területet nevesít, amelyek közül az egyik Németország megfelelő pozícionálása az európai és a nemzetközi kiberbiztonsági politikai megbeszéléseken. Ez egyértelműen mutatja, hogy a kiberdiplomácia kiemelt területté nőtte ki magát, és ország biztonságát befolyásoló alapvető tényezővé vált. Ennek részeként Németország hangsúlyozza a kétoldalú partneri kapcsolatok fontosságát is, főként olyan területeken, mint az információ-megosztás és a határon átnyúló szolgáltatásokkal kapcsolatos biztonsági kérdések összehangolása, valamint a kapacitások megosztása, másrészt a fejlesztési együttműködés terén, ahol elsősorban a biztonság- és bizalomerősítő intézkedések segítségével érhetők el sikerek.

Németország a stratégiában foglaltakat a gyakorlatba is fokozatosan átülteti, ahol fokozott szerepet szán a kétoldalú kapcsolatoknak. Kiemelt stratégiai partnere az *Egyesült Államok*, ezért nem véletlen, hogy a kiberpárbeszédük is hosszú és tartalmas múltra tekint vissza. 2012 óta évente megrendezik a kétoldalú kibertalálkozót, hol Washingtonban, hol Berlinben. A találkozások alkalmával olyan kérdéseket vitatnak meg, mint 2016-ban például a nemzetközi jog kibertérben való alkalmazhatóságának kérdése vagy az emberi jogok online érvényesülése, de jól kirajzolódik közös gondolkodásmódjuk a kibertér többszereplős (multi-stakeholder) kormányzati modelljében is.[19]

Kínával 2016 novemberében születetett megegyezés arról, hogy a két állam a kiberkérdések vonatkozásában egy speciális mechanizmus segítségével folytatja a párbeszédet, de kétoldalú szerződés aláírására a mai napig nem került sor.[20] Legutóbb 2020 januárjában folytatott Merkel kancellár tárgyalásokat Kínában egy, az amerikai–kínai egyezményhez hasonló német–kínai kiberegyezmény megalkotásáról, annak előfeltétele azonban a „no spy" klauzula beiktatása az amerikai Huawei-botránynak köszönhetően. Amikor azonban a kancellárt az egyezményről kérdezték, ő diplomatikusan mindössze annyit mondott, hogy Németország és Kína több szinten is folyamatosan tárgyal egymással számos kétoldalú és nemzetközi kérdésről.[21]

A német bilaterális paletta ugyanakkor nem szűkül le a nagy partnerállamokra, hanem rendkívül színes képet mutat. Németország például jó kétoldalú kiberkapcsolatokat ápol Szingapúrral. 2017-ben a szingapúri miniszterelnök látogatást tett Németországban, amely alkalmával a két fél közös szándéknyilatkozatot írt alá a kiberbiztonsági együttműködésről olyan területeken, mint az információmegosztás vagy a közös kutatások. A látogatást 2018 júniusában Merkel kancellár viszonozta, s ennek keretében a két ország vezetője védelmi szerződést is kötött, külön kiberklauzulával.[22]

[18] *Cyber Security Strategy for Germany 2016*.
[19] *Joint Statement on U.S.–Germany Cyber Bilateral Meeting* 2016.
[20] Burgess 2016.
[21] Chazan 2020.
[22] Parameswaran 2018

Németország számos nemzetközi intézményben aktívan lép fel a kiberbiztonsági kérdések tárgyalásakor, de talán mindezen fellépések közül kiemelkedik az *EBESZ*-ben játszott szerepe. Predesztinálva is volt arra, hogy élére álljon az EBESZ-béli kezdeményezéseknek. Egyrészt azért, mert történelmileg politikai és gazdasági szálak kötik mind a Kelethez, mind a Nyugathoz, az EBESZ pedig összeköti e térségek vezető hatalmait is. Másrészt azért, mert Németország vezető állam e területen – elég, ha az adatvédelem területén felállított technikai sztenderdekre és szabályozásra gondolunk. Harmadrészt pedig azért, mert Németország hatékonyan vesz részt olyan, a kibertérbeli normák és szabályok megalkotásával foglalkozó szervezetekben, mint a GGE, ráadásul az itt szerzett tapasztalatait kamatoztatni is tudja.[23]

Az EBESZ 2013-ban megalkotta a kibertérbeli bizalomerősítő intézkedések első csomagját, amely megfelelő alapul szolgált a továbblépéshez. A 2016-os német EBESZ elnökség alatt mindhárom kosárban külön tárgyalták a bizalom- és biztonságerősítő intézkedések lehetséges körét. Az első kosár vonatkozásában 2013-ban még csak önkéntes megállapodások sorát rögzítették a tagállamok közötti katonai együttműködésről. Megegyezés született, hogy az EBESZ-t platformként használják a kibertámadásokról szóló információcserére és a nemzeti kapacitások kiterjesztésének kölcsönös támogatására. A német elnökség kifejezett célja volt, hogy a mérnököket (elsősorban az informatikusokat) is bevonják a kiberdiplomáciába (nem csak az első kosarat érintően), amelytől olyan, a diplomáciai feszültségeket csökkentő hatást várnak, mint az 1950-es évek óta megrendezett Pugwash konferenciák[24] fejleményei. A második, gazdasági kosárba tartozó lépésekhez referenciapontként szolgált a 2015-ben elfogadott német Információbiztonsági törvény, amely a kritikus infrastruktúra védelmével kapcsolatban magasabb biztonsági követelményeket írt elő. A német törvényben foglaltak hivatkozási alapul szolgáltak a NIS-irányelv megalkotásakor is. A központi német kiberszerv, a Szövetségi Információbiztonsági Hivatal (BSI)[25] pedig számos EBESZ-partner számára a műszaki szakértelem modelljeként szolgált. Mindezek a fejlemények új horizontot nyitnak az EBESZ gazdasági együttműködés kontextusában. A harmadik kosár esetében az emberi jogok, azon belül is az interneten való szólásszabadság kérdése a problematikus. A német elnökségnek mindenekelőtt a cenzúra, a hálózati megfigyelés és a szerzői jogi kérdésekkel kapcsolatos dilemmára kellett választ találnia.

Németország kiemelt külpolitikai prioritásként kezeli a *kibertér szabályozásának* kérdéseit. Határozottan kiáll amellett, hogy a globális kérdéseket csak közös szabályozás mentén lehet megoldani – s e körbe tartozik a kiberbiztonság kérdése is. A probléma nem kezelhető csak nemzeti szinten, szükséges az államok, nemzetközi szervezetek, civil szervezetek és a tudományos szféra közti szoros együttműködés. Deklarálja a nemzetközi jog kibertérben való alkalmazhatóságát és alkalmazandóságát, valamint támogatja

[23] *Three Priorities for Cyber Diplomacy under the German OSCE Chairmanship 2016* 2015.

[24] A béke és a leszerelés kérdéseivel foglalkozó, évente megrendezett konferenciák, amelyeken a nemzetközi tudományos élet jeles képviselői vesznek részt 1957 óta.

[25] Bundesamt für Sicherheit in der Informationstechnik – Federal Office for Information Security (BSI).

a multilaterális megközelítést.[26] Mindenképp diplomáciai sikernek tekintendő, hogy 2019 novemberében Németország adhatott otthon az ENSZ Internetkormányzás Fórumának.

A vezető (európai) kiberhatalom: az Egyesült Királyság

Az Egyesült Királyság – hasonlóan a nagyhatalmakhoz – idejekorán felismerte a kiberbiztonság és a kiberdiplomácia fontosságát, amelyet a stratégiai dokumentumaiban is megjelenít, és a gyakorlatban is sikeresen alkalmaz. Az első kiberbiztonsági stratégiát még 2009-ben adták ki, azt azonban hamar, 2011-ben felváltotta egy új stratégia, amely ötéves távlatban vázolta fel a fő irányvonalakat, célkitűzéseket és a megvalósításhoz szükséges feltételrendszert. A stratégia címe: *Megvédeni és segíteni az Egyesült Királyságot egy digitális világban* (Protecting and Promoting the UK in a digital world).[27] A dokumentum négy célkitűzést fogalmaz meg, amelyek közül a második célkitűzés kapcsán van szerepe a kiberdiplomáciának. Az ország megfogalmazott célja, hogy rugalmasan tudjon reagálni a kibertérbeli fenyegetésekre és támadásokra, valamint hatékonyabban tudja érdekeit megvédeni és érvényesíteni a kibertérben. Ez proaktív magatartást és aktív részvételt feltételez a kibertér alakításának folyamatában, amelynek elsődleges eszközei mind békés eszközök: részben diplomáciai jellegűek, részben pedig gazdasági jellegűek, ugyanis a brit kormány igen nagy súllyal csatornázza be a brit vállalatok kereskedelmi érdekeinek támogatását az egyre növekvő nemzetközi kiberbiztonsági piacra. Érdemi előrelépést jelent a *harmadik kiberstratégia*,[28] amelyet a brit kormány 2016. november 1-jén adott ki ismét deklaráltan öt évre. A dokumentum három stratégiai célt fogalmaz meg, ezért nevezhetjük a 2016-os kiberstratégiát a „3D stratégiájának" is: megvédeni (defend), elrettenteni (deter), fejleszteni (develop), amelyek megvalósuláshoz elengedhetetlennek tartja a nemzetközi fellépést. A célkitűzések közül a második kapcsán kiemelt szerep jut a kiberdiplomáciának. Az elrettentést ugyanis nemcsak „hard" eszközökkel képzelik el (mint a támadó kiberképességek fejlesztése), hanem az együttműködési csatornák további szélesítésével és mélyítésével is – ahogyan a stratégia fogalmaz: a britek tovább folytatják a már megkezdett globális kiberszövetség kiépítését, és továbbra is támogatják a nemzetközi jog kibertérben történő alkalmazását. A három stratégiai cél megvalósítása csak megfelelő nemzetközi keretek között képzelhető el. Az Egyesült Királyság továbbra is élharcosa a szabad, nyitott, békés és biztonságos kibertér megteremtésének, ahol a nemzetközi jog alkalmazandó, és az alapvető emberi jogok érvényesülése biztosított online és offline egyaránt. Ebben az Egyesült Királyság számít nemcsak a hagyományos szövetségesire, hanem új partnereire is, és igyekszik kihasználni az olyan multilaterális fórumok adta befolyásolási lehetőségeit, mint az ENSZ, a G20, az Európai Unió, a NATO, az EBESZ, az Európa Tanács vagy a Brit Nemzetközösség.[29]

[26] *Cyber policy: multilateral solutions for the future* 2019.
[27] *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world* 2011.
[28] *National Cyber Security Strategy 2016–2021* 2016.
[29] Molnár 2017.

A globális kiberszövetség kiépítése célkitűzésének megvalósításában kiemelt szerep jut *kétoldalú kiberkapcsolatoknak*. A britek hagyományos szövetségesei közül kétség kívül az *Egyesült Államok* áll az első helyen, amellyel a „különleges kapcsolat" („special relationship") – vagy ahogyan az utóbbi időben hívják, „a legfontosabb kétoldalú kapcsolat" („the most important bilateral partnership") – keretében igen szoros kapcsolatokat ápol a szigetország a kiberkérdések vonatkozásában is már közel egy évtizede. Már 2011-ben rögzítették a magánszektor és az üzleti élet szereplői bevonásának, a kutatás-fejlesztésnek, valamint a joguralom alapintézményeinek kibertérben való alkalmazásának szükségességét.[30] 2015-ben Washingtonban Obama elnök és Cameron miniszterelnök egyeztetett az együttműködés részletkérdéseiről,[31] amelyet végül 2016. szeptember 7-én intézményesített a két védelmi miniszter által aláírt kiberegyezmény.[32]

Bár a szigetország még nem írt alá bilaterális egyezményt *Kínával*, azonban 2015. október 22-én a kínai elnök angliai látogatásán a két ország közös nyilatkozatot adott ki a globális átfogó stratégiai partnerségük kiépítéséről, útjára indítva ezzel a bilaterális kapcsolat „Aranykorát".[33] Ennek részeként rögzítették, hogy egymás ellen nem folytatnak, illetve nem támogatnak a szellemi tulajdon, üzleti titkok vagy bizalmas üzleti információk jogosulatlan eltulajdonítására irányuló kiberakciókat, amelyek célja a versenyelőnyhöz jutás.[34]

Az Egyesült Államokkal fennálló speciális partneri viszony nyomán nem meglepő, hogy az Egyesült Királyság 2012-ben *Japánnal* is kétoldalú kiberkapcsolatokat létesített. A kétévenként megrendezésre kerülő találkozók ötödik állomását Tokióban tartották 2020. január 31-én.[35] A megbeszélés alkalmával a kapacitásépítés és a nemzetközi porondon történő együttműködés lehetőségeiről tárgyaltak. Ez összhangban van a 2018-ban megrendezett negyedik találkozó során meghatározott fő együttműködési területekkel, amelyek között szerepel még a szabályalapú nemzetközi kiberrendszer támogatása és az IoT eszközök biztonságos használatával kapcsolatos nemzeti megoldások megosztása is.[36]

Az ázsiai bilaterális kapcsolatok közül végül *Indiát* emelem ki, amely a britek számára is hatalmas gazdasági potenciált rejt magában. Elég, ha arra gondolunk, hogy már ma is 600 millió internetfelhasználót és 650 millió mobilhasználót tudhat magáénak az ország. Az indiai–brit biztonsági együttműködés egyik fontos aspektusát jelentik a kiberkérdések, és a 2012 óta folytatott indiai–brit kiberdialógus keretében olyan kérdések vannak terítéken, mint a kiberkockázatok csökkentése, a kiberbűnözés kezelése és az internetkormányzás globális, multilaterális, transzparens és demokratikus rendszerének kiépítése. 2018 áprilisában Londonban a két ország ötéves keretmegállapodást írt alá 14 területre

[30] *US–UK Cyber Communiqué* 2011.
[31] *Fact sheet: U.S.–United Kingdom Cybersecurity Cooperation* 2015.
[32] *U.S –U.K. Cyber Agreement Opens Doors for Both Nations* 2016.
[33] A brit politika egyes elemeiről részletesebben lásd *The making of UK strategy towards China* 2019.
[34] *UK–China Joint Statement 2015* 2015.
[35] *The 5th Japan–UK Bilataral Consultations on Cyberspace* 2020.
[36] *The 4th Japan–UK Bilataral Consultations on Cyberspace* 2018.

kiterjedő együttműködéssel. India ilyen széleskörű kiberegyüttműködési megállapodást az Egyesült Királyságon kívül ezidáig csak az Egyesült Államokkal kötött.[37]

Az Egyesült Királyság az európai országok közül is számos állammal létesített már kétoldalú kiberkapcsolatot. Ezek közül a *lengyel–brit* kiberegyüttműködési megállapodást emelem ki, nem elsősorban a benne foglaltak miatt (amely lényegi újdonsággal nem szolgál), hanem regionális jelentősége okán: a britek e kapcsolaton keresztül kívánják a kelet-európai és a nyugat-balkáni kiberkapacitásépítési programokat támogatni.[38]

Végezetül az Egyesült Királysággal kapcsolatban nem szabad megfeledkezni a *Brit Nemzetközösségről*, amely már önmagában is régóta fennálló diplomáciai fórum a résztvevő államok számára, de az utóbbi években már önálló napirendi kérdésként szerepel a kiberbiztonság kérdésköre is. A résztvevő államok együttműködésüket 2018. április 20-án intézményesítették a kiberdeklaráció aláírásával.[39] A nyilatkozat rögzíti a kölcsönös segítségnyújtási kötelezettséget a kiberkapacitások építésében és a kibertérrel kapcsolatos egységes vízió megfogalmazásának igényét, amelyet az Egyesült Királyság anyagilag is támogat, 15 millió fonttal hozzájárulva a rögzített célok megvalósításához.[40]

Záró gondolatok

Az előző fejezetben már hivatkoztam a Globális Kiberbiztonsági Indexre, amely az államok kiberpotenciáljának rangsorát adja meg. Az index alapján a világ vezető kiberhatalma az Egyesült Királyság, a harmadik helyen pedig Franciaország található. A harmadik vizsgált állam, Németország a 26. helyet szerezte meg.[41] Igen érdekes ugyanakkor, hogy az ötödik vizsgált terület, az együttműködés vonatkozásában az angolok igen jó pontot értek el, míg a diplomáciai nagyhatalomnak számító Franciaország jelentős lemaradásban van. Az európai kiberbiztonság vizsgálata azonban nem ér véget a három nagy állam bemutatásával. Számos üdítő példa létezik arra, hogy kis országok milyen nagy sikereket tudnak elérni a kiberbiztonság területén. Az index ezt is visszatükrözi, ugyanis 4. helyen Litvánia, az 5. helyen pedig Észtország áll az összesített világrangsorban. Mindez természetesen nem véletlen: elég, ha arra gondolunk, hogy ezen államokat érte elsőként olyan horderejű kibertámadás a 2000-es évek vége felé, amely a kiberkérdéseket az államok biztonsági agendájának élvonalába emelte. Mindkét állam magasabb részpontszámot ért el az együttműködés területén, mint a három vezető nagy állam. Ez az eredmény jól jelzi, hogy a kis államok milyen nagy hangsúlyt helyeznek a kiberdiplomácia fontosságára, és a békés, diplomáciai eszközök használatát előrébbvalónak tartják a hard kapacitásoknál. Az európai térség pedig valamennyi részkérdés tekintetében magasan a világ előtt jár, így az együttműködés vonatkozásában is, amely talán alapul szolgálhat egy békés kibertér alapjainak lerakásához.

[37] Roy-Chaudhury 2019.
[38] *UK–Poland cyber cooperation commitment* 2017.
[39] *Commonwealth Cyber Declaration* 2018.
[40] *Analysis: Untangling the web of multi-level cyber diplomacy* 2018.
[41] *Global Cybersecurity Index* 2018.

Felhasznált irodalom

Analysis: Untangling the web of multi-level cyber diplomacy (2018). Forrás: www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/may/nalysis-untangling-the-web-of-multi-level-cyber-diplomacy/ (A letöltés dátuma: 2020. 04. 17.)

ANSSI/BSI Common situational picture (2018). Vol. 1. – July 2018. www.ssi.gouv.fr/uploads/2018/07/bilateral-french-german-it-security-situation-report.pdf (A letöltés dátuma: 2018. 11. 17.)

Appel de Paris pour la confiance et la sécurité dans le cyberespace (2018). 2018. november 12. Forrás: www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf (A letöltés dátuma: 2018. 11. 17.)

Burgess, Christopher: *Dissectiong China's Global Bilateral Cybersecurity Strategy* (2016): Forrás: https://securityboulevard.com/2017/10/dissecting-chinas-global-bilateral-cybersecurity-strategy/ (A letöltés dátuma: 2020. 04. 15.)

Chazan, Guy: German cyber security chief backs 5G 'no spy' deal over Huawei (2020). *Financial Times*, 2020. február 28. Forrás: www.ft.com/content/5a0fe826-3b34-11e9-b856-5404d3811663 (A letöltés dátuma: 2020. 04. 14.)

Commonwealth Cyber Declaration (2018). 2018. április 20. Forrás: https://thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf (A letöltés dátuma: 2020. 04. 17.)

Cyber policy: multilateral solutions for the future (2019). Federal Foreign Office, 2019. szeptember 25. Forrás: www.auswaertiges-amt.de/en/aussenpolitik/themen/multilateralism-cyber/2250332 (A letöltés dátuma: 2020. 04. 14.)

Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans la cyberespace (2018). Liste des soutiens à l'appel de Paris (actualisé le 14 novembre 2018). Forrás: www.diplomatie.gouv.fr/IMG/pdf/soutien_appel_paris_cle8e5e31.pdf (A letöltés dátuma: 2018. 11. 30.)

Cyber Security Strategy for Germany 2016 (2016). Federal Ministry of the Interior. Forrás: www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (A letöltés dátuma: 2017. 11. 11.)

Défense et sécurité des systèmes d'information: Stratégie de la France (2011). Forrás: www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf (A letöltés dátuma: 2018. 11. 01.)

Dinard Declaration on the Cyber Norm Initiative (2019). 2019. április 6. Forrás: www.diplomatie.gouv.fr/IMG/pdf/g7_dinard_declaration_on_cyber_initiative_cle4e553d.pdf (A letöltés dátuma: 2020. 03. 13.)

Fact sheet: U.S.–United Kingdom Cybersecurity Cooperation (2015). The White House, Office of the Press Secretary. 2015. január 16. Forrás: https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation (A letöltés dátuma: 2020. 04. 16.)

Indo–French Bilateral Cyber Dialogue (Paris, 20 June 2019) (2019). Forrás: www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/article/indo-french-bilateral-cyber-dialogue-20-06-19 (A letöltés dátuma: 2020. 03. 13.)

Inititative pour des normes dans le cyberespace. Synthese des enseignements tirés et des bonnes pratiques (2019). 2019. augusztus 26. Forrás: www.diplomatie.gouv.fr/IMG/pdf/_fr_synthesis_cyber_norm_initiative_cle025b33.pdf (A letöltés dátuma: 2020. 03. 13.)

Joint Statement on U.S.–Germany Cyber Bilateral Meeting (2016). 2016. március 24. Forrás: https://2009-2017.state.gov/r/pa/prs/ps/2016/03/255082.htm (A letöltés dátuma: 2020. 04. 15.)

La diplomatie française à *l'ère numérique* (2019). Consulat Général de France á Ekaterinbourg. 2019. május 29. Forrás: https://ru.ambafrance.org/La-diplomatie-francaise-a-l-ere-numerique (A letöltés dátuma: 2020. 03. 19.)

La France et la cybersécurité (é. n.). Forrás: www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/ (A letöltés dátuma: 2018. 11. 17.)

La Revue Stratégique de Cyberdéfense (2018). SGDSN, le 12 février 2018. www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf (A letöltés dátuma: 2018. 11. 15.)

La stratégie nationale pour la sécurité de la numérique 2015 (2015). Forrás: www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf (A letöltés dátuma: 2018. 11. 16.)

Laudrain, Arthur P.B. (2019): *France's New Offensive Cyber Doctrine*. 2019. február 26. Forrás: www.lawfareblog.com/frances-new-offensive-cyber-doctrine (A letöltés dátuma: 2020. 04. 19.)

Livre Blanc. Défense et sécurité nationale 2013 (2013). Forrás: www.defense.gouv.fr/content/download/206186/2286591/file/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf (A letöltés dátuma: 20018. 11. 01.)

Molnár, Dóra (2017): Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia. *Hadmérnök* 12. évf., II. különszám „KÖFOP" 2017. 136–148. Forrás: http://hadmernok.hu/170kofop_09_molnar.pdf (A letöltés dátuma: 2020. 04. 16.)

National Cyber Security Strategy 2016–2021 (2016). HM Government, United Kingdom, 2016. november 1. Forrás: www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (A letöltés dátuma: 2017. 10. 11.)

Parameswaran, Prashanth (2018): *Singapore–Germany Cyber Cooperation in Focus with Introductory Visit*. 2018. augusztus 14. Forrás: https://thediplomat.com/2018/08/singapore-germany-cyber-cooperation-in-focus-with-introductory-visit/ (A letöltés dátuma: 2020. 04. 15.)

Rapport d'Information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense (2012). Par le Sénateur M. Jean-Marie BOCKEL. Sénat Session extraordinaire de 2011–2012. Enregistré á la Présidence du Sénat le 18 juillet 2012. Forrás: www.senat.fr/rap/r11-681/r11-6811.pdf (A letöltés dátuma: 2018. 11. 01.)

Rogusky, Przemyslaw (2019): *France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I.* 2019. szeptember 24. Forrás: http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (A letöltés dátuma: 2020.04. 19.)

Roy-Chaudhury, Rahul (2019): *India–UK cybersecurity cooperation: the way forward*. 2019. november 22. Forrás: www.iiss.org/blogs/analysis/2019/11/sasia-india-uk-cyber-security-cooperation (A letöltés dátuma: 2020. 04. 16.)

Second Edition of the Franco–German Common Situational Picture (2019). 2019. május 21. Forrás: www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/D-F_Reports/Common_Situational_Picture_2019.pdf?__blob=publicationFile&v=2 (A letöltés dátuma: 2020. 04. 19.)

Troisième dialogue stratégique France-États-Unis en matière de cybersécurité (Paris, 22 janvier 2020) (2020). Forrás: www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/actualites-et-evenements-lies-a-la-cybersecurite/article/troisieme-dialogue-strategique-france-etats-unis-en-matiere-de-cybersecurite-22 (A letöltés dátuma: 2020. 03. 13.)

The making of UK strategy towards China (2019). 2019. április 4. Forrás: https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/612/61210.htm (A letöltés dátuma: 2020. 04. 16.)

The 4th Japan–UK Bilataral Consultations on Cyberspace (2018). Japan–UK Joint Press Release, 2018. március 16. Forrás: www.mofa.go.jp/press/release/press4e_001960.html (A letöltés dátuma: 2020. 04. 16.)

The 5th Japan–UK Bilataral Consultations on Cyberspace (2020). 2020. január 31. Forrás: www.mofa.go.jp/press/release/press4e_002766.html (A letöltés dátuma: 2020. 04. 16.)

The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world (2011). 2011. november. Forrás: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (A letöltés dátuma: 2017. 10. 11.)

Three Priorities for Cyber Diplomacy under the German OSCE Chairmanship 2016 (2015). German Institute for International and Security Affairs, Berlin, 2015. november 11. Forrás: www.swp-berlin.org/en/point-of-view/three-priorities-for-cyber-diplomacy-under-the-german-osce-chairmanship-2016/ (A letöltés dátuma: 2020. 04. 14.)

UK–China Joint Statement 2015 (2015). Foreign and Commonwealth Office, 2015. október 22. Forrás: www.gov.uk/government/news/uk-china-joint-statement-2015 (A letöltés dátuma: 2020. 04. 16.)

UK–Poland cyber cooperation commitment (2017). 2017. december 21. Forrás: www.gov.uk/government/publications/uk-poland-cyber-co-operation-commitment-joint-statement/uk-poland-cyber-co-operation-commitment (A letöltés dátuma: 2020. 04. 17.)

U.S.–U.K. Cyber Agreement Opens Doors for Both Nations (2016). DoD news, 2016. szeptember 18. Forrás: www.defense.gov/Explore/News/Article/Article/937878/us-uk-cyber-agreement-opens-doors-for-both-nations/ (A letöltés dátuma: 2020. 04. 16.)

US–UK Cyber Communiqué (2011). 2011. május 25. Forrás: www.gov.uk/government/publications/us-uk-cyber-communique és https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62647/CyberCommunique-Final.pdf (A letöltés dátuma: 2020. 04. 16.)

Nyáry Gábor

Kiberbiztonság és külgazdasági kapcsolatok: a digitális gazdaság dilemmái

Bevezetés

2020 májusában, mikor az új koronavírus világjárvány első hulláma kicsit engedett szorításából, szűkszavú hír jelent meg.[1] A korábbi hónapok drámai bejelentéseihez képest ártatlannak tűnő szövegre azonban okkal figyeltek fel a szakemberek. Az amerikai Szövetségi Nyomozó Iroda, az FBI és a Kiberbiztonsági és Infrastruktúra Védelmi Hatóság a Kínai Népköztársasághoz köthető kiberszereplők fokozott aktivitására figyelmeztettek. Az állami és a magánszférába tartozó „érdeklődők" a COVID-19 járványhoz kapcsolódó kutatási adatokat és szellemi tulajdont igyekeztek illegálisan megszerezni. Amerikai egészségügyi intézmények, gyógyszergyárak, kutatólaboratóriumok hálózatait támadva azonosították, gyűjtötték a koronavírus vakcinákkal, gyógyszerekkel kapcsolatos létfontosságú információkat.[2] Más szóval nemzetbiztonsági adatokat. Ám ezek az adatok, joggal mondhatjuk, ugyanakkor roppant üzleti értéket képviselő, gazdasági információk is. A 21. századi kibervalóság fontos mozzanata éppen ez: a kibertér egyszerre országok közötti politikum és nemzeteken átívelő gazdasági terep. Amikor „kiberbiztonságról" beszélünk, szinte mindig gazdasági vetületeket is érintünk alatta. És viszont: az egyre inkább digitalizálódó, globális „kibergazdaság" mindig egyfajta biztonsági téma is. Biztonság és gazdaság – a kibertér két oldala. A kiberdomén mint gazdasági mező, üzleti érdekek és ambíciók egyszerre virtuális és nagyon is valóságos térsége ma még kialakulóban van: evolúcióját, fejlődési irányait, szabályozási kereteit ma még kérdések, élénk nemzetközi viták kísérik. Minden jel arra mutat: a kibertér mint gazdasági szféra dilemmái a kiberdiplomácia napirendjének fő tételei maradnak még egy időre.

Digitális geo-ökonómia

Kötetünk bevezető tanulmányában a kibertér geopolitikai értelmű koncepcióját igyekeztünk bemutatni. Elsőnek említettük, hogy úgy tekinthetünk a kibertérre, mint az Internet, a számítástechnikai eszközök, a rajtuk futó szoftverek, sőt az őket használó, mind inkább

[1] *FBI–CSISA PSA PRC targeting of COVID-19 research organisations* 2020.

[2] A kiberdiplomácia elismert kutatóbázisa, a genfi DiploFoundation havi jelentése egyenesen úgy fogalmazott: „A világban a kiberbűnözés is visszatért a szokványos kerékvágásba." A kutatócsoport is egyértelműen jelezte: a kibertérben megszaporodott támadások többsége kórházak, kutatóintézetek ellen irányul, alapvetően a gazdasági kiberhírszerzés és kibertolvajlás eseteit szaporítva. A primér „nemzetbiztonsági", vagy politikai jellegű kiberakciók mintha háttérbe szorultak volna, noha az akciókban résztvevők között szép számmal akadnak állami aktorok is. *Digital Watch Newsletter* 2020.

hálózatokba szerveződő alkalmazók összességére. Ehhez hozzátettük a korszak (ismét divatba jövő) hatalmi-politikai koncepcióját, a geopolitika fogalmát, amely lényegét tekintve azt hangsúlyozza: a nemzetek egymás közötti viszonyát, érdekérvényesítési mozgásait nagymértékben befolyásolják bizonyos hosszú távon állandó struktúrák. Elsősorban persze maga a környezet, a fizikai tér: az ország elhelyezkedése, domborzati viszonyai, vízrajza, népesedésföldrajza.[3] Most, a kibertér gazdasági aspektusait szemügyre véve, elérkezettnek látjuk az időt arra, hogy ezzel az újabb vetülettel bővítsük koncepciónkat. Azzal a területtel, amelyet talán a digitális geo-ökonómia fogalma írhat le a legjobban.[4]

Keretek és fogalmak

Ha korábban (e kötet bevezető fejezetében) siettünk hangsúlyozni, hogy a „geopolitika" kifejezés távolról sem rendelkezik valamilyen egységes, mindenki által elfogadott jelentéstartalommal vagy akár használattal, akkor még erőteljesebben érdemes most figyelmeztetni rá: az általunk bevezetett újabb szóösszetétel, a „geo-ökonómia" sincsen jobb helyzetben. Sőt! Sokan, sokféle jelentésárnyalattal alkalmazzák: vannak, akik létjogosultságát is vitatják, de az mindenesetre jól látható, hogy még a szakmai közbeszédben sem tudott annyira gyökeret verni, mint rokona, a „geopolitika".[5] Pedig a „geo-ökonómia" – noha a szóösszetétel valóban kicsit félrevezető lehet – rendkívül pontos és fontos meglátást takar. Érdemes ehhez felidézni azt a szerzőt, aki a világpolitika tektonikus átalakulásainak időszakában, az 1990-es évek legelején (ismét) divatba hozta az elképzelést. Edward Luttwak, a stratégiaelmélet és stratégiatörténet egyik sokat kritizált, de kétséget kizáróan legeredetibb gondolkodója nyers őszinteséggel fogalmazta meg a kor egyre szembeötlőbb jelenségét: a gazdaság, és különösen a nemzetközi gazdaság – valójában harc, háború. Ennek a háborús jellegnek az érzékeltetésére vezette be a geo-ökonómia fogalmát.[6] Ugyanakkor ez az időszak volt az a történelmi pillanat, a hidegháború vége, amikor sokan gondolták úgy, hogy az államok közötti konfliktusok katonai megoldása örökre a múlté lett.[7] Luttwak geo-ökonómia kifejezése azt hangsúlyozza: immár a katonai erő helyett a gazdaság, a nemzetközi kereskedelem eszköztárával vívják majd küzdelmeiket a rivális világhatalmak. Akár úgy is fogalmazhatunk:

[3] Nyáry 2020.

[4] A koncepció nem rendelkezik túlságosam kiterjedt szakirodalommal (összevetve legalábbis a geopolitika fogalomkörével). A probléma egyik legkitűnőbb exponálására vállalkozik Moisio 2019. Ugyanakkor magyar nyelven ad kiváló betekintést és általános hátteret Pintér 2016.

[5] Wigell 2019 a terminológiai kérdések áttekintése mellett a koncepció jól alkalmazható leírását adja.

[6] Luttwak 1990 későbbi követői tovább is léptek a történelmi parafrázis-gyártás terepén, és egyenesen a 19. századi nagy porosz katonai gondolkodó, Clausewitz híres mondatát fogalmazták át így: „A gazdaság a háború folytatása más eszközökkel".

[7] Nem véletlenül éppen ez az a pillanat, amikor például megszületik – az amerikai politikatudós Joseph Nye tollából – a nemzetközi kapcsolatok elméletének egyik leghíresebb koncepciója, az államok békés érdekérvényesítését hangsúlyozó „soft power" fogalma.

a geo-ökonómia szűkebb jelentéstartalmú, mint a fegyveres erőszakot is magába foglaló geopolitika, ám a puszta külgazdasági kapcsolatrendszernél szélesebb.[8] Az elképzelés jogosságát, használhatóságát és időtálló jellegét jól bizonyítja a világ globális nagyhatalma, az USA 2017-es *Nemzetbiztonsági Stratégiája*, amely precíz erővel mondja ki: a gazdaság biztonsága – nemzetbiztonsági kérdés.[9] Ha most egy pillanatra felidézzük a jelen fejezet bevezető gondolatai között említett mostani példát, ahol állami szereplők igyekeznek nemzetbiztonsági horderejű üzleti titkokat megszerezni és eltulajdonítani a kibertérben, akkor kezdjük látni, hogyan kapcsolódnak egymásba ezek a körök.

A kibervilág mint a politikum színtere – ezt a felfogást igyekszik megragadni a „kibergeopolitika" koncepciója (erről szóltunk részletesen e könyv bevezető fejezetében). Létezik azonban egy másik dimenzió, ahol a kibertér mint gazdasági-üzleti folyamatok színtere jelenik meg. Ez a „kiber geo-ökonómia" (vagy digitális geo-ökonómia) területe. Alapvetően ez határozza meg a digitális gazdaság jellegét, működési módjait, folyamatait.

Digitális gazdaság

Digitális gazdaságot mondtunk, és okkal: ma már a szakmai nyelv bevett kifejezésévé vált ez a szókapcsolat. A 2000-es évek elejétől ugyanis érezhetően gyorsuló tempójú jelenség formálja a világ szinte valamennyi társadalmát: a digitalizáció. Sommás megfogalmazással úgy jellemezhető ez a folyamat, mint amelyben az adatok és a hálózatok körbefonják, átitatják a termelési folyamatokat, a kormányzati és személyes fogyasztást, a határokon átívelő kereskedelmi forgalmat és természetesen a gazdaságot mozgató pénzügyeket is.[10] Némi óvatosság azonban nem árt! A „digitális gazdaság" kifejezés, nyilvánvaló jelentéstartalma ellenére, tudományos értelemben nem egységes koncepció, nem elfogadott definíció. A globális gazdaságstatisztikákban megkerülhetetlen Nemzetköz Valutaalap, a digitális gazdaság teljesítményéről szólva leszögezi: még abban sincs teljes egyetértés, hogy mit értsünk a gazdaság „digitális szektorán", vagy miket soroljunk a „digitális termékek" körébe. Noha a szakmai beszédben mára teljességgel polgárjogot nyert, és így mi is használjuk a „digitális gazdaság" fogalmát, ne veszítsük szem elől, hogy ez még egy alakuló, formálódó koncepció, folyamatosan bővülő jelentéstartalmakkal.[11]

[8] Gady 2020.

[9] Gady 2020.

[10] *Measuring the Digital Economy* 2018, 6. A téma friss áttekintését adja Filippov 2019, aki rávilágít arra, hogy a meglehetősen következetlen fogalomhasználat csak tovább bővül azzal, hogy a korábbi „Internetgazdaság" kifejezés helyébe mind gyakrabban lép az „Ipar 4.0" fogalom is, tehát a Dolgok Internete (Internet of Things – IoT) által forradalmasított és átalakított gazdaság.

[11] *Measuring the Digital Economy* 2018. A pontosság kedvéért érdemes megjegyezni, hogy a nemzetközi statisztikák, egyebek mellett az ENSZ gazdaságstatisztikai rendszere „Információs és Kommunikáció Technológiai (IKT) szektorról" beszél, valamint egy „Tartalom- és Médiaipari szektorról". A kicsit szabadabban vett szakmai közbeszéd nagyjából e két kategóriához sorolható fogalomkészleteket érti a „digitális gazdaság" alatt.

A definíció feljebb ismertetett nehézsége miatt a számadatokkal is óvatosan érdemes ugyan bánni, de a digitális gazdaság teljesítménye, fejlődési üteme így is figyelemre méltó. Mértékadó számítások szerint a digitális gazdaság aránya a világgazdaság összteljesítményén belül eléri a 22,5%-ot.[12] A digitalizáció terén hagyományosan az élen szereplő Egyesült Államok 5,9 billió dolláros digitális gazdasága az ország GDP-jének mintegy 33%-ára rúg. A szakemberek különösen fontos szerepet, gazdaságnövekedési motort látnak a digitális befektetésekben: ez az USA-ban, 2020-ra számítva, további 2,2%-os GDP-növekedést eredményez.[13] A digitalizáció terjedésének, a digitális gazdaság növekvő potenciáljának kihasználásához elengedhetetlen az IKT-technológiák széleskörű társadalmi befogadása és abszorpciója is. A digitális gazdaságban rejlő lehetőségek kiaknázására való képességet mutatja a Világgazdasági Fórum Hálózatos Készenléti Indexe (NRI), ahol az Egyesült Államok már csak az 5. helyen áll, előtte Szingapúrral, Finnországgal, Norvégiával és Svédországgal.[14]

Kiberbiztonság és nemzetközi kereskedelem

Az üzlet, a gazdaság ma már ezer szálon kapcsolódik az Internethez, az IKT-technológiákhoz. Az országhatárokon átnyúló, nemzeteket összekötő külkereskedelem esetében pedig ma már nem mozdulhat áru vagy szolgáltatás a kibertér (valamilyen formában történő) érintése nélkül. A kibertér szabályozási, kormányzási-igazgatási kérdéseivel foglalkozó kiberdiplomácia fókuszában éppen ezért egyre előkelőbb helyre kerülnek a kereskedelem, sőt általában véve a *digitális* gazdaság és a kibertér kapcsolódási területein felbukkanó kockázatok, problémák.[15]

Közhely már lassan, de érdemes sokadszorra is hangsúlyozni: a modern gazdaságokban egyre nagyobb szerepet kap az *adat*; sőt hovatovább meghatározóvá válik a szerepe. Nem véletlenül élnek gyakorta az új fordulattal: az adat a 21. századi gazdaságok „olaja". Az adat pedig, nem mondunk ezzel meglepőt, a kibertérben él, ott sokasodik, ott mozog. Ahogy bővül (méghozzá exponenciális sebességgel) a világban felhalmozódó adattömeg, ahogy terjeszkedik, bővül a digitális gazdaság – egyre növekszik a kiberbiztonsági kockázatok abszolút és relatív mértéke.[16] A digitális gazdaság, és különösen az élenjáró

[12] Teoh–Mahmood 2017, 6511. A számítások természetesen eltérő eredményeket hoznak. A Foreign Policy folyóirat adatkormányzásról, nemzetközi kiberdiplomáciai és szabályozási törekvésekről szóló friss összefoglalója például a globálisan előállított GDP 15,5%-ára teszi a digitális gazdaság teljesítményét. Jellemző adat azonban ezen belül is: a nagy internetes platformok (mint a Google, Facebook, WeChat stb.) együttes értéke teszi ki a világ GDP-jének csaknem 10%-át. *Data Governance. Part I. Emerging Data Governance Practices* 2020.

[13] Teoh–Mahmood 2017, 6511.

[14] Teoh–Mahmood 2017, 6511.

[15] Brangetto 2015 egyik fő erőssége, hogy az egyes nemzeti kiberbiztonsági stratégiák explicite gazdasági vetületeit veszi számba, amire viszonylag kevés példa akad a szakirodalomban.

[16] Meltzer 2019, 7. Ugyanakkor a téma átfogó áttekintéséhez, az elsődlegesen biztonsági fókuszú kiberbiztonsági koncepciók egyre erőteljesebben jelentkező gazdasági összefüggéseihez itt találunk rendkívül hasznos adalékokat: Brangetto 2015.

technológiák, az adatok tömegének határokon átnyúló globális áramlásától függenek ma már: az adat élteti az innovációt, adatokon alapul a termelőeszközök beszerzése, és adatok teszik lehetővé a késztermékek és szolgáltatások kiszállítását is. A mesterséges intelligencia (a továbbiakban: MI), az elkövetkező évtizedek nagy ígérete adatok, méghozzá hatalmas adattömegek nélkül semmire sem menne. Az MI-technológiák egyik legfontosabb területét jelentő gépi tanuló rendszerek például hatalmas adattömegeken „tréniroznak". Ezeknek az adatoknak egy része ma már a globális digitális hálózatokon át jut felhasználási helyére.

De ott van az e-kereskedelem, amelynek révén nem csupán a gazdasági élet mamutjai, de kis- vagy akár mikrovállalkozások is szerves kapcsolatba léphetnek a kibertérrel. Az elektronikus kereskedelemben is az adat az éltető elem, és ez az esetek jó részében itt is globális forgalmat jelent. Az Egyesült Államokban például a közismert eBay-re felcsatlakozott kisvállalatok 97%-a exportál is, azaz aktívan kacsolódik be a nemzetközi kereskedelmi forgalomba.[17] De ma már az Internetes hozzáférés és a határokon átíveli adatáramlás jellemzi a szolgáltató szektor jelentős szeletét is. A szolgáltatások egyre nagyobb hányadát adják és veszik online hálózatokon át.

A digitális gazdaságot és a globális adatáramlást fenyegető kiberfenyegetések öt nagyobb területet ölelnek fel.[18] Az első terület maga a nemzetbiztonság térrendszere: a fegyveres erők, a nemzetbiztonsági szervezetek. A második nagyobb terület, ahol a kibertér fenyegetései ma már több mint kézzel foghatóak egyes esetekben, a kritikus infrastruktúra területe. A harmadik nagyobb fenyegetési terület az üzleti-kereskedelmi titkok területe. A negyedik olyan terület, ahol a kibervalóság fenyegető árnya tornyosul, az egyéb online információk hatalmas gyűjtőterülete. És van még egy ötödik tér, ahol a kiberfenyegetésekkel szembeni sérülékenység gyors tempóval növekszik: a nemzetközi befektetésekre vonatkozó (kulcsfontosságú) információk szintén hatalmas tere. Ebben az összefüggésben érthető, hogy az államokra egyre nagyobb mértékben nehezedik a magángazdaságba tartozó szereplők kiberbiztonságának védelme, garantálása, amiből a kiberdiplomácia struktúrái is kiveszik a részüket.

