TÖRÉKENY NAGYHATALMISÁG: A KIBERBIZTONSÁG

AZ EURÓPAI KIBERTÉR BRIT, NÉMET ÉS FRANCIA SZEGMENSEI

Molnár Dóra

NEMZETI KÖZSZOLGÁLATI EGYETEM
BUDAPEST

SZÉCHENYI 2020

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE

TÖRÉKENY NAGYHATALMISÁG: A KIBERBIZTONSÁG

AZ EURÓPAI KIBERTÉR BRIT, NÉMET ÉS FRANCIA SZEGMENSEI

Szerző:
Dr. Molnár Dóra

Lektorálta:
Kálovics Tamás

A kézirat lezárásának dátuma:
2018. november 30.

Kiadó:
Nemzeti Közszolgálati Egyetem
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős kiadó:
Prof. Dr. Kis Norbert rektorhelyettes
Címe: 1083 Budapest, Üllői út 82.

A kiadvány a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú,
„A jó kormányzást megalapozó közszolgálat-fejlesztés” című projekt
keretében készült el és jelent meg.

TARTALOMJEGYZÉK

BEVEZETÉS 4

1. A VÁLTOZÓ BIZTONSÁGI KÖRNYEZET 5

2. AZ EURÓPAI KIBERBIZTONSÁG ÁLTALÁNOS JELLEMZÉSE 8
2.1. Hatalmi viszonyok az európai kibertérben 8
2.2. Az európai kiberszabályozás 12

3. A BRIT, NÉMET ÉS FRANCIA KIBERBIZTONSÁG ÖSSZEHASONLÍTÁSA AZ OECD IRÁNYELVEK MENTÉN 14
3.1. Az OECD-irányelvekről általában 14
3.2. Összehasonlítás az alapvető stratégiai kérdések mentén 17
3.3. Összehasonlítás a koncepcionális kérdések mentén 22
3.4. Összehasonlítás a menedzsmentstruktúrák és akciótervek mentén 26
3.5. Összehasonlítás a szervezeti kérdések mentén 30
3.5.1. A politikai koordinációért felelős szervek 30
3.5.2. A katonai kibervédelem szervei 31
3.5.3. A kritikus infrastruktúra védelméért felelős szervek 33
3.5.4. Országspecifikus jellemzők 34
3.6. Összegző észrevételek 35

4. KIBERDIPLOMÁCIA: A JÖVŐ ZENÉJE? 37

ZÁRÓ GONDOLATOK 40

FELHASZNÁLT IRODALOM 42

BEVEZETÉS

Az Egyed István Posztdoktori Program keretei között végzett 18 hónapot átölelő kutatásom célja az volt, hogy a nagyhatalmak biztonságának kiberbiztonsági szegmensét feltárjam, elemezzem, majd ezt követően egyrészt országcsoportok kialakításának segítségével hasonlóságokat és különbözőségeket állapítsak meg, másrészt pedig egy egységes szempontrendszer mentén azokat egymáshoz mérten összehasonlítsam. A kutatások során körvonalazódott, hogy a keretek túl szűkösek ahhoz, hogy valamennyi nagyhatalmat górcső alá vegyem, ezért úgy döntöttem, hogy az európai kontinensre fókuszálva a három nagy európai állam, az Egyesült Királyság, Németország és Franciaország kiberbiztonsági kérdéseivel fogok részletekbe menően foglalkozni. Ezért az országcsoportokra vonatkozó célkitűzésem mellőzése mellett a második célként megfogalmazott összehasonlító elemzést tekintettem vezérlő elvnek, s ennek mentén vittem végig a kutatást azzal, hogy azt egykismonográfia keretei között adom közre. A deduktív módszert alkalmazva előbb feltártam az európai kibertér fejlődésének fő irányait és jelenlegi állapotát, majd ebbe ágyazva vizsgáltam a nemzetállami szintet. Valamennyi témakör esetében a kutatásaimat önálló publikáció formájában összegeztem. Ezen eredményeket jeleníti meg jelen kismonográfia azzal, hogy annak központi elemeként egy egységes szempontrendszer segítségével végzem el a három nemzetállam kiberbiztonságának összehasonlító elemzését. Kutatásaim során elsősorban a világhálón is elérhető nyílt forrásokra támaszkodtam. Ezt egészítettem ki egyrészt speciális adatbázisokban található szakcikkekben, tanulmányokban szereplő információkkal, másrészt pedig a külföldi konferenciákon szerzett ismeretekkel, tapasztalatokkal.

1. A VÁLTOZÓ BIZTONSÁGI KÖRNYEZET

A 20. század második felére a biztonsági tanulmányok önálló tudományterületté nőtték ki magukat. Kezdetben a nyugati féltekén – s elsősorban az Egyesült Államokban – honosodott meg, majd kelet felé terjeszkedve mára már meghódította az egész világot. Fejlődését nagymértékben elősegítette az, hogy világunk az utóbbi évtizedekben egyre kiszámíthatatlanabbá, egyre veszélyesebbé vált, ezért a biztonság fogalma általánosságban felértékelődött. Nem csak a magánemberek vonatkozásában, akiknek félelemérzetét egyre több nemzetközi történés befolyásolja negatívan, hanem állami szinten is.

A biztonsági tanulmányok számára a nemzetállamok biztonsága képezi a vizsgálódás kiindulópontját. A koppenhágai iskola nevével fémjelzett biztonságfogalom tradicionálisan öt biztonsági szektort különít el: a politikai, katonai, gazdasági, társadalmi és környezeti lencsén keresztül vizsgálja az államok biztonságát.[1] Ez a megközelítés azonban mára idejétmúlt, mivel biztonsági környezetünk az elmúlt évtizedekben olyannyira megváltozott, hogy egészen új biztonsági szektorok láttak napvilágot, amelyek jelentősége kezdi meghaladni a tradicionális szektorok többségének fontosságát. Itt gondolok például az energiabiztonság önállósulására, amelyet az energiahordozók szűkösségéből fakadó biztonsági kockázatok emeltek ki az általános gazdasági biztonsági területből, kutatási témám szempontjából azonban a biztonság másik új területe, az informatikai vagy kiberbiztonság emelendő ki.

A kiberbiztonság mint új biztonsági terület felértékelődése mögött számos okot nevesíthetünk.[2] Az aktorok körének kiszélesedése (úgymint a nemzetállamok, a terrorista csoportok, a kiberbűnözők és a hactivisták) mellett kiemelt jelentőséggel bír az elkövetők motivációja, a támadás célja, valamint a terület szabályozásának lemaradása, amely miatt gyakran lehetetlen az elkövetők elleni eredményes fellépés is. A 2000-es évek elejére tehető az, hogy az egyes államok hangsúlyosan kezdték el kezelni a kiberbiztonság területét, amely jelentősége mára már annyira megnőtt, hogy közvetlen hatással és befolyással van a biztonság más területeinek alakulására. A kiberbiztonságot igen gyakran a katonai biztonság lencséjén keresztül vizsgálják – tévesen. Ugyanis a kérdéskör katonai relevanciája bár adott, de az csak egy a sok egyéb részterület közül, amelyekkel a kiberbiztonság igen szoros kapcsolatban van. Összkormányzati megközelítésre van szükség, amelyben valamennyi ágazat jelen van, nemzetközi szinten szemlélve a kérdést pedig szükséges valamennyi nemzetközi szereplő bevonása. Ez a személyi kör nagyon tág: a nemzetközi szervezetektől kezdve, a nagyvállalatokon át, az igazságszolgáltatási szervezetrendszer elemein túl a média területe is beletartozik. Ami pedig elengedhetetlen, az a *bizalom* az érintett szereplők között, amely kialakulása esetén hajlandóak lesznek a kiberbiztonság formálásában részt vevő szereplők az információ-megosztásra. A bizalom kialakulásához idő kell, de a folyamatban katalizátorként hathat az egységes szabályrendszer megalkotása. A bizalom ugyanis nem más, mint az új olaj, amelyet nehéz megszerezni, ki kell próbálni, de ha egyszer megvan, igen értékes.[3]

---

1 BUZAN–Waever–WILDE (1998).

2 MOLNÁR (2017b).

3 HANULA (2018).

Nem a fogalmi alapokban való elmélyülés céljával, de mindenképpen említést kell tenni röviden a címben szereplő *kibertér* fogalmáról. Egységes definíció a mai napig nem létezik, egyes államok és szervezetek más-más elemét kihangsúlyozva közelítenek a kibertér mibenlétének megragadásához. Az ENSZ egyik szakosított szerve, a Nemzetközi Távközlési Egyesület (ITU)[4] is megalkotta saját kibertér fogalmát, amely – köszönhetően a szervezet közel egyetemes tagságának – nemzetközileg elfogadottnak tekinthető[5], de az általam vizsgált három ország is saját fogalommeghatározással rendelkezik (lásd a 3.2.5. fejezetben). A magyar kibertérfogalmat szükségesnek tartom ezen a ponton röviden ismertetni, amelyet a 2013-as *Nemzeti Kiberbiztonsági Stratégia* a következőképpen rögzít: „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."[6] Majd így folytatja: „Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett." A stratégia tehát a „globális" kibertértől elkülönülten kezeli a 'magyar kiberteret', amely első olvasatra meglepőnek tűnhet, de épp olyan kérdések kezelése kapcsán bírhat relevanciával, mint például a kiberhadviselés kérdésköre.[7]