Érdemes egy pillanatra kitekinteni: a kiberincidensekkel, kibervédelemmel kapcsolatos híradásokban – érthető módon – a nemzetbiztonsági, politikai jellegű akciók és események kapnak különös hangsúlyt.[19] Ugyanakkor, ha a bevezetőben említett, gyógyszeripai információszerző kiberakciókon elgondolkodunk, és szemügyre vesszük az (ismertté vált) ilyen incidensek folyamatosan bővülő listáját, akkor jól látható tendencia bontakozik ki a szemünk előtt.[20] Érzékelhetően növekszik a gazdasági jellegű kiberakciók mennyisége és az ilyen támadások intenzitása. A jelenség nagyobb időtávban szemlélve is ehhez hasonló képet mutat: gyors pillantást vetve például a CSIS vezető agytröszt fontosabb kiberakciókat rögzítő listájára, viszonylag nagy számban sorjáznak

[17] Meltzer 2019, 5.
[18] Meltzer 2019, 8.
[19] Hakmeh 2017.
[20] *Covid-19 Cybercrime Weekly Update* 2020.

rajta a gazdasági jellegű beavatkozások.[21] A témával kapcsolatban van olyan kutató, aki egyenesen a gazdasági kiberkémkedés aranykorát jósolja, illetve egyfajta aranylázhoz hasonlítja a virtuális terekben felerősödő, ipari-, pénzügyi-, gazdasági-, technológiai információszerző aktivitást.[22] A kiberkémkedéssel foglalkozó szakirodalom ezt a felfelé ívelő trendet egészen a hidegháború végéig vezeti vissza. Többről van szó véletlen egybeesésnél, hogy a geo-ökonómia, tehát a nemzetközi gazdasági kapcsolatok fegyverként való használatának koncepciója éppen akkor vert gyökeret, amikor a gazdasági előnyöket szem előtt tartó kibertevékenységek is sokasodni kezdtek.[23] Figyelemre méltó jelenség továbbá az is, hogy amíg korábban döntően állami szereplőkhöz kapcsolták a gazdasági jellegű kiber(kémkedési) akciók többségét[24], addig az utóbbi évtizedekben stabilan erősödik a nem-állami szereplőkhöz kapcsolható, gazdasági előnyszerzésért indított kiberhadműveletek aránya.

A fentiek fényében nem meglepő, hogy a kibertér vonatkozásában a „biztonság" és a „gazdaság" szféráinak egyre jobban kitapintható átlapolódásáról, összeolvadásáról beszélnek.[25] Összességében kijelenthető, hogy a kibertér egyre meghatározóbb szerepet játszik a nemzetközi kereskedelemben.[26] A kiberbiztonsággal kapcsolatos aggodalmak, beleértve a nemzeti és nemzetközi ellátási láncok épségével kapcsolatos kiberbiztonsági félelmeket is, arra sarkalják az államokat és a magánszféra szereplőit egyaránt, hogy hatékony lépéseket tegyenek a kibertér biztonságának megóvásáért. Egymást követően jelennek meg az újabb irányelvek és szabályozási keretrendszerek, amelyek gyors tempóban alakítják át a nemzetközi kereskedelmet. Újabb mechanizmusok és megállapodások formálódnak, amelyek a kibertér konfliktushelyzeteinek a feloldását célozzák, és hozzájárulnak a potenciális kiberbiztonsági fenyegetések csökkentéséhez. Érdemes itt kiemelni egy sajátos szegmenst, már csak azért is, mert a 2020-as év elejének globális egészségügyi krízise különösen ráirányította a témára a világközvélemény figyelmét. A globális pandémia, a koronavírus-járvány különös élességgel mutatta meg a globalizálódott gazdaság egyik legfontosabb tényezője, a globális ellátási láncolatok nagyfokú sérülékenységét. A kiberbiztonság és a kereskedelem összefüggéseit kutató szakemberek most különösen határozottan mutatnak rá a globális (és nemzeti) ellátási láncolatok kiberbiztonsági kérdéseinek fontosságára. Egyértelműnek látszik a konszenzus abban, hogy – ha az elkövetkező időszakban nem történik számottevő elmozdulás a kibertér-

[21] *Significant Cyber Incidents* 2020.

[22] D' Elia 2014, 243.

[23] Buchan 2019, 23.

[24] A teljességhez hozzátartozik az is: az 1990-es évektől felerősödő, állami szereplők által folytatott gazdasági célú kiberakciók egy jelentős részében is a magánszektor gazdasági szereplői lettek a megszerzett információk „kedvezményezettjei".

[25] A nemzetközi kereskedelem erőteljes „felköltözése" a kibertérbe a korszak egyik igazán jellemző vonásaként értékelhető. Nem véletlen, hogy az államok közötti kiberkonfliktusok egy nem jelentéktelen része már most is a globális kereskedelmi ügyletekhez és csatornákhoz kapcsolódik. *International Trade Regulation and Cybersecurity* é. n.

[26] Huang 2018, 45.

ben való viselkedés normarendszereinek kialakításában – az ennek nyomán sokasodó kiberkonfliktusok és kiberincidensek rendkívül károsan érintik majd a nemzetközi kereskedelem egészét.[27] A kiberdiplomatákon tehát ezen a rendkívüli fontosságú gazdasági területen is nagyon sok múlik majd.

A digitális gazdaság dilemmái

A kibervilág, különösen annak gazdasági dimenziója, ma még képlékeny és formálódó terület. Olyan térsége a nemzetközi kapcsolatoknak, ahol több fontos kérdésben ellentétes felfogások és érdekek feszülnek egymásnak. És a tét óriási. Sokszor ezek a viták elvi jelentőségűnek tűnnek, pedig a valóságban jól tapinthatóan ott húzódnak a pőre gazdasági célok és érdekek. Ezért is gondoljuk azt, hogy ezeket a témákat itt, a kibertér gazdasági viszonyainak ismertetésekor indokolt körbejárni. Két különböző probléma, két egymással ellenétes attitűd, magatartás, szabályozási törekvés érdemel ebben az összefüggésben említést, de közös bennük: a digitális gazdaság mindkét nagy kérdéscsoportja valójában az „adat" körül forog, az adatról szól.[28] Az ok végül is könnyen érthető: ebben a modern gazdaságban már nem a fizikailag létező javak, termékek előállítása, forgalmazása, szállítása, vásárlása és fogyasztása a meghatározó. A számítástechnikai rendszerek terjedésével óriási tömegű információ generálása, feldolgozása, tárolása, változatos célú továbbhasznosítása, a hálózatokon (elsősorban az Interneten) keresztüli továbbítása az, ami a gazdasági értékteremtő folyamatok központi mozzanatává válik. Az adat tehát az új erőforrás, ténylegesen egyfajta nyersanyag, ezért megszerzése, birtoklása, használata, feldolgozása hasonló kérdéseket vet fel, mint az ipari gazdaságok „hagyományos" nyersanyagainak esete. Az „adat" fogalmán itt általában különlegesen nagy adattömegeket értünk, ezek megjelölésére szolgál az úgynevezett „big data" fogalom.[29] Az adat különleges tulajdonságát, megváltozott gazdasági szerepét mutatja az is, hogy az illetéktelen eltulajdonítás (magyarul adatlopás) a kiberbűncselekmények egyik jellemző válfajává kezd válni.[30] Az adat tehát érték, és a roppant sok adat roppant nagy gazdasági értéket képvisel.

[27] Huang 2018. Az MI-technológiák alapvetően stratégiai jellegű orosz megítélésére és jelentőségére lásd még. Meyer 2017.

[28] Jacobson–Höhn –Kurbalija 218 kiváló, tömör áttekintését adja az adatok digitális gazdaságon belüli szerepének, és a felmerülő szabályozási kérdéseknek.

[29] Az IBM informatikai óriáscég becslése szerint világunkban naponta mintegy 2,5 exabit adat keletkezik, amit egy szám után álló 18 nullával lehet kifejezni. Ennek az óriási mennyiségű adatnak az „előállításában" persze nem kis szerepet játszik a társadalmakban élő (és egyre több IKT-eszközzel körülvett, azokat minden élethelyzetben használó) emberek sokasága.

[30] A tétek nagyságát mutatja az eddigi legnagyobb méretű adatlopás, amikor 2013-ban a Yahoo cég 3 milliárd felhasználójának személyes adatai (telefonszámoktól születési adatokon át rengeteg információ) kerültek illetéktelen adattolvajok kezébe. *Yahoo says all 3 billion accounts hacked in 2013 data theft* 2017.

Az Internet szabadsága és a kiberszuverenitás mint gazdasági szempont[31]

Az egyik legjobban exponált (és kétségtelenül a legnagyobb horderejű) dilemma így hangzik: „az Internet szabadsága", vagy a „kibertér szuverenitása". Melyik volna a kívánatosabb?[32] A probléma gyökere tulajdonképpen a kibertérnek, ennek a furcsa technológiai-társadalmi-politikai struktúrának a különlegességében gyökerezik. A fogalomhoz ugyanis, szinte születésétől fogva erősen kötődik annak „közlegelő" felfogása. Nagyon erős a vélekedés, hogy a kibervalóság egyfajta „digitális köztulajdon": olyan, mint az iparosodás előtti idők falusi társadalmainak közösen használt javai, az erdők, a halászó vizek, a legelők. Geopolitikai értelemben szemlélve olyasmi, mint a nyílt óceán vagy a világűr. Az Internet szabadsága, vagy más megfogalmazással a netsemlegesség mellett lándzsát törők ezt a felfogást képviselik, és a kibertér nemzetközi szabályozását, szabályozottságát (tehát korlátait) igyekeznek a lehető legcsekélyebb mértékűre szorítani.[33] Ezzel ellentétben azonban létezik egy másik felfogás, egy másik vízió arról, hogyan kellene kinéznie és működnie ennek az egyszerre virtuális és nagyon is kézzel fogható világnak. A „kibertér szuverenitása" mellé állók azt az elvet tartják követendőnek, hogy a térbeliség legfontosabb ismérvei, a korlátozottság, a határok éppen olyan fontos és természetes velejárói a hálózatos világnak, mint a másiknak, a „valóságosnak". Ennek a koncepciónak a hívei a kibertér alapos és aprólékos szabályozottságáért munkálkodnak a nemzetközi egyeztető fórumokon és formációkban is. A szakemberek úgy szoktak fogalmazni, hogy – nagy vonalakban persze – a liberális demokráciák képviselik a netsemlegesség elvét, és az autoriter rendszerű államok szorgalmazzák a szuverenitás elvének kiterjesztését a kibervalóságra is. Kétségtelen, hogy a formálódó multipoláris geopolitikai valóságban inkább a feltörekvő (erős regionális vagy globális pozícióra pályázó) országok ragaszkodnak a nemzeti szuverenitás elvének kiterjesztéséhez a digitális terekre is. Oroszország és Kína jellemzően e felfogás legfőbb szószólóinak számítanak, nem csupán elvben, de a nemzetközi kapcsolatok multilaterális fórumainak gyakorlatában is.[34] Természetesen az Internet erős szabályozásában, korlátokkal történő lehatárolásában felsejlenek a nyilvánvaló hatalmi-politikai szándékok is. Érdemes azonban emlékezni rá: a kiberszuverenitás (ahogy ellentétpárja a netsemlegesség is) legalább ennyire fontos gazdasági érdek.

A digitális gazdaság legfontosabb éltetője az adatok határokat átszelő, globális áramlása. Ennek az adatfolyamnak óriási a gazdasági, pénzügyi értéke: a McKinsey pénzügyi tanácsadó számításai szerint a digitális gazdaság értéke már jócskán meghaladja a külkereskedelmi forgalomba kerülő hagyományos javak által generált összegeket.[35]

[31] Riordan 2019 az Internetszabadság problematikájának legkitűnőbb bemutatását tartalmazza, miközben a kibertér diplomáciai napirendjének egyéb pontjait is példásan foglalja össze.

[32] Ayers 2016 jó összefoglalóját adja a kiberszuverenitás általános vetületeinek, hangsúlyosan a geopolitikai jellegre ügyelve.

[33] Sherman 2017.

[34] Shem 2016.

[35] DuPont 2020.

A növekedés ráadásul folytatódik, és ennél fogva a gazdaság új „olajának" tekintett adat-javak nemzetközi áramlásának szabályozása óriási gazdasági jelentőséggel bír. Az Egyesült Államok az elmúlt időszak nemzetközi kereskedelmi megállapodásai során a határokon átívelő szabad adatforgalom híveként kötelezte el magát. Amerika mind a csendes-óceáni úgynevezett TPP-egyezményben[36], mind az USA–Mexikó–Kanada közötti kereskedelmi keretmegállapodásban, mind pedig az USA és Japán közötti digitális kereskedelmi egyezményben ragaszkodott annak garantálásához, hogy az adatok szabadon áramolhassanak a határokon át, illetve hogy a helyi adatokat ne legyen kötelező helyi szervereken tárolni.[37]

Ezzel a megközelítéssel élesen szemben áll az Egyesült Államokkal egyre inkább minden fronton erőteljes rivalizálásba kezdő Kína álláspontja. A WTO-ban folyó digitális kereskedelempolitikai tárgyalásokon egyértelműen azt a szempontot igyekszik érvényesíteni, hogy az egyes államok korlátozhassák a határaikon átfolyó adatáramlást, megszűrhessék az internetes forgalmat, illetve jogukban álljon egyes külföldi digitális tartalmakat blokkolni államhatáraikon belül. Ez az egyes szakemberek megfogalmazásában „kiber vesztfáliai" álláspont[38] tükröződik a (Kínán belüli Internetet a külvilágról leválasztani képes) úgynevezett „Nagy Kínai Tűzfal" működtetésén, illetve a helyben keletkezett adatok helyi szervereken való tárolását előíró kínai jogszabályokban is. Hasonló pozíciót képvisel ebben a kérdésben Oroszország is: a globális Internetről leválaszthatóan működő saját hálózat fejlesztése és próbaüzeme (akárcsak az egyes helyi adatok helyi tárolását előíró törvényei) világosan utalnak a kiberszuverenista álláspont melletti elkötelezettségére.[39] A nemzetközi viszonyok fokozatos átrendeződésének egyik jeleként az elmúlt évben több ország (Irán, Vietnám, Kazahsztán, Indonézia) is felzárkózott az ENSZ-ben a kínai és orosz kiberszuverenista javaslatok mögé, miközben más országok is (például a korábban a szabad adatáramlás mellett elkötelezett Japán, vagy különösen India) keresik a módozatait az adatfolyamok hatékony igazgatására, kontrolálására.[40]

[36] Hivatalos nevén Transz-csendes-óceáni Partnerség, angolul Trans-Pacific Partnership.

[37] DuPont 2020. Figyelemre méltó, jelzés erejű mozzanat, hogy a nemzetközi kereskedelempolitikában a korábbi liberális felfogással sok szempontból szakító Trump-kormány alatt sem változott az USA Internetszabadságra (az adatok szabad áramlására) vonatkozó prioritása. Ezt az álláspontot Amerika következetesen érvényesíti továbbra is, például a Világkereskedelmi Szervezetben (WTO) folyó multilaterális tárgyalásokon.

[38] Demchak–Dombrowski 2014 A „Vesztfália" szó (ami néha az angolszász írásmód hatását tükröző Wesztfália formában is előfordul) gyökere a 17. század nagy európai békekonstrukciójáig nyúlik vissza. A harmincéves háborút lezáró nemzetközi szerződés teremtette meg a nemzetközi kapcsolatok modern szuverenitás-fogalmát. Manapság az erős nemzetállami lét elsőségét hangsúlyozó külpolitikai-hatalmi felfogás elnevezésére használatos a vesztfáliai jelző.

[39] Sherman 2019.

[40] Sherman 2019. A téma európai uniós megközelítéséhez, és így a formálódó multipoláris rend egyik potenciális pillérének álláspontjához, érdemes kézbe venni: Dee 2015. Ugyanakkor megkerülhetetlenül fontos ebben a témában is Riordan 2019. Fontos észrevételeket tartalmaz az európai erőközpontok (EU) pozíciójáról a befolyásos kutatóműhely, az European Council on Foreign Relations projektje. Scesanto 2017.

Nyílt adatok és adatvédelem: az adatgazdaság alapjai[41]

Az újgazdaságot éltető virtuális nyersanyag, az adat egy másik (bár az előző polémiához természetesen több szálon is kapcsolódó) összefüggésben is vitákat, egymással ellentétes koncepciókat, sőt filozófiákat generál a 21. századi kibergazdaságban. Ezt a dilemmát úgy lehetne megfogalmazni: az adatok nyíltsága, transzparenciája a fontosabb, vagy inkább az adatok (különösen a személyes adatok) védelme legyen-e a digitális gazdaság vezérlőelve? A digitális gazdaságban működő cégek folyamatosan „vadásznak" az újabb és újabb adattömegekre. Különösen érvényes ez (mint később még látni fogjuk) a mesterséges intelligencia fejlesztésekre, alkalmazásokra épülő új iparágakban, amelyek az adattömegek nélkül gyakorlatilag nem is létezhetnek.

Nyílt adatnak azokat nevezhetjük, amelyek szabadon, megkötések nélkül és bárki számára hozzáférhetőek („elvihetők", felhasználhatók, továbbadhatók), és mint ilyenek gazdasági értékteremtés céljára (magyarul üzleti célokra) is felhasználhatók.[42] Fontos azt is látni: ahhoz, hogy az adat nyílt legyen, tehát – nemcsak elvben, de ténylegesen is – szabadon hozzáférhető és felhasználható legyen, ahhoz megfelelő formátumban és adatstruktúrában kell lennie. A nyílt adatokat (azok körét, felhasználhatóságát) általában jogszabály írja körül, és jellemző módon a közszférában keletkező (illetve a közszféra szervezetei és intézményei által birtokolt, tárolt, használt) adatokat öleli fel.[43] A nyílt adatok körébe tartoznak például az időjárási adatok, a kataszteri (ingatlanügyi) információk, műholdas felvételek, közműtérképek. Ezek használata a gazdasági élet szereplőinek döntési tevékenységét segítheti. Természetesen az adatok újrahasznosításában (továbbadásában) is jelentős gazdasági értékteremtési potenciál rejlik.[44]

Az adatok szabad, korlátok nélküli felhasználásához fűződő, erős gazdasági érdekkel szemben áll ugyanakkor egy másik érdek is, amely az adatok védettségét, hozzáférhetőségének, mások által történő felhasználhatóságának erős korlátokat szabna. Ez az adatvédelem elsősorban a személyes adatok körét érinti. Az adatok védelmét szintén jogszabály rögzíti, és fontos megjegyezni, hogy ezen a téren az Európai Unió különösen élen jár (a mára közismertté váló, széles körben alkalmazott GDPR-sza-

[41] A rendkívül fontos kiberszabályozási témakör korszerű összefoglalóját mutatja be Vicente–Casimiro 2020.

[42] Charalabidis 2018 a téma jó átfogó ismertetését adja, beleértve a nyílt közadatok kérdéskörét is. Custers 2019 viszont az érem másik oldalát, az adatvédelem koncepcióját járja körül, különös tekintettel az EU gyakorlatára.

[43] *Open Government Data Report* 2018.

[44] A McKinsey pénzügyi tanácsadó cég tanulmányának becslése szerint a kormányok által szabadon hozzáférhetővé tett, nyílt adatkészletek éves szinten és globálisan mintegy 3 billió dollárnyi új értéket teremthetnek a gazdaság néhány kulcsszektorában, elsősorban az oktatásban, a közlekedésben és az egészségügyben. *Open data: Unlocking innovation and performance with liquid information. McKinsey Global Institute Report* 2013.

bályozás kidolgozásával).[45] Az adatvédelmi jogszabályok rögzítik azokat az elveket és körülményeket, feltételeket, amelyeket az adatok begyűjtőinek, tárolóinak és felhasználóinak szem előtt kell tartaniuk.[46]

Látható tendenciaként jelentkezik, hogy a mesterségesintelligencia-technológiák széleskörű elterjedésével (például az arcfelismerő vagy más bionikus azonosító rendszerek tömeges alkalmazásával) az adatvédelem kérdése a korábbinál is hangsúlyosabbá válik. Üzleti, biztonsági szempontok és elvek ütköznek itt etikai, személyiségi jogi kívánalmakkal.

Államok és magánszereplők (governance-modellek)

A nemzetközi kiberbiztonsági rendszer, ahogy egyébként maga az egész digitális ökoszisztéma, a kibertér geopolitikai és geo-ökonómiai rendszere is képlékeny, alakulóban levő formáció. Szabályozó és működtető elveinek, normarendszerének kimunkálásánál (ahogy azt az előző két alfejezetben jól láthattuk) jelentősen eltérő szemléletek, különböző érdekek, egymásnak ellentmondó törekvések munkálkodnak. A kiberteret szabályozó és irányító elképzelésekben is két jelentős megközelítés tapintható. Az egyik a kibertér „kormányzását" alapvetően a szuverén államok hatáskörébe utalná, és döntően a nemzetközi jog már létező szabályrendszereit igazítaná az új geopolitika, geo-ökonómiai térrendszer megváltozott valóságához és alkalmazná a digitáliák világában is.[47] Illetve létezik egy másik felfogás, amelyik a magángazdaság szereplőit, elsősorban a nagy internetes cégeket, technológiai globális vállalatokat is bevonná a normatív szabályozásba, a digitális geo-ökonómiai komplexum igazgatásába. Az előbbi álláspont legfajsúlyosabb szószólója a nemzetközi porondon az Egyesült Államok, amely globálisan (és önkéntesen) elfogadott normarendszerrel biztosítaná a kibertér szabályozott működését, és amely a kibertérség irányításába bevonná a magángazdaság meghatározó szereplőit is. A másik elképzelést elsősorban Oroszország és Kína képviseli a vitákban, amelyek multilaterális szerződésrendszerrel, és így értelemszerűen csak szuverén szereplők (államok) által kormányozva garantálnák a kibervilág biztonságát, kiszámítható működtetését.[48]

[45] Az Általános Adatvédelmi Szabályozás (General Data Protection Regulation) 2018-ban lépett életbe az EU tagállamaiban. Normatív szerepét jól mutatja, hogy az Unión kívüli gazdasági szereplők is csatlakoztak az alkalmazásához. A GDPR jelentős előrelépést jelentett az adatok védelme terén az EU korábbi, 1998-ban életbe léptetett adatvédelmi szabályzatához képest.

[46] Jellemzően például az adatok begyűjtőinek felelősnek (elszámoltathatónak) kell lennie az adatok „tulajdonosaival" szemben. Az adatok begyűjtése csakis jogszerűen történhet. A begyűjtött adatok köre nem lehet korlátlan, csak indokolt adatkörre és adatmennyiségre vonatkozhat. Az adatok tárolása is csak jogszabályban meghatározott, korlátozott időtartamig lehetséges. A begyűjtött adatok tárolása és felhasználása biztonságos körülmények között kell, hogy történjék.

[47] Stadnik 2017, 146. és Jaywardane 2015, 5.

[48] Stadnik 2017, 134.

Érdemes egy további pillantást vetnünk arra a megközelítésre, illetve törekvésre, amely a kibertér nemzetközi szabályrendszerének kimunkálásába kezdettől bevonná a magáncégek képviselőit is. Furcsának tűnhet, de ezt a gondolatot mindkét részről (nagyvállalati oldalról, illetve a szuverén állami aktorok térfeléről is) jelentős erők támogatják. Láttuk egy kicsit feljebb, hogy a technológiai cégek milyen óriási értékteremtő potenciállal rendelkeznek. A méretek összehasonlító érzékeltetésére érdemes rámutatni: a nagy internetes platformüzemeltető globális vállalatokat tömörítő cégcsoport együttes értéke mintegy 7 billió dollárra rúg, ami jelentősen meghaladja a világ bármely országának a GDP-jét, kivéve természetesen az USA-t és a Kínai Népköztársaságot.[49] A Rettegett Ötöknek is nevezett óriásvállalati kör teljesítményadatai egyenként is több, mint imponálóak: az élen természetesen a Microsoft áll az 1000 milliárd dollárt éppen meghaladó piaci kapitalizációs[50] értékkel, de nem sokkal marad el tőle az Amazon (888 milliárd dollár), az Apple (875 milliárd), a Google (741 milliárd) és a Facebook (496 milliárd dollár) piaci értéke.[51] A nemzetközi erőviszonyok további érzékeltetésére egyébként azt sem haszontalan megjegyezni: az első tíz ilyen technológiai óriásvállalat között két kínai található, a boly alsó végében.[52] Az ebben a roppant gazdasági erőben rejlő hatalmi realitás sok állam képviselői számára is azt diktálja, hogy célszerűbb ezeket a gigantikus szereplőket bevonni a játékszabályok kialakításába, a békés ügymenet fenntartásába. Ennek a felismerésnek válfajaként jelent meg a nemzetközi kiberdiplomáciai porondon egy merőben új tisztség és munkakör: a technonagykövet szerepköre. Első képviselője Casper Klynge, hivatásos dán diplomata lett, aki országát szabályos nagyköveti meghatalmazással képviselte az USA-ban és Kínában is.[53] Azonban nem az említett országokhoz akkreditálva kezdte meg munkáját, hanem a világ vezető technológiai cégeihez „delegálva". Elsőként ennek megfelelően az amerikai Szilícium-völgyben épített ki képviseletet 2017-ben, majd hamarosan Pekingben is megnyitotta regionális irodáját Dánia technonagykövete.[54] Működésének deklarált célja az, hogy a (digitalizációban egyébként korántsem lebecsülendő teljesítményt mutató) skandináv ország közvetlen párbeszédet kezdhessen az Internetgazdaság meghatározó szereplőivel, méghozzá éppen a nemzetközi szabályozási keretrendszer előmozdítására. Az állam–cég közvetlen együttműködés kiemelt tématerületei egyébként a kiberbiztonság, illetve a digitális gazdaság etikai kérdései is. A várakozás az, hogy ilyen új formájú „népi diplomáciai" szintek kiépítésével Dánia a technológiai fejlesztések élvonalába kerülhessen.

[49] *Data Governance. Part I. Emerging Data Governance Practices* 2020.

[50] Egy vállalat piaci kapitalizációja olyan *pillanatnyi* piaci értékösszeget mutat, amelyet a piac (a befektetők) az adott időpontban a cégnek tulajdonít. Lényegében a vállalat részvényei számának, és azok pillanatnyi piaci árfolyamának (ez folyamatosan változhat!) a szorzatával adható meg.

[51] Dominioni 2019.

[52] Dominioni 2019. A vezető technológiai nagyhatalmak között találjuk 402 milliárd dolláros piaci kapitalizációval a kínai Alibaba céget, illetve a szintén kínai Tencentet, 398 milliárd dollárral.

[53] Rohaidi 2017.

[54] *The World"s First Ambassador to the Tech Industry* 2019.

Mesterséges intelligencia: biztonság és gazdaság újraértelmezése a kibertérben

„Aki a Mesterséges Intelligencia kutatásokban az élre kerül – az uralja majd az egész világot." Vlagyimir Putyin orosz elnök két éve elhangzott idézetét nyugodt szívvel választhattuk volna jelen tanulmány mottójának.[55] Az innovációkutatók a nagy társadalmi átalakítások motorjaként úgynevezett „általános célú technológiákat" (GPT) azonosítanak, amit persze talán pontosabb volna „átfogó hatókörűnek" neveznünk. Ezek azok a technológiai újítások, amelyek (az általuk generált további rész-innovációk sorával együtt) meghatározó változásokat idéznek elő a köznapi emberi életben és az üzleti-termelői világban egyaránt.[56] Ebben a körben, az elmúlt kétszáz év nagy technológiai változtatásai négy egymást követő hullámban érkeztek: elsőnek a gőzgép, majd az elektromosság, illetve az informatika. A negyedik hullám hátán most érkezik éppen a mesterséges intelligencia.

Az innovációban rejlő geopolitikai és geo-ökonómiai[57] potenciál – amelynek érzékeltetésére a híres amerikai politikus és geopolitikai gondolkodó, Brzezinski sakktábla-metaforáját[58] emeltük ide – természetesen nem csupán az orosz vezető számára nyilvánvaló. Igazi technológiai versenyfutásnak lehetünk tanúi, amelyben egyébként Oroszország, szakértők véleménye szerint, a vezető helyről aligha álmodhat komolyan. A legesélyesebb versenyzőnek most többnyire Kínát tekintik: a 2015-ben bejelentett Made in China program 1,36 billió dolláros fejlesztési forrásai, amelynek zöme MI-kutatásokra és fejlesztésekre irányul majd, nagyságrenddel haladják meg a többi versenyző állam célzott fejlesztési befektetéseit. Ugyanakkor sokat számíthat a vetélkedésben az USA vállalkozás- és innovációbarátabb környezete, vagy az EU perspektívikusabb jogi szabályozó közegei. És a pénzügyi erőben tetten érhető hátrányos helyzet ellenére komoly versenyben van még az MI-forradalom kibontakoztatásában Japán, Nagy-Britannia, Franciaország, Németország, továbbá a már említett Oroszország és Kanada.

A verseny tehát éles, a tempó – ebben mindenki egyetért – exponenciálisan növekvő. Az elkövetkező évtized várhatóan döntő lesz ebben az új technológiai forradalomban. És ha igaz az, hogy a kibertér a geopolitikai érdekérvényesítés új, sőt meghatározó dimenziója, az egymással szemben nemzeti érdekeik érvényesítéséért küzdő szereplők 21. századi sakktáblája, akkor ezen a véresen komoly játékmezőn a mesterséges intelligencia lesz a legfontosabb bábu, a kibersakkjátszmák királynője.

A digitális diplomácia, a kiberdiplomácia szakértői nagyjából egyetértenek abban, hogy a mesterséges intelligencia két alapvető – és egymástól eltérő – módon kapcsolódhat, kapcsolódik a külügyi igazgatási struktúrák és különösen a diplomáciai

[55] Meyer 2017.

[56] Gill 2020.

[57] Filippov 2019 kitűnő, friss összegzése a digitális gazdaság problématerületeinek. Hangsúlyosan jelennek meg nála a mesterséges intelligencia alkalmazások nyomán támadó kibergeopolitikai és kiberbiztonsági kérdések is.

[58] Brzezinski 1999.

szervezetek működéséhez.[59] Érdemes felidézni, hogy hasonló a helyzet az átfogóbb „digitalizáció" fogalom és a külügyek, illetve diplomácia kapcsolódási lehetőségeinél. A digitalizáció egyfelől tématerülete lehet a diplomáciának: ezt, az online terek, működések és szereplők szabályozásával kapcsolatos diplomáciai, államközi tevékenységet nevezzük mi „kiberdiplomáciának". Másfelől a digitalizáció új eszközöket biztosíthat a nemzeti külpolitikai érdekek érvényesítéséért felelős diplomáciai szervezetek hatékony és korszerű működéséhez. Ezt a technologizált eszközparkot és működést nevezzük „digitális diplomáciának". Hasonló kettősséget találunk a digitalizáció szélesebb témakörén belüli, meghatározó technológiai fejlesztések, a mesterséges intelligencia külügyi kapcsolódásainak esetében is.

Mesterséges intelligencia: fogalmi alapok

Elsőként is fontos leszögezni, hogy a „mesterséges intelligencia" nem egyetlen technológiát jelöl, hanem sokkal inkább a komputertudomány egy jellemzően interdiszciplináris kutatási területét, illetve az ezekhez kapcsolódóan fejlesztett technológiákat és alkalmazásokat. Az MI fókuszában az emberre jellemző intelligens tevékenységek (folyamatok) számítógépes rendszerek általi szimulációját értjük.[60] E tevékenységek felölelik mindenekelőtt az emberi tanulás képességét (tehát információk és az információk használatához szükséges szabályok megszerzésének képességét); felölelik továbbá az emberi érvelés képességét (tehát azt, hogy a szabályokra támaszkodva következtetéseket tud levonni); és különösen fontos képességként ölelik fel az önkorrekció képességét.

Érdemes kiemelni azt is: a mesterséges intelligencia szorosan kapcsolódik a big data fogalmához. A big data nagymennyiségű, rendkívüli változatosságú/összetettségű és gyorsan változó adattömeget takar. Ezek az adattömegek a hagyományos eszközökkel (például adatbázis-kezelőkkel) nem kezelhetők már. Feldolgozásukhoz éppen az MI-technológiák nyújtanak segítséget. Ugyanakkor elmondható az is: az MI egyik fontos technológiáját jelentő gépi tanulási eljárások nem képzelhetők el olyan (számottevő, többnyire a big data fogalomkörébe sorolható) adattömeg nélkül, amely az algoritmusok tréningezésére szolgál.

Fontos megemlíteni a mesterségesintelligencia-technológiák klasszifikációját, azaz főbb csoportjait vagy alosztályait. A diplomácia működési területén jelenleg alkalmazott okosmegoldások kapcsán szokás néha megemlíteni, hogy azok még aligha tekinthetők „igazi" mesterségesintelligencia-technológiáknak; valójában csak azokhoz hasonló, ám

[59] A fogalmi rendszer olyan kulcselemeinek, mint a „digitális diplomácia", illetve a „kiberdiplomácia" tisztázásához, illetve az átfogó digitális diplomáciai keretrendszer elemeivel kapcsolatos különbségtételekhez vö. Nyáry 2019.

[60] A mesterséges intelligencia áttekintéséhez jó kiindulás pontot ad a téma egyik legkiválóbb magyar kutatójának kötete: Futó 1999. A mérnöki-informatikusi előképzettséggel nem rendelkező humán szakembereknek, olvasóknak különösen nagy segítség jelenthet egy friss angol nyelvű monográfia: Taulli 2019.

valójában inkább csak „pszeudó-MI”-technológiáknak nevezhetjük azokat.[61] Ez az óvatos megközelítés annak a tényleges jelenségnek egyfajta ellenhatása, amely a modern korban (különösen a nem szakmai közbeszédben), alapvetően divatmegfontolásból használ megalapozatlan fogalmakat.

Ténylegesen az MI-technológiákat szokás úgynevezett általános képességű mesterséges intelligencia, más néven „erős MI” kategóriába, illetve szűk alkalmazási képességű mesterséges intelligencia, más megnevezéssel „gyenge MI” kategóriába sorolni. A „gyenge MI” lényegében egyetlen célfeladat elvégzésére tervezett és betanított MI-technológiát takar. Jellemző példája a közönségkapcsolati rendszerekben alkalmazott beszélgetőrobot. Természetesen igaz, hogy ma még a diplomáciai feladatkörökben is többnyire ilyen MI-alkalmazásokat találunk. Akad azonban – igaz, egyelőre kísérleti jelleggel – példa az „erős MI” külügyi célú alkalmazására is: a lejjebb felvillantott esettanulmányoknál több példát is bemutatunk majd rá. Ezeknél a technológiáknál részben vagy egészben sikerül immár szimulálni az általános hatókörű emberi kognitív képességeket (tehát például egy addig ismeretlen feladat eredményes megoldásához szükséges „intelligenciát”).

Az MI a diplomáciai szervezetek eszköztárában[62]

A bevezető részekben szó volt a geopolitikát várhatóan átformáló fejleményekről. Ugyanakkor a mesterségesintelligencia-technológiák nem csupán a nemzetközi kapcsolatok környezetét, az államok közötti vetélkedés geopolitikai sakktábláját rajzolhatják át teljesen, de az államközi érdekérvényesítés békés intézményrendszerének tekinthető diplomácia eszköztárát is. Az adatok már ma is a diplomáciai háttérműveletek éltető alapanyagát szolgáltatják. A big datára alapozott eszközök, részben már MI-alkalmazások a digitális diplomácia eszközrendszerének gerincét képezik ma is az információgyűjtéstől és feldolgozástól kezdve, a szoftverrel támogatott külügyi döntéshozatalig sok területen. És a nyersanyag, az adat szédítő tempóban növekszik tovább, a nap minden percében. Ami – ha figyelembe vesszük, hogy egyetlen év alatt mintegy 370 millióval nőtt az internethasználók száma – nem is meglepő. A mesterséges intelligencia tehát egyfelől eszközként kapcsolódik a külügyi szervezetekhez, mindenekelőtt (de, mint az esettanulmányokból látni fogjuk, nem kizárólagosan) a politika végrehajtásáért felelős diplomáciai szervezetekhez és működésekhez.[63]

A tájékozódás és tájékoztatás a diplomáciai munka alapvető funkciója volt és maradt. Jelentősége mindkét irányú információáramoltatásnak növekedett, noha természetesen – a közösségi platformokon zajló közdiplomácia népszerűségének szárnyalásá-

[61] Nyáry 2020.

[62] *Mapping the challenges and opportunities of artificial intelligence for the conduct of diplomacy* 2019.

[63] A mesterséges intelligencia külügyi, diplomáciai alkalmazásaiban rejlő lehetőségeket és kihívásokat a digitális diplomácia egyik legfigyelemreméltóbb európai kutatóműhelye, a genfi székhelyű DiploFoundation tanulmányozza önálló programként immár két éve. *Mapping the challenges and opportunities of artificial intelligence for the conduct of diplomacy* 2019.

val – elsősorban a tájékoztatás jut róla az eszünkbe. Az MI-projektek jó része ugyanakkor a diplomáciai információszerző, rendszerező, elemző, prezentáló munkát igyekszik új minőségi szintre emelni. Közben a tájékoztatáshoz kapcsolódóan is egyre több az MI-kezdeményezés, elsősorban az álhírprobléma kezelésére.[64]

Az adattudomány, a mesterséges intelligencia, a különféle modellezések alkalmazásának érdekes példáját adja a brit külügyi szervezet fejlesztése. Az általuk kialakított MI-alapú informatikai eszközrendszer több százezer, különböző nyelvű információs forrást képes automatikusan figyelni, angolra fordítani és valós időben megjeleníteni egy központi felhasználói felületen. Korábban a diplomatáknak rengeteg időt kellett fordítaniuk a helyi hírforrások olvasására. Most az így szerzett információkat az online források tömegéből beszerezhető értesülésekkel lehet számottevően kiegészíteni. A „gyorsreagálású" külügyi csoportok (például válságok idején) rövid határidő alatt készülhetnek fel olyan információtömegből, amelynek megszerzésére korábban egyszerűen nem volt lehetőség. Az adatok hasznosulásához azonban nélkülözhetetlen az is, hogy azokat a maguk „emberi kontextusába" helyezzék. Ezért foglalkoztatnak viselkedéstudományban járatos szakembereket is. Az ő feladatuk, hogy felfedezzék az adatokból kirajzolódó tendenciákat, rámutassanak a mögöttük megbúvó emberi viselkedésekre. A csoport egyik fontos profilja ugyanis az „extrém megnyilvánulások" figyelése.[65]

A konzuli feladatok, a külügyi szervezet par excellence igazgatási típusú feladatai zömében nem egyedi, típusproblémák kezelését igénylik, viszont sokszor rövid határidővel, és néha jelentős távolságokból is. A konzuli ügyintézés éppen ezért ideális terepet kínál az egyszerű „gyenge MI"-technológiák alkalmazására, a hatékonyság számottevő növelése érdekében. A legjellemzőbb és ma már széles körben elterjedt ilyen MI-technológiákra támaszkodó alkalmazások a konzuli tevékenységhez kapcsolódó chatbotok. A konzuli beszélgető robotok elsősorban utazással kapcsolatban segítik az ügyfelet, másrészt a tipikus külföldön előforduló vészhelyzetekkel kapcsolatban biztosítanak gyors, hatékony tájékoztatást – ráadásul a nap minden szakában.[66]

A diplomáciai szervezetek működésének – ahogy a diplomata munkának is – máig egyik legfontosabb, meghatározó feladata, funkciója maradt a nemzetközi (két- vagy többoldalú) tárgyalások folytatása. E már-már művészetnek számító munkafolyamat technológiai támogatására fejlesztették ki a „Debatör" projektet, amelynek algoritmusa beszélgető interfészen keresztül vitába képes szállni emberi partnerekkel. A fejlesztés mögött álló izraeli külügyi szakemberek a diplomácia máig legfontosabb funkciója, a tárgyalások támogatásának új eszközét remélik ettől a speciális MI-fejlesztéstől.[67]

A kereskedelmi attaséi hálózatokkal, illetve a külképviseletektől sokszor elkülönülve működő, de azok általános irányítása alatt maradó kereskedelmi képviseletekkel

[64] A tájékoztatási funkcióhoz kapcsolódó MI-alapú alkalmazásra példának lásd a Brit Külügyminisztérium Nyílt Forrású Osztályát (OUSU). Hasonlóan jó bepillantást enged a legújabb adatalapú külügyi fejlesztések irányába a Svéd Intézet közösségi média hírszerző funkciója.

[65] Nyáry 2019, 11., továbbá *Exclusive: Meet the UK's „Data Diplomat"* (é. n.).

[66] Nyáry 2020, 9.

[67] Nyáry 2019, 12., továbbá *Inside Project Debater Speech by Crowd* (é. n.).

kapcsolatos megnövekedett elvárásoknak azonban az emberi és tárgyi erőforrásokban többnyire szűkölködő szervezetek mind nehezebben képesek megfelelni. Nem véletlen, hogy a diplomáciai tevékenység ezen speciális szekciójában is nagy reményeket fűznek az IKT-technológiák, és specifikusan az MI-fejlesztésekben rejlő „erősokszorozó" lehetőségekhez. Erre példa a Portugál Külügyminisztérium égisze alatt kifejlesztett „Portugal Exporta" portál, számos MI-vel támogatott funkcióval segítve az ország külkereskedelmét.[68]

Utoljára hagytuk az MI-technológiákra támaszkodó „diplomáciai" fejlesztések legérdekesebbikét. Merthogy nem a külpolitika végrehajtásáért felelős diplomáciához (tehát a taktikai szinthez) kapcsolódik, hanem magához a nemzeti külpolitika formáláshoz, a külügyi stratégiaalkotáshoz. A Kínai Tudományos Akadémia által fejlesztett, MI-alapú külpolitikai döntéstámogató rendszer korai változatát már használja is a feltörekvő ázsiai nagyhatalom külügyi apparátusa. A szoftver óriási adattömeget elemez, a diplomáciai koktélpartik pletykáitól a nemzetbiztonsági stratégiákig. Ha a külpolitika alakítói egy komplex helyzeten belüli konkrét külkapcsolati cél eléréséhez szükséges döntéseket latolgatják, akkor a szoftver villámgyorsan több, nagyon pontos döntési alternatívát rajzol fel nekik.[69]

Kiberdiplomácia az MI nemzetközi szabályozásában

A mesterséges intelligencia ugyanakkor a diplomáciai tevékenységek új tématerületeként is jelentkezik. Azaz: nemcsak a mesterségesintelligencia-technológia segíti a diplomácia működését, de a diplomácia is támogatja működésével a mesterséges intelligencia térhódítását. Láttuk, hogy ennek az új technológiának mekkora jelentőséget tulajdonítanak a modern geopolitikai kapcsolatrendszerekben. Nem meglepő, hogy a mesterséges intelligencia, annak technológiai, alkalmazási, személyes adatvédelmi, sőt etikai vonatkozásai erősen foglalkoztatják a nemzetközi közvéleményt. Ebből következően az ezeknek a – sok szempontból újszerű, analógiák és megszokott fogódzkodók nélküli – helyzeteknek a kezelésére szolgáló nemzetközi szabályozások kidolgozására növekszik az igény.[70] Már most látható, hogy az MI-tématerület a diplomácia, és ezen belül is az úgynevezett multilaterális kapcsolatok egyik legfontosabbjaként kezd szerepelni. Ezen a területen különösen aktív az Európai Unió, de az ENSZ is fontos kezdeményezésekkel, célzott munkacsoportokkal és más nemzetközi fórumokkal törekszik e nagyhatású geopolitikai vonatkozású technológia nemzetközi szabályrendszerének kidolgozására.