Az utóbbi években érzékelhető az a szemléletváltás, amely a defenzív megközelítés helyett már a támadó kapacitások meglétére helyezi a hangsúlyt. Az államok részéről megtett kezdeti lépések a kiberbiztonságuk megteremtése érdekében ugyanis elsősorban az állampolgáraik, az állami szervezetrendszer és a kritikus infrastruktúra megvédését szolgálták a kibertámadásokkal és fenyegetésekkel szemben. Ezzel szemben – köszönhetően az elmúlt évek eseményeinek – mára több ország is szükségesnek érzi kiber-támadóképességek megszerzését, amelyet vagy nyilatkozatok formájában[8], vagy stratégiai dokumentumaiban rögzítetten deklarál. A sikeres fellépésnek záloga azonban a gondolkodásmód megváltoztatásában rejlik. A döntéshozóknak úgy kell gondolkodniuk, ahogyan az ellenség gondolkodik: első a cél felderítése, ezt követi a gyenge pontok felderítése és azonosítása, végül pedig a sérülékenységet ki kell küszöbölni. Ehhez szükséges volna az ellenfél ismerete, amely változatos formát ölthet. Ha a hagyományos hadviselés-elméletekből indulunk ki, akkor a szimmetrikus-aszimmetrikus fajták közül első ránézésre azt mondanánk, hogy a kiberhadviselés tipikus aszimmetrikus hadviselési fajta, hiszem a szembenálló felek aszimmetriája figyelhető meg: egy államot támadás ér egy csoport(ok) vagy magánszemély(ek) részéről. Ha azon-

4 International Telecommunication Union.

5 Az ITU a kiberkörnyezet (cyber environment) fogalmat használja, amely alatt érti: „felhasználók, hálózatok, eszközök, valamennyi szoftver, eljárások, tárolt vagy továbbított információ, alkalmazások, szolgáltatások és rendszerek, amelyek közvetve vagy közvetlenül hálózatokhoz tudnak kapcsolódni". In: ITU Recommendation X.1205. (2008).

6 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. 1. sz. melléklet I.3. pontja

7 KOVÁCS (2018).

8 2016 októberében a brit külügyminiszter oroszországi látogatása alkalmával már úgy fogalmazott, hogy az Iszlám Állam ellen kiberműveletek megindítása szükséges. A miniszter ezen kijelentése már egyértelműen az offenzív megközelítést tükrözi. Ugyanakkor a nemzetközi szervezeteknél egyelőre még nagy az ellenállás a támadó kiberképességekkel való rendelkezés ellen. A NATO például kizárólag védelmi kiberképességekkel rendelkezik és engedélyez, támadó képességeket nem.

ban kicsit mélyebbre tekintünk, általában fény derül arra, hogy adott csoport vagy személy állami „megrendelésre" dolgozik a komoly gazdasági érdekei mentén, tehát az egyes, kibertérben elkövetett támadások mögött az esetek többségében valójában az államok (mint a legnagyobb gazdasági erővel bíró érdekcsoportok) állhatnak az elkövetői és az áldozati oldalon egyaránt. Ez alapján gyakran állam–állam küzdelmet láthatunk, amely magánviseli a szimmetrikus hadviselés valamennyi jellemzőjét, így azt mondhatjuk *a kiberhadviselés szimmetrikus hadviselési mód*.

A kiberbiztonság fogalmának definiálása kapcsán is kisebb nehézségbe ütközünk, amely áthatja e biztonsági terület egészét is.[9] Ugyanakkor ezt természetesnek is tekinthetjük, hiszen olyan ez, mint egy gyermekkori betegség, amelyen át kell esni. Ha a nemzetállamoknak sikerül konszenzusra jutniuk olyan alapfogalmakról, mint a kibertér, kibertámadás, akkor létrejön az alap ahhoz, hogy ezen a területen is hatékonyan és eredményesen tudjanak együttműködni. Addig azonban még nagyon hosszú utat kell bejárni. Az információ ugyanis nem más, mint a 21. század olaja, az elemzés pedig annak a motorja.[10] Napjainkban a fejlődés mozgatórugója az információ, ezért annak birtoklásáért harc folyik. Ezt szó szerint kell érteni, mivel a kibertérben tényleges küzdelem folyik az államok között az információ megszerzéséért, megtartásáért, manipulálásért és felhasználásért. A „harc" keretei azonban még kialakulatlanok, mivel az államok még nem jutottak konszenzusra a vonatkozó nemzetközi szabályrendszer megalkotását és tartalmi elemeit illetően. Márpedig új szabályokra szükség van, mert az mindig a fejlődés szükségszerű velejárója. Norbert Wiener, a kibernetika atyja ezt úgy fogalmazta meg, hogy „a fejlődés nem csak új lehetőségeket teremt, hanem új korlátokat is".[11] A korlátokat ezek a megalkotandó szabályok jelentik, amelyek kialakítása már kezdeti szakaszába lépett, de a továbblépés irányai még nem rajzolódtak ki egyértelműen. Ugyanis vannak olyan biztató előrelépések, mint az egyre több állam által megalkotott nemzeti kiberbiztonsági stratégiák, vagy említhetjük a nemzetállami szintet túllépve például a *Tallinni jegyzőkönyv*et. A kiberbiztonság tényleges megteremtéséhez azonban még igen hosszú és fáradtságos út vezet, s kérdéses a végeredmény is. Ugyanis egy olyan közegben, mint a kibertér, amely maga is a számtalan eltérő érdek mentén rendkívül széttöredezett, és amelyben napról napra újabb és újabb fenyegetések jelennek meg (elég ha a választási botrányokra vagy a különböző személyes adatok ellopására gondolunk), nagyon nehéz, de optimistán tegyük hozzá, hogy talán nem lehetetlen a biztonság megteremtése és garantálása úgy az egyes állampolgárok , mint a nemzetállamok számára. S ekkor talán véget érhet napjaink korszaka, amelyet még bátran nevezhetünk a Virtuális Vadnyugat világának.

[9] MUHA (2017).

[10] Gartner Says Worldwide Enterprise IT Spending to Reach $2.7 Trillion in 2012 (2011).

[11] Norbert Wiener-idézetek.

2. AZ EURÓPAI KIBERBIZTONSÁG ÁLTALÁNOS JELLEMZÉSE

A kiberbiztonság olyan új, igen dinamikusan fejlődő biztonsági terület, amely egyre több és egyre veszélyesebb fenyegetést rejt magában. Ha önmagában ez a tény nem állítaná elég kihívások elé a nemzetközi rendszer szereplőit, akkor az már bizonyosan elgondolkodtatja valamennyi államot, hogy a világot átszövő interdependens kapcsolatok hálójában képtelenek lesznek magukat függetleníteni egy látszólag őket nem érintő eseménnyel szemben. Ugyanis a kibertérben – egyszerű szóhasználattal élve – minden mindennel összefügg, s ebben a szövevényes hálórendszerben valamennyi államnak újra kell definiálnia biztonságfogalmát és a biztonsága fenntartása érdekében megteendő lépéseket.

Ez alól nem képez kivételt az Öreg Kontinens sem. Az egyik oldalról az európai országok sorra válnak kibertámadás áldozatául, a másik oldalról viszont egymás után teszik meg az ilyen jellegű támadásokkal szemben szükséges védekezés lépéseit – amelyek akár támadó jellegűek is lehetnek a brit példa alapján.

2.1. HATALMI VISZONYOK AZ EURÓPAI KIBERTÉRBEN

Ahogyan a kiberbiztonság fogalmával kapcsolatban is némi bizonytalanságot érezhetünk, úgy nincs egy egységesen elfogadott kibertérfogalom sem. Abban azonban valamennyi szakember egyetért, hogy a kibertér egyesít valamennyi hálózatot és kapcsolódó eszközt. Ebben az új közegben élik mindennapjainkat az európai polgárok is, akik már nem csak a számítógépes munkavégzésük során állnak közvetlen kapcsolatban az internettel, hanem a dolgok internetének (Internet of Things – IoT) köszönhetően az otthonuk is a kibertér részévé válik az internetre csatlakozott számtalan eszköznek köszönhetően.[12] Érezhető tehát, hogy a kibertértől való függőségünk napról napra növekszik, amely maga után vonja növekvő sebezhetőségünket is. Az átlagpolgár számára ez napi szinten akkor érzékelhető, ha például akadozik a levelezőrendszere, sokkal veszélyesebbek azonban azok a kibertérben jelentkező fenyegetések, amelyek célzottan egyes emberek, szervezetek, akár államok ellen irányulnak és hatásukat tekintve óriási méreteket ölthetnek.

[12] Külön problémát jelent, hogy az otthoni rendszerek többsége olyan sérülékenységgel rendelkezik, amely alapján az adott eszközt távolról tönkre lehet tenni, és a hiba ugyanakkor nem kijavítható. Sérülékenységi probléma továbbá, ha a szoftvereket nem frissítik (mint például a légitársaságok, a szórakoztató elektronika esetében), de az is, ha a munkavállaló a munkahelyén a helyi, védett hálózatra USB segítségével rácsatlakoztatja a saját eszközét, amely így utat enged a világháló valamennyi leselkedő veszélyének.