A mesterségesintelligencia-kutatások, fejlesztések és alkalmazások körülményeinek átfogó szabályozása minden kétséget kizárólag ma az egyik legégetőbb feladat. A technológiában rejlő elképesztő potenciálok, és így a várható fejlődés üteme és kiterjedése

[68] Nyáry 2020, 37.
[69] Nyáry 2020, 37.
[70] Az MI-problematika nemzetközi szabályozásával kapcsolatos törekvések egyik legkitűnőbb összefoglalója: Rugge 2019.

nélkülözhetetlenné teszi a szabályrendszerek kidolgozását. Éppen ezért az elkövetkező időszakban vélhetően ez a tématerület áll majd a kiberdiplomaták figyelmének fókuszában. Ugyanakkor a mesterséges intelligencia szabályozására, illetve a kapcsolódó szakpolitikákra vonatkozó nemzetközi jogi környezet még maga is csupán kialakulóban van.

Az MI-szabályozás részben a technikai, részben a gazdasági, részben pedig a társadalmi alkalmazási (etikai) aspektusokra fókuszál. Maga a jogi szabálykörnyezet kialakítása jelenleg az alábbi fő témákkal foglalkozik elsősorban: autonóm intelligens rendszerek, az MI-rendszerek felelőssége és számon kérhetősége, valamint a személyiségi jogi és biztonságossági kérdések.[71] A szabályozás nemzetközi kereteinek megteremtése a 2010-es évtized második felétől került a multilaterális fórumok érdeklődési körébe. 2018-ban közös kanadai–francia kezdeményezésre merült fel az elképzelés, hogy (a klímaváltozással foglalkozó nemzetközi panel példájára) a G7-es csoport égisze alatt induljon el egy Mesterséges Intelligencia Nemzetközi Panel az új technológiai fejlesztési terület lehetséges globális kihatásainak tanulmányozására. 2019 tavaszán elfogadták az OECD *Mesterséges Intelligencia Ajánlásait*, majd néhány hónapra rá a G20-as csoport *Mesterséges Intelligencia Alapelvet*. Még szintén 2019-ben a Világgazdasági Fórum is kibocsátott egy útmutatót a kormányzati MI-beszerzések támogatására.[72]

A világ vezető multilaterális tömörüléseihez hasonlóan az EU is a mesterségesintelligencia-szabályozás előmozdítása mellett kötelezte el magát az évtized utolsó éveiben. 2018 nyarán a Bizottság független Magas szintű Szakértői Csoportot állított fel a mesterséges intelligencia kérdéseinek – elsősorban a technológia megbízhatóságának – tanulmányozására.[73] Az MI-szabályozás témájában mérföldkőnek tekinthető 2020 februárja, amikor az EU Bizottság publikálta a *Mesterséges Intelligencia Fehérkönyvét*.[74] A dokumentum azonosította a mesterséges intelligencia fejlesztések és alkalmazások kapcsán felmerülő legfontosabb kockázati tényezőket: az alapvető jogok sérülhetősége, az adatokhoz fűződő személyiségi jogok sérülhetősége, a biztonsággal és a hatékony működéssel kapcsolatos problémák, valamint a felelősségre vonhatóság kérdése. A Bizottság úgy határozott, hogy a fejlesztéseknek ebben a relatíve korai fázisában nem bocsát még ki részletes szabályozást a témában, hanem csupán felvázolt egy jogi követelményrendszert, amely értelmében minden jövőbeli keretszabályozásnak garantálnia kell az MI-rendszerek megbízhatóságát, illetve azt, hogy tiszteletben tartják az Európai Unió alapvető elveit és értékeit. A követelményrendszer kitér arra is, hogy a hatályos EU jog alkalmazandó – technikai tisztázásokat követően – az MI-kérdésekre is.

[71] Wheeler 2019.

[72] *France and Canada create new expert International Panel on Artificial Intelligence* (2018) és *OECD Principles on AI* (2019), valamint *G20 human-centered AI Principles* (2019), továbbá *World Economic Forum AI Government Procurement Guidelines* (2019).

[73] Findlay 2020.

[74] *White Paper on Artificial Intelligence. A European approach to excellence and trust* 2020.

Kitekintés

A kibertér geo-ökonómiáját, kiberdiplomáciai témáit és kihívásait és szabályozási törekvéseit bemutatni szándékozó áttekintésünket a nemzetközi szabályozási törekvések ellentmondásaival és ellentéteivel, majd a digitális gazdaságot a várakozások szerint gyökerestül felforgatni készülő mesterséges intelligencia témáival zártuk. Nem haszontalan, ha most zárszóként egy pillanatra mondandónk első részeihez kanyarodunk vissza, oda, ahol az újra megjelenő, majd mind jobban élesedő geo-ökonómiai szembenállások rendszeréről szóltunk. Esetleg azért is, hogy a két végpontot most mintegy egybeöltsük. A kibertér egyre inkább a hatalom meghatározó dimenziója.[75] És, ha lettek volna illúzióink, akkor most már kristálytisztán láthatjuk: a gazdaság (a termeléssel és ellátási láncokkal, nemzetközi kereskedelemmel és technológiával) jórészt nemzetbiztonság is – hatalom. Kibertér és digitális gazdaság: egymásba fonódó hatalmi dimenziók tehát. Az egyik jeles kiberszakmai szervezet, az Internet Governance közelmúltban megjelent írása arra figyelmeztet: az Egyesült Államok és Kína között a tavalyi évben elmélyülő, majd mostanra végképp elmérgesedő kereskedelmi háború ma már egyértelműen technológiai konfrontációt takar. A tét nem egy-egy jól jövedelmező fejlesztés vagy versenyelőny, hanem a globális hegemóniában kulcsszerepet kapó kibertér, a geopolitika 5. dimenziójának uralása. Azé a közegé, ahol hamarosan a mesterséges intelligenciával támogatott rendszerekre támaszkodva igyekszik majd operálni a támadó és a védekező fél egyaránt. Sokan úgy tartják: ez (is) egy olyan terület, ahol a rendet, biztonságot megőrizni akarók vannak hátrányban. A gépi tanulás ugyanis ma már olyan gyorsan képes megkerülni, lebontani a kibervédelmi rendszereket, amellyel a szokványos védelmi eszközök nem tudnak lépést tartani. A gépi tanulást persze a kibervédelemért felelős szakemberek is csatasorba állítják. Az MI segítségével a fenyegetést jelentő online viselkedési mintákat igyekeznek felderíteni. És, miközben a kiberharcosok a hálózatos térben keresik a megfelelő fegyvert, addig ugyanott keresik a rendezés lehetőségeit mások is. A ma már egyre gyakrabban csak fejlett technológiájú „új hidegháborúként" emlegetett szembenállás ugyanis ösztönzi a kibertér békés rendezésén, kollektív szabályozásán munkálkodó szakembereket, a kiberdiplomatákat is.

Felhasznált irodalom

Ayers, Cynthia (2015): *Rethinking Sovereignty in the Context of Cyberspace*. Carlisle, US Army War College.

Barrinha, André – Renard, Thomas (2020): Power and Diplomacy in the Post-Liberal Cyberspace. *International Affairs*, vol. 96, Issue 3, May 2020, 749–766.

Brangetto, Pascal et al. (2015): *Economic aspects of national cyber security strategies. Project report.* Tallin, CCDCOE.

Buchan, Russell (2019): *Cyber Espionage and International Law.* Oxford, Hart.

[75] Barrinha–Renard 2020, 756.

Charalabidis, Yannis (2018): *The World of Open Data. Concepts, Tools and Experiences*. Cham, Springer Nature.

Covid-19 Cybercrime Weekly Update (2020). Forrás: www.riskiq.com/blog/analyst/covid19-cybercrime-update/ (A letöltés dátuma: 2020. 06. 11.)

Custers, Bart et al. (2019): *EU Personal Data Protection in Policy and Practice*. Berlin, Springer.

Data Governance. Part I. Emerging Data Governance Practices (2020). Forrás: https://foreignpolicy.com/2020/05/13/data-governance-privacy-internet-regulation-localization-global-technology-power-map/?utm_source=PostU (A letöltés dátuma: 2020. 04. 24.)

D' Elia, Danilo (2014): La Guerre économique a l'Ére du Cyberspace. *Hérodote*, 2014/1, No. 152–153, 240–260.

Dee, Megan (2015): *The European Union in a Multipolar World. World Trade, Global Governance and the Case of the WTO*. London, Palgrave MacMillan.

Demchak, Chris – Dombrowski, Peter (2014): Cyber Westphalia: Assessing State Prerogatives in Cyberspace. *Georgetown Journal of International Relations* (2013–14) 29–38.

Digital Watch Newsletter (2020). Issue 50, May 2020.

Dominioni, Samuele (2019): *Digital Economic Powers and Digital Political Rulers*. Forrás: www.ispionline.it/en/pubblicazione/digital-economic-powers-and-digital-political-rulers-24187 (A letöltés dátuma: 2020. 06. 14.)

DuPont, Sam (2020): *An Open Alliance for Digital Trade*. Forrás: www.csis.org/analysis/open-alliance-digital-trade?utm_source=Members&utm_campaign=aba3460b2a-EMAIL_CAMPAIGN_2020_01_29_04_21_COPY_01&utm_medium=email&utm_term=0_e842221dc2-aba3460b2a-221725217 (A letöltés dátuma: 2020. 05. 21.)

Exclusive: Meet the UK's „Data Diplomat" (é. n.) Forrás: https://govinsider.asia/innovation/uk-foreign-office-open-source-unit-data-diplomat-graham-nelson/ (A letöltés dátuma: 2019. 03. 14.)

FBI–CSISA PSA PRC targeting of COVID-19 research organizations (2020). Forrás: www.cisa.gov/publication/fbi-cisa-psa-prc-targeting-covid-19-research-organizations (A letöltés dátuma: 2020. 06. 15.)

Filippov, Vladimir M. et al. (2019): *The Cyber Economy. Opportunities and Challenges for Artificial Intelligence in the Digital Workplace.* Cham, Springer Nature.

Findlay, Buddle (2020): *Artificial intelligence and the regulatory landscape*. Forrás: www.lexology.com/library/detail.aspx?g=4c845762-e954-4f47-8809-f5ad0f5d3716 (A letöltés dátuma: 2020. 03. 14.)

France and Canada create new expert International Panel on Artificial Intelligence (2018). Forrás: www.gouvernement.fr/en/france-and-canada-create-new-expert-international-panel-on-artificial-intelligence (A letöltés dátuma: 2020. 06. 08.)

Futó Iván (1999): *Mesterséges Intelligencia*. Budapest, Aula Kiadó Kft.

G20 human-centered AI Principles (2019) Forrás: www.mofa.go.jp/files/000486596.pdf (A letöltés dátuma: 2020. 06. 08.)

Gady, Franz-Stefan (2020): *Interview: Robert Ward and Yuka Koshino on Geo-Economics in East Asia*. Forrás: https://thediplomat.com/2020/04/interview-robert-ward-and-yuka-koshino-on-geo-economics-in-east-asia/ (A letöltés dátuma: 2020. 06. 10.)

Gill, Indermit (2020): *Whoever leads in artificial intelligence in 2030 will rule the world until 2100*. Forrás: www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/?fbclid=IwAR3UJSDfUG4aFGXpHRDdch76HQu9ZgDIOQXGZo2t8iVjn-0HIQPNPnD42MM (A letöltés dátuma: 2020. 01. 28.)

Hakmeh, Joyce (2017): *Cybercrime and the Digital Economy in the GCC Countries*. London, Chatham House.

Huang, Keman et al. (2018): *Interactions between Cybersecurity and International Trade: A Systematic Framework.* Cambridge, MIT Sloan.

Inside Project Debater Speech by Crowd (2019). Forrás: https://mc.ai/inside-project-debater-speech-by-crowd/ (A letöltés dátuma: 2020. 06. 22.)

International Trade Regulation and Cybersecurity (é. n.). Forrás: www.hoganlovells.com/en/publications/international-trade-regulation-and-cybersecurity (A letöltés dátuma: 2020. 04. 02.)

Jacobson, Barbara Roseb – Höhne, Katharina E. – Kurbalija, Jovan (2018): *Data diplomacy.* Genf, DiploFoundation.

Mapping the challenges and opportunities of artificial intelligence for the conduct of diplomacy (2019). Geneva, DiploFoundation.

Jaywardane, Sash (2015): *Cyber Governance: Challenges, Solutions and Lessons for Effective Global Governance.* The Hague, The Hague Institute for Global Justice.

Luttwak, Edward (1990): From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce. *The National Interest*, No. 20 (Summer 1990), 17–23.

Measuring the Digital Economy (2018). Washington, International Monetary Fund.

Meltzer, Joshua (2019): *Cybersecurity, digital trade, and data flows. Re-thinking a role for international trade rules.* Forrás: www.brookings.edu/research/cybersecurity-digital-trade-and-data-flows-re-thinking-role-for-international-trade-rules/ (A letöltés dátuma: 2020. 03. 17.)

Meyer, David (2017): *Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World*, *Fortune, 2017. 09. 04.* Forrás: https://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/ (A letöltés dátuma: 2020. 05. 23.)

Moisio, Sami (2019): Re-thinking geoeconomics: Towards a political geography of economic geographies. *Geography Compass*, vol. 13, Issue 10, October 2019, 1–13.

Nyáry, Gábor (2020): Kiber geopolitika. Mesterséges Intelligencia alkalmazások az államigazgatás külpolitikai alrendszereiben. Új Magyar Közigazgatás, 2020. 1., 32–39.

OECD Principles on AI (2019). Forrás: www.oecd.org/going-digital/ai/principles/ (A letöltés dátuma: 2020. 06. 08.)

Open data: Unlocking innovation and performance with liquid information. McKinsey Global Institute Report (2013). Forrás: www.mckinsey.com/business-functions/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information (A letöltés dátuma: 2020. 05. 28.)

Open Government Data Report (2018). Paris, OECD.

Pintér István szerk. (2016): *Műhelymunkák. A virtuális tér geopolitikája. 2016/1* Budapest, Geopolitikai Tanács Közhasznú Alapítvány.

Riordan, Shaun (2019): *Cyberdiplomacy. Managing Security and Governance Online.* Cambridge, Polity Press.

Rohaidi, Nurtilzah (2017): *Exclusive: Meet the World's first Tech Ambassador.* Forrás: https://govinsider.asia/innovation/danish-tech-ambassador-casper-klynge/ (A letöltés dátuma: 2020. 05. 31.)

Scesanto, Stefan (2017): *Europe's digital Power: From geo-economics to cybesrsecurity.* London, European Council on Foreign Relations.

Shem, Yi (2016): Cyber Sovereignty and the Governance of Global Space. *Chinese Political Science Review* (2016) 1, 81–93.

Sherman, Justin (2017): *How Much Cyber Sovereignty Is Too Much Cyber Sovereignty?* Forrás: www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty (A letöltés dátuma: 2020. 05. 30.)

Sherman, Justin (2018): *To Preserve a Global and Open Internet, We Need to Invest in Cyber Diplomacy.* Forrás: www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/preserve-global-and-open-internet-we-need-invest-cyber-diplomacy/ (A letöltés dátuma: 2020. 05. 30.)

Significant Cyber Incidents (2020). Forrás: www.csis.org/programs/technology-policy-program/significant-cyber-incidents (A letöltés időpontja: 2020. 06. 14.)

Stadnik Ilona (2017): What is an International Cyber Regime and How We Can Achieve It? *Masaryk University Journal of Law and Technology* 11 (1): 129, June 2017, 129–154.

Taulli, Tom (2019): *Artificial Intelligence Basics. A Non-Technical Introduction*. Monrovia, Apress.

Teoh, Chooi Shi – Mahmood, Ahmad Kamil (2017): National Cyber Security Strategies for Digital Economy. *Journal of Theoretical and Applied Information Technology*, vol. 95, No. 23, 6510–6522.

The World"s First Ambassador to the Tech Industry (2019). Forrás: www.nytimes.com/2019/09/03/technology/denmark-tech-ambassador.html (A letöltés dátuma: 2020. 06. 14.)

Vicente, Dário Moura – Casimiro, Sofia de Vasconcelos (2020): *Data Protection in the Internet*. Cham, Springer Nature.

Wheeler, Tom (2019): *History's message about regulating AI*. Forrás: www.brookings.edu/research/historys-message-about-regulating-ai (A letöltés dátuma: 2020. 03. 15.)

White Paper on Artificial Intelligence. A European approach to excellence and trust (2020). Brussels, European Commission.

Wigell, Mihael et al. szerk. (2019): *Geo-economics and Power Politics in the 21st Century.* London, Routledge.

World Economic Forum AI Government Procurement Guidelines (2019). Forrás: www.weforum.org/whitepapers/ai-government-procurement-guidelines (A letöltés dátuma: 2020. 06. 08.)

Yahoo says all three billion accounts hacked in 2013 data theft (2017). Forrás: www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1 (A letöltés dátuma: 2020. 06. 14.)

2. Cyberdiplomacy from a European Perspective

VÁKÁT OLDAL

Balázs Mártonffy[1]

Cyberdiplomacy: A Review from the Literature

An introduction to the cyber world amid the Covid-19 pandemic

In 2013, the U.S. Department of Defense alone, one of the institutions that is most active in the cyber realm, reported 10 million efforts at intrusion each day.[2] Five short years later, in 2018, this figure was 36 million.[3] The numbers in the cyber realm do not stay constant for long; the cyber world changes extremely quickly. Thus, it will come as no surprise that any text on an issue as complicated and quickly changing as the cyber domain is bound to be outdated quickly. This review from the literature on cyberdiplomacy is particularly prone to be overtaken by events as our society undergoes and fights the implications of the global pandemic of the early 2020s, the novel coronavirus that began in Wuhan, China, in late December 2019. Further, as this review work is written during the time that European Union member states fight the coronavirus and enter into force restrictions on movement, universities have undergone work-from-home transitions, this work relies fundamentally on literature that was available online when the research for this chapter was written. The irony of course, for a text on cyberdiplomacy, is not lost on the author.

In the 21st century, the question of how much our society changes continues to linger. As mentioned above, this chapter is written during the global pandemic caused by the virus Sars-Cov-2 and the associated disease, Covid-19. The results and implications of this truly global crisis cannot be understated, and in April 2020, when this chapter is concluded, much remains to be determined. What we do know is that the effects will reverberate deeply through what has become a widely interdependent and truly globalised society across our globe by 2020.

Of course connecting cyber threat and global pandemics is not impossible: case in point is the 2018 study on the countermeasures available to protect healthcare critical infrastructure.[4] The study concluded that, if for example a pandemic like Covid-19 were to be compounded with an insider attack on a state's critical healthcare infrastructure, the results would be devastating.[5] Inasmuch as our current awareness of the implications of the virus's origins presumes to endeavour to analyse, this is not the case for the novel coronavirus, but certain conclusions must be drawn. Health care systems globally

[1] The author would like to thank Anna Urbanovics, doctoral student at the National University of Public Service in Budapest, for her excellent research assistance.

[2] Fung 2013.

[3] Konkel 2018.

[4] Walker-Roberts et al. 2018.

[5] Walker-Roberts et al. 2018.

are under strain, and coupled with a kinetic-or-cyber-kinetic attack, the system could have been seriously upset. The transatlantic regions' prime politico-military alliance, NATO, is also concerned: its Secretary General, Jens Stoltenberg, continues to state that the prime directive of the Alliance is to make sure that the public health crisis does not become a security crisis.

This chapter serves to provide the reader with a general introduction into the world of cybersecurity and cyberdiplomacy. The latter is a somewhat novel term that has been seen employed rarely in academic texts but is somewhat more prevalent in popular and media punditry. The specific goal of this chapter is to provide the reader with a conceptual understanding of what, as to the best of social scientific knowledge, cyberdiplomacy is, and how it is being used in general language and in policy as well.

To begin with, let us examine some of the key terms that are needed to grapple with cyberdiplomacy. For general considerations, when thinking about issues in the cyber world and specifically about cyberdiplomacy, I turn to Joseph S. Nye, Professor at Harvard University, who writes the following:

"Cyber is a prefix standing for computer and electromagnetic spectrum-related activities. The cyber domain includes the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications. Cyberspace has a physical infrastructure layer that follows the economic laws of rival resources and the political laws of sovereign jurisdiction and control. This aspect of the Internet is not a traditional "commons". It also has a virtual or informational layer with increasing economic returns to scale and political practices that make jurisdictional control difficult. Attacks from the informational realm, where costs are low, can be launched against the physical domain, where resources are scarce and expensive. Conversely, control of the physical layer can have both territorial and extraterritorial effects on the informational layer. Cyber power can produce preferred outcomes within cyberspace or in other domains outside cyberspace."[6]

Cyber as the reader is undoubtedly well aware refers broadly speaking to the culture of computers, information technology and virtual reality. But the term is at times used interchangeably with 'e', virtual and digital. The specific etymology of the word cyber is also interesting. Why did we settle on cyber instead of virtual or electronic or digital? How do the terms interrelate? Here is what is commonly accepted on the terms etymology and how to differentiate between cyber, 'e', virtual and digital.

The etymology of 'cyber' goes back to the ancient Greek meaning of 'governing'. Cyber came to our time via Norbert Weiner's book *Cybernetics* and William Gibson's science-fiction novel *Neuromancer.* The growth in the use of the prefix 'cyber' followed the growth of the Internet. Today, cyber mainly refers to security issues; 'e-' is the preferred prefix for economic issues, digital is mostly used by the government sector, while virtual has been practically abandoned.

[6] Nye 2011a.

'E' is the abbreviation for 'electronic'. It got its first use through e-commerce, as a description of the early commercialisation of the Internet. In the EU's Lisbon Agenda (2000) and the WSIS declarations (Geneva 2003; Tunis 2005), 'e-' was the most frequently used prefix. The WSIS follow-up implementation is centred on action lines including e-government, e-business, e-learning, e-health, e-employment, e-agriculture and e-science. Nonetheless, e- is not as present as it used to be. Even the EU recently abandoned e-, trying, most likely, to distance itself from the failure of its Lisbon Agenda.

Digital refers to '1' and '0' – two digits that are the basis of the whole Internet world. In the past, digital was used mainly in development circles to represent the digital divide. During the last few years, digital has started conquering the Internet linguistic space, especially in the language and strategy of the European Union. Virtual relates to the intangible nature of the Internet.

Virtual reality could be both an intangible reality, (something that cannot be touched) and a reality that does not exist (a false reality). Academics and Internet pioneers used virtual to highlight the novelty of the Internet, and the emergence of 'a brave new world'. Virtual, because of its ambiguous meaning, rarely appears in policy language and international documents.[7]

Cyber is thus the broadest category and the most useful one when it comes to conceptualising diplomacy. The term cyberdiplomacy itself refers to diplomacy, and a specific form thereof and thus subpart thereof, diplomacy in the cyber realm. Diplomacy as a term is widely accredited to be a practice of states, and the easiest way to begin grappling with the term is to start there. Thus, cyberdiplomacy at its core is simply diplomacy conducted in the cyber realm. Cyberdiplomacy is both much larger then this simple definition and has much smaller integral parts. As I demonstrate later, one key differentiation that has to be made is that cyberdiplomacy is a separate concept from digital or e-diplomacy, but digital diplomacy and e-diplomacy are used interchangeably. But why is diplomacy in the cyber realm different then in the traditional world? Let us examine in brief how it functions in the non-cyber realm.

States, as sovereign entities with a defined population and territory, territorial integrity, and external and internal legitimacy with some form or type of authority that holds the monopoly on the legitimate use of violence, have been a central actor in international relations theory. The modern state's emergence is attributed to the Peace of Westphalia, where the feudal system of overlapping realms of authority were channelled into hierarchical entities, with founts of authority resting with the state as an actor. Diplomacy, the profession, activity, or skill of managing international relations typically by a country's representatives abroad now was without question the mandate of states.

Diplomacy thus can be understood to be grouped into two large buckets. The first bucket is that of the specific, the note verbales, the demarches, the embassies, consulates, Ambassadors Extraordinary and Plenipotentiaries, Agréments, and other instances when states interact with each other. This is usually on two separate levels in our modern world:

[7] Kurbalija 2016.

bilaterally, i.e. for example the deputy chief of mission of France to the Court of St. James delivers a demarche to the State Secretary of the Foreign and Commonwealth Office in London, the United Kingdom. But another type of fora is the multilateral realm, when states interact, usually as equals, in intergovernmental organisations such as the United Nations, or the World Health Organization.

The more general idea of diplomacy of course is what Kissinger in his world-famous book explores (aptly named Diplomacy) – the broadly understood conduct of states as actors in an international system, the manner in which they define their own national interest and the general way they carry these out. In this approach, diplomacy is one tool in the grand strategy toolkit of states to "get what they want". Usually separated from war, which is the "ultima ratio regum" as the cannons of Louis XIV had epitomised, diplomacy then is a term that relates to the use of power without active violence.

Cyberdiplomacy can be defined as "an attempt to facilitate communication, negotiate agreements, gather intelligence and information from other countries to avoid friction in cyberspace, bearing in mind the foreign policy agenda".8 It is important to note that while "in many articles, cyber-diplomacy is considered to be same as e-diplomacy or digital diplomacy. However, these concepts differ from each other. While cyber-diplomacy involves managing foreign policy in today's age, e-diplomacy or digital diplomacy reflects on the impact of new technology on the objective, tools, and structure of diplomacy. Digital diplomacy or e-diplomacy is the study of the use of ICT tools and method for diplomacy and foreign affairs. However, cyber-diplomacy involves diplomacy, conflict resolution, agreements and policies that is surrounding cyberspace".9 This divide is the most important differentiation, to know when to refer to cyberdiplomacy in practice, that is instances of diplomacy conducted through cyber means as digital diplomacy (which is also called e-diplomacy) and when to refer to cyberdiplomacy proper when it is the conduct of diplomacy that affects the cyberspace domain.

The difference between e/digital diplomacy and cyberdiplomacy is visible in the U.S. academic language and if not quite so clearly elaborated, in the European academia as well. For example, Mureșan's study on the "Current approaches of diplomacy in the cyberspace"[10] clearly recognises the need for cyberdiplomacy. Mureșan argues that "more and more frequently, the Internet has also been the target of many cyber attacks, generating data leaks and financial loses. The vast majority of financial and telecommunication systems have been affected by numerous such intrusions. These incidents are more and more common and they impact heavily both on governments and businesses or individual users".[11] But here the digital and the cyber realms of diplomacy are still conflated.

[8] Cyberdiplomacy 2019.
[9] Cyberdiplomacy 2019.
[10] Mureșan 2017.
[11] Mureșan 2017.

Illustrating the differences between cyberdiplomacy and digital diplomacy

To illustrate with a concrete example the difference between the two major conceptual buckets of the term, let us take a recent example of cyberdiplomacy and e-diplomacy or digital diplomacy.[12] The North Atlantic Treaty Organization, NATO, makes decisions as set forth in its charter, the Washington Treaty of 1949, by convening senior leaders of the Alliance in a room to approve certain documents that task the alliance to carry forth certain actions. The Foreign Ministers meet in addition to other times every spring. But the Covid-19 crisis did not allow for this to take place, as all NATO member states restricted travel out, and the usual host nation of the meeting, Belgium, where NATO's Headquarters are located in Brussels, did not allow non-nationals to visit. So the meeting was held via secured video teleconference, with the NATO Secretary General in Brussels, while the foreign ministers of the 30 member states joined from their capitals. The meeting itself was an instance of digital diplomacy. The tweets that followed, on Twitter as part of the cyberspace, were also digital diplomacy.

But cyberdiplomacy, as a tool of grand strategy of a nation state to affect the cyber domain is very different. Sticking with our example of a NATO senior decision-makers meeting, let us examine how NATO member states conduct cyberdiplomacy proper. NATO's mutual defence clause, Article 5 of the Washington Treaty, states the following:

"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."[13]

But would an instance of a Russian hacker that disables the national banking computer system of a NATO member state fit this criteria? Is that an armed attack? Legal scholars were conflicted by the issue. So as the Alliance took action through cyberdiplomacy: it announced that a cyberattack could trigger Article 5 of our founding treaty at a NATO Summit in Wales in 2014, and later other Cyber Defence Pledges were taken as well. This type of general cyberdiplomacy action constitutes a broader category, and of course incorporates direct instances of practical cyberdiplomacy, i.e. the concrete steps

[12] Barrinha–Renard 2017.
[13] NATO 2019.

of diplomacy that happen in the cyber, computer, informational technological world; it is a broader type of policy – a set of diplomatic actions that a state undertakes that affect the cyber domain.

Nevertheless, NATO took a more proactive stance to combat this ambiguity. In 2016, Allied Ministers issued a Cyber Defence Pledge, which, while not naming Article 5, took note of the following:

1. In recognition of the new realities of security threats to NATO, we, the Allied Heads of State and Government, pledge to ensure the Alliance keeps pace with the fast evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea.

2. We reaffirm our national responsibility, in line with Article 3 of the Washington Treaty, to enhance the cyber defences of national infrastructures and networks, and our commitment to the indivisibility of Allied security and collective defence, in accordance with the Enhanced NATO Policy on Cyber Defence adopted in Wales. We will ensure that strong and resilient cyber defences enable the Alliance to fulfil its core tasks. Our interconnectedness means that we are only as strong as our weakest link. We will work together to better protect our networks and thereby contribute to the success of Allied operations.[14]

In addition, the Alliance also decided to act on seven action items, all of which would deserve to be analysed on their own, but I list them here as potential actions of multilateral cyberdiplomacy.

1. Develop the fullest range of capabilities to defend our national infrastructures and networks. This includes: addressing cyber defence at the highest strategic level within our defence related organisations, further integrating cyber defence into operations and extending coverage to deployable networks; 2. Allocate adequate resources nationally to strengthen our cyber defence capabilities; 3. Reinforce the interaction amongst our respective national cyber defence stakeholders to deepen co-operation and the exchange of best practices; 4. Improve our understanding of cyber threats, including the sharing of information and assessments; 5. Enhance skills and awareness, among all defence stakeholders at national level, from fundamental cyber hygiene to the most sophisticated and robust cyber defences; 6. Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance; 7. Expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends.[15]

These Cyber Defence Pledge action items, which NATO follows up on and continues to place emphasis on, are not the only actions this multilateral alliance has taken in the cyber realm. Further, NATO member states adopted the Tallinn Manual, showcasing their approach to cyberdiplomacy – a rules-based approach to the cyber realm. The Tallinn Manual has two editions, one from 2013 and an updated one from 2017. The

[14] NATO 2016.
[15] NATO 2016.

newer, 2017 edition covers a "full spectrum of international law applicable to cyber operations ranging from peacetime legal regimes to the law of armed conflict, covering a wide array of international law principles and regimes that regulate events in cyberspace. Some pertain to general international law, such as the principle of sovereignty and the various bases for the exercise of jurisdiction. The law of state responsibility, which includes the legal standards for attribution, is examined at length. Additionally, numerous specialised regimes of international law, including human rights law, air and space law, the law of the sea, and diplomatic and consular law, are examined in the context of cyber operations."[16]

Nevertheless, it is important to note that while the Tallinn Manual and the NATO group of countries have their own alliance and policies advocating the liberalisation of cyberspace, countries in the Shanghai Cooperation Organisation advocate National Cyber Sovereignty, a fundamentally different approach.[17] The two approaches are at odds with each other and the ongoing and future conflicts in the cyber realm are where we will witness the greatest cyberdiplomacy.

After that introduction, the rest of the chapter examines the conceptually useful terms one needs to be aware of in the cyber realm. As with most literature on diplomacy as the conduct between states, cyberdiplomacy is theorised about and analysed within the journal of international relations. As a subfield of political science, international relations focuses on the interactions between states and has three major paradigms: realism, liberalism and constructivism. These three, focusing on the role of power, reciprocity and norms in general, link how the cyber realm and cyberdiplomacy within it, break up the literature on the topic fairly well.

Cyberdiplomacy in theory

As is evident by now, cyber is in a realm of its own. Thus, there is a theoretical imperative to classify it in some manner, or to liken the topic to something else. It would be easy to classify a new topic as sui generis, i.e. that it has not ever been seen before and is not comparable to anything else. The most widespread use of this term in international relations theory applies to the European Union, which is, as much as there can be consensus in academic literature, sui generis. As the European Union can be understood to be an intergovernmental organisation, a supranational endeavour, a spirit or Zeitgest, a regional security organisation, and a myriad of other things, all valid from their own perspective, the argument holds. But cyberdiplomacy is not sui generis and in fact is mostly understood to be a concept that has precedents in international, intersocietal and intra-societal relations.

[16] CCDCOE 2017.
[17] Cyberdiplomacy 2019.

Etymologies, conceptualisations and definitions

Before we explore the limits of cyberdiplomacy, the question is what exactly does the term cyber mean and where would cyberdiplomacy operate. As a quick reminder, in general analysts use the prefix "cyber" to refer to a variety of digital, wireless and computer-related activities. But differences persist, and the approach one takes to the definition varies. The mandate of organisations that deal with some part of the cyber realm usually dictates the approach.

The U.S. Department of Defense, for example, defines "*cyberspace* as a global domain within the information environment consisting of the interdependent networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers and *Cyberspace operations* as the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace".[18] Of course, for them, the focus is on the military angle. Specifically, the U.S. military refers to cyber as a domain or sector of action (like land, sea, air and space), but it is also sometimes used to refer to a range of instruments or tools that can be employed along with others across a number of sectors".[19]

But what do foreign ministries do? Let us examine what the U.S. foreign ministry, the largest and most widely credited such organisation, the Department of State, writes on this topic. "The State Department is leading the U.S. Government's efforts to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation".[20] Quite notably different from what the military does, but both are even more different from the realm of theory.

Cyberdiplomacy in theory and in academic literature where the main locus of theoretical debates reside is a relatively recent entry, given the relatively recent introduction of the term in 2002 with a manuscript entitled *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century.* As such, the concept of cyberdiplomacy is still conceptually contested. In fact, the manuscript in question meant only cyberdiplomacy in practice, solely digital or e-diplomacy when it referred to the term. Since then, the peer-reviewed academic literature on the topic specifically of cyberdiplomacy is relatively recent and somewhat under-published. Perhaps the most prominent example of this is a study entitled "Cyber-diplomacy: the making of an international society in the digital age", published in the *Journal of Global Affairs* by Barrinha and Renard. The authors argue that cyberdiplomacy, "which in spite of its rising importance [cyberdiplomacy] has remained a peripheral issue in the International Relations (IR) literature".[21]

[18] Jabbour–Ratazzi 2012.
[19] Nye 2011b.
[20] U.S. Department of State 2020.
[21] Barrinha–Renard 2017.

The authors argue that while cyber incidents, which this chapter details as well, has gained much more prominence in the media then cyberdiplomacy.

As our analysis centres squarely on the level of states as actors, it is worth noting what other levels of analysis will certainly arise later. The upper echelon of analysis, the "cyber international system", while feasibly a possibility to explore, is not quite at the level of academic theoretical analysis yet. This is no surprise; the study of foreign policy first amounted to exploring how states, as the most powerful actors in international relations, behaved. Only relatively recently, with the rise of structural or systemic explanations of patterns of interstate behaviour, did the systemic level of analysis prove useful. Thus while the analysis of the conduct of state behaviour dates back quite a while, only with Kenneth Waltz' *Theory of International Politics* of the 1960s did truly systemic levels of analysis begin. It is thus perfectly plausible that system levels of analysis for the cyber realm will arise in the future. This would focus on establishing certain components of the cyberspace that define the manner in which behaviour, including cyberdiplomacy, could be conducted. Until then, I focus on the state-level with an eye for the international organisations that do work here as well, but some work on non-governmental organisations and actors that have a meaningful role to play in the cyber realm also.

To begin the state-level analysis, a search for a clear definition of cyberdiplomacy provides a strong starting point. Given the relative dearth of academic literature, definitions are not too abundant. Most of these start with defining diplomacy and then link it to the cyber realm. We note that the definitions of diplomacy vary with whether power, reciprocity, or norms are the key drivers behind international relations for the authors. Thus, diplomacy can for once be understood as the attempt to adjust conflicting interests by negotiation and compromise. For others, diplomacy is a central institution in the definition and maintenance of international society. As for the English School and for Hedley Bull, diplomacy is a custodian of the idea of international society, with a stake in preserving and strengthening it. For Bull, diplomatic practice has five main functions: to facilitate communication in world politics, to negotiate agreements, to gather intelligence and information from other countries, to avoid or minimise friction in international relations and, finally, to symbolise the existence of a society of states. Cyberdiplomacy then is the conduct of such practices in the cyber realm. For Barrinha and Renard, "cyber-diplomacy can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace".[22]

Regardless of which definition one accepts, follow-on questions are intent on delimiting cyberdiplomacy. If we accept the most general definition of cyberdiplomacy, as the use of diplomatic resources to secure national interests with regard to cyberspace, then what is it not? Conceptualisations must be made by clearly delimiting the term. Cyberdiplomacy is then by definition, not cyber war, not cyber defence, not cybersecurity, and

[22] Barrinha–Renard 2017.

not cyber deterrence, cyber compellance, or cyber coercion. These terms would apply to the use of other types or national resources in some other way.

To continue the conceptualisation process, the division between cyberdiplomacy and cyber war or cyber warfare must be made. In sharp contrast to the academic theoretical analysis of cyberdiplomacy, cyber war has been relatively well studied. The first question of course is whether cyber war can be understood to be warfare in the general sense. Stone's seminal piece from 2013 published in the notable *Journal of Strategic Studies,* entitled "Cyber War Will Take Place"[23] clearly answers in the positive. He determines that cyber warfare meets the criteria of the concepts of force, violence and lethality, and as such, should be able to be considered war. Of course others disagree somewhat, focusing on the fact that there is no agreed upon definition of cyber war and cyber warfare, noting in particular that even the two are not quite readily distinguishable.[24] Joseph Nye, an authority on the topic, makes a similar point: "A more useful definition of *cyber war* is, hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence".[25] But cyber war is not by necessity simply an amalgamation of a number of cyberattacks (the term cyberattack covers a wide variety of actions ranging from simple probes, to defacing websites, to denial of service, to espionage and destruction),[26] and is noticeably different from conventional wars. One such major difference is that "the barriers to entry in the cyber domain are so low that nonstate actors and small states can play significant roles at low cost".[27] In conclusion, and underlining why we have to make sure we differentiate between the terms exactly, in the current literature "the term *cyber war* is used very loosely for a wide range of behaviors. In this, it reflects dictionary definitions of war that range from armed conflict to any hostile contention".[28]

The purpose of cyberdiplomacy

What function one purports cyberdiplomacy to serve depends significantly on one's look on how the international system functions. As such, the most useful manner in which to conceptually categorise the literature is to follow the three major paradigms of international relations. As a reiteration, this categorisation is interested in literature on cyberdiplomacy proper, and not on what is conceptually covered under the term digital or e-diplomacy.

The literature on cyberdiplomacy falls under three broad categories. The first is interested in grappling with the linkages of cyberdiplomacy to power; the second, to reciprocity and interdependence, many times through the use of law and legal treaties; and the third, linkages to norms and patterns of behaviour. It is thus not surprising that

[23] Stone 2013.
[24] Robinson et al. 2015.
[25] Nye 2011a.
[26] Nye 2011a.
[27] Nye 2011a.
[28] Nye 2011a.

the three major schools of thought, realism, liberalism and constructivism, is what is used here to create these categories.

Broadly speaking, cyberdiplomacy also takes place in what scholars of international relations theory would label as the condition of anarchy. There is no supra-national 'cyber authority' in the world, and the realm of cyber is, and often here only partially and superficially, regulated by governments. One thus could assume that cyberdiplomacy follows similar rules to what diplomacy between states follows. But unlike traditional diplomacy and its counterpart, war, three major differences of state behaviour are clearly visible, all of which are polar opposites between traditional and cyberdiplomacy.

The first is that the assets, parts, individuals and components of cyberdiplomacy lack a clear spatial designation. They are interspersed throughout our globe and are interconnected in ways that make clearly separable modes of power distinction unrealistic. For regular diplomacy, an Ambassador Extraordinary and Plenipotentiary is the clear, singular fount of sender state jurisdiction in the host state. The Ambassador is a single person, and only holds this special capacity while in the host country, as dictated by a bilateral agreement covered in the international treaty known as the Vienna Convention on Diplomatic Relations of 1961. For the cyber world, by definition, the bits and bytes that actually contain data that is used as the medium for cyberdiplomacy is spread out. Efforts and policy, in the same vein, that target cyber issues, cannot be spatially bound. This makes the matter much more complex and interdependent, where lines of demarcation are not readily apparent.

A second issue is the question of intermediaries or the degrees of separation of action. In traditional diplomacy, once the ambassador is absent, his deputy assumes this role, usually under the title charge d'affaires. If for some reason an ambassador is not present for an extended period of time, the charge d'affaires becomes ad interim, a.i., and assumes the role of the ambassador. In cyberdiplomacy, there are numerous intermediaries that may come between the policy and the effect of the policy or the start state and the end result. A Russian government directive may result in the government tasking an intelligence directorate, which is still part of the state apparatus. The intelligence director then asks a private hacker to fulfil a request, who then outsources it to a hacker in Belgium but who is a South African national. The intermediaries are numerous and vary between public and private.

Third and finally, in much the same vein how cyber demarcation is hardly possible, as Virtual Private Networks for example mask our I.P. addresses, the issue of attribution surfaces as well. Reverting back to our traditional diplomatic example, attribution is quite simply taken for granted: in fact, only quite readily attributable diplomats and diplomatic instances are allowed in the host state. Attribution is a key component in traditional diplomacy. In cyberdiplomacy, and in the cyber realm writ large, attribution or more specifically the lack of credible attribution, is a fundamental issue. Cyber incidents have clear end-points. Distributed Denial of Service Attacks (DDoS) clearly affect host computers or websites which are shut down. But where the attack originates is a much more complex issue and at many times impossible to determine with any degree of cer-

tainty. Deputy Secretary of Defense William Lynn wrote in 2010: "Whereas a missile comes with a return address, a computer virus generally does not. The forensic work necessary to identify an attacker may take months, if identification is possible at all."[29] Or for example in the Stuxnet attack of 2010, the question of verifiable attribution is foundationally uncertain even today, although there is a clear consensus that it was a joint operation of the United States and Israeli governments.

Thus, cyberdiplomacy operates in a space that is clearly different, in fact quite the opposite of the realm of traditional diplomacy. It is geographically unbound, operates with potentially significant chains of intermediaries where functions and roles differ significantly, and is in a plethora of cases virtually without credible attribution. And while almost all scholars agree on these differences, the role of cyberdiplomacy is best examined through the lenses of international relations theories.

Cyberdiplomacy and power

One chain of thought that connects literature on cyberdiplomacy is the realist approach. Here authors are primarily interested in how cyberdiplomacy can act as a complement to efforts of war and violence; that is, diplomacy in itself is meaningless, only in juxtaposition (or at times subjugation) to military efforts can it be understood. Cyberdiplomacy here is often simply considered a function of an exertion of power in the national interest by states.

Many authors focus on the role of cyberdiplomacy as a function of cybersecurity and examine whether cyberdiplomacy can affect cyberattacks. As Nye writes: "There are three main vectors of cyberattack: via networks, via supply chains, and by human insiders who may be malicious or just careless. Disconnecting from the network is costly, and the "air gaps" it creates do not guarantee security".[30] Others are intent on differentiating between the levels of cyber defence.[31] O'Connell for example points out that the U.S. has clearly pursued a realist approach, by first setting up and devoting sizable funds to the U.S. Department of Defense and the armed services.[32] This of course raises the question of the legality of action in the cyber realm, and here O'Connell exposes the deep divide between approaches. Here the question of attributing intent is one of the key issues, called AIOS by experts. AIOS stands for *attacker intent, objectives and strategies,* and academics have even attempted to present a "general incentive-based method to model AIOS and a game-theoretic approach to inferring AIOS".[33] Further, if cyberdiplomacy is merely an extension of cyber warfare, then the question of deterrence comes to mind. Here cyberdiplomacy is the sum of efforts that would make deterrence credible. Some

[29] Lynn 2010.
[30] Nye 2016.
[31] Denning 2014.
[32] O'Connell 2012.
[33] Liu 2005.

point out that "the attribution problem appears to make retaliatory punishment, contrasted with defensive denial, particularly ineffective".[34]

Further, notable scholars argue that "many of the properties of cybersecurity assumed to be determined by technology, such as the advantage of offense over defense, the difficulty of attribution, and the inefficacy of deterrence, are in fact consequences of political factors like the value of the target and the scale-dependent costs of exploitation and retaliation".[35] This, in line with traditional realist arguments, does not agree that the cyber realm is sui generis by nature. Geers for example made a compelling comparison between cyberdiplomatic efforts that complement cyber deterrence and nuclear deterrence, by analysing "two deterrence strategies available to nation states (denial and punishment) and their three basic requirements (capability, communication and credibility) in the light of cyber warfare".[36] As such, deterrence is critically important. But some question the point of transference of nuclear deterrence to the cyber world. Richard Clark and Robert Knake for example argue that "of all the nuclear strategy concepts, deterrence theory is probably the least transferable to cyber war".[37] And noted Columbia professor Richard Betts has argued that deterrence does not work well in cyberspace because of the problem of attribution.[38] Others, quite naturally, completely disagree and instead search for a new paradigm in cyber deterrence, criticising "the current discourse in the field, including some 'common knowledge' (mis)understandings of cyberspace and the ways it affects the possibility of deterrence".[39]

The question of how far cyberdiplomacy extends of course does not stop with assuming that power is solely interested in traditional methods of warfare. The debate about the role of national interest and diplomatic efforts versus military efforts is also picked up in the topic of cyber terrorism. Some, like Hua and Bapna, examine the interlinkages of cyber terrorism with the possible economic impact.[40] Others focus on determining whether the level of threat, that is usually taken for granted, truly can be assessed in a valid manner as such. For example Brunst writes: "Although it is known that terrorists already routinely use the Internet for purposes such as spreading propaganda or conducting internal communication, the threat that results from this use is heavily debated."[41]

Finally, how useful can cyber coercion be? One of the most studied examples is the 2014 North Korean operation against Sony. While there are still multiple aspects that are not fully developed, the widely shared narrative argues that "through cost imposition and leadership destabilization, the North Korean operation, despite its lack of physical

[34] Lindsay 2015a.
[35] Lindsay 2005a.
[36] Geers 2010.
[37] Clark–Knake 2010, 189.
[38] Betts 2002.
[39] Tor 2017.
[40] Hua 2013.
[41] Brunst 2010.

destructiveness, caused Sony to make a series of costly decisions to avoid future harm".[42] This is a major challenge to the conventional wisdom that cyber operations cannot conduct successful coercion. In fact, as this demonstrates, it is perfectly feasible, as costs mount and the expected utility of capitulation surpasses the costs of defiance. Guarding against coercion of course requires resilience. But when it comes to cyber resilience, "there is a dawning realisation that the best technical solutions offer only partial assurance. Paradoxically, in an era when the Internet seems ubiquitous, a mixture of analogue and manual systems – often called systems diversity – offers a solution".[43]

In short, realist approaches to cyberdiplomacy focus on traditional themes that are also present in international relations literature from a realist perspective elsewhere. The role of power is paramount, and the most analysed form for the use of power is through military means. Cyberdiplomacy is defined and examined as a complement to the use of force, specifically as an addition to deterrence, compellance, coercion and even war. Unsurprisingly, linkages to the economy are examined from an International Political Economy perspective. The securitisation of cyberdiplomacy is bound to follow on the pages of relevant journals as well, as it has clearly begun with the literature on cyber terrorism. The already established use of force linkages established in the nuclear proliferation literature surface here as well, with articles examining the possibility of deterring cyber terrorists.

But as with all research programs, such as realist agendas in international relations theory, a paradigm shift is sometimes called for. Sharma for example argues that "the last couple of decades have seen a colossal change in terms of the influence that computers can have on the battlefield. [The] article tries to shatter myths woven around cyber warfare so as to illuminate the strategic aspects of this relatively misinterpreted notion, thus identifying a paradigm shift, making cyber war the primary means of achieving grand strategic objectives in the contemporary world order".[44] But when a paradigm shift may actually happen is a matter of debate and uncertainty, and in academic literature, may take time.

Cyberdiplomacy and reciprocity

Another broad bucket of international relations literature takes a different approach to cyberdiplomacy and highlights other priorities. Instead of focusing on cyberdiplomacy as a complement to military and use of force, the large house of liberalism focuses on interdependence, international organisations, reciprocity between state actors, and legal treaties as central tenets. This set of literature highlights the central role of cyberdiplomacy in regulating cyberspace and increasing cybersecurity. Here the efforts of authors

[42] Sharp 2017.
[43] Herrington–Aldrich 2013.
[44] Sharma 2010.

begin with the core ideas of liberalism or liberal institutionalism: economic interdependence, the role of international organisations, and the democratic peace theory.

Beginning with economic interdependence, the authors here focus on how cyberdiplomacy could be used to mitigate issues that may affect cybersecurity. Hausken for example highlights the role of income and substitution effects in cyberspace.[45] In his journal article, Hausken uses the Sarbanes-Oxley Act to demonstrate that when such an act "strengthens internal controls, and the government encourages information sharing, accounting gains significance through secure representation, storage, and transfer of information, and by laying the foundation for assessing costs and benefits, resulting in individual optimization implying free riding".[46] Other authors who can be argued to fall under the broad liberal agenda focus on the role of information sharing as a form of interdependence, by highlighting that as "the Internet threat landscape is fundamentally changing, a major shift away from hobby hacking toward well-organized cyber crime can be observed [and] new paradigms are required for detecting contemporary attacks and mitigating their effects".[47]

Other forms of interdependence are examined from a liberal angle as well, even those of the military, but these are somewhat more nuanced. One of the articles argues that "the globalization and increasing complexity of modern cybersecurity operations have made it virtually impossible for any organization to properly manage cyber threats and cyber incidents without leveraging various collaboration instruments with different partners and allies".[48] This of course postulates that cyberdiplomacy is most efficiently served through interdependence, even when it comes to issues of cybersecurity.

In addition to interdependence, many discussions centre on internet freedom, and the interlinkages with political economy abound as well. Shawn Powers and Michael Jablonski "conceptualize this real cyber war as the utilization of digital networks for geopolitical purposes, including covert attacks against another state's electronic systems, but also, and more importantly, the variety of ways the internet is used to further a state's economic and military agendas".[49] The State Department is singled out as an actor that is looking to connect actors in the cyber realm. Others highlight the State Department's role and argue that cyberdiplomacy is only a smaller portion of a larger whole, namely public diplomacy. One prime example is Cull's article, which lists seven lessons of public diplomacy, namely: 1. public diplomacy begins with listening; 2. public diplomacy must be connected to policy; 3. public diplomacy is not a performance for domestic consumption; 4. effective public diplomacy requires credibility, but this has implications for the bureaucratic structure around the activity; 5. sometimes the most credible voice in public diplomacy is not one's own; 6. public diplomacy is not "always

[45] Hausken 2007.
[46] Hausken 2007.
[47] Hausken 2007.
[48] Hernandez-Ardieta et al. 2013.
[49] Powers 2015.

about you"; and 7. public diplomacy is everyone's business, and demonstrates how these also apply to cyberdiplomacy.50

One of the most critical components of liberal tenets is reciprocity, mainly through equal treatments and legal guarantees. Two major venues of analysis are examined in this approach. The first usually links cyberdiplomacy to international legal treaties, in no small part to International Humanitarian Law. The second focuses on the legal use of force and where cyberattacks warrant a cyberdiplomatic response and where they would fall under the purview of the military.

International Humanitarian Law is one issue that is under scrutiny in the cyberdiplomatic realm. One key article attempts to examine this specific issue. It asks the following question: when is cyber war really war in the sense of "armed conflict"? Powers and Jablonski go on to look at some of the most important rules of "IHL governing the conduct of hostilities and the interpretation in the cyber realm of those rules, namely the principles of distinction, proportionality, and precaution. With respect to all of these rules, the cyber realm poses a number of questions that are still open. In particular, the interconnectedness of the cyberspace poses a challenge to the most fundamental premise of the rules on the conduct of hostilities, namely that civilian and military objects can and must be distinguished at all times".[51]

Of course, in liberal international relations tenets, the question of the use of force is also examined, but through a legal lens. Here cyberdiplomacy is approached as a lens of approach. Buchan for example argues that the "legality of cyber attacks is generally approached from the use of force prohibition contained in Article 2(4) UN Charter".[52] He goes on to ask whether an unlawful use of force in the cyber realm can be squared with the fact that an intervention must produce physical damage. Simply stated, a cyber attack can cause physical damage and therefore violate Article 2(4), but what if it does not? Questions on this are not yet resolved in theory nor in policy.

Finally, scholars question whether the existing legal framework in the cyber realm is sufficient for cyberdiplomacy to function properly. Turns writes: "The domain of cyber warfare being relatively new, it is not yet matched by any comparatively novel international legal paradigm; the cyber conflicts of the present and (probably) the future therefore fall to be regulated under the existing lex lata."[53] If of course cyber warfare lacks regulation, then the first priority of cyberdiplomacy should be to establish such rules.

In conclusion, liberal approaches to cyberdiplomacy focus on theoretical linkage between already established key concepts, such as economic interdependence, rule of law and international organisations. They are adapted to be functions that cyberdiplomacy can fulfil. But the linkages are not always readily apparent in theory at least. One clear argument, in line with how nuclear non-proliferation talks have gone, is the reciprocal

[50] Cull 2010.
[51] Droege 2012.
[52] Buchan 2012.
[53] Turns 2012.

disarmament vein. Here there are certain issues, as the largest player in the world who could champion this is currently its most capable military actor as well. As Gjelten argues, "the US disadvantage would be compounded by the fact that, by most analyses, no other military has such an advanced offensive capability for cyber war. Under a comprehensive cyber arms limitation agreement, the US would presumably have to accept deep constraints on its use of cyber weapons and techniques".[54]

But when it comes to the economic realm, "from a security perspective, there is a misalignment of economic incentives in the cyber domain. Firms have an incentive to provide for their own security up to a point, but competitive pricing of products limits that point. Moreover, firms have a financial incentive not to disclose intrusions that could undercut public confidence in their products and stock prices".[55] This, of course, complicates issues here, but as with many economic theories, norms govern our behaviour sometimes unbeknownst to us.

Cyberdiplomacy and norms

A final large group of approaches to cyberdiplomacy can be categorised under the broad paradigm of international relations, constructivism. When it comes to examining cyberdiplomacy, these theoretical works highlight the importance of social constructions, identity and norms. Here the works focus mainly not on the cyberattacks or incidents themselves, as those are given, but instead attempt to figure out why the attacks or incidents occur and what explains their drivers and outcomes. It is not that "cyberattacks" are thought to be social constructs, but rather their effect and causes are argued to be governed by principles that are constructed in nature.

For example, the role of norms can be used to assess whether there will be an increase in the frequency of cyberattacks. One approach that Valeriano and Maness take is highlighting that "restraint is the norm in cyberspace and suggests that there is evidence this norm can influence how the tactic is used in the future".[56] They argue that norms are the most prominent drivers of state behaviour in the constructivist vein, and their theory of cyber conflict is predicated on empirical patterns. An alternate view is that norms are not quite as widespread across the cyber realm as Valeriano and Maness argue, but in fact, the norms vary significantly across states and within their pattern of behaviour. Kshetri argues that symbolic significance and criticalness, the degree of digitisation of values and weakness in defence mechanisms are the key factors, and not norms, that determine whether restraint or more aggressive cyberattacks are taken.[57]

Of course, the follow on question is equally important. Why bother with cyberdiplomacy? Is cyber war even likely? Junio argues in "How Probable is Cyber War? Bringing

[54] Gjelten 2010.
[55] Nye 2011a.
[56] Valeriano–Maness 2015.
[57] Kshetri 2005.

IR Theory Back In to the Cyber Conflict Debate" (Junio 2013) that, in line with the offence–defence theory, cyber weapons will most likely be used offensively, and makes the argument that they will be done because of the principal agent problem. Another argument in the same journal, by Liff, set forth in an article that examines proliferation of cyberwarfare capabilities and its implications for the character and frequency of war. Here the author states that "consideration of strategic logic, perceptions, and bargaining dynamics finds that the size of the effect of the proliferation of cyberwarfare capabilities on the frequency of war will probably be relatively small".[58] This is of course in line with what we have seen in practice as well with Stuxnet. Probably the most widely cited study of this is Farwell and Rohozinski's work in *Survival,* where the authors demonstrate that there is a striking confluence between cyber crime, cyber threats and state actions.[59]

The opposite has been argued as well, that cyber war in fact will not take place, because "all politically motivated cyber attacks are merely sophisticated versions of three activities that are as old as warfare itself: sabotage, espionage, and subversion".60 Here Rid, writing for the *Journal of Strategic Studies,* argues that "cyber war has never happened in the past, that cyber war does not take place in the present, and that it is unlikely that cyber war will occur in the future".[61] The argument of course, and the division over the debate, is about definitions of the purpose, scope and motivation of cyberattacks, and whether they meet the criteria of cyber war. Yet it seems that this debate has been roughly concluded. While the side arguing for cyberattacks to not meet the threshold of cyber war, the argument that there are easy connections between cyber-attacks and kinetic responses and outcomes clearly link cyber events to acts of war, and states, for example NATO's Article 5 and U.S. policy statements, clearly are in line with this analytical approach.

The argument most closely mirroring this is McGraw's "Cyber War is Inevitable (Unless We Build Security In)".[62] This piece's argument – information systems controlling our critical infrastructure are vulnerable to cyberattacks, and as such, cyber war is therefore inevitable unless we improve our cyber defences – is the approach that most governments have taken and will be explored deeply in the Cyber Diplomacy in Policy Portion. Of course, others point out that there is no readily accepted level that reaches this threshold. "Computer Network Attacks (CNAs) do not automatically come within the framework of the definition of 'attack' in conformity with the law of armed conflict (LOAC). Consequently, some so-called CNAs (especially, those used only as means of intelligence gathering) do not qualify as 'attacks'."[63] The debate will continue here, but policy may lead and theory may only follow.

[58] Liff 2012.
[59] Farwell 2011.
[60] Rid 2012.
[61] Rid 2012.
[62] McGraw 2013.
[63] Dinstein 2012.

What we have witnessed in this section is a similar nuclear non-proliferation debate of the Cold War. In the middle of the Cold War, debates were held, most notably between Kenneth Waltz and Scott Sagan, about whether the spread of nuclear weapons will increase or decrease stability in the international system. Waltz argued that the more states with nuclear weapons, the more stability in the system, as nuclear weapons disincentive warfare by raising its cost. Sagan argued the opposite, mainly focusing on misappropriation, mistakes and miscalculations. Interestingly a policy consensus arose over Sagan's approach, endorsed by even "realist" political leaders who would have otherwise agreed with Waltz's approach of state pattern of behaviour. Once the consensus developed, the nuclear-non-proliferation regime began in earnest. The signing of the Treaty on Nuclear Non-Proliferation began the era, but the Intermediate and Medium-Range Nuclear Forces Treaty, the Strategic Arms Limitations Talks I and II, the Strategic Arms Reduction Talks I, II and III, and the Fissile Material Cut-off Treaty, the Comprehensive Test Ban Treaty all followed. The state groupings such as the Wassenaar Group, the Zangar Commission and other formats followed. If the cyberdiplomatic realm follows suit, then once the consensus on how to conceptualise cyber war emerges, cyberdiplomatic efforts will follow. The following section presents some of these efforts and anticipates the potential future for some others.

Unsurprisingly there is a prevalent counter-argument. Lawson "argues that current contradictory tendencies are unproductive and even potentially dangerous. [His article] argues that the war metaphor and nuclear deterrence analogy are neither natural nor inevitable and that abandoning them would open up new possibilities for thinking more productively about the full spectrum of cybersecurity challenges, including the as-yet unrealized possibility of cyber war".[64] As with the nuclear non-proliferation debate, which leads and which follows is yet to be determined.

As within the pages of international relations journals, in the constructivist groups of works are to be found the most ventures away from states and organisations as actors. De Bruijn and Janssen highlight the need to bring individuals into the framework of assessment. They showcase that while everybody has heard of cybersecurity, still, the urgency and behaviour of individuals' actions do not reflect a high level of awareness.[65] The authors "discuss the challenges in framing policy on cybersecurity and offer strategies for better communicating cybersecurity. Communicating cybersecurity is confronted with paradoxes, which has resulted in society not taking appropriate measures to deal with the threats"[66] – which, as they attempt to highlight, can be best done by putting the issues in perspective.

Finally, there are of course works that attempt to demonstrate that even the virtual space designated for cyberspace is somewhat a construct. Barnard-Wills and Ashenden's article "examines the problems of construction of virtual space and current efforts to

[64] Lawson 2012.
[65] De Bruijn–Janssen 2017.
[66] De Bruijn–Janssen 2017.

secure this space political and technologically".[67] The authors present a model of cybersecurity discourse that is argued to be ungovernable, unknowable, a cause of vulnerability, inevitably threatening, and a home to threatening actors. It is in this vein that cyberdiplomacy has to operate, but there is a major challenge the authors present actors in the cyberdiplomatic realm with: should they attempt to conduct cyberdiplomacy in a cyber realm governed by this modus operandi or attempt to alter the fundamental underlying discourse? The pattern of behaviour, or even the ethics of which type of cyberdiplomacy has been conducted, can also be at least tangentially explored by examining its counter-part, war. Lucas argues that cyber "technologies offer prospects for lessening the indiscriminate destructive power of war, and enhance prospects for the evolution from state-centred conventional war, to discriminate law enforcement undertaken by international coalitions of peacekeeping forces".[68]

As Nye writes "norms can be suggested and developed by a variety of policy entrepreneurs. For example, the new non-governmental Global Commission on Stability in Cyberspace, chaired by former Estonian foreign minister Marina Kaljurand, has issued a call to protect the public core of the internet (defined to include routing, the domain name system, certificates of trust, and critical infrastructure)".69 Practitioners of cyberdiplomacy should well keep all this in mind.

Cyberdiplomacy in policy and practice

The theoretical differentiation is of course only one aspect of the review of the literature of cyberdiplomacy. Another key component is the review of literature that examines not theoretical issues, conceptualisations, definitional squabbles, or operationalised variables, but concrete state policies in concrete issues both at the state and at the intergovernmental level, namely the UN. The goal of this chapter is not to provide a detailed analysis of each, but rather to give a glimpse into the various national and international actors who are most involved in the world of cyberdiplomacy.

Here the literature is much more varied and vast, but much more dispersed as well. Larger case studies may incorporate some angles of diplomacy, some of which may be cyberdiplomacy, but that foray would be too large to present here. Instead, articles and reports are selected, which attempt to capture writings that grapple with some larger diplomatic or strategic issues and incorporate a significant cyber component as well. The prime actor of course is still the United States as a hegemon, but the U.S. has already been examined here in various ways.

As with many newer topics in international relations, the question of the rise of China is also examined in a cyberdiplomatic context. While this is not the most frequently studied question in cyberdiplomacy, the Covid-19 crisis has exacerbated the issue sig-

[67] Barnard-Wills–Ashenden 2012.
[68] Lucas 2010.
[69] Nye 2018.

nificantly. On the one hand, a battle of narratives is happening, with a significant prize at the end, including in electronic media and as such e-diplomacy. Further, the Covid-19 pandemic will most likely accelerate the digital transformation, leading to an increase in digital diplomacy, too. The question of this chapter is fundamentally the broader issue of cyberdiplomacy so only selected works are presented here.

One of the fundamental works on the topic attempts to reconcile the U.S.–China relationship in the cyber realm, with a focus on cybersecurity and as such, cyberdiplomacy. Lindsay's work highlights the "exaggerated fears about the paralysis of digital infrastructure and the loss of competitive advantage contribute to a spiral of mistrust in U.S.–China relations".70 But perhaps the most significant addition of Lindsay's work is the extension of the great power hegemonic struggle into the cyber realm. Lindsay argues that the "cyber version of the stability-instability paradox constrains the intensity of cyber interaction in the U.S.–China relationship – and in international relations more broadly – even as lesser irritants continue to proliferate".71 In line with how the most recent assessments of this great power competition are examined, Lindsay's words may serve as a warning to the West when he writes: "China is resorting to a strategy of international institutional reform, but it benefits too much from multistakeholder governance to pose a credible alternative".72 Of course, whether this is because of the fact that "although China also actively infiltrates foreign targets, its ability to absorb stolen data is questionable, especially at the most competitive end of the value chain, where the United States dominates",[73] or a more deeply enshrined co-optation strategy by Beijing remains to be seen.

The second major actor where cases of cyberdiplomacy can be studied is with Russia. The rhetoric that surrounds cyber campaigns may be a key indicator in studying cyberdiplomacy in the future. Here information shaping may play a key role. Deibert, Rohozinski, and Crete-Nishihata argue that "while the rhetoric of cyber war is often exaggerated, there have been recent cases of international conflict in which cyberspace has played a prominent role".[74] They study the case of Georgia and Russian actions in the conflict over the disputed territory of South Ossetia in August 2008. The outcomes they highlight: the unavoidable internationalisation of cyber conflicts, and the tendency towards magnifying unanticipated outcomes in cyber conflicts, both increase the need for a more robust response in the cyberdiplomatic realm as well.

The most frequently associated follow on topic after China and Russia has to do with terrorism, another widely studied topic in international relations. There usually are two approaches when it comes to cyberdiplomacy: the first concerns cyber terrorism, and the relevant aspects such as cyber deterrence detailed earlier in this chapter, or the use of social media and digital diplomacy as a second large bucket. Awan's study, "Cyber-Ex-

[70] Lindsay 2015b.
[71] Lindsay 2015b.
[72] Lindsay 2015b.
[73] Lindsay 2015b.
[74] Deibert et al. 2012.

tremism: Isis and the Power of Social Media" is a prime example.[75] Here the author argues that "these modern day tools are helping Isis spread their propaganda and ideology to thousands of online sympathizers across the world".[76] In fact, since the "Internet therefore is becoming the virtual playground for extremist views to be reinforced and act as an echo chamber",[77] cyberdiplomatic efforts must also combat these here. Another study explores the connection between cyber warriors and the state, and argues that some such groups, for example the Syrian Electronic Army, is "closely connected to the Syrian government in order to serve two main goals: serving as a public relations tool for the Syrian government to draw the world's attention to the official Syrian version of events taking place in the country and countering the impact of Syrian oppositional groups".[78]

Finally, the United Nations as an actor in cyberdiplomacy deserves a significant analysis. It is both a platform for action by member states through the Security Council and an independent actor through the Secretariat on its own, headed by the Secretary General. At the Security Council, the issues date back to 1998, when Russia first proposed a UN treaty to ban electronic and information weapons (this included its use for propaganda purposes). Russia, together with China and other members of the Shanghai Cooperation Organisation, has continued to push for a broad UN-based treaty, but in sharp contrast, the U.S. continues to view such a treaty as unverifiable.

When it comes to the Secretariat, the UN Secretary-General appointed a Group of Governmental Experts (UNGGE), which first met in 2004, and in July 2015 proposed a set of norms that was later endorsed by the G20. The UNGGE's success was great, but even so, it could not agree to its 2017 report, suggesting deep dissent. The UN Secretary-General, and other respected private and public entities, may also work on facilitating Track 1.5 and Track 2 dialogues. These are efforts that engage government and industry in discussions on cybersecurity outside the formal constraints of multilateral interactions. There is also an open-ended working group that studies this, and numerous other UN institutions, but other chapters in this work detail those more. Suffice to say, that at first blush, why the UN is such a large actor in the cyberdiplomatic world, is because the "legality of cyber attacks is generally approached from the use of force prohibition contained in Article 2(4) UN Charter".79

Conclusion

As we have seen in this review of the literature, there is a growing consensus that cyberdiplomacy deserves a study on its own. The evolution of the literature clearly demonstrates conceptual advances, distinguishing between cyberdiplomacy and digital diplomacy. It is also clear that the initial literature on cyberdiplomacy follows the

[75] Awan 2017.
[76] Awan 2017.
[77] Awan 2017.
[78] Al-Rawi 2014.
[79] Buchan 2012.

traditional international relations paradigms, and can be grouped around realist, liberal and constructivist thinking. The United Nations, as an independent actor and also as a forum for intergovernmental rule and norm setting, deserves separate studies, which is not part of this literature review. Its role will most likely be extremely important in the future of cyberdiplomacy.

At the state level, even for an organisation as powerful as the U.S. Government, the cyber realm brings with it notable challenges and issues. When it comes to the military, it must realise that "cyber operations do not fit neatly into this paradigm because although they are 'non-forceful' (that is, non-kinetic), their consequences can range from mere annoyance to death".[80] And when it comes to cyberdiplomacy, the State Department and policy makers must understand that "there is no international consensus on a precise definition of a use of force, in or out of cyberspace".81

Finally, what this literature review only touched upon due to space constraints, is the role of non-governmental organisations and individuals. How does civil society fit into the world of cyberdiplomacy? Who and when will challenge the supremacy of the state as an actor in the world of cyberdiplomacy? Does the problem of attribution hinder or accelerate this process? These are all questions that future research must answer as we determine where we go from here.

References

Abomhara, Mohamed – Køien, Geir M. (2015): Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security and Mobility,* Vol. 4, No. 1. 65–88.

Al-Rawi, Ahmed K. (2014): Cyber warriors in the Middle East: The case of the Syrian Electronic Army. *Public Relations Review,* Vol. 40, No. 3. 420–428.

Awan, Imran (2017): Cyber-Extremism: Isis and the Power of Social Media. *Society,* Vol. 54, No. 2. 138–149.

Barford, Paul – Dacier, Marc – Dietterich, Thomas G. – Fredrikson, Matt – Giffin, Jon – Jajodia, Sushil – Jha, Somesh – Li, Jason – Liu, Peng – Ning, Peng – Ou, Xinming – Song, Dawn – Strater, Laura – Swarup, Vipin – Tadda, George – Wang, Cliff – Yen, John (2010): Cyber SA: Situational awareness for cyber defense. *Advances in Information Security,* Vol. 46, No. 3. 3–13.

Barnard-Wills, David – Ashenden, Debi (2012): Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture,* Vol. 15, No. 2. 110–123.

Barrinha, André – Renard, Thomas (2017): Cyber-diplomacy: the making of an international society in the digital age. *Journal of Global Affairs,* Vol. 3, No. 4–5. 353–364.

Betts, Richard K. (2002): The Soft Underbelly of American Primacy: Tactical Advantages of Terror. *Political Science Quarterly,* Vol. 117, No. 1.

Brunst, Philip W. (2010): Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet. In Wade, Marianne – Maljević, Almir eds.: *A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications.* New York, Springer. 51–78.

[80] Schmitt 2011.
[81] Schmitt 2011.

Buchan, Russell (2012): Cyber attacks: Unlawful uses of force or prohibited interventions? *Journal of Conflict and Security Law,* Vol. 17, No. 2. 212–227.

Cavelty, Myriam D. (2012): *The Militarisation of Cyberspace: Why Less May Be Better.* 4th International Conference on Cyber Conflict, CYCON 2012.

CCDCOE (2017): *Tallinn Manual 2.0.* Source: https://ccdcoe.org/research/tallinn-manual/ (Accessed: 02.04.2020.)

Chen, Yu – Hwang, Kai – Ku, Wei-Shinn (2007): Collaborative Detection of DDoS Attacks over Multiple Network Domains. *IEEE Transactions on Parallel and Distributed Systems,* Vol. 18, No. 12. 1649–1662.

Clark, Richard A. – Knake, Robert K. (2010): *Cyber War: The Next Threat to National Security and What to Do About It.* New York, HarperCollins.

Cull, Nicholas J. (2010): Public diplomacy: Seven lessons for its future from its past. *Place Branding and Public Diplomacy,* Vol. 6, No. 1. 11–17.

Cyberdiplomacy (2019): Cyber Diplomacy: Governance Beyond Government. *CyberPeace Alliance,* 12 October 2019. Source: https://medium.com/@cyberpeacealliance/cyber-diplomacy-governance-beyond-government-e8b92effff8f (Accessed: 02.04.2020.)

D'Amico, Anita – Whitley, Kirsten – Tesone, Daniel – O'Brien, Brianne – Roth, Emilie (2005): Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting,* Vol. 49, No. 3. 229–233.

De Bruijn, Hans – Janssen, Marijn (2017): Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly,* Vol. 34, No. 1. 1–7.

Deibert, Ronald J. – Rohozinski, Rafal – Crete-Nishihata, Masashi (2012): Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue,* Vol. 43, No. 1.

Denning, Dorothy E. (2014): Framework and principles for active cyber defense. *Computers and Security,* Vol. 40. 108–113.

Dinstein, Yoram (2012): The Principle of Distinction and Cyber War in International Armed Conflicts. *Journal of Conflict and Security Law,* Vol. 17, No. 2. 261–277.

Droege, Cordula (2012): Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross,* Vol. 94, No. 886. 533–578.

Elliott, David (2011): Deterring Strategic Cyberattack. *IEEE Security and Privacy,* Vol. 9, No. 5. 36–40.

Eom, Jung-Ho – Kim, NamUk – Kim, Sunghwan – Chung, Tai-Myoung Myoung (2012): *Cyber military strategy for cyberspace superiority in cyber warfare.* 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec.

Farwell, James P. – Rohozinski, Rafal (2011): Stuxnet and the Future of Cyber War. *Survival,* Vol. 53, No. 1. 23–40.

Farwell, James P. – Rohozinski, Rafal (2012): The New Reality of Cyber War. *Survival,* Vol. 54, No. 4. 107–120.

Fung, Brian (2013): How Many Cyberattacks Hit the United States Last Year? *Nextgov,* 08 March 2013. Source: www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/ (Accessed: 02.04.2020.)

Geers, Kenneth (2010): The Challenge of Cyber Attack Deterrence. *Computer Law and Security Review,* Vol. 2, No. 3. 298–303.

Gjelten, Tom (2010): Shadow Wars: Debating Cyber 'Disarmament'. *World Affairs,* Vol. 173, No. 4. 33–42.

Golling, Mario – Stelte, Björn (2011): *Requirements for a future EWS – Cyber Defence in the internet of the future.* 2011 3rd International Conference on Cyber Conflict.

Gutzwiller, Robert S. – Fugate, Sonny – Sawyer, Benjamin D. – Hancock, P. A. (2015): The Human Factors of Cyber Network Defense. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting,* Vol. 59, No. 1.

Hausken, Kjell (2006): Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy,* Vol. 25, No. 6. 629–665.

Hausken, Kjell (2007): Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy,* Vol. 26, No. 6.

Healey, Jason – Jenkins, Neil (2019): Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing. In Minárik, Tomáš – Alatalu, Siim – Biondi, Stefano – Signoretti, Massimiliano – Tolga, Ihsan – Visky, Gábor eds.: *11th International Conference on Cyber Conflict: Silent Battle.* Tallinn, NATO CCD COE Publications. 123–142.

Heckman, Kristin E. – Walsh, Michael J. – Stech, Frank J. – O'Boyle, Todd A. – Dicato, Stephen R. – Herber, Audra F. (2013): Active cyber defense with denial and deception: A cyber-wargame experiment. *Computers and Security,* Vol. 37. 72–77.

Hernandez-Ardieta, Jorge L. – Tapiador, Juan – Suarez-Tangil, Guillermo (2013): *Information Sharing Models for Cooperative Cyber Defence.* Tallinn, 5th International Conference on Cyber Conflict, CYCON.

Herrington, Lewis – Aldrich, Richard (2013): The Future of Cyber-Resilience in an Age of Global Complexity. *Politics,* Vol. 33, No. 4. 299–310.

Hua, Jian – Bapna, Sanjay (2012): How Can We Deter Cyber Terrorism? *Information Security Journal,* Vol. 21, No. 2. 102–114.

Hua, Jian – Bapna, Sanjay (2013): The economic impact of cyber terrorism. *The Journal of Strategic Information Systems,* Vol. 22, No. 2. 175–186.

Jabbour, Kamaal T. – Ratazzi, Paul E. (2012): Does the United States Need a New Model for Cyber Deterrence? In Lowther, Adam B. ed.: *Deterrence.* New York, Palgrave Macmillan.

Junio, Timothy J. (2013): How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate. *Journal of Strategic Studies,* Vol. 36, No. 1. 125–133.

Knapp, Kenneth J. – Boulton, William R. (2006): Cyber-warfare threatens corporations: Expansion into commercial environments. *Information Systems Management,* Vol. 23, No. 2. 76–87.

Konkel, Frank R. (2018): Pentagon Thwarts 36 Million Email Breach Attempts Daily. *Nextgov,* 11 January 2018. Source: www.nextgov.com/cybersecurity/2018/01/pentagon-thwarts-36-million-email-breach-attempts-daily/145149/ (Accessed: 02.04.2020.)

Kotenko, Igor (2005): *Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in Internet.* 2005 Simulation in Wider Europe – 19th European Conference on Modelling and Simulation, ECMS 2005.

Kshetri, Nir (2005): Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management,* Vol. 11, No. 4. 541–562.

Kurbalija, Jovan (2016): *An Introduction to Internet Governance.* DiploFoundation, 7th edition.

Lawson, Sean (2012): Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday,* Vol. 17, No. 7.

Liff, Adam P. (2012): Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies,* Vol. 35, No. 3. 401–428.

Lindsay, Jon R. (2015a): Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity,* Vol. 1, No. 1. 53–67.

Lindsay, Jon R. (2015b): The Impact of China on Cybersecurity: Fiction and Friction. *International Security,* Vol. 39, No. 3. 7–47.

Liu, Peng – Zang, Wanyu – Yu, Meng (2005): Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Transactions on Information and System Security,* Vol. 8, No. 1. 78–118.

Lucas, George R., Jr. (2010): Postmodern War. *Journal of Military Ethics,* Vol. 9, No. 4. 289–298.

Lynn, William J. III (2010): Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs,* Vol. 89, No. 5. 97–108.

McGraw, Gary (2013): Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies,* Vol. 36, No. 1. 109–119.

McQueen, Miles A. – Boyer, Wayne F. (2009): *Deception Used for Cyber Defense of Control Systems.* 2009 2nd Conference on Human System Interactions, HSI 2009. 624–631.

Mullins, Barry E. – Lacey, Timothy H. – Mills, R. F. – Trechter, Joseph M. – Bass, Samuel D. (2007): How the Cyber Defense Exercise Shaped an Information-Assurance Curriculum. *IEEE Security and Privacy,* Vol. 5, No. 5.

Mureşan, Radu Constantin (2017): Current approaches of diplomacy in the cyberspace. *Studia Universitatis Babeş-Bolyai,* Vol. 62, No. 2.

NATO (2016): *Cyber Defence Pledge.* Source: www.nato.int/cps/en/natohq/official_texts_133177.htm (Accessed: 02.04.2020.)

NATO (2019): *Washington Treaty of 1949.* Source: www.nato.int/cps/en/natolive/official_texts_17120.htm (Accessed: 02.04.2020.)

Nazir, Sajid – Patel, Shushma – Patel, Dilip (2017): Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers and Security,* Vol. 70. 436–454.

Nye, Joseph S., Jr. (2011a): Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly,* Vol. 5, No. 4. 18–38.

Nye, Joseph S., Jr. (2011b): *The Future of Power.* New York, PublicAffairs.

Nye, Joseph S., Jr. (2016): Deterrence and Dissuasion in Cyberspace. *International Security,* Vol. 41, No. 3. 44–71.

Nye, Joseph S., Jr. (2018): *How Will New Cybersecurity Norms Develop?* The Belfer Center for Science and International Affairs, Harvard University. Source: www.belfercenter.org/publication/how-will-new-cybersecurity-norms-develop (Accessed: 20 May 2020.)

O'Connell, Mary E. (2012): Cyber Security without Cyber War. *Journal of Conflict and Security Law,* Vol. 17, No. 2. 187–209.

Power, Marcus (2007): Digitized virtuosity: Video War Games and Post-9/11 Cyber-Deterrence. *Security Dialogue,* Vol. 38, No. 2.

Powers, Shawn M. – Jablonski, Michael (2015): *The Real Cyber War: The Political Economy of Internet Freedom.* Urbana–Chicago–Springfield, University of Illinois Press.

Rid, Thomas (2012): Cyber War Will Not Take Place. *Journal of Strategic Studies,* Vol. 35, No. 1. 5–32.

Robinson, Michael – Jones, Kevin I. – Janicke, Helge (2015): Cyber warfare: Issues and challenges. *Computers and Security,* Vol. 49. 70–94.

Sangster, Benjamin – O'Connor, T. J. – Cook, Thomas – Fanelli, Robert – Dean, Erik – Adams, William J. – Morrell, Chris – Conti, Gregory (2009): *Toward Instrumenting Network Warfare Competitions to Generate Labeled Datasets.* 2nd Workshop on Cyber Security Experimentation and Test, CSET 2009.

Schmitt, Michael N. (2011): Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review,* Vol. 56, No. 3.

Schreiber-Ehle, Sabine – Koch, Wolfgang J. (2012): *The JDL model of data fusion applied to cyber-defence – A review paper.* 2012 Workshop on Sensor Data Fusion: Trends, Solutions, Applications, SDF 2012.

Sharma, Amit (2010): Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis,* Vol. 34, No. 1.

Sharp, Travis (2017): Theorizing cyber coercion: The 2014 North Korean operation against Sony. *Journal of Strategic Studies,* Vol. 40, No. 7. 898–926.

Skopik, Florian – Settanni, Giuseppe – Fiedler, Roman (2016): A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers and Security,* Vol. 60. 154–176.

Sridhar, Siddharth – Govindarasu, Manimaran (2014): Model-Based Attack Detection and Mitigation for Automatic Generation Control. *IEEE Transactions on Smart Grid,* Vol. 5, No. 2. 580–591.

Stone, John (2013): Cyber War Will Take Place! *Journal of Strategic Studies,* Vol. 36, No. 1. 101–108.

Taddeo, Mariarosaria (2018): The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology,* Vol. 31. 339–355.

Tor, Uri (2017): 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence. *Journal of Strategic Studies,* Vol. 40, No. 1–2. 92–117.

Turns, David (2012): Cyber Warfare and the Notion of Direct Participation in Hostilities. *Journal of Conflict and Security Law,* Vol. 17, No. 2. 279–297.

Uma, M. – Padmavathi, Ganapathi (2013): A survey on various cyber attacks and their classification. *International Journal of Network Security,* Vol. 15, No. 5. 390–396.

U.S. Department of State (2020): *Office of the Coordinator for Cyber Issues.* Source: www.state.gov/bureaus-offices/bureaus-and-offices-reporting-directly-to-the-secretary/office-of-the-coordinator-for-cyber-issues/ (Accessed: 22.05.2020.)

U.S. Department of the Treasury (2018): *Treasury Sanctions Russian Federal Security Service Enablers.* Source: https://home.treasury.gov/news/press-releases/sm0410 (Accessed: 22.05.2020.)

Valeriano, Brandon – Maness, Ryan C. (2015): *Cyber War versus Cyber Realities: Cyber Conflict in the International System.* Oxford, Oxford University Press.

Walker-Roberts, Steven – Hammoudeh, Mohammad – Dehghantanha, Ali (2018): A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. *IEEE Access,* Vol. 8. 25167–25177.

Yu, Jia – Ren, Kui – Wang, Cong (2016): Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates. *IEEE Transactions on Information Forensics and Security,* Vol. 11, No. 6. 1362–1375.

Whitehouse (2018): *Statement from the Press Secretary.* Source: www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ (Accessed: 22.05.2020.)

VÁKÁT OLDAL

Anna Molnár

European Union – Cybersecurity

Introduction

It is a commonplace to state that European societies, governmental and private sectors are increasingly dependent on digital technologies. Electronic networks and information systems have developed to be part of our daily lives. In recent years, digital technology has become an essential tool on which not only all sectors of the economy, but also every area of our lives rely. Highlighting only a few of them, such as electricity or transport networks, production and financial processes, and health care systems, a significant degree of interdependence and interconnection can be observed.

As a result, the European economies, governmental or defence infrastructures, and in this context, even the functioning of democracy, European values and liberties can be threatened by malicious cyber activities. To a large extent, Europe's security depends on the cyber resilience of Member States and the EU institutions: the ability to prepare for and to respond to the ever-changing and growing intensity of cyber threats. Today, many business models rely on the smooth operation of the Internet and information systems. In parallel, the economic impact of cybercrime is steadily increasing. In addition to racketeering, many other threats are a major challenge for European economic and political actors. In today's computer age, the protection of personal data also plays a crucial role in the implementation of cybersecurity.