Ezek alapján jól kirajzolódik az is, hogy ki válhat áldozattá a kibertérben:

- a *kormányzati szektor* teljes egészében – amelyre jó példa az orosz–amerikai „vetélkedés", az egyes szabotázsakciók, mint az észtek esetében[13], az államtitkok kiszivárogtatása, ahogyan az a Wikileaks-botrány kapcsán történt[14] vagy említhetjük a kritikus infrastruktúra intézményei elleni támadásokat is az ukrán eset nyomán[15] vagy legújabban a „Stuxnet 2" néven elhíresült, az iráni infrastruktúra és stratégiai hálózatok elleni támadást[16],
- a *vállalati szektor* elleni támadások száma is egyre nő: gondoljunk a felhőkben tárolt adatok ellopására vagy az ipari létesítményeket érő tényleges támadásokra, mint a német vasmű elleni támadás[17],
- végül a *magánszemélyek* elleni fenyegetések köre is fokozatosan bővül: részben az előbbi két szektort érintő támadás rögtön érezteti hatását az egyes emberek vonatkozásában is, másrészt viszont a zsarolóprogramok által ellopott levelezések vagy számítógépen tárolt egyéb adatok elvesztése közvetlen veszteséggel is jár.

Az európai kibertér fent említett szereplői közül jelen monográfia keretei között az állami szinttel foglalkozom – összhangban a biztonsági tanulmányok referenciaszintjével. Az európai kibertér fogalmába valamennyi európai állam beletartozik, formálásában azonban nem csak európai államok vesznek részt köszönhetően a kibertér és a benne fellelhető fenyegetések határokat nem ismerő természetének.

S ez jelenti az egyik legnagyobb problémát. Az európai országok ugyanis olyan demokratikus országok, amelyek a demokratikus vívmányaikat igyekeznek megvédeni, ez azonban napjainkban egyre nehezebb feladattá válik, mert a külföldi érdekek óriási mértékben áramlanak be a kibertéren keresztül az egyes nemzetállami rendszerekbe.[18] Ez egyúttal azt is jelenti, hogy békeidőben lényegében háború zajlik a kibertérben, amely jelenleg még teljes mértékben szabályozatlan terület. Nem tisztázottak a mesterséges intelligencia alkalmazásának keretei[19], a drónok használatának kérdései, a tömeges megfigyelések keretei – sok más kérdés mellett –, s mindez elvezet az olyan demokratikus elemek sérelméhez, mint a választási rendszer megfelelő működése és a választások tisztasága[20] vagy az egyes szabadságjogok megvédése és érvényesülésük garantálása.

---

13 MCGUINNESS (2018).

14 2016 Presidential Campaign hacking Fast Facts (2018).

15 ZETTER (2016).

16 ILASCU (2018).

17 Hack attack causes'massive damage' at steel works (2014).

18 Gondolhatunk itt a cseh külügyminiszter levelezésének feltörésére (TAYLOR [2017]) vagy az ügyfélkapuk, rendőrségi kamerarendszerek és köztisztviselői adatbázisok feltörésére.

19 Etikai bizottságok felállításának gondolata is csak két éve merült fel, de érdemi előrelépés a mai napig nincs. In: STONE (2018). Pedig a kérdés egyre akutabb lesz például az önvezető autók vonatkozásában, amelyek használata során olyan kérdésekkel fogunk majd szembesülni, mint egy baleset esetén ki a felelős, melyik algoritmus volt rosszabb és kit terhel fizetési kötelezettség.

20 Ez a kérdés már az „Obama-kampány" kapcsán is felmerült 2012-ben, amely során igazoltan befolyásolták az állampolgárok preferenciáját a közösségi médián keresztül célzottan elküldött, személyre szabott üzenetekkel, de ugyanilyen hatása lehet a szintén már többször alkalmazott hamis hírek tömeges publikálásának („trollgyár").

Napról napra több azon európai országok száma, amelyek áldozattá válnak – érzékelve ezzel a szabályozatlanság közvetlen negatív hatását. A brit kiberbiztonsági központ vezetője, Ciaran Martin 2018 januárjában úgy fogalmazott, hogy a kérdés nem az, hogy egyáltalán lesz-e egészpályás kibertámadás az Egyesült Királyság ellen, hanem az, hogy mikor, és csodának nevezné, hogy ha erre a következő két évben nem kerülne sor.[21] Megjegyzendő, hogy alappal borúlátó a világ egyik legnagyobb kiberközpontjának vezetője, mert az elmúlt néhány évben bő 700 közepes támadást (C3-as besorolású) és közel 100 erős támadást (C2-es besorolású) sikerült elhárítaniuk. Az Egyesült Királyság elleni legmagasabb szintű támadásra (C1-es besorolású) tehát még nem került sor – szemben Franciaországgal, ahol a vezető médiaszolgáltató, a TV5 televízió ellen 2016-ban elkövetett támadás már ilyen erősségűnek minősül.[22]

A kiberbiztonság tehát a demokratikus társadalmi berendezkedés és hatalomgyakorlás új oszlopává válik, amely ha bárhol elkezd repedezni, az egész struktúrát veszélyezteti.[23] Ezért csak egy egységes kibertérszemlélet és kialakult szabályrendszer segítségével lehet az elmúlt évszázadok vívmányait a kibertérben is megvédeni.