The widely used term of cybersecurity is not limited to network and information security in the EU's policy circles. According to a report prepared by the European Court of Auditors, the cybersecurity ecosystem includes any illegal activity realised by the use of digital technologies in cyberspace. It refers to cybercrimes like computer virus attacks and non-cash payment fraud, and the dissemination of online child sexual abuse material. It includes disinformation campaigns to influence online debate and suspected electoral interference. According to the definition of Europol, a connection between cybercrime and terrorism can be observed.[82] Not only government institutions, but also European Internet users and companies have experienced several cybersecurity incidents. It is crucial to guarantee that devices and networks are protected to deter cyberattacks. Despite the fact that the European Union has started to strengthen its comprehensive cybersecurity governance, the analysis prepared by the European Court of Auditors has highlighted several weaknesses and shortfalls in the governance and in the legislative framework in 2019. The complex ecosystem of the EU's cybersecurity policy is closely linked to internal policy areas; regarding internal policy areas, it covers justice and

[82] European Court of Auditors 2019, 6.

home affairs, the digital single market and research policies as well. The EU has become increasingly active in external policy areas as well, and cybersecurity is closely linked to diplomacy, and to security and defence policy.[83]

The European Union's strategic framework and regulations

The strategic framework since 2000

The EU has been an observer organisation to the Council of Europe's Cybercrime Convention Committee since 2001 (the Budapest Convention), which provided a framework for the promotion of international cooperation and legislation against cybercrime. Despite the growing awareness, the threats and challenges related to cybersecurity were only briefly mentioned by the EU's strategies during the first decade of the 21st century. In 2003, the European Security Strategy already implicitly referred to cybersecurity. The document developed by Javier Solana, High Representative for the Common Foreign and Security Policy, only highlighted the danger of terrorist movements connected by electronic networks.[84] In 2005, the European Commission published a comprehensive strategy entitled *i2010: A European Information Society for growth and employment.* The new strategy aimed to promote the development of an open and competitive digital economy and emphasised the key role of ICT (information and communication technology) in social inclusion and quality of life. The document mentions the issue of security in many cases. In the interests of a secure and reliable ICT, the European Commission articulated the need to develop a Strategy for a Secure Information Society.[85]

Additionally, the 2008 review of the European Security Strategy has already addressed the basic issues of cybersecurity in a short section. The document emphasised that modern economies are highly dependent on critical infrastructure such as the Internet. Internet-based crime was mentioned in the Strategy for a Secure European Information Society, adopted in 2006. However, as a result of attacks on Member States' government or private IT systems, a new dimension related to a potential new economic, political and military weapon was added. The document underlined the need for more work to explore a comprehensive EU approach, raise awareness and enhance international cooperation.[86] The European Union's Internal Security Strategy, adopted in 2010, drew attention to the dangers of cybercrime in the Union.[87]

In May 2010, after the Lisbon Strategy, the European Commission launched the Europe 2020 Strategy, which aimed at reducing vulnerability and increasing competitiveness.[88] As one of the flagship initiatives of the new strategy, the European Commission

[83] European Court of Auditors 2019, 12.
[84] Council of the European Union 2003, 30.
[85] European Commission 2005.
[86] Council of the European Union 2008, 5.
[87] Council of the European Union 2010, 7.
[88] Kovács 2018, 85.

has launched the Digital Agenda for Europe (DAE). The agenda aimed to make the use of information and communication technologies (ICT) a key factor in achieving the goals set in the Europe 2020 Strategy. The European Commission has built a Digital Single Market Strategy on three pillars to ensure a fair, open and secure digital environment: 1. ensuring better access to digital goods and services for consumers and businesses across Europe; 2. creating the right conditions for digital networks and services; and 3. maximising the growth potential of the digital economy.[89]

In particular, the EU intended to respond adequately to challenges in the digital domain, such as the fragmentation of the digital market, interoperability issues, the very rapid spread of cybercrime, the low level of R&D and investment in it, or the low level of digital literacy in many regions of the EU.[90]

Table 1: Strategy Papers of the European Union on Cybersecurity

Year	Strategy Papers of the European Union
2003	European Security Strategy
2005	I2010: European Information Society for growth and employment
2006	A strategy for a secure European information society
2008	Report on the Implementation of the European Security Strategy. Providing Security in a Changing World
2010	Internal Security Strategy for the European Union. Towards a European Security Mode
2010	European Commission: A Digital Agenda for Europe
2013	Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
2014	EU Cyber Defence Policy Framework
2015	Council Conclusions on Cyber Diplomacy
2015	Digital Single Market Strategy for Europe
2016	Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy
2017	Resilience, Deterrence and Defence: Building strong cybersecurity for the EU
2018	EU Cyber Defence Policy Framework

Source: Compiled by the author based on Rehrl 2018, 26.

The EU began developing its first comprehensive cybersecurity strategy in 2012–2013. All of this happened at a time when developed countries were realising the strategic importance of cybersecurity challenges. Compared to NATO, whose first strategies (2008, 2011) focused solely on protecting its own IT network, the first EU strategy covered almost all areas of EU competences.[91]

Following the entry into force of the Lisbon Treaty, the European External Action Service and the European Commission, under the leadership of EU High Representative for Foreign Affairs and Security Policy Catherine Ashton, also worked together to draft the joint communication. In 2013 the *Cybersecurity Strategy of the European Union:*

[89] European Commission 2020.
[90] Kovács 2018, 86.
[91] Rehrl 2018, 18.

An Open, Safe and Secure Cyberspace was adopted by the European External Action Service and the European Commission. This document first mentioned the need for a coherent EU international cyberspace policy and cyber defence objectives. One of the main goals and principles of the strategy was to uphold EU core values and promote a peaceful, open and transparent use of cyber technologies.[92]

The implementation of the strategy was primarily the responsibility of some Directorates-General of the European Commission. The Directorate-General for Content, Technology and Communication Networks (DG CNETC) was responsible for legislation, industrial policy and research and development in the new cyber areas. The Directorate-General for Migration and EU Home Affairs (DG HOME) has been responsible for shaping the cyber law enforcement policy and promoting cooperation between Member States in this area.

The principles set out in the strategy were in line with the general principles and values of the EU: 1. the core values of the European Union apply to the digital world as much as to the physical world; 2. protection of fundamental rights, freedom of expression, personal data and privacy; 3. access for all; 4. democratic and efficient multi-stakeholder governance; 5. shared responsibility to ensure security.

However, the strategy sets out five priorities: 1. achieving resilience to cyberattacks; 2. a drastic reduction in cybercrime; 3. developing cyber defence policy and capabilities for the Common Security and Defence Policy (CSDP); 4. development of cybersecurity industry and technological resources; 5. establishing a coherent international policy on cyberspace for the European Union and promoting the Union's core values.[93]

EU Cyber Defence Policy Framework (2014)

The European External Action Service (EEAS) is responsible for promoting cyber defence activities and developing international cyber policy goals including cyberdiplomacy and strategic communication, and hosts intelligence and analysis centres.[94] According to the European Council Conclusions on CSDP in December 2013, the cyber defence policy framework was developed by the EEAS together with the European Commission and the European Defence Agency.[95] Under the leadership of the EEAS, the EU Cyber Defence Policy Framework was completed in 2014.

The document established the following objectives:

- supporting the development of Member States' cyber defence capabilities in areas related to the common security and defence policy
- enhancing the protection of communication and information networks used by the EEAS in the field of CSDP

[92] European Commission 2013.
[93] European Commission 2013.
[94] European Court of Auditors 2019, 10.
[95] European Council 2013.

– promoting civil-military cooperation and synergies with the wider EU cyber policies to address the new challenges
– help cooperation with the private sector on cyber defence capability development
– improving training, education and exercise opportunities
– enhancing cooperation with relevant international partners, in particular with NATO[96]

Directive on the security of network and information systems (2016)

The European Union adopted the first EU-wide legislation on cybersecurity in 2016 with the Directive (EU) 2016/1148 of the European Parliament and the Council on the security of network and information systems (NIS). The NIS directive had to be transposed into national laws of the EU Member States by 9 May 2018 and the units providing essential services had to be identified by 9 November 2018.

The aim of the NIS directive is to introduce comprehensive measures that can increase the level of security of network and information systems and services, which play a vital role in the Union's economy and society. Implementing the directive will enable EU countries to prepare for and respond to cyberattacks. To this end, it has become necessary at Member State level to 1. designate competent authorities; 2. set up Computer Security Incident Response teams (CSIRTs); and 3. adopt national cyber security strategies. The measures introduced will strengthen cooperation at both strategic and technical levels in the European Union.[97]

However, the Directive obliges essential and digital service providers (such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructures) to take appropriate security measures and to inform the relevant national authorities of serious incidents.

Under the new rules, EU Member States must also adopt national cybersecurity strategies for network and information systems. Strategies at the national level should include the following issues:

"(a) the objectives and priorities of the national strategy on the security of network and information systems;

(b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;

(c) the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;

(d) an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems;

(e) an indication of the research and development plans relating to the national strategy on the security of network and information systems;

[96] Council of the European Union 2014.
[97] European Parliament and Council 2016.

(f) a risk assessment plan to identify risks;

(g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems."[98]

It is the responsibility of the national competent authorities to monitor the application of the Directive. To this end, national authorities should assess the level of the security of network and information systems. They should also participate in the work of the Cooperation Group, which is composed of representatives of the Member States, the Commission and European Commission and the European Network and Information Security Agency (ENISA). The national competent authorities shall inform the public about individual incidents where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.[99]

Global Strategy (2016)

The European Union's Global Strategy for Foreign and Security Policy (hereinafter: Global Strategy), adopted in 2016, has already addressed the issue of cybersecurity in details. The strategy calls for the strengthening of the EU as a security community and the development of capabilities for the protection of EU citizens and the response to external crises. In addition, the interoperability of civilian and military capabilities needs to be strengthened.

The Global Strategy emphasises that the Union will focus on cybersecurity in the future and will be able to respond more effectively to cyber threats. With this new strategy, the EU intended to address open, free and secure cyberspace in all policy areas.[100]

Cyber Security in the Global Strategy

"The EU will increase its focus on cyber security, equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace. This entails strengthening the technological capabilities aimed at mitigating threats and the resilience of critical infrastructure, networks and services, and reducing cybercrime. It means fostering innovative information and communication technology (ICT) systems which guarantee the availability and integrity of data, while ensuring security within the European digital space through appropriate policies on the location of data storage and the certification of digital products and services. It requires weaving cyber issues across all policy areas, reinforcing the cyber elements in CSDP missions and operations, and further developing platforms for cooperation. The EU will support political, operational and technical cyber cooperation between Member States, notably on analysis and consequence management, and foster shared assessments between EU structures and the relevant institutions in Member States. It will enhance its cyber security cooperation with core partners such as the US and

[98] European Parliament and Council 2016.
[99] European Parliament and Council 2016.
[100] European External Action Service 2016.

NATO. The EU's response will also be embedded in strong public-private partnerships. Cooperation and information-sharing between Member States, institutions, the private sector and civil society can foster a common cyber security culture, and raise preparedness for possible cyber disruptions and attacks."[101]

Review of the Cyber Security Strategy (2017)

As the goals set in the 2013 cybersecurity strategy were not always met and changes in cybersecurity threats have taken place to such an extent in recent years, it has become inevitable to review the first strategy and develop a new one. Disruptive computer operations against critical infrastructures, democratic institutions and the Internet of Things (IoT), as well as large-scale botnet attacks and global ransomware infections such as "WannaCry" and "NotPetya" drew attention to cyber risks and the need for proactive action at EU level.[102]

Under the leadership of the European Commission, the revision of the EU cybersecurity strategy was completed in 2017. The joint communication from the EC and the High Representative for Foreign Affairs and Security Policy to the European Parliament and the Council was entitled *Resilience, Deterrence, Defence: Building Strong Cybersecurity for the EU.*[103]

The strategy highlights as it follows:
"Cybersecurity is critical to both our prosperity and our security. As our daily lives and economies become increasingly dependent on digital technologies, we become more and more exposed. Cybersecurity incidents are diversifying both in terms of who is responsible and what they seek to achieve. Malicious cyber activities not only threaten our economies and the drive to the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values. Our future security depends on transforming our ability to protect the EU against cyber threats: both civilian infrastructure and military capacity rely on secure digital systems. This has been recognised by the June 2017 European Council, as well as in the Global Strategy on Foreign and Security Policy for the European Union."[104]

The document underlines that: "While Member States remain responsible for national security, the scale and cross-border nature of the threat make a powerful case for EU action providing incentives and support for Member States to develop and maintain more and better national cybersecurity capabilities, while at the same time building EU-level capacity."[105]

[101] European External Action Service 2016, 21–22.
[102] Rehrl 2018, 23.
[103] European Commission 2017a.
[104] European Commission 2017a.
[105] European Commission 2017a.

The new strategy proposed new measures to ensure the EU's resilience, deterrence and protection against cyberattacks. These proposals included the strengthening of the European Network and Information Security Agency (ENISA), the development of a voluntary EU cybersecurity certification framework to enhance the cybersecurity of digital products and services, and a plan for rapid, coordinated response to large-scale cybersecurity incidents and crises. The Commission proposed a permanent mandate for the ENISA, which, having a strong advisory role on policy development and implementation, will support Member States, EU institutions and businesses in key areas. The joint communication highlights cyber defence as a priority for EU actions. According to the document, the 2014 EU cyber defence policy framework needed to be renewed.[106]

The 2017 Cybersecurity Package and the digital single market strategy

In September 2017, in his annual speech at the European Parliament (State of the Union), President Jean-Claude Juncker highlighted the importance of the progress during the previous three years in keeping Europeans safe online. But he also stated that Europe was not well prepared against cyberattacks. Jean-Claude Juncker argued strongly in favour of establishing new tools against cyberattacks, such as the European Cybersecurity Agency. The European Commission and the High Representative proposed a Cybersecurity Package, a wide-ranging set of measures to strengthen cybersecurity in the EU. This included a proposal for an EU Cybersecurity Agency, a new EU-wide certification framework for products and services in the digital world, organisation of yearly pan-European cybersecurity exercises. According to Federica Mogherini, High Representative of the Union, the EU is developing an international cyber policy supporting an open, free and secure cyberspace. It also promotes all efforts in order to establish "norms of responsible state behaviour, apply international law and confidence building measures in cybersecurity".[107]

Cybersecurity Act

As part of the cybersecurity package adopted in September 2017, the realisation of a new legislation on cybersecurity (known as the Cybersecurity Act), which is one of the priorities of the Digital Single Market Strategy, has begun. In September 2018, the European Commission proposed the establishment of a European Cybersecurity Industrial, Technology and Research Competence Centre and a network of cybersecurity competence centres.[108]

[106] European Commission 2017a.
[107] European Commission 2017b.
[108] European Commission 2018.

The priority of the Digital Single Market Strategy (2015) was to remove barriers to online transactions and provide consumers with secure access to products and services.[109] The new European Cybersecurity Act was proposed in 2017 and was adopted in 2019 by the European Parliament and the Council. The new legislation covered the following areas: setting the new mandate of ENISA, the EU Agency for Cybersecurity, and establishing the European cybersecurity certification framework. ENISA will support Member States in effective response to cyberattacks in the new cybersecurity certification framework. With the entry into force of the Cybersecurity Act, the ENISA, the EU Agency for Cybersecurity will have a permanent mandate, strengthened responsibilities and increased resources.[110]

Cyber Defence and Permanent Structured Cooperation (PESCO)

From 2017, the process of implementing the permanent structured cooperation (PESCO) provided by the Lisbon Treaty began with the participation of 25 Member States. The participating Countries have committed themselves to stepping up their efforts in the field of cyber defence as well. Since 2017, 6 cyber-related PESCO projects have been launched:

1. European Secure Software defined Radio (ESSOR)
2. Cyber Threats and Incident Response Information Sharing Platform
3. Cyber Rapid Response Teams and Mutual Assistance in Cyber Security
4. Strategic Command and Control (C2) Systems for CSDP Missions and Operations
5. European High Atmosphere Airship Platform (EHAAP) – Persistent Intelligence, Surveillance and Reconnaissance (ISR) Capability
6. One Deployable Special Operations Forces (SOF) Tactical Command and Control (C2) Command Post (CP) for Small Joint Operations (SJO) – (SOCC) for SJO.[111]

European Union cyber defence policy framework (2018)

In October 2018, the European Council called for measures able to respond to and deter cyberattacks and to build strong cybersecurity in the EU in order to strengthen its capacities. In view of the changing security challenges, the Council adopted a revised version of the EU cyber defence policy framework in October 2018. The updated version of the framework identified priority areas for cyber defence and clarified the roles of actors.

Scope and Objectives

"To respond to changing security challenges, the EU and its Member States have to strengthen cyber resilience and to develop robust cyber security and defence capabilities.

[109] European Commission 2015.
[110] European Parliament and Council 2019.
[111] EU Cyber Direct 2019; Council of the European Union 2019a.

The EU Cyber Defence Policy Framework (CDPF) supports the development of cyber defence capabilities of EU Member States as well as the strengthening of the cyber protection of the EU security and defence infrastructure, without prejudice to national legislation of Member States and EU legislation, including, when it is defined, the scope of cyber defence.

Cyberspace is the fifth domain of operations, alongside the domains of land, sea, air, and space: the successful implementation of EU missions and operations is increasingly dependent on uninterrupted access to a secure cyberspace, and thus requires robust and resilient cyber operational capabilities.

The objective of the updated CDPF is to further develop EU cyber defence policy by taking into account relevant developments in other relevant fora and policy areas and the implementation of the CDPF since 2014. The CDPF identifies priority areas for cyber defence and clarifies the roles of the different European actors, whilst fully respecting the responsibilities and competences of Union actors and the Member States as well as the institutional framework of the EU and its decision-making autonomy."[112]

The document refers to the implementation of the goals and priorities set in the 2016 Global Strategy and the Joint Declaration on EU–NATO Cooperation. However, it emphasised that a number of other EU policies also contribute to achieving the objectives of cyber defence policy. This policy framework also takes into account regulations in civil areas (e.g. the Network and Information Security Directive) in order to contribute to the EU's strategic autonomy also in the area of cyberspace.

The policy framework highlights that, in accordance with the Council Conclusions on Cybersecurity of November 2017, there are growing linkages between the areas of cybersecurity and defence, and that there is a need to encourage cooperation between civilian and military incident response communities. The Council document emphasised that in a particularly serious cyber incident or crisis, the Solidarity Clause and/or the Mutual Assistance Clause of the Lisbon Treaty could also be activated.[113]

The policy framework identifies six priority areas: 1. developing cyber defence capabilities, 2. protecting EU CSDP communication and information networks; 3. training and exercises; 4. research and technology; and 5. civil-military cooperation; 6. international cooperation.[114]

The EU's institutional framework regarding cybersecurity

Due to the comprehensive nature of this issue, practically all institutions, bodies and agencies in the European Union are involved in the preparation and implementation of the cybersecurity policy.

[112] Council of the European Union 2018.
[113] Council of the European Union 2018, 6.
[114] Council of the European Union 2018, 8.

Table 2: Cybersecurity in the EU: Areas of Responsibility and institutional framework

Single Market	Freedom, security and justice	CFSP: Cyber Diplomacy	CSDP: Cyber Defence
European Commission DGs		EEAS	
CERT-EU	Europol (EC3)	SIAC (EU INTCEN, Hybrid Fusion Cell, EUMS INT)	
ENISA	Eurojust	EU SITROOM	
CSIRT network	EU-LISA	ESDC	
			EDA
			GSA

Source: Compiled by the author based on Bendiek 2018, 4.

European Commission

The European Commission intends to strengthen cybersecurity capabilities. It also initiates and promotes policy-making and legislative processes in this field. The main Directorates-General (DG) responsible for areas related to cybersecurity are DG CONNECT (Communications Networks, Content and Technology) and DG Migration and HOME (cybercrime). The Directorate-General CONNECT's main tasks are linked to developing a digital single market and promoting policy-making processes related to cybersecurity. The Directorate-General Migration and HOME is responsible for initiating and developing cybercrime policy. The Directorate-General for Informatics (DG DIGIT) provides digital services for departments of the European Commission and other EU institutions. DIGIT hosts CERT-EU (Computer Emergency Response Team).[115] DG Human Resources and Security is responsible for the Commission's staff, information and assets. It also provides investigations regarding incidents that cover counter-intelligence and counter-terrorism activities as well.[116]

Computer Emergency Response Team (CERT-EU)

In the Digital Agenda for Europe adopted in 2010, the European Commission decided to establish a Computer Emergency Response Team for the EU institutions (CERT-EU) supporting all Union institutions, bodies and agencies. According to the Agenda, these CERTs had to be set up not only at EU level but also at Member State level in order to have a network of national and governmental CERTs in place by 2012. The CERT-EU was established in 2011 hosted by the European Commission. Following a one-year pilot phase, the CERTs have been operating at full capacity since September 2012. The CERT-EU is composed of IT security experts from the main EU Institutions, and it cooperates with other CERTs in the Members States and with specialised IT security companies. The task of the newly set up permanent groups is to help them to respond to

[115] European Court of Auditors 2019, 31.
[116] European Commission s. a.

incidents, particularly those affecting information security. CERT-EU prepares reports and briefings on cyber threats concerning EU institutions, bodies and agencies. It provides an information-sharing platform. In 2018, CERT-EU finalised a non-binding memorandum of understanding with ENISA, EC3 and the European Defence Agency in order to increase cooperation and coordination with those agencies. It also signed a technical agreement with NATO's computer incident response capability (NCIRC).[117]

The role of CERTs is to prevent weaknesses in network security, to identify threats and to address vulnerabilities. In order to maintain and restore system security, the groups warn their clients about existing security vulnerabilities and threats, propose measures to reduce the risks.

European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency (ENISA) was established in 2004. The agency, which has a mainly advisory role, has been operating in Athens and has had a second office in Heraklion since 2005. From 2005, the Agency's role was to "contribute to securing Europe's information society by raising awareness of network and information security and to develop and promote a culture of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organizations in the Union."[118] In parallel with the development of the first cybersecurity strategy, a new Regulation of the European Parliament and of the Council on the operation of ENISA was adopted on 21 May 2013, extending the Agency's mandate until 2020 and strengthening its capacity to tackle cyberattacks and other information security challenges.[119]

The first EU legislation on cybersecurity, the 2016 NIS Directive gave a central role to the ENISA in supporting the implementation of the Directive. The Agency provides the secretariat for the Network Security Response Teams (CSIRTs) and actively supports cooperation between CSIRTs.

Since 2019, following the new legislation of the Cybersecurity Act (Regulation 2019/881), ENISA has been tasked to support Member States, EU institutions and all other stakeholders in their cyber policies, and to prepare the 'European cybersecurity certification schemes' that serve as the basis for certification of ICT products, processes and services that support the proper delivery of the Digital Single Market. ENISA will play a central role in the development of certification schemes.
The Agency's new tasks will include:

- organising pan-European Cybersecurity Exercises
- the development and evaluation of National Cybersecurity Strategies
- CSIRTs cooperation and capacity building

[117] European Court of Auditors 2019, 6.
[118] European Parliament and Council 2013.
[119] European Parliament and Council 2013.

- studies on IoT and smart infrastructures, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, identifying the cyber threat landscape, and others
- supporting the development and implementation of the European Union's policy and law on matters relating to network and information security (NIS)
- assisting Member States and European Union institutions, bodies and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis[120]

The exercises organised by ENISA have helped to prepare national authorities, to strengthen preparedness and resilience to cyber threats.

Computer Security Incident Response Team (CSIRTs)

The transposition of the 2016 Directive of the European Parliament and of the Council on the security of network and information systems (2016/1148) at Member State level necessitated the establishment of a network of Computer Security Incident Response Teams, i.e. CSIRTs. The EU-wide network is composed of CSIRTs in the Member States and representatives of the Network Security Emergency Response Teams (CERT-EU).

Europol EC3

In 2013, the European Cybercrime Centre (EC3) was set up at Europol's headquarters in The Hague. The aim of the new centre was to protect European citizens and businesses from cyber threats and help governments against cybercrime. From the outset, the new EU headquarters focused on illegal online activities by organised criminal groups, in particular attacks on electronic banking and other financial activities. The centre provides support for more effective protection of social networking profiles against cybercrime and information and analysis to national law enforcement authorities. Since its inception, the EC3 publishes yearly the Internet Organised Crime Threat Assessment (IOCTA). EC3 has made a significant contribution to the fight against cybercrime by participating in a number of outstanding operations and providing operational support on the ground.[121]

Eurojust

According to the Lisbon Treaty, Eurojust is responsible for supporting and strengthening the coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States (Article 85). The European Union Agency for Criminal Justice Cooperation (Eurojust) is the successor

[120] ENISA s. a.
[121] Europol s. a.

to the European Union's Judicial Cooperation Unit created in 2002. The new regulation of Eurojust was adopted in 2018.[122]

The European Judicial Cybercrime Network (EJCN) was established in 2016 to promote "contacts between practitioners specialised in countering the challenges posed by cybercrime, cyber-enabled crime and investigations in cyberspace, and to increase efficiency of investigations and prosecutions".[123]

European Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA)

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA), was established in 2011 [Establishing Regulation (EU) No 1077/2011] and started its activities in 2012. The headquarters of this agency are in Tallinn, Estonia, and its operational centre is in Strasbourg, France. A business continuity site for the systems under management is situated in Sankt Johann im Pongau, Austria and a Liaison Office in Brussels, Belgium.

The EU-LISA is responsible for the operational management of large-scale IT systems, which are essential instruments in the implementation of the Union's policies in the area of justice, security and freedom. It facilitates the implementation of the asylum, border management and migration policies of the EU.

The Agency is currently providing operational management of the Eurodac (a large-scale fingerprint database mainly for asylum applications), the SIS II (the second generation Schengen Information System) and the VIS (Visa Information System).[124]

European External Action Service (EEAS)

The European External Action Service manages the diplomatic relations of the European Union conducting CFSP. The EEAS has a central role in the field of cyberdiplomacy, strategic communication and the policies concerning cyber defence. This body hosts intelligence and analysis centres dealing with cyber issues as well for civilian and military situational awareness (the Single Intelligence Capability: European Union Intelligence Analysis Centre (INTCEN) and the Military Staff Intelligence Directorate). The Hybrid Fusion Cell was established in 2016 within the EU Intelligence Analysis Centre to improve situational awareness and support decision-making. It gathers and analyses classified and open source information concerning hybrid threats.[125]

[122] European Parliament and Council 2018.
[123] Eurojust s. a.
[124] EU-LISA s. a.
[125] European Court of Auditors 2019, 50.

European Defence Agency (EDA)

The European Defence Agency was established in 2004 as an intergovernmental agency of the Council of the European Union. The EDA support the Member States and the Council in their effort to improve defence capabilities through European cooperation. According to the Council conclusion, EDA aims to develop cyber defence capabilities related to CSDP, to civil-military cooperation and synergies, to raise awareness and to cooperate with relevant international partners.[126]

The EU approach to cyberdiplomacy

The EU has started to play an increasingly active role not only in deepening the integration process between its own Member States, but also in resolving international disputes related to cybersecurity and cyber defence.[127] The 2013 strategy set out the EU's international cyber policy. In addition to protecting a free and open internet, the new policy aimed to promote international law of responsible state behaviour and confidence-building measures in cyberspace and to improve cooperation with the EU's strategic partners. To this end, negotiations have begun with the United States, China, Japan, South Korea, India and Brazil. During the negotiations, the parties discussed, inter alia, the areas of international security in cyberspace, resilience, cybercrime, internet governance and cybersecurity standards. An important milestone in 2015 was the adoption of Council conclusions on cyberdiplomacy to support the EU's collective efforts.[128]

The EU's approach to cyberdiplomacy at global level:

- promotes and protects human rights and is grounded on the fundamental EU values of democracy, human rights and the rule of law, including the right to freedom of expression; access to information and right to privacy
- ensures that the Internet is not abused to fuel hatred and violence and safeguards that the Internet remains, in scrupulous observance of fundamental freedoms, a forum for free expression in full respect of law
- promotes a cyber policy informed by gender equality
- advances European growth, prosperity and competitiveness and protects EU core values, inter alia, by strengthening cybersecurity and improving cooperation in fighting cybercrime
- contributes to the mitigation of cybersecurity threats, conflict prevention and greater stability in international relations through the use of diplomatic and legal instruments
- promotes the efforts to strengthen the multi-stakeholder model of Internet governance
- fosters open and prosperous societies through cyber capacity building measures in third countries that enhances the promotion and protection of the right to freedom of expression and access to

[126] Rehrl 2018, 93–94.
[127] Renard 2018.
[128] Rehrl 2018, 23.

information and that enables citizens to fully enjoy the social, cultural and economic benefits of cyberspace, including by promoting more secure digital infrastructures
– promotes the sharing of responsibilities among relevant stakeholders, including through cooperation between the public and private sectors as well as research and academic institutions on cyber issues[129]

According to Bendiek "it is a politically and legally controversial issue whether attacked states should adopt offensive countermeasures, such as hack-backs, to neutralise the source of a cyber-attack, […] and the state requires military and strategic cyber weapons as well as a legal basis for their deployment in order to respond to cyberattacks."[130]

At the international level, the EU attached importance to the strict application of international law, in particular the UN Charter and international humanitarian law, and the full implementation of universal non-binding cyber norms, rules and principles of responsible state behaviour in cyberspace for conflict prevention and stability. The EU also promotes the development of confidence building measures and cooperation with other international organisations. According to Rehrl, the OSCE that is a very important partner of the EU is the most advanced organisation in the field of confidence-building measures at the regional level.[131]

Due to the growing level of cyber threats and challenges in recent years, cyberdiplomacy has become an integral part of the Common Foreign and Security Policy. EU Member States agreed on strengthening cyberdiplomacy capabilities within the European External Action Service in 2015. The implementation plan on security and defence confirmed this intention in 2016. Important bodies (EU INTCEN and EUMS INT) started to deal with cyber issues.[132]

In 2017, the Council of the European Union agreed to develop a framework for joint EU diplomatic action against malicious cyber activities by state and non-state actors. The so-called Cyber Diplomacy Toolbox was built on the EU's CFSP Policy Toolbox. The EU stands ready to take action on Common Foreign and Security Policy measures, including restrictive measures against activities using information and communication technologies (ICT) that could exhaust the notion of an act of violation of international law.[133]

In line with the EU's cyberdiplomatic approach, the joint action will contribute to conflict prevention, the reduction of cybersecurity threats and the enhancement of stability in international relations. The Council set the goal of providing a framework for joint EU diplomatic action to facilitate cooperation, promote risk reduction and influence the behaviour of potential attackers. This EU diplomatic response will make full

[129] Council of the European Union 2015.
[130] Bendiek 2018, 1–2.
[131] Rehrl 2018, 25.
[132] Bendiek 2018, 1–2.
[133] Council of the European Union 2017a.

application of measures used under the Common Foreign and Security Policy, including restrictive measures and possible sanctions. According to the Council conclusions, "a joint EU response to malicious cyber activities would be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity."[134] On 11 October 2017, the Political and Security Committee adopted implementing guidelines for the Cyber Diplomacy Toolbox. The document listed five categories of measures within the cyberdiplomacy toolkit. These included restrictive measures and the procedure for imposing such measures.[135]

According to the 2018 Cyber Defence Policy Framework, the events of previous years have further highlighted the need for more cooperation within the international community in order to prevent conflicts and strengthen the stability of cyberspace. "The EU is promoting, in close cooperation with other international organisations, in particular the UN, the OSCE and the ASEAN Regional Forum, a strategic framework for conflict prevention, cooperation and stability in cyberspace, which includes (i) the application of international law, and in particular the UN Charter in its entirety, in cyberspace; (ii) the respect of universal non-binding norms, rules and principles of responsible State behaviour; (iii) the development and implementation of regional confidence building measures (CBMs). The Cyber Defence Policy Framework should also support this endeavour."[136]

In 2019, the EU made significant progress in making the Cyber Diplomacy Toolbox against malicious cyber activities operational and effective. In order to achieve the objectives laid down in its conclusions of June 2018 and October 2018, the European Council decided to introduce EU restrictive measures to help improve the response and deterrence capacity of the Union. On 17 May 2019, a Council Decision [(CFSP) 2019/797] and a Council Regulation [(EU) 2019/796] was taken on restrictive measures against cyberattacks threatening the Union or its Member States.[137] The decision identifies the applicability of measures within the CFSP, if necessary, restrictive measures against malicious cyber activities, and the regulation allows the EU to impose sanctions as a response to cyberattacks with a significant effect which constitute an external threat to the Union or its Member States.[138]

The new legal framework has thus made it possible for the EU to impose sanctions (e.g. asset freeze, travel ban) to deter and respond to cyberattacks that constitute an external threat to the Union or its Member States. Those sanctions should be effective, proportionate and dissuasive.[139]

[134] Council of the European Union 2017b.
[135] Council of the European Union 2019b.
[136] Council of the European Union 2018, 8.
[137] Council of the European Union 2019b.
[138] Council of the European Union 2019b.
[139] European Commission 2019, 8.

References

Bendiek, Annegret (2018): The EU as a Force for Peace in International Cyber Diplomacy. *SWP Comment,* No. 19 April 2018. 1–2. Source: www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf (Accessed: 22.05.2020.)

Council of the European Union (2003): *European Security Strategy, a Secure Europe in a Better World.* Brussels, 12 December 2003. Source: www.consilium.europa.eu/media/30823/qc7809568enc.pdf (Accessed: 22.05.2020.)

Council of the European Union (2008): *Report on the Implementation of the European Security Strategy. Providing Security in a Changing World.* Brussels, 11 December 2008. Source: www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf (Accessed: 22.05.2020.)

Council of the European Union (2010): *Internal security strategy for the European Union. Towards a European security model.* Source: www.consilium.europa.eu/media/30753/qc3010313enc.pdf (Accessed: 22.05.2020.)

Council of the European Union (2014): *EU Cyber Defence Policy Framework.* Brussels, 18 November 2014, 15585/14. Source: www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf (Accessed: 22.05.2020.)

Council of the European Union (2015): *Council Conclusions on Cyber Diplomacy.* Brussels, 11 February 2015 (OR. en)6122/15. Source: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf (Accessed: 22.05.2020.)

Council of the European Union (2017a): *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") 9916/17.* Source: http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf (Accessed: 22.05.2020.)

Council of the European Union (2017b): *Cyber attacks: EU ready to respond with a range of measures, including sanctions.* Source: www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/pdf/ (Accessed: 22.05.2020.)

Council of the European Union (2018): *EU Cyber Defence Policy Framework,* (as updated in 2018). Brussels, 19 November 2018(OR. en) 14413/18. Source: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf (Accessed: 22.05.2020.)

Council of the European Union (2019a): *Permanent Structured Cooperation (PESCO)'s projects – Overview.* Source: www.consilium.europa.eu/media/39762/pesco-overview-of-first-collaborative-of-projects-for-press.pdf (Accessed: 22.05.2020.)

Council of the European Union (2019b): *Council Decision (CFSP) 2019/797, of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States.* Source: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019D0797&from=EN (Accessed: 22.05.2020.)

Council of the European Union (2019c): *Council Regulation (EU) 2019/796 of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States.* Source: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0796&from=EN (Accessed: 22.05.2020.)

ENISA (s. a.): *About ENISA.* Source: www.enisa.europa.eu/about-enisa (Accessed: 22.05.2020.)

EU Cyber Direct (2019): *Cyber-related PESCO projects.* The Council of the EU, 12 November 2019. Source: https://eucyberdirect.eu/content_knowledge_hu/cyber-related-pesco-projects/ (Accessed: 22.05.2020.)

EU-LISA (s. a.): *EU-LISA. Who We Are.* Source: www.eulisa.europa.eu/About-Us/Who-We-Are (Accessed: 22.05.2020.)

Eurojust (s. a.): *European Judicial Cybercrime Network.* Source: www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx (Accessed: 22.05.2020.)

European Commission (2005): *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. "i2010 – A European Information Society for growth and employment".* Brussels, 1.6.2005, COM(2005) 229 final, Commission of the European Communities. Source: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF (Accessed: 22.05.2020.)

European Commission (2013): *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/01 final.* Source: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf (Accessed: 22.05.2020.)

European Commission (2015): *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe.* Brussels, 6.5.2015, COM(2015) 192 final. Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192 (Accessed: 22.05.2020.)

European Commission (2017a): *Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.* Brussels, 13.9.2017, JOIN(2017) 450 final. Source: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450 (Accessed: 22.05.2020.)

European Commission (2017b): *State of the Union 2017 – Cybersecurity: Commission scales up EU's response to cyber-attacks.* European Commission, 19 September 2017. Source: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193 (Accessed: 22.05.2020.)

European Commission (2018): *Shaping Europe's digital future. Policy. European Cybersecurity Industrial, Technology and Research Competence Centre.* European Commission, 19 September 2018. Source: https://ec.europa.eu/digital-single-market/en/european-cybersecurity-industrial-technology-and-research-competence-centre (Accessed: 22.05.2020.)

European Commission (2019): *Joint Communication to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions. Report on the implementation of the Action Plan Against Disinformation.* Brussels, 14.6.2019 JOIN(2019) 12 final. Source: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0012&from=EN (Accessed: 22.05.2020.)

European Commission (2020): *Shaping the Digital Single Market.* Source: https://ec.europa.eu/digital-single-market/en/europe-2020-strategy (Accessed: 22.05.2020.)

European Commission (s. a.): *Departments/Executive agencies.* Source: https://ec.europa.eu/info/departments (Accessed: 22.05.2020.)

European Council (2013): *European Council Conclusions 19/21 December 2013.* Source: www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/140245.pdf (Accessed: 22.05.2020.)

European Court of Auditors (2019): *Challenges to effective EU cybersecurity policy. Briefing Paper, March 2019.* Source: www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf (Accessed: 22.05.2020.)

European External Action Service (2016): *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy.* Source: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf (Accessed: 22.05.2020.)

European Parliament and Council (2013): *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and*

Information Security (ENISA), Article 1(1). Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0526 (Accessed: 22.05.2020.)

European Parliament and Council (2016): *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (Accessed: 22.05.2020.)

European Parliament and Council (2018): *Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA.* Source: www.eurojust.europa.eu/doclibrary/Eurojust-framework/EurojustRegulation/Eurojust%20Regulation%20(Regulation%20(EU)%202018-1727%20of%20the%20European%20Parliament%20and%20of%20the%20Council)/2018-11-21_Eurojust-Regulation_2018-1727_EN.pdf (Accessed: 22.05.2020.)

European Parliament and Council (2019): *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA, (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1.* Source: https://eur-lex.europa.eu/eli/reg/2019/881/oj (Accessed: 22.05.2020.)

Europol (s. a.): *European Cybercrime Centre – EC3.* Source: www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Accessed: 22.05.2020.)

Kovács László (2018): *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus Kiadó.

Rehrl, Jochen ed. (2018): *Handbook on Cybersecurity. The Common Security and Defence Policy of the European Union.* Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria. Source: https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1 (Accessed: 22.05.2020.)

Renard, Thomas (2018): EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society,* Vol. 19, No. 3. 321–337.

Dóra Molnár

European Cyberdiplomacy Landscape – France, the United Kingdom and Germany

When it comes to cybersecurity, the saying "as many states, so many approaches" is certainly true. This is true not only globally, but also for European states. States have recognised the growing importance of this area at different times and have described a different trajectory in both the development of their cybersecurity strategic culture and its implementation. Accordingly, the importance of cyberdiplomacy varies from state to state, although it is an undoubted fact that most states now emphasise the strategic importance of cyber relations, the need for cooperation and the need to establish rules of conduct in cyberspace at the strategic level. However, the proposed solutions are very different. For example, one group of states considers it necessary to create a comprehensive cyber convention, while others strongly oppose it along arguments based on the characteristics of cyber weapons.[1] Most states in the Western world are pushing for a multi-stakeholder governance model of the Internet, while the developing world, led by China and supported by Russia, is in favour of a multilateral solution in every possible forum. However, in addition to the many different approaches, there are several commonalities in public policies. Most states seek to make the most of the opportunities offered by international fora and organisations, but they also seek to build the widest possible network of bilateral contacts. The fault lines between individual states are well delineated on the basis of whether they manage to bring a bilateral cyber agreement under the roof.

The study examines three European states. Today, the United Kingdom is the world's leading cyber state, so it is impossible not to describe the British cyberdiplomatic solutions. However, when it comes to diplomacy, France comes to mind as the first European state, so I will also start my study by presenting French characteristics. The third state surveyed is Germany, due to the country's leading European position and the unique intertwining of the economy and cyber politics. Each of the states surveyed has been advocating the need to regulate cyberspace for years, most recently joining the Joint Statement on Advancing Responsible State Behavior in Cyberspace on 23 September 2019, along with a further 24 states.[2] The US-initiated statement underlined the need for a concerted and coordinated cyber effort to protect citizens, among other things, from a series of cyber-attacks – adding that the attacks are being carried out by Russia and other adversaries. It has also been declared that inappropriate cyberspace behaviour will have consequences. In the following, I present the international activities of the three states and/or the main actors of the network of bilateral contacts, based on the national cyber strategies.

[1] These include, for example, the unresolved nature of control issues and the difficulty of rapid technological change and adaptation. See Nabeel 2018.

[2] U.S. Department of State 2019.

France as a cyberdiplomatic power

Perhaps it is no exaggeration to say that France has been a stronghold of diplomacy for centuries, and that the French are great masters of the use of "soft" tools in politics. The country's strength is given by its global role, based on its extensive diplomatic network: it has an unparalleled membership in multilateral and international organisations, with the highest number of foreign cultural missions and the 5th largest donor state.[3] It is therefore not surprising that French politics prefers to use the tools of diplomacy in cyberspace effectively – so much so that it is at the forefront of this field at European level. This justifies me starting my study of European countries with France, even if there is another European state in terms of cyber power potential that is ahead of the country.

The need for international cooperation in cyberspace as one of the necessary areas for action is already reflected in the first cyberstrategy, *Protection and Security of Information Systems: A Strategy for France,* published in 2011.[4] This is specified in the Senate Information Report No. 681, adopted in 2012, by emphasising the importance of bilateral relations as one of the ten priorities, and calling for joint action with the North Atlantic Treaty Organization (NATO) and the European Union (EU), dialogue with China and Russia, and supports the adoption of international confidence-building measures.[5] The 2013 White Paper emphasises the need for a "global governmental approach" to combat cyberattacks, in which France builds on its diplomatic, legal and political instruments.[6]

The country's cyberstrategy was released in 2015 under the title *National Digital Security Strategy.*[7] The strategy sets out five main objectives, the fifth of which is entitled *Europe, Digital Strategic Autonomy, Cyberspace Stability.* France intends to participate in Europe's digital transformation through its allied relations, in three main ways: by setting out a roadmap for a European strategy with other EU volunteers, by strengthening the French presence and influence in international cyber talks, and by supporting other states in building cyber capabilities, thereby contributing to the global stability of the cyberspace. According to the strategy, the main venues for increasing influence among the international organisations are the United Nations (hereinafter: the United Nations) and the Organization for Security and Cooperation in Europe (hereinafter: the OSCE), active participation in bilateral relations in the framework of diplomatic dialogue at ministerial level and in informal international fora with political decision-makers and academia. The area of cyberdiplomacy was centralised to implement the strategy, and in 2015 the position of ambassador for cyberdiplomacy and the digital economy was set up in the Ministry of Foreign Affairs.[8]

[3] Ministère de l'Europe et des Affaires Étrangères 2019a.
[4] ANSSI 2011.
[5] Sénat 2012.
[6] Ministère de la Défense 2013.
[7] SGDSN 2015.
[8] The position, which has been called Digital Ambassador since 22 November 2017, was filled by David Martinon.

Since the adoption of the 2015 strategy, the international environment has changed significantly. It is enough to think of the series of cyberattacks following the terrorist attack on Charlie Hebdo or against the television channel TV5. The events also shed new light on the issue of cybersecurity in France and encouraged the country to take more active and vigorous national and international action.

The new approach is reflected in the Offensive Cyber Operations Doctrine, published on 18 January 2018, about three weeks before the release of the Cyber Defence Strategic Review. In the document, France openly states that cyber capabilities are part of its military activities and are ready to be deployed if necessary. This certainly marks a turning point in French cyber politics, which has so far been characterised by discreet diplomatic actions: even in case of blatant cyber conflicts such as the Russian-sponsored cyberattack on the Navy to find out about oil supply channels, France did not use offensive rhetoric, but sought to defuse tensions by using the means of dialogue (Laudrain 2019).

On 8 February 2018, the latest Cyber Defence Document, entitled Cyber Defence Strategic Review, was issued as the official material summarising the country's cyber defence ambitions.[9] Also known as the White Paper on Cyber Defence, the document sets out in several chapters the need for some cyberdiplomatic action and sets out France's position on the issue. There is a separate chapter on international negotiations on the regulation of cyberspace, highlighting the role of the UN and the Group of Governmental Experts (GGE) and their achievements since 2013. At the 2016–2017 session, France put forward a separate proposal for a deeper regulation of the non-refoulement ban, which, although supported by the participating states, was stalled due to differing views on how to apply international law. Another chapter shows how the country performs internationally in cyberspace. It promotes dialogue and cooperation with its allies in order to prevent cyber conflicts, urges the regulation of cyberspace and aims to ensure European security and autonomy in cyberspace as well. From among its bilateral relationships, it highlights its cyber relations with the United States,[10] China, India,[11] Brazil and Japan, adding that it will continue to cultivate deep ties with its Western allies, but will place increasing emphasis on the sub-Saharan region, where it urges the establishment of relations with the Francophone states. European cyber relations need to be organised along three issues: technical, regulatory and capacity issues, which require the formulation and adoption of a common ground. The Franco–German system of relations occupies a prominent place in both bilateral and European relations.

[9] SGDSN 2018.

[10] The third stop of the Franco–American cyber dialogue was held on 22 January 2020 in Paris. The central topic of the meeting was the applicability of international law to cyberspace (Ministère de l'Europe et des Affaires Étrangères 2020).

[11] The India–France Bilateral Cyber Dialogue was held for the third time on 20 June 2019, discussing primarily issues related to cyber norms. The importance of bilateral cyber relations is well signalled by India's invitation to the 2019 G7 summit from France, which held the presidency in 2019 (Ministère de l'Europe et des Affaires Étrangères 2019c).

Cooperation between the two countries is very intensive and extensive, as evidenced by the two joint reports published so far.[12] Finally, the document calls for the adoption of an action doctrine that sets out fundamental issues such as the classification system for cyberattacks and the range of responses to cyber incidents. A global system for regulating cyberspace can only be implemented along the lines of principles such as prevention, cooperation and stability.

Despite a more "offensive" attitude, diplomatic moves will certainly continue to play a key role in French politics in the future. It is no coincidence that France is one of the most active Member States in various international organisations when it comes to cybersecurity issues. Not only in the UN, as discussed above in relation to the GGE, but also in NATO, the G7 and the OSCE.[13] In the latter organisation, France played a very important role in the adoption of the two packages of confidence-building measures related to cybersecurity. With regard to the French participation in the G7, I would like to highlight the meeting held in the small French town of Dinard on 5–6 April 2019, where the so-called Dinard Declaration on the Initiation of Cyberspace Rules was accepted.[14] It welcomed the UN General Assembly's supportive approach to the applicability of international law in cyberspace and reaffirmed their intention to promote an open, secure, stable, accessible and peaceful cyberspace. At the same time, they reaffirmed their intention to formulate a Cyber Norm Initiative – CNI, which was finalised on 26 August 2019 with ten basic rules applicable in cyberspace.[15] All of this fits well with the success story of French soft politics, although it should be added that there was no precedent for the adoption of such an initiative. From 12 to 14 November 2018, the UNESCO Headquarters in Paris hosted the thirteenth annual meeting of the Internet Governance Forum, where French President Emmanuel Macron himself announced the Paris Call for Confidence and Security in Cyberspace.[16] The widespread acceptance of the call is well indicated by the fact that it was immediately supported by more than 500 entities (state, organisation and company).[17] However, the completeness of the picture also includes the fact that each of the three "big" states rejected the initiative, torpedoing its global acceptability. With the call and a number of similar initiatives, France aims to see the country as a cyber power worldwide. Perhaps this goal also guided the country on 9 September 2019, when the French Ministry of Defence set out in an official document its views on how international law, according to France, could be applied in cyberspace[18] – thereby also taking on a pioneering role in cyberdiplomacy.

[12] ANSSI/BSI 2018; ANSSI/BSI 2019.
[13] Ministère de l'Europe et des Affaires Étrangères 2019b.
[14] Ministère de l'Europe et des Affaires Étrangères 2019d.
[15] Ministère de l'Europe et des Affaires Étrangères 2019e.
[16] Ministère de l'Europe et des Affaires Étrangères 2018a.
[17] Ministère de l'Europe et des Affaires Étrangères 2018b.
[18] Rogusky 2019.

Germany

Although Germany has been actively involved in UN cybersecurity consultations and other bilateral and multilateral fora since 2004, cooperation has been limited to technical issues. Although the first German cybersecurity strategy in 2011 mentioned the international and diplomatic dimensions of cybersecurity, until the Snowden case, Germany did not play a significant role in cyber floor. Only after the case, Germany together with Brazil, due to the involvement of German Chancellor Angela Merkel, initiated the adoption of a UN resolution on the protection and inviolability of the right to privacy in the digital age, which resulted in the adoption of UN General Assembly resolution no. 68/167 on 18 December 2013. This was a major cyberdiplomatic success for Germany, especially because it managed to raise this issue to global level with South American support. From then on, Germany has become an active supporter of cyberdiplomacy. In 2016, under the German chairmanship of the OSCE, the second package of confidence-building measures in cyberspace was adopted, and in 2016–2017, German diplomatic representatives also chaired the UN GGE.

The foundations for increasingly active German action must be found in the country's cybersecurity strategy. In 2016, the country's second cyberstrategy was released[19] that already highlighted the importance of cooperation, which, however, must not be limited to national frameworks, but must establish pan-European and even global channels of cooperation. The document identifies four areas for action, one of which is the appropriate positioning of Germany in European and international cybersecurity policy discussions. This clearly shows that cyberdiplomacy has established itself as a priority area and has become a fundamental factor influencing the security of a country. As part of this, Germany also emphasises the importance of bilateral partnerships, especially in areas such as information sharing and the coordination of security issues related to cross-border services as well as capacity sharing. On the other hand, in the field of development cooperation, where security and confidence-building measures are the key to success.

Germany is also gradually putting the strategy into practice with bilateral relations playing an enhanced role. The *United States* is a key strategic partner, so it is no coincidence that their cyber dialogue also has a long and meaningful history. Since 2012, a bilateral cyber meeting has been held annually, one year in Washington, the other in Berlin. During the meetings, issues such as the applicability of international law in cyberspace or the online enforcement of human rights are discussed like in 2016, but their common thinking of the multi-stakeholder model of cyberspace is also well established.[20] A consensus was reached with *China* in November 2016 that the two states would continue the dialogue on cyber issues through a special mechanism, but no bilateral agreement has been signed to date.[21] Most recently, Chancellor Merkel held talks

[19] Federal Ministry of the Interior 2016.
[20] U.S. Department of State 2016.
[21] Burgess 2016.

in China in January 2020 to create a German–Chinese cyber agreement (similar to the U.S.–China agreement), but its precondition was the introduction of a "no spy" clause thanks to the American Huawei scandal. However, when asked about the convention, the chancellor only said diplomatically that Germany and China have been constantly discussing a number of bilateral and international issues with each other on several levels.[22] At the same time, the German bilateral palette is not limited to the large partner states, but presents an extremely colourful picture. Germany, for example, has good bilateral cyber relations with Singapore. In 2017, the Prime Minister of Singapore paid a visit to Germany, during which the two sides signed a joint memorandum of understanding on cybersecurity cooperation in areas such as information sharing or joint research. The visit was reciprocated by Chancellor Merkel in June 2018, and the leaders of the two countries also concluded a defence treaty with a separate cyber clause.[23]

Germany is active in discussing cybersecurity issues in a number of international institutions, but perhaps the role of the *OSCE* stands out among all these actions. At the same time, Germany was predestined to take the lead in OSCE initiatives. On the one hand, because historically they are linked by political and economic threads to both the East and the West, and the OSCE also connects the leading powers in these regions. On the other hand, because Germany is a leading state in this area – it is enough to think about the technical standards and regulations set up in the field of data protection. Thirdly, because Germany participates effectively in organisations (such as the GGE) that set standards and rules in cyberspace, furthermore it can also benefit from the experience it has gained here.[24]

In 2013, the OSCE developed the first package of confidence-building measures in cyberspace, which provided an appropriate basis for moving forward. During the 2016 German OSCE Chairmanship, the possible scope of confidence- and security-building measures was discussed separately in all three baskets. For the first basket, only a series of voluntary agreements on military cooperation between Member States were recorded in 2013. It was agreed that the OSCE would be used as a platform to exchange information on cyberattacks and to mutually support the expansion of national capabilities. The German presidency explicitly aimed to involve engineers (primarily IT professionals) in cyberdiplomacy (not just concerning the first basket), which is expected to have the effect of reducing diplomatic tensions, such as the developments at the Pugwash conferences since the 1950s. The German Information Security Act, adopted in 2015, which set higher security requirements for critical infrastructure protection, served as a reference point for the second step in the economic basket. German law also served as a reference when the NIS Directive was drafted. The central German cyber body, the Federal Office for Information Security (BSI)[25] has served as a model of technical expertise for many OSCE partners.

[22] Chazan 2020.
[23] Parameswaran 2018.
[24] SWP 2015.
[25] Bundesamt für Sicherheit in der Informationstechnik.

All these developments open a new horizon in the context of OSCE economic co-operation. In case of the third basket, the issue of human rights, including freedom of expression on the Internet, is problematic. Above all, the German Presidency had to find an answer to the dilemma of censorship, network surveillance and copyright issues.

Germany makes the regulation of cyberspace a top foreign policy priority. It strongly advocates that global issues can only be resolved through common regulation – and this includes cybersecurity. The problem cannot be tackled at national level alone, but requires close cooperation between states, international organisations, NGOs and academia. It declares the applicability of international law in cyberspace and supports the multilateral approach.[26] In any case, it should be considered a diplomatic success that in November 2019, Germany was able to give home to the UN Internet Governance Forum.

The leading (European) cyber power: The United Kingdom

The U.K., like the great powers, recognised the importance of cybersecurity and cyberdiplomacy at an early stage, which it reflected in its strategic documents and successfully put into practice. The first cybersecurity strategy was issued in 2009, but was soon replaced in 2011 by a new strategy outlining the main guidelines, objectives and conditions for implementation over a five-year period. The title of the strategy is *Protecting and Promoting the UK in a digital world.* The document[27] sets out four objectives, the second of which has a role to play in cyberdiplomacy. The stated goal of the country is to be able to respond flexibly to cyber threats and attacks, and to be able to defend and enforce its interests more effectively in cyberspace. This presupposes proactive behaviour and active participation in the process of shaping cyberspace, the primary means of which are all peaceful: partly diplomatic and partly economic, as the British Government channels the commercial interests of British companies into the growing international cybersecurity market. The third cyberstrategy, re-issued by the British Government on 1 November 2016 for another five years, is a significant step forward.[28] The document sets out three strategic goals – that is why we can call the 2016 cyberstrategy the "3D strategy": 'defend, deter and develop' for the realisation of which it considers international action to be essential. In the second of the objectives, cyberdiplomacy has a key role to play. Deterrence is envisaged not only by "hard" means (such as developing offensive cyber capabilities) but also by further broadening and deepening cooperation channels – as the strategy states: the British will continue to build on the global cyber alliance that has already begun and continue to support application of international law in cyberspace. Achieving the three strategic goals is only conceivable within an appropriate international framework. The U.K. continues to be at the forefront of creating a free, open, peaceful and secure cyberspace where international law is applicable and fundamental human

[26] Federal Foreign Office 2019.
[27] Cabinet Office 2011b.
[28] HM Government 2016.

rights are guaranteed both online and offline. In doing so, the U.K. is counting not only on its traditional allies, but also on its new partners, and is seeking to leverage the power of multilateral fora such as the UN, the G20, the European Union, NATO, the OSCE, the Council of Europe or the British Commonwealth.[29]

Bilateral cyber relations have a key role to play in achieving the goal of building a global cyber alliance. The *United States* is undoubtedly the number one country from among the British traditional allies with which the island nation has had a very close relationship on cyber issues for more than a decade in the context of the so-called "special relationship" – or as it has recently been called "the most important bilateral partnership". The need to involve private sector and business actors, research and development and the application of the basic institutions of the rule of law in cyberspace was already recorded in 2011.[30] In 2015, President Obama and Prime Minister Cameron discussed the details of cooperation in Washington,[31] which was finally institutionalised on 7 September 2016 by the cyber agreement signed by the two defence ministers.[32]

Although the U.K. has not yet signed a bilateral agreement with *China,* on 22 October 2015, during the Chinese President's visit to England, the two countries issued a joint statement on building their comprehensive global strategic partnership, launching the "Golden Age" of bilateral relations.[33] As part of this, it was stated that cyber actions aimed at unauthorised theft of intellectual property, trade secrets or confidential business information aimed at gaining a competitive advantage would not be conducted or supported against each other.[34]

Given the special partnership with the United States, it is not surprising that the United Kingdom also established bilateral cyber relations with Japan in 2012. The fifth stop of the biennial meetings was held in Tokyo on 31 January 2020.[35] Opportunities for capacity building and cooperation on the international stage were discussed during the meeting. This is in line with the main areas of cooperation identified at the fourth meeting in 2018, including support for a rules-based international cyber system and the sharing of national solutions for the safe use of IoT devices.[36]

Among the Asian bilateral relations, I would finally like to highlight *India,* which also has huge economic potential for the British – enough to think about the fact that the country already has 600 million Internet users and 650 million mobile users. An important aspect of India–U.K. security cooperation is cyber issues, and the India–U.K. cyber dialogue since 2012 has addressed issues such as cyber risk reduction, cybercrime management and building a global, multilateral, transparent and democratic system

[29] Molnár 2017, 144.
[30] Cabinet Office 2011a.
[31] The White House 2015.
[32] Moon Cronk 2016.
[33] For more details on some elements of the British China policy see U.K. Parliament 2019.
[34] Foreign and Commonwealth Office 2015.
[35] Ministry of Foreign Affairs of Japan 2020.
[36] Ministry of Foreign Affairs of Japan 2018.

of Internet governance. In April 2018, the two countries signed in London a five-year framework agreement of cooperation in 14 areas. India has so far only concluded such a comprehensive cyber cooperation agreement with the United States outside the United Kingdom.[37]

The U.K. has already established bilateral cyber relations with a number of European countries. Of these, I highlight the Polish–British cyber cooperation agreement, not primarily because of its content (which is not a significant novelty), but because of its regional significance: through this relationship, the British want to support cyber capacity building programs in Eastern Europe and the Western Balkans.[38]

Finally, with regard to the United Kingdom, we must not forget the *Commonwealth,* which in itself is a long-standing diplomatic forum for the participating states, but in recent years the issue of cybersecurity has also been on the agenda on its own. The participating states institutionalised their cooperation on 20 April 2018 with the signing of the cyber declaration.[39] The declaration reaffirms the obligation of mutual assistance in building cyber capabilities and the need to formulate a common vision for cyberspace, which the UK is also financially supporting, contributing £ 15 million to the stated goals.[40]

Closing remarks

The cyber preparedness of European states is also outstanding globally. This is well indicated by the Global Cybersecurity Index of the UN International Telecommunication Union (ITU) that provides a ranking of the cyber potential of states. According to the index, the U.K. is the world's leading cyber power, with France in third place. The third state surveyed, Germany, took 26th place.[41] It is very interesting, however, that in the fifth area examined, in terms of cooperation, the English have achieved a very good point, while France, a major diplomatic power, is lagging far behind. However, the examination of cybersecurity in Europe cannot end with a presentation of the three leading European states. There are many refreshing examples of how small countries can achieve great success in cybersecurity. The index also reflects this, with Lithuania in 4th place and Estonia in 5th place in the overall world ranking. In addition, both states scored higher in the area of cooperation than the three leading major states. This result is a good indication of how small states place emphasis on the importance of cyberdiplomacy and see the use of peaceful, diplomatic tools as superior to hard capabilities. In the case of Estonia, for example, it is no exaggeration to say that it has a global leadership role in cybersecurity. The headquarters of NATO and the EU are located in the capital of Estonia, where a number of international cyber arrangements have already been concluded. The small country's guiding role in organisational solutions is also

[37] Roy-Chaudhury 2019.
[38] Foreign and Commonwealth Office 2017.
[39] The Commonwealth 2018.
[40] Derschewsky 2018.
[41] Global Cybersecurity Index 2018.

evident: in the autumn of 2019, an independent cyberdiplomacy unit was set up in the Ministry of Foreign Affairs, headed by ambassadors, with the task of representing the country in international organisations and fostering bilateral cyber relations – a model worth following.[42] So overall, the European area is at the forefront of the world in all its sub-issues, including cooperation, which could perhaps be the basis for laying the foundations for a peaceful cyberspace.

References

ANSSI (2011): *Défense et sécurité des systèmes d'information: Stratégie de la France.* Source: www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf (Accessed: 01.11.2018.)

ANSSI/BSI (2018): *ANSSI/BSI Common situational picture.* Vol. 1 – July 2018. Source: www.ssi.gouv.fr/uploads/2018/07/bilateral-french-german-it-security-situation-report.pdf (Accessed: 17.11.2018.)

ANSSI/BSI (2019): *Second Edition of the Franco–German Common Situational Picture.* Source: www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/D-F_Reports/Common_Situational_Picture_2019.pdf?__blob=publicationFile&v=2 (Accessed: 19.04.2020.)

Burgess, Christopher (2016): Dissecting China's Global Bilateral Cybersecurity Strategy. *Security Boulevard,* 09 October 2016. Source: https://securityboulevard.com/2017/10/dissecting-chinas-global-bilateral-cybersecurity-strategy/ (Accessed: 15.04.2020.)

Cabinet Office (2011a): *US–UK Cyber Communiqué.* Source: www.gov.uk/government/publications/us-uk-cyber-communique (Accessed: 16.04.2020.)

Cabinet Office (2011b): *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world.* Source: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (Accessed: 11.10.2017.)

Chazan, Guy (2020): German cyber security chief backs 5G 'no spy' deal over Huawei. *Financial Times,* 28 February 2020. Source: www.ft.com/content/5a0fe826-3b34-11e9-b856-5404d3811663 (Accessed: 14.04.2020.)

Derschewsky, Katharina (2018): *Analysis: Untangling the web of multi-level cyber diplomacy.* Source: www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/may/nalysis-untangling-the-web-of-multi-level-cyber-diplomacy/ (Accessed: 17.04.2020.)

Federal Foreign Office (2019): Cyber policy: multilateral solutions for the future. Source: www.auswaertiges-amt.de/en/aussenpolitik/themen/multilateralism-cyber/2250332 (Accessed: 14.04.2020.)

Federal Ministry of the Interior (2016): *Cyber Security Strategy for Germany 2016.* Source: www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (Accessed: 11.11.2017.)

Foreign and Commonwealth Office (2015): UK–China Joint Statement 2015. *Foreign and Commonwealth Office,* 22 October 2015. Source: www.gov.uk/government/news/uk-china-joint-statement-2015 (Accessed: 16.04.2020.)

Foreign and Commonwealth Office (2017): UK–Poland cyber cooperation commitment. *Foreign and Commonwealth Office,* 21 December 2017. Source: www.gov.uk/government/publications/uk-poland-cyber-co-operation-commitment-joint-statement/uk-poland-cyber-co-operation-commitment (Accessed: 17.04.2020.)

[42] Plantera 2019.

Global Cybersecurity Index (2018). Source: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (Accessed: 22.05.2020.)

HM Government (2016): National Cyber Security Strategy 2016–2021. *HM Government, United Kingdom,* 01 November 2016. Source: www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (Accessed: 11.10.2017.)

Laudrain, Arthur P. B. (2019): France's New Offensive Cyber Doctrine. *Lawfare,* 26 February 2019. Source: www.lawfareblog.com/frances-new-offensive-cyber-doctrine (Accessed: 19.04.2020.)

Ministère de la Défense (2013): *Livre Blanc. Défense et sécurité nationale 2013.* Paris, Direction de l'information légale et administrative. Source: www.defense.gouv.fr/content/download/206186/2286591/file/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf (Accessed: 01.11.2018.)

Ministère de l'Europe et des Affaires Étrangères (2018a): *Appel de Paris pour la confiance et la sécurité dans le cyberespace.* Source: www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf (Accessed: 17.11.2018.)

Ministère de l'Europe et des Affaires Étrangères (2018b): *Cybersécurité: Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans la cyberespace. Liste des soutiens à l'appel de Paris (actualisé le 14 novembre 2018).* Source: www.diplomatie.gouv.fr/IMG/pdf/soutien_appel_paris_cle8e5e31.pdf (Accessed: 30.11.2018.)

Ministère de l'Europe et des Affaires Étrangères (2019a): *La diplomatie française à l'ère numérique.* Consulat Général de France á Ekaterinbourg, 29 May 2019. Source: https://ru.ambafrance.org/La-diplomatie-francaise-a-l-ere-numerique (Accessed: 19.03.2020.)

Ministère de l'Europe et des Affaires Étrangères (2019b): *La France et la cybersécurité.* Source: www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/ (Accessed: 17.11.2018.)

Ministère de l'Europe et des Affaires Étrangères (2019c): *Indo–French Bilateral Cyber Dialogue (Paris, 20 June 2019).* Source: www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/article/indo-french-bilateral-cyber-dialogue-20-06-19 (Accessed: 13.11.2020.)

Ministère de l'Europe et des Affaires Étrangères (2019d): *Dinard Declaration on the Cyber Norm Initiative.* Source: www.diplomatie.gouv.fr/IMG/pdf/g7_dinard_declaration_on_cyber_initiative_cle4e553d.pdf (Accessed: 13.03.2020.)

Ministère de l'Europe et des Affaires Étrangères (2019e): *Inititative pour des normes dans le cyberespace. Synthese des enseignements tirés et des bonnes pratiques.* Source: www.diplomatie.gouv.fr/IMG/pdf/_fr_synthesis_cyber_norm_initiative_cle025b33.pdf (Accessed: 13.03.2020.)

Ministère de l'Europe et des Affaires Étrangères (2020): *Troisième dialogue stratégique France–États–Unis en matière de cybersécurité (Paris, 22 janvier 2020).* Source: www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/actualites-et-evenements-lies-a-la-cybersecurite/article/troisieme-dialogue-strategique-france-etats-unis-en-matiere-de-cybersecurite-22 (Accessed: 13.03.2020.)

Ministry of Foreign Affairs of Japan (2018): *The 4th Japan–UK Bilataral Consultations on Cyberspace.* Source: www.mofa.go.jp/press/release/press4e_001960.html (Accessed: 16.04.2020.)

Ministry of Foreign Affairs of Japan (2020): *The 5th Japan–UK Bilateral Consultations on Cyberspace.* Source: www.mofa.go.jp/press/release/press4e_002766.html (Accessed: 16.04.2020.)

Molnár, Dóra (2017): Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia. *Hadmérnök,* Vol. 12, Special Issue "KÖFOP". 136–148. Source: http://hadmernok.hu/170kofop_09_molnar.pdf (Accessed: 16.04.2020.)

Moon Cronk, Terri (2016): U.S.–U.K. Cyber Agreement Opens Doors for Both Nations. *DoD News,* 18 September 2016. Source: www.defense.gov/Explore/News/Article/Article/937878/us-uk-cyber-agreement-opens-doors-for-both-nations/ (Accessed: 16.04.2020.)

Nabeel, Fahrad (2018): International Cyber Regime: A Comparative Analysis of the US–China–Russia Approaches. *Strategem,* Vol. 1, No. 2. 8–27. Source: www.academia.edu/38296708/International_Cyber_Regime_A_Comparative_Analysis_of_the_US-China-Russia_Approaches (Accessed: 08.04.2020.)

Plantera, Federico (2019): *Estonia takes on a major role in cyber diplomacy with a new department for international cooperation.* Source: https://e-estonia.com/estonia-cyber-diplomacy-international-cooperation/ (Accessed: 26.04.2020.)

Parameswaran, Prashanth (2018): Singapore–Germany Cyber Cooperation in Focus with Introductory Visit. *The Diplomat,* 14 August 2018. Source: https://thediplomat.com/2018/08/singapore-germany-cyber-cooperation-in-focus-with-introductory-visit/ (Accessed: 15.04.2020.)

Rogusky, Przemyslaw (2019): France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I. *Opinio Juris,* 24 September 2019. Source: http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (Accessed: 19.04.2020.)

Roy-Chaudhury, Rahul (2019): India–UK cybersecurity cooperation: the way forward. *IISS,* 22 November 2019. Source: www.iiss.org/blogs/analysis/2019/11/sasia-india-uk-cyber-security-cooperation (Accessed: 16.04.2020.)

Sénat (2012): *Rapport d'Information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense.* Par le Sénateur M. Jean-Marie Bockel. Sénat Session extraordinaire de 2011–2012. Enregistré á la Présidence du Sénat le 18 juillet 2012. Source: www.senat.fr/rap/r11-681/r11-6811.pdf (Accessed: 01.11.2018.)

SGDSN (2015): *La stratégie nationale pour la sécurité de la numérique 2015.* Source: www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf (Accessed: 16.11.2018.)

SGDSN (2018): *La Revue Stratégique de Cyberdéfense.* Source: www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf (Accessed: 15.11.2018.)

SWP (2015): Three Priorities for Cyber Diplomacy under the German OSCE Chairmanship 2016. *German Institute for International and Security Affairs,* 11 November 2015. Source: www.swp-berlin.org/en/point-of-view/three-priorities-for-cyber-diplomacy-under-the-german-osce-chairmanship-2016/ (Accessed: 14.04.2020.)

The Commonwealth (2018): *Commonwealth Cyber Declaration.* Source: https://thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf (Accessed: 17.04.2020.)

The White House (2015): Fact sheet: U.S.–United Kingdom Cybersecurity Cooperation. *The White House, Office of the Press Secretary,* 16 January 2015. Source: https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation (Accessed: 16.04.2020.)

U.K. Parliament (2019): *The making of UK strategy towards China.* Source: https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/612/61210.htm (Accessed: 16.04.2020.)

U.S. Department of State (2016): *Joint Statement on U.S.–Germany Cyber Bilateral Meeting.* Source: https://2009-2017.state.gov/r/pa/prs/ps/2016/03/255082.htm (Accessed: 15.05.2020.)

U.S. Department of State (2019): *Joint Statement on Advancing Responsible State Behavior in Cyberspace.* Source: www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/ (Accessed: 25.04.2020.)

Dóra Dévai

The International Cyberspace Policy of the European Union

By the 2010s, as cyberspace has become a scene for geopolitical contest, the need arouse in several areas for the European Union to take a more coherent and unified stance globally. The growing number of significant cybersecurity incidents prompted a mindset change from handling these as law enforcement or critical infrastructure technical issues. In the assessment of the European Commission looking back at that period: "As far as the national level of preparedness was concerned, Member States had very different level of capabilities and only a few Member States had adopted national cyber security strategies. The EU also had no diplomatic engagement with key partners on cyber issues with participation of Member States, cybersecurity was dealt with sporadically within sectorial dialogues."[43]

In response to this demand, the international cyberspace policy of the EU was established as one of the five strategic priorities of the 2013 Cybersecurity Strategy. Ever since then, this policy dimension gets increasingly integrated, or in EU jargon mainstreamed, into the existing External Action instruments of the Union. As a result, the international cyberspace policy is an umbrella term comprising a set of multifaceted areas aiming to promote wide-ranging EU political, economic and strategic interests.

The global context

The number of people using the Internet is grown exponentially, in particular in the developing countries where the online population is beyond 2.5 billion, surpassing the 1 billion users in the developed world. The digital divide still exists: almost 78% of the people in Africa and 56% in the Asia-Pacific region are still offline. The growing importance of emerging or mid-income economies plays a growing role in generating Internet-linked wealth.[44] Digital questions are gathering an increased attention in the agendas of the African Union Commission and of African leaders. The group of digital giants have been joined by companies like the China-based e-commerce giant Alibaba or Tencent. Analyses show the increasing competitiveness of IT hubs like Beijing, Singapore, São Paolo, Moscow and Bangalore.[45]

In line with the immense role of digital data, data governance is a major preoccupation. Russia, for example, is moving towards more digital sovereignty, requesting tech giants to store the data of Russian users on data centres in Russia. A new bill propositions the creation of Runet, a Russian Internet infrastructure that could operate independently

[43] European Commission 2017, 7–10.
[44] Pawlak 2018.
[45] Pawlak 2018.

of the rest of the Internet. Other countries are still looking for a strategy. In particular for small countries, international solutions remain the best way to protect their digital interests. At the same time, there is a very little appetite for multilateral solutions. 2019 was marked by major divisions.[46]

Internet governance

In broad terms, Internet governance covers the technical, regulatory and policy issues concerning the infrastructure of the Internet and the data transmitted thereby. The list is ever extending, but some of the subject areas in focus are: artificial intelligence, data governance, digital inclusion and safety, security, stability and resilience. The Internet consists of the infrastructural and the logical layers. Some of the core elements of the infrastructure are, for example, the Internet backbone (IP networks), Internet exchange points, terrestrial and cables undersea cables, or communications satellites. The logical layer consists of root services, domain names, IP addresses, Internet protocols. These governance activities are embraced by a large number of international public and private organisations.

Table 1: Some key Internet governance actors

Infrastructure layer					
ITU International Telecommunication Union	IEEE Institute of Electrical and Electronics Engineers	IETF Internet Engineering Task Force	Network Operator Groups	GSMA Global System for Mobile Communications Association	National ICT Ministers
Logical layer					
ICANN Internet Corporation for Assigned Names and Numbers IANA Internet Assigned Numbers Authority	ISO International Organization for Standardization	W3C World Wide Web Consortium	ISOC Internet Society	TLD Operators (Top-level domain)	ETSI The European Telecommunications Standards Institute

Source: Compiled by the author based on Pawlak 2018, 17.

Internet governance has high-stake cross-cutting effects, ranging from human rights to digital economy, and thus it is a highly contested area. This is well reflected by the long-standing debate on the different governance models prompted. The EU's standpoint was established in 2012 and updated in 2014 in the Council Conclusions on Internet Governance. From the onset of the debates, the EU has advocated that the Internet should be treated as a single unfragmented space. In order to achieve legitimacy, accessibility and transparency, a multi-stakeholder approach. This means an amalgam of non-state and state ownership and governance model, and inclusive bottom-up dialogue in deci-

[46] DiploFoundation 2019.

sion-making. With the leadership of China and Russia at global forums, the opposing group often identified by the Shanghai Cooperation Organization and the MENA nations among others, is committed to a government-led Internet governance, exercising state control over ownership and content.

Cyberspace as a diplomatic field

The promotion of a rules-based international system is a core value of EU foreign and security policy. In this dimension, the main aim is to establish international stability and conflict prevention in cyberspace via engagement with key international partners and organisations. The landmark event generally considered as a launching point was when in 1998 Russia brought on the agenda a draft resolution on 'Developments in the field of information and telecommunications in the context of international security' in the First Committee of the UN General Assembly advocating the regulation of the use of ICT tools for national security purposes. In 2004, the first UN Group of Governmental Experts (UN GGE) was convened to deliberate threats in the sphere of information security and possible cooperative measures to address them, hence, the UN GGEs have become the main source for the discussion about international security and stability in cyberspace based on three main pillars:

- The application of existing *international law* in cyberspace. Broadly speaking, there is a fragile consensus agreed in the 2013 UN GGE report that international law is applicable to maintain peace and stability in cyberspace. Nonetheless, there is a stark debate about how to implement the existing international law in cyberspace.
- *Norms of responsible state behaviour* in cyberspace. The same UN GGE report included 11 recommended norms and principles for responsible behaviour in cyberspace for the purposes of international security. Norms in international relations are based on the agreement between states, and thus shape the expectations of state behaviour in the international community. These are conditioned on mutual understanding, and are voluntary and non-binding.
- *Confidence-Building Measures (CBMs)* in cyberspace. Rooted in arms control regimes, these steps aim to build transparency, predictability and thus stability in order to restrain the use of force by reducing the causes of mistrust, misunderstanding and miscalculation between states. The UN GGE has developed a list of voluntary CBMs for cyberspace. These were then adopted at regional settings, most notably at the Organisation for Security and Cooperation in Europe. The OSCE adopted two sets of CBMs in 2013 and 2016.[47]

The EU in a strong co-operation with the U.S. has been at the forefront of the above diplomatic avenues. The list of norms, rules and principles of responsible behaviour

[47] Pawlak 2018.

based on the UN GGE 2015 Report set the basis for the norms promoted collectively by the EU cyberdiplomacy policy. For example:[48]

- States should not knowingly allow their territory to be used for internationally wrongful acts[49] using ICTs.
- States should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.
- States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts.

These were also refined in legal terms by an academic group of experts in so far, the most comprehensive resource in the Tallinn Manual 1.0 and 2.0 on the International Law of Cyber Operations.[50]

The other end of the spectrum is co-lead by Russia and China. Russia's Information Security Doctrine, adopted in 2016, acknowledges that universally recognised principles and norms of international law form the legal framework of the doctrine but does not include any specific reference to whether or not existing laws apply to cyberspace. Similarly, China's International Strategy of Cooperation on Cyberspace, released in 2015, merely contains a commitment to "study the application of international law in cyberspace from the perspective of maintaining international security, strategic mutual trust and preventing cyber conflicts".[51] Furthermore, both countries promote a new set of rules to govern cyberspace. The last GGE in 2016–2017 ended without being able to reach a consensus.

One of the most controversial international law concepts in the 2013 and 2015 UN GGE reports is that of sovereignty. States, mostly authoritarian that are concerned about exercising governmental control over their 'information space' generally interpret sovereignty as a right to be free from outside interference and influence. Liberal democracies deem such an understanding of sovereignty unacceptable as it is contrary to their commitment to human rights. For them, sovereignty as a foundational principle of international law entails sovereign equality, meaning that all are equal before the law.[52] The interpretation of sovereignty is far from unified even among liberal democracies. The question whether sovereignty is a principle or a legal rule that places practical limits on states' cyber activities has significant implications on the threshold at which offensive cyber activities violate international law. In the first case, the threshold will be relatively

[48] This listing has been edited by the author based on United Nations 2015, 7–8.

[49] Rule 14 – Internationally wrongful cyber acts: "A State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation" (Schmitt 2017, 84).

[50] Rehrl 2018.

[51] Pawlak 2018.

[52] Rehrl 2018; Schmitt 2017.

high: unless they constitute a prohibited intervention or use of force, they are likely to be held as lawful. Conversely, cyber operations below that threshold may nevertheless constitute a violation of sovereignty.[53] Other international law rules and principles, notably the rules regarding jurisdiction, the prohibition of intervention, and the obligation of due diligence are also derived from the principle of sovereignty.[54]

The EU's International Cyberspace Policy Framework

The watershed moment arrived with the Joint Communication entitled *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* The document laid down the principles, the statutory and institutional foundations of the policy. "Mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy [CFSP]" entails that the same body of statutory and institutional rules and instruments apply to the EU's international cyberspace policy. The EU's stance on global cyberspace security and stability has been described above. The next section provides an overview of the major policy areas embraced by the EU's international cyberspace policy.

Human rights and the policy principles

The EU often instrumentalises its normative authority, and one of the five key principles in the 2013 EU Cybersecurity Strategy is that the same laws apply in the cyber domain as in other areas of our daily lives. It should be stressed that cybersecurity is closely interlinked with human and fundamental rights, such as the rights to freedom of expression and the protection of personal data. The General Provisions on the Union's External Action also highlight human rights as a core value.

As a result, in 2014 the Foreign Affairs Council adopted *The EU Human Rights Guidelines on Freedom of Expression Online and Offline.* These principles facilitate building trust, and provide legitimacy and authority to the EU's international efforts. The two other principles in the Strategy are interrelated, too. Shared responsibility is a derivative of the multi-stakeholder Internet governance,[55] and emphasises the whole-of-government approach to cybersecurity.

[53] Rehrl 2018.

[54] Rehrl 2018; Schmitt 2017.

[55] "The EU recognizes that the interconnected and complex nature of cyberspace requires joint efforts by governments, private sector, civil society, technical community, users and academia to address the challenges faced and calls on these stakeholders to recognize and take their specific responsibilities to maintain an open, free, secure and stable cyberspace." Council conclusions on malicious cyber activities, Brussels, 16 April 2018.

Dialogue with third countries

The Strategy designates a number of External Action and CFSP areas to further align cybersecurity with the diplomatic domains. Most of these have been mentioned above. In addition, engaging in dialogue with third countries to build trust, reduce risks, promote information sharing and co-operation, and EU interests, a number of partnerships with third countries have been formalised. New regular policy dialogues on cyber issues got on their way with the technologically developed strategic partners and major emerging markets – the U.S., Japan, South Korea, India and China as well as with key international organisations.[56] Nevertheless, these dialogues are delivering at a varying degree.[57]

Cybersecurity capacity building and development

The 2013 Strategy also addresses channelling cybersecurity capacity building systematically into development and neighbourhood policies. The document highlights that:

- Building resilient information infrastructures and the prevention of cyber threats can contribute to a safer global cyberspace.
- Capacity building can embrace different EU aid instruments including assisting the training of law enforcement, judicial and technical personnel to address cyber threats; as well as supporting the creation of relevant national policies, strategies and institutions in third countries on cybersecurity and resilient information infrastructures in third countries.[58]

The EU has become one of the main actors with regard to cyber capacity building in third countries. A set of *Council Conclusions on EU External Cyber Capacity Building Guidelines* were adopted in June 2018.

The governance of this policy area is predominantly shared between the EEAS and the Commission. Within the Commission DG Connect, the Cybersecurity Technology and Capacity Building (Unit H.1) is playing a significant role in devising and implementing and synthesising these policy measures with other cybersecurity areas such as the investment in research and innovation, or the international cybersecurity cooperation and negotiation in general.

The EU has allocated a remarkable amount of funding for cyber capacity building in third countries. Under the Instrument contributing to Stability and Peace, the European Neighbourhood Instrument and the Instrument for Pre-accession Assistance, the total allocation amounted to €21.5 million between 2014 and 2017.[59]

[56] European Commission 2017.
[57] Rehrl 2018.
[58] High Representative of the European Union for Foreign Affairs and Security Policy 2013.
[59] Missiroli 2016.

Internet governance

The EU is mainly represented at these discussions by the Commission, for example, the Next-Generation Internet (Unit E.3) within the Commission's DG Connect. "The Unit is the centre of competence for Next Generation Internet focussing on novel technological breakthroughs, new architectural solutions and advanced service concepts. It also ensures the EU vision and voice on Internet Governance in fora such as IGF, ICANN, G8, ITU and WSIS."[60] The EU's overall Internet strategy is set by two Council Conclusions on Internet Governance (2012, 2014) whereby the EU supports a multi-stakeholder governance model of the Internet that is based on clear principles, in line with the "Netmundial" principles endorsed by EU Member States.[61]

The cyberspace diplomacy of the EU

Pursuant to the institutional setting of the EU's External Actions and CFSP, the main political decision-making and legislative power for cyberspace diplomacy rests with the Member States through the Council of the EU. The Commission and the High Representative (HR), the European External Action Service are responsible for the development of strategies, policies and draft legislation, as well as for their execution.

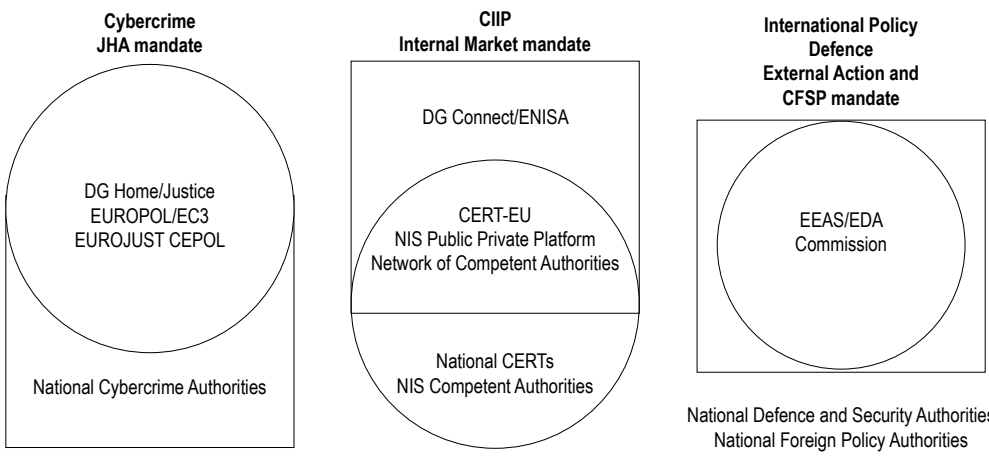


Figure 1: The main pillars of the EU Cybersecurity Strategy
Source: Christou 2016.

Within the Security Policy Directorate (SECPOL) of the EEAS, there is a cyber sector responsible for the formulation, implementation and coordination of cybersecurity and

[60] DG Connect, Next-Generation Internet (Unit E.3) s. a.
[61] European Commission 2017.

defence issues under the Common Foreign and Security Policy. The SECPOL is actively engaged in the multilateral diplomatic activities.[62]

The European Commission helps to shape the EU's overall strategy, proposes new EU laws and policies, monitors their implementation and manages the EU budget. Along the HR and the Member States, the Commission actively engages in policy dialogue with international partners and with global, regional, sectoral and specialised international organisations.

The changing cybersecurity threat landscape and the EU's strategy development

By 2015, at the global and regional fora, cyberdiplomatic negotiations came to a second round and the Russian military intervention in Ukraine reshaped security thinking in Europe. The EU had endorsed a number of new security policy documents. The *Council Conclusions on Cyber Diplomacy,* adopted in February 2015, catalogued and consolidated the cyberdiplomacy objectives of the 2013 Strategy.

The threat landscape has evolved significantly in the period between 2015 and 2017 as well: disruptive cyber operations against critical infrastructures in Ukraine; the midterm elections meddling in the U.S.; massive botnet attacks and global ransomware cases like 'WannaCry' and 'NotPetya' shaped the political climate. Moreover, ICANN was freed from U.S. government oversight. Six EU Member States were engaged in the 2016–2017 UN GGE work – the United Kingdom, France, Germany, Estonia, the Netherlands, Finland – which ended without being able to establish a consensus report.

Consequently, the EU's approach was altered. The 2012 *Communication on the EU Strategic Approach to Resilience* defines resilience as "the ability of an individual, a household, a community, a country or a region to withstand, adapt and quickly recover from stress and shocks".[63] The EU's approach to cybersecurity issues shifted from crisis containment to a more structural and long-term approach to vulnerabilities, with an emphasis on anticipation, prevention and preparedness.[64] The Joint Communication on *A Strategic Approach to Resilience in the EU's External Action* adopted in 2017 also marked this new direction.