Az európai kibertér vizsgálatához segítségünkre van több mutató is. Az ITU által jegyzett *Globális kiberbiztonsági index*[24] átfogó módon értékeli a világ országainak kiberbiztonságát öt kategória 25 alkategóriájában osztályozva őket.[25] A 2017-es adatok alapján az első 10 ország között kettő európai ország található: Észtország az ötödik, Franciaország pedig a 9. helyen áll. Az alábbi 1. sz. kép két mutatót jelenít meg: a függőleges tengelyen a *Globális kiberbiztonsági index*et, a vízszintes tengelyen pedig az *Infokommunikációs fejlettségi index*et.[26] Az ábra alapján nem csak az rajzolódik ki, hogy e két biztonsági terület milyen szoros összefüggésben van egymással, hanem az európai országok kimagasló fejlettsége is. Pirossal jelölik ugyanis az európai államokat, s ezen államok egyértelműen a legfejlettebbek mindkét vizsgált területen.

21 MACASKILL (2018).

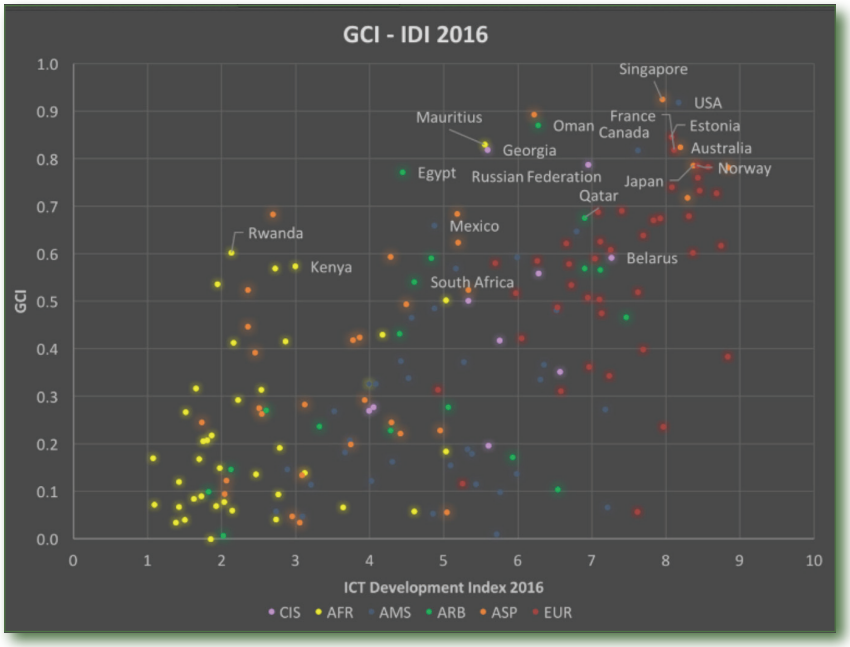
22 CORERA (2016).

23 FELEDY (2018).

24 Global Cybersecurity Index 2017.

25 Ezek a jogi, a technikai, a szervezeti, a kapacitásépítési és együttműködési területek.

26 ICT for Development Index.



1. sz. kép: A Nemzetközi Távközlési Egyesület (ITU) Globális kiberbiztonsági indexének és az Infokommunikációs fejlettségi indexének összefüggései

(Forrás: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf *[Letöltve: 2018.10.13.])*

A *Globális kiberbiztonsági index*nél maradva a regionális összesítés egyértelműen kimutatja az európai kibertér vezető szerepét mind az öt vizsgált területen.[27] Ehhez azonban azt is hozzá kell tenni, hogy bár Európa a jogi és technikai területen jól teljesített, a szervezeti, kapacitásépítési és együttműködési képességeket vizsgálva még az európai államoknak is bőven van hová fejlődniük.

Az általam vizsgált három ország vonatkozásában megállapítható, hogy mindhárom állam az index mutatói alapján is kimagasló teljesítményt nyújt a kiberbiztonság területén. Franciaország globális 9. helyezése önmagában is figyelemre méltó, ha azonban ehhez hozzátesszük azt is, hogy a kapacitásépítés területén 100%-os eredményt ért el, ez világviszonylatban is egyedülálló. Az index rangsora alapján az Egyesült Királyság a 11. helyen áll, míg Németország a 24. helyen.

A képet azonban árnyalja az ún. *Kiberfelkészültségi index*[28], amely kilenc[29] vezető hatalmat rangsorol hét szempont[30] alapján. Az index alapján megállapítható, hogy még egyik állam sem tekinthető teljeskörűen felkészültnek kiberbiztonsági viszonyait tekintve. Az Egyesült Királyság, Németország és Franciaország is csak részben tekinthető működőképesnek mind a hét vizsgált területen.

[27] A jogi területen Európa 0,61 átlagponttal rendelkezik (szemben a legkevésbé fejlett afrikai régióval, amely 0,29 pontot ért el). A technikai területen 0,6 pont az európai átlag (míg az afrikai 0,18), a szervezeti kérdéseknél 0,45 pont (Afrika esetében 0,16), a kapacitásépítés terén 0,49 pont (az afrikai országoknál 0,17), míg az együttműködés terén 0,46 pont (szemben az afrikai országok 0,25 pontjával).

[28] Cyber Readiness Index 2.0. A plan for cyber readiness: a baseline and an index. Country Profiles (2015).

[29] Ezek az Egyesült Államok, Japán, Franciaország, Németország, az Egyesült Királyság, Olaszország, India, Hollandia, Szaúd-Arábia.

[30] A hét vizsgált szempont a nemzeti kiberstratégia, az incidenskezelés, az e-bűnüldözés, az információ-megosztás, a beruházások és K+F, a diplomácia és kereskedelem, valamint a védelem és válságkezelés.

2.2. AZ EURÓPAI KIBERSZABÁLYOZÁS

Európa kiberbiztonságának megerősítése évek óta égető probléma. Szükségességére olyan események világítottak rá, mint a brit egészségügyi rendszer megbénítása, az európai vezetők levelezésének feltörése vagy az ukrán elektromos hálózat lekapcsolása – csak hogy néhányat említsek a sok ezer eset közül. Emellett a kibertámadások és a kiberbűnözés okozta költségek is évek óta exponenciálisan emelkednek, 2017-ben már a globális GDP 0,8%-át tették ki, összesen 600 milliárd dollár értékben[31], ezért ezzel a fenyegetéssel az Uniónak a legmagasabb szinten kell foglalkoznia.

Az európai szabályozás elmúlt 15 évének sarokpontjai körében elsőként a stratégiai szintet vizsgálva mindenképpen az Unió első biztonsági stratégiáját kell megemlíteni, amelyet még 2003-ban fogadott el és adott ki a szervezet *Egy biztonságos Európa egy jobb világban. Az Európai Biztonsági Stratégia* címmel.[32] Bár ez a dokumentum a kiberfenyegetések körét még sem a globális, sem a kifejezetten Európára leselkedő veszélyek körében nem nevesíti, az rejtetten a társadalmak sebezhetőségével és a terrorizmussal összefüggésben mégis megjelenik. A stratégiát felülvizsgáló, 2008 decemberében kiadott jelentés ezzel szemben a kiberbiztonság kérdéskörét már kiemelten kezeli, ami annak is köszönhető, hogy a digitális technológiáktól való függés az évek során jelentősen megnőtt mind az államok, mind az állampolgárok vonatkozásában, és a biztonságos internet biztosítása a lakosság számára az elsődleges érdekek közé lépett elő. Az új biztonsági stratégia elfogadására hosszas egyeztetéseket követően csak 2016 nyarán került sor. A *Közös jövőkép, közös cselekvés: erősebb Európa. Az EU globális kül- és biztonságpolitika stratégiája* címet viselő dokumentumban a kiberbiztonság már nemcsak hogy nevesítve szerepel, hanem kiemelt figyelem övezi a kihívások kezelésében rendelkezésre álló eszközök és szakpolitikák körében.[33]

Az általános stratégiai szinttől eggyel konkrétabb szintre lépve már kifejezetten az információs rendszerek védelmével kapcsolatban az első dokumentum, az *Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása* című bizottsági közlemény 2009-ben jelent meg.[34] A közlemény a kibervédelmi gyakorlatok hiányosságaira hívja fel a figyelmet és kiemeli a nemzetközi szervezetekkel (úgy mint az ENSZ, a NATO, az OECD és a G8) való együttműködés fontosságát e téren.

Az Unió kiemelten kezeli a digitális élet vívmányainak biztonságos használatát. Jelenleg[35] ezt egy 10 éves program[36] keretei között kívánja megvalósítani 2020-as céldátummal, amely során olyan hiányosságokat igyekeznek kiküszöbölni, mint a digitális piac töredezettsége, az interoperabilitás és a szakképzett munkaerő hiánya, emellett ösztönzik a befektetéseket és cél a kiberbűnözés visszaszorítása is. Ez a *Digitális Menetrend*, amely döntő lökést adott a terület iránti érdeklődés fellendüléséhez és a szabályozási folyamat beindulásához. Előbb az Európai Par-

31 LEWIS (2018).

32 Az Európai Biztonsági Stratégia. Egy biztonságos Európa egy jobb világban (2003).

33 Az EU globális kül- és biztonságpolitikai stratégiája – 2016 (2016).

34 COM (2009), 149.

35 A jelenlegi 10 éves programot két ötéves program is megelőzte: 2000 és 2005 között az eEurope Action Plan (eEurope Action Plan [1999]), 2005 és 2010 között pedig az i2010 – European Information Society for growth and employment (2005).