In 2017, a progress report was conducted on the achievements of the 2013 Strategy. The Commission recognised that many of the objectives "were defined in very general terms, showing the direction the EU should follow. Therefore, the assessment looks at the degree of progress made without the assumption that the objective could have been fully met".[65] In September 2017, the HR and the Council's Joint Communication on *Resilience, Deterrence and Defence: Building strong cybersecurity for the*

[62] Rehrl 2018.
[63] European Commission 2012, 5.
[64] Pawlak 2018.
[65] European Commission 2017, 53.

EU was endorsed as a result. The document aims at creating a more coherent policy framework by:

- Building EU resilience to cyberattacks through the instalment of established institutional procedures, such as the *Blueprint* for EU-wide cyber crisis management.
- Creating effective cyber deterrence in particular through *The Cyber Diplomacy Toolbox*.[66]

A turning point came in the first half of 2016, when the Dutch EU presidency circulated a non-paper among Member States on the concept of co-ordinated response to coercive cyberattacks. The document defined coercive cyberattacks as "cyber operations that constitute an internationally wrongful act intended to exert undue diplomatic, informational, military or economic pressure on a target State".[67] State and non-state actors carry out such operations for politico-military purposes on the basis of a rational cost/benefit analysis. Therefore, cyberdiplomacy is one of the tools to influence this analysis by increasing the costs of coercive cyber operations and establishing a deterrent effect. The non-paper also emphasised that unlike the earlier cyberdiplomacy concepts that aimed at increasing global cybersecurity in general, the optional diplomatic measures suggested in this non-paper are intended to respond to specific incidents threatening the security of the EU and its citizens and territory.[68]

Cyber Diplomacy Toolbox

The *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* was endorsed in June 2017. The Council Conclusion affirms that malicious cyber activities might constitute wrongful acts under international law.[69] Up to this point, the EU treated 'cyber activities against information systems' and joint investigation and prosecution response mechanism under criminal law.[70] This time, the Conclusion "affirms that the existing measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures, adopted under the relevant provisions of the Treaties, are suitable for a Framework for a joint EU diplomatic response to malicious cyber activities". Furthermore, the document premises that thereby signalling the likely consequences of such malicious cyber activities influences the long-term behaviour of potential aggressors.[71]

[66] Pawlak 2018.
[67] Presidency of the European Council 2016, 4.
[68] Presidency of the European Council 2016, 3.
[69] The Council of the European Union 2017b.
[70] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems. The Directive contains minimum rules on the definition of criminal offences and sanctions in the area of attacks against information systems and provides for operational measures thus facilitating cross-border cooperation by law enforcement authorities.
[71] The Council of the European Union 2017b.

Wrongful acts by a state are based on the customary international law of State responsibility and refer to the breaches of international law obligations of states.[72] What constitutes a malicious cyber activity and how to respond to them are highly contentious and politicised subjects in cyberdiplomacy debates.[73] Based on the Tallinn Manual 2.0, the responsive measures can range from retorsion to self-defence. Retorsion is the "taking of measures that are lawful, albeit 'unfriendly'".[74] States have the right to apply retorsion, even when the original malicious cyber activity does not reach the threshold of an internationally wrongful act, or cannot be attributed to another state.[75] Countermeasures would otherwise be unlawful, but they are permissible if undertaken in response to another state's unlawful conduct. However, the original malicious cyber activity has to be attributed to a state, not merely to a non-state actor operating from the state's territory.[76] According to Article 51 of the UN Charter, a state's right to self-defence arises in the cyber context when a hostile cyber operation amounts to an 'armed attack'. In case of a cyber armed attack, the state is permitted to resort to force, including cyber operations at the 'use of force' level, to defend itself. Most 'Western powers' share in the understanding that certain malicious cyber operations may amount to the use of force or armed attack, and that it has a deterrent effect.[77]

After following the Draft Conclusions for months, the *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities* was presented by the EEAS and the Commission containing the details of the Toolbox.[78] The guidelines provide a broad set of conditions under which the collective response measures can be applied: for example, they can be used "to prevent or respond to a malicious cyber activity, including in case of malicious cyber activities that do not rise to the level of internationally wrongful acts but are considered as unfriendly acts"; they have to be based on shared situational awareness agreed among Member States. The scope of the perpetrators is not restricted to states; however, the document focuses primarily on state responsibility.

The CFSP instruments[79] that have been partially discussed above, for instance, international dialogue, or confidence and capacity building measures, provide the pool of collective diplomatic response measures. Response measures in this Framework are organised in five categories: Preventive measures; Cooperative measures; Stability measures; Restrictive measures; Possible EU support to Member States' lawful responses. Under the process to invoke the measures within the framework, the two CFSP crises management

[72] Schmitt 2017, 84.
[73] Rehrl 2018.
[74] Schmitt 2017, 112.
[75] Härmä–Minarik 2017.
[76] Härmä–Minarik 2017.
[77] Rehrl 2018.
[78] The Council of the European Union 2017a.
[79] The legal basis for the CFSP was set out in the TEU and revised in the Lisbon Treaty Title V, Articles 21–46.

mechanisms can be mobilised as well: the Integrated Political Crisis Response (IPCR), and the invocation of the solidarity clause (Article 222 TFEU).

Attribution is a pivotal issue in response mechanisms. According to the guidelines: "Attribution of a malicious cyber activity remains a sovereign political decision based on all-source intelligence, taken on a case-by-case basis. Every Member State is free to make its own determination with respect to attribution of a malicious cyber activity".[80] "Not all of the measures presented in this Framework will require attribution: they are a means of preventing or resolving a cyber incident, expressing concerns and signalling them in another way. Furthermore, the use of the measures within the Framework can be tailored to the degree of certainty that can be established in any particular case".[81]

Cybersecurity attribution

In order to fully comprehend the evolution of the EU's International cybersecurity policy, and especially the Cyber Diplomacy Toolbox, the problems stemming from the attribution need to be surveyed systematically. In the cybersecurity context, the so-called attribution problem is one of the most difficult technical hurdles to overcome. Moreover, attribution is also at the core of the response measures at the political and strategic level. In March 2019, the EEAS presented a non-paper on the *Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Attribution of malicious cyber activities* that defines attribution "as a practice of assigning responsibility for a malicious cyber activity to a specific actor".[82] The problem arises from the fact that there is no standardised agreement on how to achieve reliable attribution at the technical or the political level. Moreover, the technical, human and political attributions all have significant barriers. On the other hand, those deficiencies offer plausible deniability for cyberspace perpetrators.

First, it is essential to consider the different attribution layers. One prominent academic researcher, Thomas Rid, for example, differentiates between three levels of attribution:

"The tactical goal is understanding the incident primarily in its technical aspects, the how. The operational goal is understanding the attack's high-level architecture and the attacker's profile the what. The strategic goal is understanding who is responsible for the attack, assessing the attack's rationale, significance, appropriate response the who and why. Finally, communication is also a goal on its own: communicating the outcome of a labour-intensive forensic investigation is part and parcel of the attribution process, and should not be treated as low priority".[83] Technical attribution consists of analysing malevolent functionality and malicious packets, and using the results of the analysis to locate the node that initiated, or is controlling the attack.[84] Next, what Rid classified as

[80] The Council of the European Union 2017a.
[81] The Council of the European Union 2017a.
[82] The Council of the European Union 2019a, 4.
[83] Rid–Buchanan 2015, 4.
[84] Boebert 2010.

the operational layer of the attribution process strives to synthesise all-source intelligence. Analysts functioning on the operational layer develop competing hypotheses to explain the incident. However, the uncertainty of attributive statements is likely to increase as the analysis moves from technical to political, including the question of the attacker's motivation.[85]

On a strategic level, leaders and top analysts are tasked with aggregating the answers to operational questions, such as intelligence gain/loss, in order to draw meaningful conclusions. Finally, political leaders have to decide about the optimal response measure involving the dilemma of public attribution that best suits the state's interest in the given situation, as well as on a strategic time scale.

According to the EU non-paper *Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Attribution of malicious cyber activities,* "coordinated attribution could signal strong EU Member States' capabilities to establish with certainty that an actor holds responsibility for a malicious cyber activity could be also taken into account, as it can diminish an actor's willingness and ability to carry out further malicious activities".[86] Coordinated attribution has come to the forefront of recent political and diplomatic discussions. Based on the precedent set over the past years, some nation states have increasingly resorted to public attribution as an important diplomatic asset of their cyberattack response strategy, which also means that they become more willing to overcome information sharing barriers to achieve shared situational awareness. For instance, in December 2017 the Five Eye countries, the U.K., the USA, Canada, Australia and New Zealand have often joined to call out cyberattacks that have been attributed to nation states, among others, pointing the finger at North Korea for WannaCry. In February 2018, the U.K. and Denmark, together with the USA and Australia, publicly attributed the NotPetya cyberattack to the Russian Government. In these collective actions there is also the intention of setting norms of what is not acceptable state behaviour in cyberspace, and thus signalling that it will have repercussions. So far, some of the joint public EU response measures to malicious cyber activity are:

- Declaration by the High Representative on behalf of the EU condemning the cyberattack against Georgia (February 2020)
- Declaration by the High Representative on behalf of the EU stressing the need to respect the rules-based order in cyberspace (April 2019)
- Statement by Commission President Juncker, High Representative Mogherini and Council President Tusk on the targeted cyberattack against OPCW (October 2018)
- Council Conclusions responding to malicious cyber activities, including Wannacry and NotPetya (April 2018)

[85] Rid–Buchanan 2015.

[86] The Council of the European Union 2019a, 4.

EU cyber sanctions

On 17 May 2019, the Council of the European Union adopted *Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States,*[87] and *Council Regulation concerning restrictive measures against cyber-attacks threatening the Union or its Member States.*[88] The new legislation was a follow-up on the Conclusions establishing the Cyber Diplomacy Toolbox. The Council Decision and Regulation constitute a remarkable step forward in the line of thought on responsive measures to cyberattacks. Before, the EU could impose sanctions only on persons and entities involved either in terrorism, or in the proliferation of chemical weapons. Consequently, it is essential to have a legislation that specifically tackles cyberspace-related threats.

A cyber activity for consideration here means an action that includes: access to information systems; information system interference; data interference; or data interception. Sanctions can be imposed on planned attacks as well. To be subject to sanctions, a cyberattack must fulfil two criteria: the attack has a significant effect; and the attack constitutes an external threat to the Union or its Member States. When deliberating whether a cyberattack has a significant effect, a series of indicators are to be considered: the scope, scale, impact or severity of disruption caused; the number of natural or legal persons, entities or bodies affected; the number of Member States concerned; the amount of economic loss caused; the economic benefit gained by the perpetrator, for themselves or for others; the amount or nature of data stolen or the scale of data breaches; and the nature of commercially sensitive data accessed.[89] The ruling only applies to external cyberattacks targeted against an EU institution, Member State. In addition, when it is necessary to achieve an EU common security and defence policy objective, sanctions can also be imposed as a response to cyberattacks with a significant effect against third States or international organisations. Sanctions can materialise essentially in two ways: a prevention of the entry of the sanctioned into, or transit through, territories of EU Member States; second, no funds or economic resources shall be made available directly or indirectly to or for the benefit of the listed.

In sharp contrast to the legislation's antecedents, namely the 2017 Conclusion on the Toolbox, its Implementing Guidelines and the non-paper on Attribution, the sanctions can be directed only against natural or legal persons, other entities or bodies different from a State. Focusing on individually listed non-state actors, the sanctions are targeted or 'smart', i.e. intended to harm a precisely defined subject that represents a threat, not to affect a whole State and its population.[90]

[87] The Council of the European Union 2019b.
[88] The Council of the European Union 2019c.
[89] Botek 2019.
[90] Botek 2019.

References

Boebert, W. Earl (2010): A Survey of Challenges in Attribution. Sandia National Laboratories. In *Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy.* Washington, D.C., The National Academies Press. Source: www.nap.edu/catalog/12997/proceedings-of-a-workshop-on-deterring-cyberattacks-informing-strategies-and (Accessed: 18.02.2020.)

Botek, Adam (2019): *European Union establishes a sanction regime for cyber-attacks.* Source: https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/ (Accessed: 21.04.2020.)

Christou, George (2016): *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy.* Palgrave Macmillan.

DG Connect, Next-Generation Internet (Unit E.3) (s. a.): *Shaping Europe's Digital Future: Mission.* Source: https://ec.europa.eu/digital-single-market/en/content/next-generation-internet-unit-e3 (Accessed: 02.05.2020.)

DiploFoundation (2019): *Diplo's crystal ball exercise: Digital policy in 2019.* Source: www.diplomacy.edu/blog/diplo%E2%80%99s-crystal-ball-exercise-digital-policy-2019 (Accessed: 02.05.2020.)

EU Cyber Direct (2019): *Council Conclusions on Cyber Diplomacy.* Source: https://eucyberdirect.eu/content_knowledge_hu/council-conclusions-on-cyber-diplomacy/ (Accessed: 21.04.2020.)

European Commission (2012): *Communication from the Commission to the European Parliament and the Council. The EU Approach to Resilience: Learning from Food Security Crises.* COM(2012) 586 final. Source: https://ec.europa.eu/echo/files/policies/resilience/com_2012_586_resilience_en.pdf (Accessed: 18.02.2020.)

European Commission (2017): European Commission Working Staff Document SWD 295 final.

EUINTCEN Fact Sheet (2015). *The EU Intelligence Analysis Centre.*

Härmä, Katriina – Minárik, Tomáš (2017): *European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox.* NATO Cooperative Cyber Defence Centre of Excellence. Source: https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/ (Accessed: 21.04.2020.)

High Representative of the European Union for Foreign Affairs and Security Policy (2013): *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* JOIN(2013) 1 final.

Missiroli, Antonio ed. (2016): *The EU and the World: Players and Policies post-Lisbon. A Handbook.* European Union Institute for Security Studies. Source: www.iss.europa.eu/content/handbook-%E2%80%93-eu-and-world-players-and-policies-post-lisbon (Accessed: 21.04.2020.)

Pawlak, Patryk (2018): *Operational Guidance for the EU's international cooperation on cyber capacity building.* Source: www.google.com/search?q=Operational+Guidance+for+the+EU%E2%80%99s+international+cooperation+on+cyber+capacity+building&rlz=1C1GCEA_enHU829HU829&oq=Operational+Guidance+for+the+EU%E2%80%99s+international+cooperation+on+cyber+capacity+building&aqs=chrome..69i57.926j0j4&sourceid=chrome&ie=UTF-8 (Accessed: 22.03.2020.)

Presidency of the European Council (2016): *Non-paper: Developing a joint EU diplomatic response against coercive cyber operations.* 5797/4/16 REV 4. Source: https://data.consilium.europa.eu/doc/document/ST-5797-2016-REV-1/en/pdf (Accessed: 05.01.2020.)

Rid, Thomas – Buchanan, Ben (2015): Attributing Cyber Attacks. *Journal of Strategic Studies,* Vol. 38, No. 1–2. 4–37.

Rehrl, Jochen (2018): *Handbook on Cybersecurity. The Common Security and Defence Policy of the European Union.* Luxembourg Publications Office of the European Union.

Schmitt, Michael N. ed. (2017): *Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations.* NATO Cooperative Cyber Defence Centre of Excellence.

The Council of the European Union (2017a): *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities.* 13007/17.

The Council of the European Union (2017b): *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* 9916/17.

The Council of the European Union (2019a): *Implementation of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Attribution of malicious cyber activities.* 6852/1.

The Council of the European Union (2019b): *Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.*

The Council of the European Union (2019c): *Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.*

United Nations (2015): *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (A/70/174).* United Nations, General Assembly. Source: https://undocs.org/pdf?symbol=en/a/70/174 (Accessed: 04.05.2020.)

VÁKÁT OLDAL

Csaba Krasznay

Case Study: The NotPetya Campaign

Introduction

The range of malicious acts affecting cyberspace is endless, but there are events that provide a red line and a point of reference for researchers. The attack on Estonia in 2007, the deployment of the Stuxnet malicious code, the leak of information by Edward Snowden were all such events when we had to re-evaluate our views on cyberspace. From the perspective of the present study, the NotPetya malicious code campaign is a turning point that explains the importance of international law and international relations in connection to cyber events. This incident has highlighted some critical points on the field of external relations, which showed in practice that the creation of the Tallinn Manual or the proposal for a Digital Geneva Convention was necessary because of the practice of some countries in interpreting international norms freely.

The technical perspective

According to a summary in the Wired magazine, the NotPetya campaign started on the afternoon of 27 June 2017, in the last working hours of the working day before the celebration of the Ukrainian Constitution. The date of the first infections was food for thought, as choosing a prominent holiday of the Republic of Ukraine as the beginning of the attack was a signal message. Meanwhile, at that moment it was still probable that the time was also chosen based on the fact that the majority of IT operators would be on leave, so the defence would work with lower resources. Although the malware appeared soon in other countries, most of the infected machines were reported from Ukraine, so it is suspected that the target was Ukraine as a state and not some companies were on the crosshairs. In other countries, including Germany, France, Italy, Poland and the United States, there were only collateral damages. This theory is further reinforced by the fact that an explosive device hidden in a motor vehicle killed a member of the Special Forces in Kiev on the same day.[1]

The malicious code had the characteristics of a ransomware, encrypting the hard drive after infection and asking for 300 USD in bitcoin in exchange for unlocking the machine. However, it soon became clear that the email address provided for the contact was not alive, so there was no chance of recovering the lost data. If the attack was financially motivated, as in case of WannaCry a month before NotPetya, the attacker would have remained available and would have secured the return of the data in exchange

[1] Greenberg 2017.

for a ransom, as the victim only paid if there was a chance for the decryption as it was learnt from similar crimes. The characteristics of a ransomware in the early hours was also emphasised by the fact that the code showed similarities to the well-known Petya ransomware, but it was soon discovered that it was an intentional camouflage, so the name NotPetya, or Non Petya became widespread among cybersecurity experts.

In terms of mechanism of action, the malicious code infected the computer's master boot record, the hard disk segment responsible for loading the operating system, and began encrypting the file system after the machine was started. If that succeeded, it showed a typical ransomware message on the screen, indicating how much money it was asking for the decryption and how the communication was possible with the cybercriminals. Before making the machine unusable, it tried to spread to the network on which the infected machine was located. It used the EternalBlue vulnerability, and as it could be seen in case of WannaCry, it started to spread on the previously non-updated computers, meanwhile it collected the administrator password from the infected machine's memory, that also could give access to other networked machines.

The first infections were assumed to have come through a software update mechanism of the MEDoc application. This software is one of the officially approved tax return programs, so it runs on a significant part of Ukrainian companies. This program indicated that it needed to be updated, and then after the user allowed the patches to be installed, the infection began. There is no information on how they could influence the MEDoc update process. From remote hacking to direct, physical access to the update server, there are a number of possible solutions to consider. It seems certain that the attacker gained administrative privileges on one of MEDoc's servers, which allowed him to intervene in the update mechanism as well. According to an investigation by the cybersecurity company Talos, as early as 24 April 2017, an update was released to users that included a backdoor, so in principle, it allowed the attack to be carried out. Therefore, the attackers started preparing for the action months earlier. Against WannaCry, there was not any hidden code or so-called "kill switch", which would have enabled the rapid shutdown of the infection. The attacker's goal was clearly the largest, geographically most localised destruction.[2]

Eventually, thousands of Ukrainian companies were hit by the incident. The victims include certain critical Ukrainian infrastructures, including Ukrainian banks, Kiev Borispol Airport, and energy companies such as Kyivenergo and Ukrenergo. But several foreign companies have also reported infections, such as the American medical company Merck, the Russian Rosnyeft and the Hungarian OTP Bank in Ukraine, whose ATMs displayed the images of the NotPetya infection for days. Most publicity was given to the devastation at A.P. Moller–Maersk. This company is the 558th largest conglomerate in the world according to the Forbes Global 2000 list of companies, one of the largest logistics companies in the world. The NotPetya infection reportedly made it impossible for the company to operate for two days. Loading of cargo ships worldwide had to be controlled

[2] Maynor et al. 2017.

manually, relying on paper and pencil instead of a computer. This was also reflected in the Danish company's revenue, with their quarterly report estimating that they suffered between $200 million and $300 million in damage from this two-day shutdown.[3]

International law perspective

The NotPetya malicious code is the first cyber incident that appears to be a coordinated attack on a sovereign state in peacetime, attacking its critical infrastructures, civilian facilities, causing additional damage to civilian companies operating in other countries as well. Its purpose was clearly destruction. Tools used by the malicious code were previously known, as neither the vulnerability exploited for network propagation nor the software that was used to access the credentials of privileged users caused a surprise to professionals. However, attack tactics were completely new, preceded by a thorough operational planning, as the MEDoc software chosen for distribution was unknown beyond Ukraine, only adequate intelligence could confirm that this propagation vector could be so effective in carrying out a geographically focused cyberattack. The psychological or social engineering twist in the attack should also be emphasised, which led the victims to believe that a version of MEDoc that would open a backdoor for malicious code should be installed. For decades, cybersecurity professionals have been aware that both end-users and IT operators need to use the latest version of software, so if a software update is available, it should be installed as soon as possible. Therefore, the attacker built the distribution on this foundation, believing that users would install anything that appears to be an update as soon as possible, without question, so attacking the update server and using it as a distribution point is a brilliant choice.

From the states' perspective, the right answer should be decided if there is a cybersecurity incident that looks like a cyberwarfare activity, in which an advanced cyber weapon was deployed in a country that has previously suffered such targeted attacks and it is used regularly as a weapons test site by another country. Can it be said that this incident is classified as an attack within the meaning of international law? Can they use the means of attribution, or name a country an attacker? On the other hand, the question is also whether international diplomacy is prepared to deal with the countermeasures of the named country by traditional diplomatic means after such a declaration? Finally, the question is also whether the named attacking country can be put under pressure as a result of which it will reduce or end its hostilities in cyberspace?

Schmitt and Biller examined how the incident relates to the requirements of international law a few weeks after the NotPetya attack. Their first remark was that the malicious code was not reported to have caused injury or death. The author of the present study adds that, although no direct deaths were reported for either NotPetya or WannaCry, it cannot be excluded that non-functioning electronic information systems in some healthcare facilities, especially in case of WannaCry, may have contributed indirectly to deaths

[3] A.P. Moller–Maersk 2017.

in the U.K. healthcare system that could have been prevented if the patient had been provided with appropriate care in a timely manner. Schmitt and Biller link accountability to attribution, i.e. the main question is whether the attack was backed by a country's armed forces, intelligence agencies, or whether the instructions were given by a state actor in case of a non-state attacker. Assuming that this has happened, a breach of three state obligations can be presumed. These are respect for sovereignty, the principle of non-interference and the prohibition of the use of force.

According to Schmitt and Biller, sovereignty was violated during the NotPetya attack because of two conditions. On the one hand, a violation of territorial integrity, which in cyberspace can be imagined as an attack causing physical damage or personal injury, possibly death. In a broad interpretation, if a cyber infrastructure becomes unavailable for an extended period of time, in the opinion of the authors, a violation of territorial integrity can also be formulated. Because NotPetya went beyond the effects of an average distributed denial of service attack, specifically involving the loss of key data and the need to deploy new machines instead of disrupted critical computer systems, this can be seen as damage to physical facilities. The other condition would be the disruption of core government activities, but this was not the case for NotPetya. Although the IT systems that enable financial institutions to operate are damaged, they do not support basic government functionality, so this condition for violating sovereignty did not exist.

Violations of the principle of non-interference are accompanied by coercive actions taken by one state against another in order to change its political, economic, social and cultural order and to influence foreign policy. Schmitt and Biller did not see evidence that the NotPetya malicious code was capable of achieving these purposes, given that its purpose was destruction and not influence. If the cyber weapon had indeed been a ransomware virus, which seemed at first glance, coercion would in principle have been possible since the essence of ransom is to extort some decision from the other party.

The principle of the use of force in peacetime means that a state engages in a violent activity that does not qualify as self-defence or collective defence without a UN mandate. Activities in the cyberspace typically have little impact on the physical environment, making it difficult to imagine an attack that reaches an unauthorised level of use of force. The long-term outage of a cyber infrastructure as computers or network devices become inaccessible due to a malicious code like NotPetya, however, could be classified as unauthorised use of force. According to the authors, economic destabilisation may also fall into this category. According to the Ukrainian Government, the cyberattack has reached this level, but international practice in mid-2017 has not yet provided a clear answer as to where the threshold is.

The authors' opinion is that international humanitarian law would be valid in this case if there were an international armed conflict between two states, namely Ukraine and, suppose, Russia. The condition in that case is that one country occupies the territory of another country or supports a non-state group that engages in hostile activity against the other country. Given the support of the Crimean Peninsula and the uprisings in eastern Ukraine, the authors see a legitimate presumption of an armed conflict between the

two states, therefore the use of NotPetya should also be examined under international humanitarian law, despite the fact that in the UN GGE there is no full agreement on this.[4] The classification of this malicious code should be examined in the light of the Tallinn Handbook, which states that the use of such cyber weapons is an attack even if it does not directly damage the cyber infrastructure, only has indirect effects. According to some experts, the inaccessibility of such infrastructure also belongs to that set.

NotPetya's targets included Kiev Airport, the Chernobyl power plant, and the Ukrainian healthcare system. If it can be assumed that this was done in accordance with the attacker's intention and not due to the uncoordinated spread of the malicious code, this can be classified as an attack according to the authors. Although some of the disputed facilities could be classified as dual use, such as the airport, most elements of cyber infrastructure are clearly civilian, not serving military purposes, so the act could even fall into the category of a war crime. In addition, the impact of cyber weapons went beyond Ukraine, it also had an impact on third countries, so their neutrality was violated by the attacker.[5]

All of these are, of course, only the scientific thinking of researchers, as mentioning war crimes in case of a cyberattack can have serious diplomatic implications, if it is done by a politician in charge. As it can be read in the next chapter, states use moderate expressions, even if they have a strong diplomatic reaction. NotPetya, on the other hand, is special that in addition to researcher positions, there have been comments and then political resolutions that should be taken more seriously than theoretical reasoning. First, researchers from NATO's Center for Excellence in Cooperative Cyber Defense analysed the situation. The quoted Michael Schmitt also belongs to this scientific circle, but the analysis quoted earlier did not appear on the organisation's website; therefore, the article by Blumbergs, Minárik, van der Meij and Lindström has already been published by the world press as NATO's position. Thus, special emphasis is placed on what Minárik said: "If the operation is related to an international armed conflict, it is subject to the legislation on armed conflict." Previously, NATO CCD COE commentaries had not visited the world press on such a delicate matter, so it could be perceived that NotPetya weighed significantly more than any other previous case.[6]

The states' answer

Countries were not prepared for such a serious violation of international norms. The really big breakthrough came only in February 2018, when 7 countries, the United States, the United Kingdom, Denmark, Lithuania, Estonia, Canada and Australia, jointly condemned Russia for the NotPetya attack, which was officially supported by New Zealand, Norway, Latvia, Sweden and Finland. Never before have several countries used the means of

[4] Schmitt–Vihul 2017.
[5] Schmitt–Biller 2017.
[6] Blumbergs et al. 2017.

attribution together, that is, they have pointed out the attacker in unison. Attribution is always a political decision that can be supported by technical or intelligence evidence, but without political will, they are not worth much. Tobias Feakin, Australia's Ambassador for Cyber Affairs, summed up excellently why this joint stand was an important step and what it means for the attackers: "What we're doing is maturing this approach in order that the consequences will be felt further in the future. So another key part of deterrence is signalling to another country, to provide clear, consistent, and credible messaging to adversaries that there will be repercussions for the behaviour that they're conducting."[7]

Depending on the attribution's certainty, there are several tools in the hand of nation states to give answer to a cyberattack. Moret and Pawlak give an example, how individual countries or EU institutions, member states in the EU Council or the EU in cooperation with international organisations can choose from the following answers:[8]

- statements and demarches
- international agreements
- capacity building
- strategic communication
- joint investigations
- statements by HR/VP
- EU demarches
- formal request for assistance
- Council conclusions
- political and cyber dialogues
- recalling diplomats
- sanctions
- solidarity clause
- countermeasures
- Mutual Defence Clause
- military response

At the time of NotPetya only the United States implemented unilateral cyber sanctions. In 2015, President Barack Obama used this format against North Korea in response to the attack against Sony Pictures. Therefore, other countries have not had any tested and proven responses against devastating cyberattacks. Until 2017, most countries officially treated the threats in cyberspace as an internal defence question; however, they agreed that international norms and legislation are valid in the cyberspace as well. Attribution, diplomatic or even military responses were not part of the common diplomacy toolbox. Only the United States had enough power to publicly attribute another country, generally speaking Russia, Iran and North Korea in connection with cyberattacks. That is why

[7] Stilgherrian 2018.
[8] Moret–Pawlak 2017.

NotPetya was a game changer. The U.S. Government attributed the NotPetya attack to Russia with the following statement from the Press Secretary of the Whitehouse:

"In June 2017, the Russian military launched the most destructive and costly cyber-attack in history. The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences."[9]

The Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security (DHS) together with the Federal Bureau of Investigation (FBI) even created a separate investigation and attribution stream to the Russian cyberattacks. It is called Grizzly Steppe. Both agencies analyse the tactics, techniques and procedures (TTPs as it is used in cybersecurity) of Russian state sponsored actors. Codename Grizzly Steppe was chosen right after the alleged intervention of Russian secret services in the 2016 Presidential Election. The list of cyberattacks was later enhanced with NotPetya and the cyber activity of the Russian Government targeting energy, other critical infrastructure sectors and network infrastructure devices.[10] DHS summarised such activities with the following sentences:

"Russia's civilian and military intelligence services engaged in aggressive and sophisticated cyber-enabled operations targeting the U.S. government and its citizens. The U.S. Government refers to this activity as GRIZZLY STEPPE. These cyber operations included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations, and theft of information from these organizations. This stolen information was later publicly released by third parties.

In operations targeting other countries, including U.S. allies and partners, Russian intelligence services (RIS) have undertaken damaging or disruptive cyber-attacks, including on critical infrastructure—in some cases masquerading as third parties or hiding behind false online personas designed to cause the victim to misattribute the source of the attack."[11]

A similar approach can be seen in other countries. Close U.S. allies like the United Kingdom or Australia also had clear statements on NotPetya. On 15 February 2018, U.K. Foreign Office Minister Lord Ahmad attributed this cyberattack to Russia highlighting that the U.K. and its allies will not tolerate malicious cyber activities.

"The UK Government judges that the Russian Government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017. The attack showed a continued disregard for Ukrainian sovereignty. Its reckless release disrupted organisations across Europe costing hundreds of millions of pounds. The Krem-

[9] Whitehouse 2018.
[10] CISA 2018.
[11] DHS 2016.

lin has positioned Russia in direct opposition to the West yet it doesn't have to be that way. We call upon Russia to be the responsible member of the international community it claims to be rather then secretly trying to undermine it. The United Kingdom is identifying, pursuing and responding to malicious cyber activity regardless of where it originates, imposing costs on those who would seek to do us harm. We are committed to strengthening coordinated international efforts to uphold a free, open, peaceful and secure cyberspace."[12]

On the next day, 16 February 2018, Australian Minister for Law Enforcement and Cyber Security, Angus Taylor released the following statement:

"Australian Government attribution of the 'NotPetya' cyber incident to Russia. The Australian Government has joined the governments of the United States and the United Kingdom in condemning Russia's use of the 'NotPetya' malware to attack critical infrastructure and businesses in June 2017. Based on advice from Australian intelligence agencies, and through consultation with the United States and United Kingdom, the Australian Government has judged that Russian state sponsored actors were responsible for the incident. Computers were infected by a sophisticated piece of malware – or malicious software – that masqueraded as ransomware. 'NotPetya' interrupted the normal operation of banking, power, airports and metro services in Ukraine. While the brunt of the impact was felt in Ukraine, the malware spread globally, affecting a number of major international businesses causing hundreds of millions of dollars in damage. The Australian Government condemns Russia's behaviour, which posed grave risks to the global economy, to government operations and services, to businesses activity and the safety and welfare of individuals. The Australian Government is further strengthening its international partnerships through an International Cyber Engagement Strategy to deter and respond to the malevolent use of cyberspace. The Government is committed to ensuring the Australian public sector, businesses and the community are prepared for evolving cyber threats."[13]

Estonian Minister of Foreign Affairs, Sven Mikser reflects to the U.K. Government in his press release:

"The NotPetya cyber-attack which targeted Ukraine's financial, energy and government sectors and undermined the sectors' resilience, demonstrated disrespect for Ukrainian sovereignty and caused significant economic losses in other countries too. It is very important for Estonia to maintain an open, stable and secure cyber space and for that, countries have to act responsibly and follow the rules of international cooperation and the norms of international law that apply in cyber space just like everywhere else."[14]

As we can see, those countries who officially attributed Russia, draw up their views by the foreign ministers or ministers responsible for cybersecurity. Supporting nations of this diplomatic step also emphasised the role of Russia, but the announcements were

[12] Foreign and Commonwealth Office 2018.
[13] Parliament of Australia 2018.
[14] Republic of Estonia 2018.

made by lower ranked government officials. For example, in New Zealand, Director-General of the Government Communications Security Bureau (GCSB) Andrew Hampton released the statement.

"While NotPetya masqueraded as a criminal ransomware campaign, its real purpose was to damage and disrupt systems […]. Its primary targets were Ukrainian financial, energy and government sectors. However, NotPetya's indiscriminate design caused it to spread around the world affecting these sectors world-wide. While there were no reports of NotPetya having a direct impact in New Zealand, it caused disruption to some organisations while they updated systems to protect themselves from it. This reinforces that New Zealand is not immune from this type of threat. In a globally connected world our relative geographic isolation offers no protection from cyber threats. We support the actions of our cyber security partners in calling out this sort of reckless and malicious cyber activity."[15]

In case of Latvia, the public reaction was a short message on Twitter from the Ministry of Foreign Affairs: "#Latvia is deeply concerned about the findings of UK & US attribution of #NotPetya #Cyber_attacks and stands for responsible state behaviour in cyberspace."

Deterrence in cyberspace

NotPetya was the red line for Western countries that invoked not only diplomatic reactions as it was mentioned in the previous section, but after 2018, some countries, especially the United States have publicly introduced some retaliatory actions against Russia. This is not surprising as according to the traditional deterrence theory, three elements should be present to stop a rogue activity: attribution, credible signalling and deterrence strategies. Taddeo explains that as follows: "A believes that B is planning to attack it. In order to avoid the attack, A makes an explicit commitment to take action against B, should B decide to attack. A's commitment should be such that B is convinced that any action against A will fail, because A has the capacity either to resist or punish B, and to outweigh any prospective gains for B. B's conviction hinges on A's signalling and credibility to act as it threatens. According to this model, we find here the three core elements of deterrence theory: the identification of the opponent (attribution); defence and retaliation as types of deterrence strategies; and the capability of the defender to signal credible threats."[16]

In that sense, attribution is only the first step. However, responsible attribution is not as easy as it seems to be, that is why only the United States, the only superpower used this tool before NotPetya. In the cyberspace, attribution needs both convincing technical evidence and reliable intelligence sources. Due to the anonym and global nature of the Internet, collection of hard evidence from computers and networks is struggling. What can be seen on the defenders' side is only a few technical information or indicators of

[15] GCSB 2018.
[16] Taddeo 2018.

compromise (IoC). They are usually files and operating system activities or source/destination IP addresses. Security researchers should prove who are behind NotPetya by finding evidence in the following infection process:[17]

- dropped files
- process hashes and process privilege checks
- credential theft
- token impersonation
- malware propagation
  - network node enumeration
  - SMB copy and remote execution
  - SMBv1 exploitation via EternalBlue
- UNC write malware to admin$ on remote target
- remote execution of the malware
  - MBR ransomware
  - physical drive manipulation
  - MFT encryption
- file encryption
- system shutdown
- anti-forensics

In case of NotPetya, the EternalBlue vulnerability, used for malware propagation was originated from the National Security Agency in the United States. For credential theft, the attackers used Mimikatz, originally created as a proof of concept by French security researcher Benjamin Delpy in 2011. There was not a complex network infrastructure with millions of previously infected computers in the botnet, as the attack was targeted, originated from the MEDoc update server and it is still not known who and how has hacked this server. In such cases, researchers can only rely on the coding style of the malware. Source codes are similar to fingerprints. A programmer usually has his own coding style; a group of programmers are usually using the same framework to improve their software. Cybercriminals are usually lazy enough to make only minor changes, "feature releases" in different campaigns. But that is not true in case of sophisticated, state sponsored targeted attacks. The name NotPetya was chosen as for first sight, it was similar to Petya ransomware, although it is now obvious, that there is no connection between the two malwares. It is possible that the original source code of NotPetya was stolen or bought from the original author who was convicted by a regional court in Nikopol in the Dnipropetrovsk Oblast of Ukraine to one year in prison in 2018 after pleading guilty to having spread a version of Petya online. He is an unnamed Ukrainian citizen.

NotPetya's traces were well hidden from the technical perspective. Neither governmental, nor industry sources have uncovered any "smoking guns" that underpins the

[17] Sood–Hurley 2017.

role of Russia in this cyberattack. However, many countries attributed them with high confidence. We can assume that the United States and maybe other countries had indisputable intelligence information. As Carr wrote: "The most likely adversary responsible for a covert attack against those critical systems is an extremist group (religious, political, or anarchist), and the best way to learn which of those groups may have been responsible post-attack is to already have in place a long-term counter-intelligence campaign of infiltration and the development of trusted contacts with access. This cannot be done virtually or from behind a computer. Rather, those intelligence agencies that have yet to devote the bulk of their budget to signals capabilities may be best positioned to tackle the problem of attribution. They understand the need to continue to fund and even expand human intelligence – this is still vital, despite the fact that we are living in the age of Facebook, Twitter and Instagram."[18]

The assumption about the U.S. and allies' capabilities on cyber intelligence against Russia can be confirmed with some examples after NotPetya. We can count such leaked information and direct responses as credible signalling according to the deterrence theory. As Taddeo defines, "Signaling can be either general or tailored. General signaling conveys a message about the overall deterrence strategy to the rest of the international arena, through open statements released by a state conveying information about its approaches, commitments, and capabilities […]. Tailored signaling—the conveying of a threat to a specific offender indicating the possible targets of retaliation—is more problematic than general signaling and constitutes a significant obstacle to delivering effective deterrence strategies in cyberspace. This kind of signaling is effective if attribution is certain. If the defender has not identified the offender correctly, tailored signaling can be counterproductive given it may be directed to the wrong actor. Tailored signaling also requires a careful finetuning in order not to expose the defender's capabilities and assets, especially when the defender is considering retaliation in-kind. The risks are multiple and range from exposing knowledge about the opponent's cyber assets, which would imply that the defender has also run cyber operations (sabotage or espionage) against the opponent, to revealing the defender's assets and strategies, which may expose and therefore render futile its cyber capabilities, such as zero-day exploits (for example)."[19]

First of all, on 11 June 2018, the U.S. Department of Treasury's Office of Foreign Assets Control designated five Russian entities and three Russian individuals under Executive Order (E.O.) 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." All property and interests in property of the designated persons subject to U.S. jurisdiction are blocked, and U.S. persons are generally prohibited from engaging in transactions with them.[20]

[18] Carr 2014.
[19] Taddeo 2018.
[20] U.S. Department of Treasury 2018.

Some notable cyberattacks can also show how Western countries retaliated Russian cyber (and other military) activities by flashing their capabilities:

- Panama Papers: In 1 April 2016, Mossack Fonseca, Panamanian law firm and corporate service provider notified its customers that millions of digital documents were stolen after a targeted cyberattack. These documents consisted detailed information about the tax avoidance and money laundry of many notable persons. The hack was committed by an unknown hacker, "John Doe", who said that he had never worked for any intelligence agency. Whether it is true or not, the Süddeutsche Zeitung published an interview with Alexey Navalny, head of the Moscow-based NGO Anti-Corruption Foundation on the connection of President Putin and other leading figures with Panama Papers.
- Dutch intelligence against Cozy Bear: In January 2018, Dutch news sources published a story on how their domestic intelligence service, AIVD access the IT system of Cozy Bear hacker group that is believed to be associated with Russian intelligence. This group is suspected with many notable cyberattacks, such as attacks during the 2016 Presidential Election.
- Bellingcat and Skripal Poisoners: In 2018 and 2019, Bellingcat, the online investigative journal has published a series of articles about the poisoners of Sergei Skripal and his daughter, who died in the United Kingdom. Based on open source intelligence, they could identify the poisoners and track back their lives even until high school. Although such investigative journalism is highly appreciated, it can be assumed that some kind of official intelligence support was provided by Western countries.
- U.S. cyberattacks on Russian Power Grid: In response to the cyberattacks against its critical infrastructures, the U.S. has conducted a similar attack and shared this information with the press in June 2019. As President Trump's national security adviser, John R. Bolton, said the United States was now taking a broader view of potential digital targets as part of an effort "to say to Russia, or anybody else that's engaged in cyberoperations against us, 'You will pay a price.'"

Conclusion

Traditional deterrence theory proposes two potential deterrence strategies: deterrence by defence and by retaliation. In the cyberspace, believing solely in deterrence by defence is not a real option. Simply, because the already developed tools, techniques and procedures set are enormous, and attackers can easily create a previously non-existing attack path. From their point of view, one weak link in the defence chain is enough for success. Therefore, countries should rely more on defence by retaliation, not forgetting to improve their defence capabilities as well. We can see such efforts all over the world.

The EU Cyberdiplomacy Toolbox is an example for that. As the press release of the Council of the EU states: "On 17 May 2019, the Council established a framework which allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks which constitute an external threat to the EU or its member states, includ-

ing cyber-attacks against third States or international organizations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP)."[21] Lack of EU reaction to NotPetya is a symptom why this Toolbox is necessary. As EU members' relation to Russia is complicated, without such common understanding, it is difficult to find a harmonised way for joint sanctions. But states do not forget and forgive. After 5 years of a cyberattack against the German Parliament, Chancellor Angela Merkel seeks EU sanctions as they have hard evidence against Russian actors. This will be the first test of the Toolbox where EU members can prove their willingness for a coordinated response.[22]

"Cyberattacks falling within the scope of this new sanction's regime are those which have significant impact and which:

- originate or are carried out from outside the EU or
- use infrastructure outside the EU or
- are carried out by persons or entities established or operating outside the EU or
- are carried out with the support of person or entities operating outside the EU.

Attempted cyber-attacks with a potentially significant effect are also covered by this sanction's regime. (…) Restrictive measures include a ban on persons travelling to the EU, and an asset freeze on persons and entities. In addition, EU persons and entities are forbidden from making funds available to those listed."[23]

We can see that the U.S. government is actively using the deterrence by retaliation strategy. Currently, it seems to be successful, as since 2017 there was not any major cyberattack attributed to Russia. However, most of the actions on that field are covert and the public audience will get information decades later. Jason Healey, one of the best scholars in this topic and Neil Jenkins tried to measure the success of deterrence from the U.S. perspective. Their article ends with the following thoughts: "We can't assess what we don't try to measure. Together, the frameworks in this paper can act as a check on whether these new, riskier U.S. cyber policies and operations are succeeding in suppressing incoming attacks, or inciting them […] the U.S. Government cannot easily even know all its own operations against adversaries: some will be covert actions, others espionage, while others are "traditional military operations." Each is held in a separate compartment and few individuals have the full picture."[24]

Whatever will happen, the alleged attackers' response will be the same what we could hear from Kremlin spokesman Dmitry Peskov in February 2018, right after the attribution of many countries: "We categorically reject such accusations. We consider them unsubstantiated and groundless. This is nothing but a continuation of a Russophobic campaign that is not based on any evidence."[25]

[21] Council of the EU 2019.
[22] Stupp 2020.
[23] Council of the EU 2019.
[24] Healey–Jenkins 2019.
[25] AFP 2018.

References

AFP (2018): *Kremlin 'categorically' denies Russia behind NotPetya cyber-attack.* Source: www.france24.com/en/20180215-kremlin-categorically-denies-russia-behind-notpetya-cyber-attack (Accessed: 06.05.2020.)

A.P. Moller–Maersk (2017): *A.P. Moller–Maersk improves underlying profit and grows revenue in first half of the year.* Source: www.maersk.com/press/press-release-archive/20170816-a-p-moller-maersk-improves-underlying-profit-and-grows-revenue-in-first-half-of-the-year (Accessed: 21.04.2020.)

Blumbergs, Bernhards – Minárik, Tomáš – Van Der Meij, Kris – Lindström, Lauri (2017): *NotPetya and WannaCry Call for a Joint Response from International Community.* Source: https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html (Accessed: 21.04.2020.)

Carr, Jeffrey (2014): *Responsible Attribution: A Prerequisite for Accountability.* Source: https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-6-Carr.pdf (Accessed: 06.05.2020.)

Council of the EU (2019): *Cyber-attacks: Council is now able to impose sanctions.* Source: www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/ (Accessed: 06.05.2020.)

CISA (2018): *Grizzly Steppe – Russian Malicious Cyber Activity.* Cybersecurity and Infrastructure Security Agency. Source: www.us-cert.gov/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity (Accessed: 06.05.2020.)

DHS (2016): *Executive Summary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale.* Department of Homeland Security. Source: www.dhs.gov/news/2016/12/30/executive-summary-grizzly-steppe-findings-homeland-security-assistant-secretary (Accessed: 06.05.2020.)

Foreign and Commonwealth Office (2018): *Foreign Office Minister condemns Russia for NotPetya attacks.* Source: www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks (Accessed: 06.05.2020.)

GCSB (2018): *New Zealand joins international condemnation of NotPetya cyber-attack.* Government Communications Security Bureau. Source: www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack/ (Accessed: 06.05.2020.)

Greenberg, Andy (2017): *Petya Ransomware Epidemic May Be Spillover From Cyberwar.* Source: www.wired.com/story/petya-ransomware-ukraine/ (Accessed: 21.04.2020.)

Healey, Jason – Jenkins, Neil (2019): Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing. In Minárik, Tomáš – Alatalu, Siim – Biondi, Stefano – Signoretti, Massimiliano – Tolga, Ihsan – Visky, Gábor eds.: *11th International Conference on Cyber Conflict: Silent Battle.* Tallinn, NATO CCD COE Publications. 123–142.

Maynor, David – Nikolic, Aleksandar – Olney, Matt – Younan, Yves (2017): *The MeDoc Connection.* Source: https://blog.talosintelligence.com/2017/07/the-medoc-connection.html (Accessed: 21.04.2020.)

Moret, Erica – Pawlak, Patryk (2017): *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?* Source: www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf (Accessed: 21.04.2020.)

Parliament of Australia (2018): *Australian Government attribution of the "NotPetya" cyber incident to Russia.* Source: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F5793917%22 (Accessed: 06.05.2020.)

Republic of Estonia (2018): *Foreign Minister Mikser condemns Russia for NotPetya attacks against Ukraine.* Source: https://vm.ee/en/news/foreign-minister-mikser-condemns-russia-notpetya-attacks-against-ukraine (Accessed: 06.05.2020.)

Schmitt, Michael N. – Biller, Jeffrey (2017): *The NotPetya Cyber Operation as a Case Study of International Law.* Source: www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/ (Accessed: 21.04.2020.)

Schmitt, Michael N. – Vihul, Liis (2017): *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms.* Source: www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ (Accessed: 08.05.2020.)

Sood, Karan – Hurley, Shaun (2017): *NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft.* Source: www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ (Accessed: 06.05.2020.)

Stilgherrian (2018): *Blaming Russia for NotPetya was coordinated diplomatic action.* Source: www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/ (Accessed: 21.04.2020.)

Stupp, Catherine (2020): *Germany Seeks EU Sanctions for 2015 Cyberattack on Its Parliament.* Source: www.wsj.com/articles/germany-seeks-eu-sanctions-for-2015-cyberattack-on-its-parliament-11591867801 (Accessed: 08.07.2020.)

Taddeo, Mariarosaria (2018): The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology,* Vol. 31. 339–355.

U.S. Department of Treasury (2018): *Treasury Sanctions Russian Federal Security Service Enablers.* Source: https://home.treasury.gov/news/press-releases/sm0410 (Accessed: 06.05.2020.)

Whitehouse (2018): *Statement from the Press Secretary.* Source: www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ (Accessed: 06.05.2020.)

VÁKÁT OLDAL

Anita Tikos

Cyberdiplomacy and the V4 Countries

Introduction

If we think about diplomacy, it is commonly understood as a task of the Ministries of Foreign Affairs to influence decisions, conduct dialogues and negotiations between representatives of states or international groups, forums. Due to the digital development, in the 21st century, the use of IT solutions and tools in diplomatic services became more and more widespread starting from public relations and information sharing, to data collection for intelligence purposes.

In view of all this, it is more and more important to establish common rules, code of conducts, security related requirements within the cyberspace.

We can find several different meanings and definitions for cyberdiplomacy. In this article, cyberdiplomacy is understood, when country representatives (not only form the Ministry of Foreign Affairs, but from any governmental cyber related institution) share information, conduct dialogues or negotiations regarding any cybersecurity related topic (about an incident, about existing regulatory or organisational experiences, common EU regulations, exercises etc.) in general (not going deeply into restricted or sensitive technical details).

The Central European Cyber Security Platform is a regional cooperation where members use strategical cooperation or cyberdiplomacy to get the necessary information, experience or knowledge from the other countries and to get enough support to be able to effectively promote their interests in the bigger international communities.

First, I would like to introduce the development of the international forums and cooperation to get a full picture about the colourful palette of the different international cooperation platforms and forums where CECSP was born.

In the last decade, cybersecurity has appeared as a key challenge for all countries and organisations, resulting in the establishment of organisations or divisions that are responsible for the creation and maintenance of information security (e.g. authorities, CSIRTs,[1] Security Operation Centres, cyber defence agencies or centres of excellence, etc.). Due to the possible cross-border nature of threats and incidents, it became relatively clear at an early stage that there is a need for international forums and mechanisms for the structured international cooperation of the specialised IT security organisations.

Regarding cybersecurity, cooperation is one of the most important and at the same time the most challenging issue for every country. Although it is essential for all entities

[1] Computer Security Incident Response Team.

in the cyberspace to get relevant information on the latest threats but giving such threat intelligence for others usually encounter obstacles because of several aspects (for example national and security interest, data protection aspects etc.).

First, a technical international cooperation has been established by setting up communities of incident management centres (CERT[2]/CSIRT); after the CSIRT communities the political, strategical cooperation has been established in different forms (groups of authorities, strategic working groups by decision-makers etc.). As of today, the main international organisations (NATO, EU, ITU, OSCE) all put cybersecurity on their agenda.

This wide list of international cooperation is always growing because of the different cooperation models (who are the involved players) and because of the developing technology (technology creates new and new policy areas) as well.

In 2013, the Czech Republic and Austria has enriched this huge cooperation with initiating the establishment of the Central European Cyber Security Platform or CECSP as a new regional cooperation. The regional agreement has created strategic and operational cooperation between the four Visegrád countries (the Czech Republic, Hungary, Poland, Slovakia), as well as Austria. The regional cooperation of the Central European countries is not a completely new initiative; there was another similar regional cooperation initiative like the CECSP, the so-called Central European Defence Cooperation (CEDC) established in 2011, aiming to facilitate the military-focused collaboration. Maybe the CECSP is the next step or the extension of the CEDC as all of the CECSP members are also members of the defence cooperation (Poland only as an observer). But it is important to highlight that the CEDC itself was not involved in the latter established CECSP cooperation, but as we will see later, the military cyber groups were also involved in it. There is only one similar, regional defence platform in Europe, NORDEFCO, founded by the Nordic countries, but it does not have a specific, cybersecurity-oriented agreement.[3]

The question may arise, considering that CECSP countries are participating in several already existing organisations, why do we need a regional cooperation, and what new role can be played by the CECSP in strategical or operational level cooperation. Is it possible to reach real operational cooperation or it is rather a strategic and diplomatic level regional cooperation?

To find the possible answers, I will give an overview on the cybersecurity policy of the platform's member states and their goals and activities in the cyberspace. I will present the history of the CECSP cooperation and its relations to the V4 cooperation and to the EU level regulation: *Directive on security of network and information systems* (NIS Directive). This study was prepared by using and updating an earlier case study: *Cybersecurity in the V4 Countries – A Cross-border Case Study.*[4]

[2] Computer Emergency Response Team.

[3] Németh 2017.

[4] Tikos–Krasznay 2019.

The cybersecurity structure of CECSP countries

Countries that are members of the platform participate in the cyberspace related work of the major international communities without exception. As the cybersecurity regulations of these communities are developing into the same direction and their members must implement these regulations, the CECSP countries have essentially similar legal and organisational structures.[5]

It is important to emphasise that before the *Directive on security of network and information systems* (NIS Directive) had been adopted in 2016, only guidelines and strategic objectives from international organisations and studies or guides about best practices showed examples internationally; therefore, the legal and organisational system of the countries was quite different.[6]

To understand and clearly see the full picture about the regional cooperation, it is worth comparing the cybersecurity preparedness and system of the countries that are members of the platform based on their national strategy and organisation system. It will not be a detailed strategic and organisational analysis; the aim is only to highlight the main similarities and differences by drawing up a comprehensive picture.

The first national cybersecurity strategies were established at about the same time by the CECSP countries in the early 2010s. The Czech Republic was the first who published a national strategy on cybersecurity in 2008, then Slovakia in 2011, and finally Austria, Poland and Hungary, all in 2013.[7]

Of course, over the years these strategies have been reviewed, because the period of their effect has expired and/or the development of the technology brought new challenges to cover.

Therefore, Slovakia and the Czech Republic formulated their new second generational national strategy for the period 2015–2020, meanwhile Poland published its own in 2017.

After the NIS Directive was adopted, it became the obligatory model for all future strategy of every country. These principles do not have new strategic elements compared to the existing international practice, but this is the first time when these are not just optional elements of the national strategies.

Hungary found a special solution to comply with these requirements; as the strategy accepted in 2013 is a general one and the main aims are still valid, Hungary extended this cybersecurity strategy with the Network and Information Systems Security Strategy of Hungary in 2018, which is a "so-called" sectoral strategy.[8] As the title suggests, this sectoral strategy covers the main strategic requirements of the NIS Directive.

Poland decided to strengthen and develop systematically its national cybersecurity system while implementing the EU cybersecurity regulatory framework (including the

[5] Berzsenyi 2014.
[6] Council of the EU 2016.
[7] Government of Hungary 2013; Republic of Austria 2013; Republic of Poland 2017; Republic of Slovakia 2015; The Czech Republic 2015.
[8] Government of Hungary 2018.

NIS Directive and Cyber Act); therefore, a new Cybersecurity Strategy of the Republic of Poland for 2019–2024 has been accepted.[9] The strategy of Slovakia and the Check Republic is valid and has aims until 2020, so they have to review their strategy at the latest this year. Austria still has not published a new strategy since 2013, or any assessment about the compliance of the strategy with the requirements of the NIS Directive and the new threats and challenges within the cyberspace.

We can say that all national strategies (every generation) of all five countries include the relevant areas from international (ENISA, NATO, ITU) cybersecurity strategy guidance, such as objectives for education, research and development, awareness raising, public–private partnership, law enforcement, international cooperation and critical infrastructure protection.

In case of the first and second generational strategies, they vary from the legislative perspective. Some of the strategies aims at the creation or the update of a comprehensive information security regulation (in case of Slovakia or Poland), while for other countries they refer specifically to the legal regulation of one or two areas in the strategy paper (for example in case of Hungary).

Regarding cybersecurity organisations, it must be highlighted that all evaluated strategies identify the governmental and/or national incident management centre (GovCERT/national CERT), the regulatory body with rights and responsibilities and the organisation or ministry responsible for coordination and for decision-making.[10]

There is a discrepancy between the strategies – in the first two generations – regarding the non-governmental areas (for example: regarding the critical infrastructure sectors), and in the organisational coverage. The other difference is that, the development of regulations and the creation of specialised organisations can be observed only as a goal in some sectors, while in other cases the critical infrastructure and/or sectoral regulations are already existing, and the goal is to strengthen and further develop them.

Each evaluated strategy deals with the question of non-governmental, sectoral CERTs and the establishment military CERTs. The countries have a same approach in terms of the need for the creation of special sectoral CERTs, but they are in different stages in the implementation. In Austria, there are many commercial CERTs operating together with a military CERT (MilCERT), whereas in Hungary and the Czech Republic one of the objectives is the establishment of a sectoral CERT.

Each strategy highlights the importance of the active international cooperation, mainly referring to the European Union and NATO, but in several cases, the regional cooperation (especially the Central European cooperation) has been highlighted as a priority.

Regarding the third generational strategies (adopted after the NIS Directive) we have small experience as only two new strategies has been accepted since then (by Hungary and Poland).

[9] Republic of Poland 2019.
[10] Kovács 2018.

In case of these strategy we can say that they cover the same main elements, sectors and institutional requirements but they still vary in detail (regarding their prioritisation and the chosen legal and organisational solutions).

In the Hungarian sectoral strategy, one important aim is to strengthen the international and regional cooperation.

In the new Polish strategy, the active international cooperation at strategic and political level is also an important aim, where the Visegrád cooperation is also mentioned as an important element.

It is important to know, that the strategies cannot be used to draw a conclusion on the similarity or differences of the organisational structures, as a number of organisational development and transformation took place in the countries during the adoption of their strategies, that cannot be read out directly from the strategy itself, such as the creation of commercial CERTs or the military CERTs. For example, in Hungary the organisational structure has changed several times, and the main changes in the last five years (for example: in 2015, the National Cyber Security Centre, so-called NCSC was set up by uniting three existing cybersecurity related organisations, or the Defence Sector Electronic Information Security Incident Management Centre – MilCERT – was established on 1 March 2016) were also not covered directly by the national cyberstrategy but still supported the implementation of the strategical aim to create the necessary specialised cybersecurity related institutions.

In conclusion, the national strategies show us that the CECSP countries have similar priorities and timelines at the strategic level, and the international and regional cooperation is an important aspect for every country.

The historical background and the main aims of the Central European Cyber Security Platform

In accordance with the fundamental objectives of the CECSP countries, the main aims of the thematic regional cooperation are to work together in accordance with the guidelines and initiatives of the EU and NATO and to support each other with their experiences in developing a national cybersecurity legislation and organisational structure. The most important goal of the platform is to gain more defence and resiliency in case of cyber-attacks through this regional cooperation.

The idea of setting up this regional platform could be originated from the historical foundations of the Visegrád countries and the fact that they have been resting on a cooperative approach since 1991. The Visegrád cooperation was laying on the main common aims of the Visegrád countries like geographical relations, historical traditions, the Euro-Atlantic security system and the accession to the Euro-Atlantic organisations.

Twenty years later, when the CECSP cooperation was created, the original aims of the Visegrád cooperation was already achieved, but the cooperation was still preserved, to support each other in development and to be able to assert their interest in the international communities. Therefore, the original political Visegrád cooperation has been supplemented with an independently operating thematic cooperation like the CEDC and CECSP.

The Central European cybersecurity cooperation is a comprehensive approach to cybersecurity issues, covering major levels of cybersecurity (strategic–operative, government–military, national–international). Accordingly, representatives of the platform include the ministries responsible for cybersecurity, military and national CSIRTs and authorities responsible for information security. In addition, the European Network and Information Security Agency (ENISA) has an observer position in the platform to support the aims and work of the platform with its international experience.[11]

In CECSP, the most important strategical aim of the members is to be more successful in international, community (EU) or allied (NATO) lobbying and to be able to represent a regionally discussed and agreed single position. As a result, Member States will have an opportunity to better reach out the consideration and validation of their positions and proposals on community or allied level. This also can be an important element of cyberdiplomacy, to be able to assert our position by getting support from our regional partners. Such co-operation has been observed over the past years during the negotiation of cybersecurity regulations within the European Union (such as the NIS Directive or the EU Cybersecurity Act).

After the establishment of a common, European level international regulation (for example, the adoption of the NIS Directive), the support function of the platform is still important for all of the members, as it can also provide a podium for discussing legal and technical questions arising during the implementation and evaluating cooperation mechanisms.

Another objective of this cooperation at the strategic level is to create a platform between the countries to support cooperation and share experience in R&D projects, but in practice, there was no visible cooperation or even information sharing within (or with the support of) the platform about their experiences in R&D projects. Probably the regulatory questions were a bigger priority or R&D is still such a sensitive topic and national interest that it is more important than information sharing and cooperation.

At the beginning, the establishment of cooperation on the operational level was also a huge priority, which is realised in the CERTs/CSIRTs cooperation. As it was seen in the strategies, most of the countries' aim was to set up different CSIRTs or to develop the existing ones; for the CSIRTs information sharing and learning from others' experiences are essential. Just like in other CSIRT communities, members share their experiences, report lessons learnt of major successful or failed attacks and good practices to community members, and make their collaboration more effective by organising cybersecurity exercises in order to develop the skills and preparedness of IT security professionals for current cybersecurity challenges and attacks.

At the beginning, the most important elements on the agenda of the Platform was the CSIRT cooperation (and practice the possible cooperation forms by cyber exercises) and to present and explain to each other their regulatory and organisational framework.

[11] ENISA 2014.

The operational model of the CECSP

In 2013, during the establishment of the Platform, the main goal was to build trust, to define a cooperation framework and its rules. After all, there was a need to develop a work program also for the platform.

According to the defined rules, the Platform has at least one strategic and operational meeting each year. The members decided to set up a presidency model, where the presidency is responsible for the management of the platform and the organisation of the meetings. Member States fill the presidency in a rotating system for one year (in alphabetical order). Hungary acted as chairman of the platform in 2015, and in 2020 also Hungary has the chairman position and responsibility.

During the first Hungarian platform presidency (in 2015), there was a strategic decision-makers working group meeting and an operational level meeting in Budapest.

Unfortunately, the official work programs of the CECSP presidencies are not publicly available, but we could identify the main aims and most important tasks of the presidency periods thanks to the published presidency summaries after the events, and to the references to the CECSP's aims and activities in the V4 presidency programs.

In the first few years, the platform organised various cybersecurity exercises for its members yearly, despite the fact that all participating national CERTs in the platform were taking part in EU and NATO exercises. Involving cybersecurity professionals in red and blue teaming exercise can also provide an opportunity to test and discuss the experiences gained in the allied and community exercises.

Until now, Hungary has organised two exercises for the members of the platform. The first one was held on 23 June 2014, right after the establishment of CECSP.[12] The second one was a decision-making and procedural exercise (Table Top Exercise, TTX) in 2015, during the Hungarian presidency period of the platform. The latest exercise took place in May 2017 in Brno, the Czech Republic. It was developed by the Masaryk University and was held in a special environment. This exercise did not focus on cooperation, but on testing and developing the technical skills of participating players.[13] In 2018, there was not any regional exercise, as all countries participated in ENISA's Cyber Europe 2018 cyber crisis exercise event.

Cybersecurity on the political level in the V4 cooperation

As it was mentioned and explained before, CECSP is independent from the Institutional Visegrád 4 cooperation and from the Central European Defence Co-operation (CEDC) either, but it could not come into existence without the political support of the governments of the affected countries. As soon as the political leaders realised the potential impact of cyberattacks, the need of cyber defence on regional level has appeared in the

[12] Draveczki-Ury 2014.

[13] National Cyber Security Center, the Czech Republic 2017.

presidency programs (with respect to the CECSP work program itself) and has evolved parallelly with the NATO–EU objectives.

Naturally the higher politically represented V4 cooperation have affect and/or refer to the CECSP aims and work program, therefore, it is important to collect and see the cyber-related goals of each V4 presidency from 2012, where this issue was first mentioned.

2012–2013 Polish Presidency

Cybersecurity was first mentioned in the Visegrád 4 work program in a military context: "There will be a need for V4 consultations on NATO Russian relations, a V4 common position on Missile Defence and on the Russian response, on NATO cooperation with Ukraine and Georgia, consultations on CFE and force deployment in the region, consultations, in the broader format of V4 + Baltic states + Romania and Bulgaria, on common security issues, and with regard to cyber security and energy security."[14]

2013–2014 Hungarian Presidency

In 2013, cybersecurity got a higher focus because of the establishment of the CECSP, and there was already technical meetings as well, led by the Check Republic.[15] The V4 members described their goals on political level as follows:

- "Emphasising the importance of cyber security awareness and strengthening dialogue and cooperation at policy and operational level in the field of cyber defence;
- Promoting efforts to make information exchange and knowledge transfer (lessons learned and best practices) more efficient in the field of cyber and information security.
- Exchange of knowledge and practical expertise countering cybercrime with Western Balkan countries."[16]

The military approach can also be found in this presidency program of this year, as well as cybercrime and cyberdiplomacy. The V4 countries proposed discussion "include the setting up of a long-term cyber security cooperation mechanism" in the context of security policy and related to NATO and the Common Security and Defence Policy of the European Union. They also "endeavour to strengthen the V4-B3 cooperation, particularly in the fields of […] cyber security" and promote further cooperation with the Western Balkan countries "on judicial cooperation in criminal matters and fight against corruption, and fight against cybercrime."[17]

[14] Ministry of Foreign Affairs of the Republic of Poland 2012.
[15] CSIRT.CZ 2013.
[16] Ministry of Foreign Affairs and Trade of Hungary 2013.
[17] Ministry of Foreign Affairs and Trade of Hungary 2013.

2014–2015 Slovak Presidency

Information and cybersecurity got a separate chapter in this presidency program and became one of the major issues. "The primary objective is to increase the immunity of information systems in the V4 countries against cyber-attacks and to decrease computer-based crime." To reach this goal, the Slovak presidency focused on the following topics:

- "Streamlining management of information/cyber security, security risk management;
- Protecting human rights and fundamental freedoms in connection with the use of information and communication infrastructure (including the Internet);
- Increasing awareness and competencies, education in the area of information/cyber security;
- Cooperation at international level in the area of information/cyber security (exchanging skills, experience and sharing information);
- Completing mutual consultations in order to harmonize the approaches taken by V4 countries and considering mutual support when adopting decisions and their subsequent implementation within international organizations (EU, NATO, UN and others);
- Supporting an improvement in the standing of the Central European Cyber Security Platform;
- Creating a safe environment (prevention, response to security incidents, the scope of specialized CSIRT/CERT-type teams, for example the implementation of joint simulation exercises on critical information infrastructure protection, creating a secure communication channel to share information on current threats and on-going large-scale security incidents, linking of early warning and information sharing in the V4."[18]

This program has defined the scope of CECSP cooperation, and the platform is still working according to the above-described principles. In this year, cyber did not appear in any other relation, except the defence and security policy part, where it was treated as a general security risk.

2015–2016 Czech Presidency

The Czech Presidency placed cybersecurity to the operational level. As CECSP's operational capability has been proven, this issue disappeared from the list of strategic questions. The Presidency Program has the following statement: "Cybersecurity is also a prospective topic for the Visegrád cooperation. The CZ V4 PRES will push to deepen and increase the efficiency of cooperation within the Central European Cyber Security Platform (CECSP). This will particularly include harmonising the positions of the V4 countries on fundamental topics of cyber security, including their

[18] Ministry of Foreign and European Affairs of the Slovak Republic 2014.

positions within international organisations, organising expert workshops and introducing standards and secured channels as part of communication among the CECSP states. The V4 will also continue in the practice of cooperation among specialised police units and national "centres of excellence" focused on research in the area of cybernetic crime.[19]

The Czech National Security Authority got the task to facilitate the operational level cooperation. For this, their planned activities also were specified in the program:

- "At the strategic level, the CZ V4 PRES will seek progress in harmonising the approach of individual states and their positions and opinions on major cyber security issues within international organisations, forums and discussions. This includes primarily the legislation being negotiated in the working bodies of the Council of the EU and European Commission and documents negotiated under the OSCE and International Telecommunication Union;
- At the operational level among top CERT sites, we want to organise workshops on selected topics (e.g. intrusion detection and honeypots, penetration testing, etc.);
- The CZ V4 PRES is committed to implementing standards and secure channels in communications among CECSP states."[20]

2016–2017 Polish Presidency

Following the previous year's approach, cybersecurity remained on the technical level and highlights the importance of the CECSP. This area is summarised only in one paragraph:

"Cyber-security: cooperation to enhance the protection against cyber threats inter alia by means of CSIRT cooperation and the Central European Cyber Security Platform (CECSP); building permanent relations between the CECSP and the V4. Furthermore, encouraging cooperation between special Police units and national "centres of excellence" that focus on conducting research in the field of cyber-crime."[21]

Cybersecurity also disappeared from the defence policy and was only mentioned once under the police cooperation part, in relation with cybercrime. Probably the reason behind this reduced priority can be found in the European legislation. As, in this period, the NIS Directive was adopted and required a pan-European approach for cyber defence. The need for a regional cooperation has seemingly decreased.

2017–2018 Hungarian Presidency

2017 was a turning point in the era of cybersecurity. There were two state sponsored malware campaigns (WannaCry and NotPetya) that caused global chaos, meanwhile

[19] Ministry of Foreign Affairs of the Czech Republic 2015.
[20] Ministry of Foreign Affairs of the Czech Republic 2015.
[21] Ministry of Foreign Affairs of the Republic of Poland 2016.

more and more details had been revealed on the effects of cyberattacks during the U.S. presidential election. The Hungarian Presidency Program clearly reflects to these threats and cyber defence got a higher focus than in the previous year.

First of all, due to hybrid threats, cybersecurity is mentioned in a military context again: "Defence policy cooperation in the V4+Ukraine and V4+Moldova formats, focusing on examining possibilities for joint work on defence sector reform, sharing experience on cyber defence and hybrid war, resilience and a potential involvement in the V4 EU Battlegroup (in the case of Ukraine)." This is emphasised with a planned Cyber Workshop between the V4 countries and the United States.[22]

On the other hand, the operational cooperation is described in more details: "In the field of cyber security, the Presidency's goal is to strengthen the resilience of critical infrastructure, especially with the aim of revealing and averting risks and attacks coming from the cyberspace. The Hungarian Presidency will carry on the cooperation between cyber security organisations and network security centres of V4 countries, for which information-sharing on incidents is indispensable. In cooperation with the rotating Chair of the Central European Cyber Security Platform, the Hungarian Presidency will organise expert meetings and joint exercises and trainings related to incident management. The Presidency also plans to hold consultations aiming to formulate joint V4 positions on current topics of the EU's agenda, in particular on the implementation of the Directive on Security of Network and Information Systems (NIS Directive), and the revision of the Cybersecurity Strategy of the EU."[23]

2018–2019 Slovak Presidency

This Presidency Program also deals with cybersecurity, but it is not as ambitious as it was in the previous year. It focuses on cybercrime and the usage of cryptocurrencies: "Digital evolution and the development of cyber space bring an increasing number of cyberattacks, which, in some EU Member States, even exceed the number of standard crimes. Therefore, within the Presidency of the V4, we shall focus on the strengthening and improvement of cooperation in the fight against cybercrime connected with the misuse of crypto currencies, especially bitcoin."

Then it turns to CECSP and highlights the success of the Slovak Presidency of this forum in 2017: "With regard to CECSP cooperation, during the Slovak Presidency in 2017 the member countries started to coordinate their activities, stances, and positions even on the EU level. This initiative did not go unnoticed by other members of the EU. For example, as a result France joined in on the coordination of CECSP activities in matters of the cybersecurity of the European Union."[24]

[22] Ministry of Foreign Affairs and Trade of Hungary 2017.
[23] Ministry of Foreign Affairs and Trade of Hungary 2017.
[24] Ministry of Foreign and European Affairs of the Slovak Republic 2018.

2019–2020 Czech Presidency

This presidency program is also not too ambitious regarding cybersecurity as it is nearly just mentioned in the detailed presidency program.

The Czech presidency program has three main priority areas (mentioned as a 3R), and cybersecurity related topics are covered in the second one. This area is the area of the Revolutionary technologies, where the presidency aims to deal with "innovative economy and its social impacts: CZV4PRES will concentrate on support for research, development and innovation, innovative ecosystem, Digital Single Market, artificial intelligence but also on education and adaptability of people to the related changes in the labour market."[25]

As a part of the detailed presidency program, the Czech presidency mentions cybersecurity related topics also as part of the security policy "to include European defence initiatives and the development of the civilian component of the Common Security and Defence Policy. The objective is to enhance security and defence cooperation especially in collective defence, military mobility, cyber security, hybrid threats, terrorism, strategic communication capabilities, and regarding challenges emanating from the South".

Cybercrime, and critical infrastructure protection is also mentioned in the presidency program, with the aim to "promote closer V4 exchange of experience and cooperation on cybercrime, especially between national cybercrime contact points and law enforcement authorities (public prosecutors and the police). The focus should be on the protection of critical information infrastructure and important information systems."[26]

Supporting these goals, only one event, a conference has been organised (and planned in the work program) in November 2019, by the Czech Republic Police about the current trends in cybercrime and cybersecurity.

In this presidency program, the CECSP cooperation or the operational cybersecurity cooperation has not been mentioned, furthermore the work program defines tasks and cooperation only for the police and for the Ministries of Foreign Affairs.

Probably the reason of the disappearance of the CECSP and operational cyber policy from the V4 presidency programs could be found in the developed EU cyber policy. For this time, this cooperation form was established on EU level by the NIS Directive and Cyber Act, and the possible future work must be raised within the parties in the future.

2020–2021 Polish Presidency

The pandemic situation and its consequences have a huge effect on the presidency program of 2020–2021; therefore, the Polish presidency will mainly focus on the Covid

[25] Ministry of Foreign Affairs of the Czech Republic 2019a.
[26] Ministry of Foreign Affairs of the Czech Republic 2019b.

related issues, but cybersecurity also can be found in its agenda, as an important issue in a pandemic situation like the Covid-19.

The Polish presidency is planning to discuss its initiatives in the cybersecurity area:

"Signing a joint declaration on mutual cooperation in cyber security, to serve as a roadmap for V4 activities – main activity areas include:

- increasing the capability for reacting to incidents by, among others, developing the management of cross-border incidents in combination with consultations, as well as conducting international exercises to improve adaptation in taxonomy, collection and analysis of digital evidence and collaboration in prosecuting cybercriminals;
- building common situational awareness in cyber space, especially by exchanging information on cyber threats in real time between national level CSIRT teams;
- developing new methods and tools to test, assess and certify ICT products, processes and services (as part of the Cyber Security Act);
- developing a new generation of cryptographic algorithms resistant to quantum computing;
- improving multilateral collaboration and national capabilities in cyber security, among others in the R&D area."[27]

Furthermore, the Polish presidency is planning to consult within the CECSP platform about the other possible topics (like cross-border incident handling; situational awareness; R&D, supply chain security; digital evidence and international law applicable to cyberspace operations) that can be involved within the regional cooperation.

Efficiency, benefits and future of the CECSP cooperation

As we saw before, the participating countries have common objectives, basic regulations and organisational system for the operation of the Central European Platform. Since the establishment of the cooperation, mainly operational and strategic discussions and cybersecurity exercises were on their agenda. The essential and basic requirement for the effective functioning of the cooperation is to build trust between the parties involved in the agreement. We can say that the countries participating in the platform are familiar with the legal and organisational specialties of each other in detail and had the opportunity to build up trust and to understand other parties. This completely meets our definition of cyberdiplomacy.

As a result, they had opportunity for detailed technical consultations, discussions and could identify additional actors and areas of expertise for the further development and deepening of the cooperation.

After examining the work programs of the platform, we could see that this cooperation mainly stayed in the strategic cooperation level, where political (EU, NATO and national) legal and diplomatic questions have been discussed. We also saw some intention for

[27] Ministry of Foreign Affairs of the Republic of Poland 2020.

a deeper cooperation, by involving CSIRTs in this cooperation, but it stayed on a higher level by sharing best practices, introducing themselves and their main knowledge (but not in detail). Cyber exercises do not mean real cooperation either; it is just practicing their ability and cooperation model. IT helps to build trust, but it is still far from real life technical cooperation (in case of an incident, or a project etc.).

As it was mentioned above, the NIS Directive, adopted in 2016, is the first European regulation to provide mandatory legislative and technical (CSIRT) cooperation and defines minimum requirements in the national regulation for the Member States. Accordingly, the CECSP Member States had to review their national cybersecurity strategy, in line with NIS requirements, as well as their national legislation for the core services sectors and the sectors providing digital services. As a result, the CECSP member states have the same national strategy, national regulations and organisational structure and are set up on the same basis.

Thanks to the directive, collaboration and information sharing between CSIRTs is implemented through binding rules, in case of incident reporting and cross-border incident management as well. The technical training and testing area are also covered by the European Union regulations, as there are mandatory exercises, like the Cyber Europe exercise in every two years, and the exercises of the CSIRTs Network.

The question may arise that after these rules and cooperation mechanisms established by NIS Directive, what can be the role of the CECSP regional cooperation if all its countries are members of the EU and must apply the EU level cooperation.

It is undeniable that the strategic and technical cooperation elements of the Platform are covered by the new EU rules, and the V4 presidency programs and the decrease of the operation of the CECSP meetings also pointing to the direction that CECSP has been replaced by the EU level cooperation.

On the other hand, the members still mention the need and the importance of the regional cooperation in their new cybersecurity strategies, so probably they do not plan to terminate the platform.

There are several areas still not regulated by the EU that could add value to the regional work. The participants can review the existing CECSP cooperation and involve more professionals from other areas, and extend the cooperation with some other, more specialised areas (such as research and development, education, awareness raising, law, professional training, common EU research applications, cross-sectoral issues etc.). The support of actual CECSP parties (ministries, authorities and CSIRTs) for the new areas of the regional cooperation could help for the new partners in trust- and confidence-building and could be a good basis to start a valuable, deep and daily cooperation.

Finally, it should be emphasised that the platform still gives a good opportunity for its members to develop a stronger common position on international level and can be a forum to discuss ideas, questions and experiences at the transposition stage as they have already done regarding the NIS Directive and the Cybersecurity Act.

As we can see, cyberdiplomacy is an important and integral element of the regional cooperation of the Visegrád countries, were they have opportunity to discuss any legal,

co-operational, organisational (and maybe technical) question, to develop together with different cyber exercises, and to have opportunities to establish a common position to be able to validate their position in other international forums.

References

Berzsenyi Dániel (2014): Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése. *Nemzet és Biztonság,* Vol. 7, No. 6. 110–136.

Council of the EU (2016): *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148 (Accessed: 11.04.2020.)

CSIRT.CZ (2013): *Zástupci CSIRT.CZ se zúčastnili setkání platformy CECSP.* CSIRT.CZ, 28 December 2013. Source: www.csirt.cz/page/1836/zastupci-csirt.cz-sezucastnili-setkani-platformy-cecsp/ (Accessed: 11.04.2020.)

CSIRT.SK (2014): *Tretie rokovanie Stredoeurópskej platform kybernetickej bezpečnosti.* CSIRT.SK, 11 April 2014. Source: www.csirt.gov.sk/aktualne-7d7.html?id=69 (Accessed: 11.04.2020.)

Digitales Österreich (2014): *Central European Cyber Security Platform.* Digitales Österreich, 11 April 2014. Source: www.digitales.oesterreich.gv.at/-/central-europeancyber-security-platform (Accessed: 11.04.2020.)

Draveczki-Ury, Ádám (2014): Szoros együttműködés a kibertérben. *Honvedelem.hu,* 27 June 2014. Source: https://honvedelem.hu/cikk/szoros-egyuttmukodes-a-kiberterben/ (Accessed: 11.04.2020.)

ENISA (2014): *Meeting of the Central European Cyber Security Platform 2014.* European Union Agency for Network and Information Security, 10 April 2014. Source: www.enisa.europa.eu/news/enisa-news/central-european-cyber-security-platform-2014 (Accessed: 11.04.2020.)

Government of Hungary (2013): *Government Decision No. 1139/2013 (March 21) on the National Cyber Security Strategy of Hungary.* ENISA, 21 March 2013. Source: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (Accessed: 11.04.2020.)

Government of Hungary (2018): *Government Decision No. 1838/2018 (December 28) Strategy for Network and Information Security.*

Kovács László (2018): *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus Kiadó.

Ministry of Foreign and European Affairs of the Slovak Republic (2014): *Programme of the Slovak Presidency of the Visegrad Group, July 2014 – June 2015.* International Visegrad Group, 1 July 2014. Source: www.visegradgroup.eu/documents/presidencyprograms/sk-v4-pres-program-2014 (Accessed: 11.04.2020.)

Ministry of Foreign and European Affairs of the Slovak Republic (2018): *Dynamic Visegrad for Europe, Slovak Presidency 2018/2019 of the Visegrad Group.* International Visegrad Group, 1 July 2018. Source: www.visegradgroup.eu/documents/presidency-programs/slovak-v4-presidency-en (Accessed: 11.04.2020.)

Ministry of Foreign Affairs and Trade of Hungary (2013): *Hungarian Presidency of the Visegrad Group (2013–2014).* International Visegrad Group, 1 July 2013. Source: www.visegradgroup.eu/documents/presidency-programs/hu-v4-presidency-2013 (Accessed: 12.04.2020.)

Ministry of Foreign Affairs and Trade of Hungary (2017): *Hungarian Presidency 2017/2018 of the Visegrad Group.* International Visegrad Group, 1 July 2017. Source: www.visegradgroup.eu/documents/presidency-programs/hungarian-v4-presidency (Accessed: 12.04.2020.)

Ministry of Foreign Affairs of the Czech Republic (2015): *Programme for the Czech Presidency of the Visegrad Group 2015–2016.* International Visegrad Fund, 1 July 2015. Source: www.visegradgroup.eu/documents/presidency-programs/cz-v4-pres-2015-2016 (Accessed: 12.04.2020.)

Ministry of Foreign Affairs of the Czech Republic (2019a): *The Czech Republic holds the Presidency of the Visegrad Group from 1 July 2019 to 30 June 2020.* International Visegrad Fund, 25 June 2019. Source: www.mzv.cz/jnp/en/foreign_relations/visegrad_group/index.html (Accessed: 12.04.2020.)

Ministry of Foreign Affairs of the Czech Republic (2019b): *Programme for the Czech Presidency of the Visegrad Group 2019/2020.* International Visegrad Group, 06 September 2019. Source: www.mzv.cz/file/3626458/Programme_CZ_V4_PRES_2019_2020_A.pdf (Accessed: 12.04.2020.)

Ministry of Foreign Affairs of the Republic of Poland (2012): *Programme of the Polish Presidency of the Visegrad Group.* International Visegrad Fund, 1 July 2012. Source: www.visegradgroup.eu/documents/presidency-programs/programme-of-the-polish (Accessed: 12.04.2020.)

Ministry of Foreign Affairs of the Republic of Poland (2016): *Programme of the Polish Presidency of the Visegrad Group 2016–2017.* International Visegrad Fund, 1 July 2016. Source: www.visegradgroup.eu/documents/presidency-programs/pl-v4-pres-2016-17 (Accessed: 12.04.2020.)

Ministry of Foreign Affairs of the Republic of Poland (2020): *Presidency Programme of the Polish Presidency of the Visegrad Group 2020–2021.* International Visegrad Fund, 1 July 2020. Source: www.visegradgroup.eu/documents/presidency-programs/2020-2021-polish (Accessed: 03.07.2020.)

National Cyber Security Center, Hungary (2013): Megrendezésre került a Közép-európai Kiberbiztonsági Platform (CECSP) konferencia. Source: https://nki.gov.hu/figyelmeztetesek/archivum/megrendezesre-kerult-a-kozep-europai-kiberbiztonsagi-platform-cecsp-konferencia/ (Accessed: 11.04.2020.)

National Cyber Security Center, the Czech Republic (2014): *Central European Cyber Security Platform 2014.* Source: www.govcert.cz/cs/informacni-servis/akce-udalosti/2140-central-european-cyber-security-platform-2014/ (Accessed: 12.04.2020.)

National Cyber Security Center, the Czech Republic (2017): *National Cyber Security Centre Held Exercise for CECSP Partners.* NCKB, 24 May 2017. Source: www.govcert.cz/en/info/events/2532-national-cyber-security-centre-held-exercise-for-cecsp-partners/ (Accessed: 11.04.2020.)

Németh, Bence (2017): *Outside NATO and the EU. Sub-Regional Defence Co-Operation in Europe.* King's College London. Source: https://kclpure.kcl.ac.uk/portal/files/80807208/2017_Nemeth_Bence_1212105_ethesis.pdf (Accessed: 11.04.2020.)

Republic of Austria (2013): *Austrian Cyber Security Strategy.* ENISA, 10 March 2013. Source: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (Accessed: 11.04.2020.)

Republic of Poland (2017): *National Framework of Cybersecurity Policy of the Republic of Poland.* ENISA, 30 November 2017. Source: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013 (Accessed: 11.04.2020.)

Republic of Poland (2019): *Uchwała Nr 125, Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.* Source: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf (Accessed: 12.04.2020.)

Republic of Slovakia (2015): *Cyber Security Concept of the Slovak Republic.* ENISA, 01 June 2015. Source: www.enisa.europa.eu/topics/national-cyber-securitystrategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (Accessed: 11.04.2020.)

The Czech Republic (2015): *National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020.* ENISA, 16 January 2015. Source: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (Accessed: 11.04.2020.)

Tikos, Anita – Krasznay, Csaba (2019): *Cybersecurity in the V4 Countries – A Cross-border Case Study.* Central and Eastern European e|Dem and e|Gov Days. 163–174.

Napjaink társadalmát információs társadalomnak szokás nevezni. A kifejezés abban a tekintetben mindenképpen jól ragadja meg a társadalmi-gazdasági folyamatok ismertetőjegyét, hogy egyéni és közösségi életünkben is meghatározó szerepet játszik a rendelkezésre álló információknak az a bősége, amelyet az egyre terjedő digitalizáció termel.

Az előttünk álló korszak egyik legnagyobb stratégiai kihívása a minket körülvevő hömpölygő információáradat kordában tartása – nem abban az értelemben, hogy miként fékezzük azt le, hanem hogy miként garantáljuk biztonságos folyását, illetve hogy mi magunk miként maradjunk a felszín fölött. A kötetben szereplő tanulmányok különféle nézőpontból ugyanarról szólnak, ugyanazt hangsúlyozzák: elsődleges feladattá vált, hogy a mindent átszövő információs hálózatainkra, az egyre összetettebbé váló elektronikus és online tereinkre, valamint a folyton-folyvást fejlődő új technológiákra ne az öncélú technikai haladás termékeiként tekintsünk, hanem életünk kibontakoztatásának szolgálatába állítsuk őket.