36 Az Európai Digitális Menetrend (2010).

lament fogadott el egy határozatot 2012-ben *Kritikus információs infrastruktúra védelme: a globális kiberbiztonság megteremtése felé* címmel[37], amely bár nem volt kötelező érvényű a tagállamokra nézve, mégis az abban foglalt olyan kívánalmak nagy részét a tagállamok megvalósították, mint a nemzeti kiberbiztonsági stratégia és a vonatkozó nemzeti szabályok megalkotása vagy az önálló kibervédelmi szervezetrendszer felállítása. Innét pedig már csak egy lépés volt az önálló uniós kiberbiztonsági stratégia megalkotása.

Az Európai Unió 2013-ban fogadta el hivatalos *kiberbiztonsági stratégiáját Nyílt, biztonságos és megbízható kibertér – Az Európai Unió kiberbiztonsági stratégiája* címmel.[38] A stratégia megalkotása jelentős lépés volt az Unió részéről, a lefektetett prioritások[39] pedig nagy ívű célokat állítanak a szervezet elé. Az, hogy ezeket mennyiben sikerül elérni, még a jövő zenéje. Problémás ugyanakkor, hogy a stratégia csak az európai infokommunikációs rendszerek meghibásodásának és ellenük intézett támadások megelőzésére és a válaszlépésekre vonatkozik, s még az olyan kérdések is megválaszolatlanok maradnak, mint például az, hogy a *Lisszaboni szerződés* záradéka alapján az Európai Unió mint egész hogyan reagáljon egyik tagállamát ért kibertámadás esetén.[40] Minta pedig van, a NATO ugyanis 2016 óta a *Washingtoni szerződés* 5. cikkelyét ilyen esetek vonatkozásában is alkalmazni rendeli.[41]

Az informatikai biztonság területe igen széles, az uniós szabályozás pedig igyekszik valamennyi kérdéskört szabályozni. Az utóbbi években a szabályozás terén olyan új irányok jelentek meg, mint a napjainkban igen gyakran emlegetett adatvédelem területe. Az Unió e területen világviszonylatban is az „úttörők" között szerepel, köszönhetően a 2016. május 4-én elfogadott ún. *adatvédelmi rendeletnek*.[42] Emellett mindenképpen meg kell említeni a 2016. július 6-án elfogadott *hálózatbiztonsági irányelvet*, rövid nevén a NIS-irányelvet[43], amely számos kötelezettséget is ró a tagállamokra, a terjedelmi korlátok miatt azonban ezek bemutatásától eltekintek.

37 2013/C 332 E/03 EP állásfoglalás (2012).

38 Az Európai Unió kiberbiztonsági stratégiája (2013).

39 A stratégia öt prioritást nevesít: a kibertámadások megelőzéséhez, feltárásához és kezeléséhez szükséges képességek kifejlesztése; a kiberbűnözés nagymértékű visszaszorítása; az önálló kibervédelmi politika és képességek fejlesztése az Unió közös biztonság- és védelempolitikáján belül; a szükséges ipari és technológiai kapacitások és feltételek megteremtése; valamint az önálló, uniós szintű kiberpolitika mint szakpolitika létrehozása az EU alapértékei mentén.

40 MOLNÁR (2017a).

41 A valóságban ez sem feltétlenül „hibátlan megoldás", mert csak az esetek mintegy 10%-ában lehet kétséget kizáróan bizonyítani, hogy ki volt a támadó a kibertérben. A támadó kilétének ismerete hiányában pedig igen aggályos az 5. cikkely alapján retorzióként fizikai erőszakot alkalmazni.

42 2016/679/ EP-Tanácsi rendelet (GDPR-rendelet).

43 2016/1148/EP-Tanácsi irányelv (NIS-irányelv).

3. A BRIT, NÉMET ÉS FRANCIA KIBERBIZTONSÁG ÖSSZEHASONLÍTÁSA AZ OECD IRÁNYELVEK MENTÉN

3.1. AZ OECD-IRÁNYELVEKRŐL ÁLTALÁBAN

A Gazdasági Együttműködési és Fejlesztési Szervezet (Organisation for Economic Co-Operation and Development, a továbbiakban: OECD) először 1992-ben fogadott el irányelveket az információs rendszerek biztonságával kapcsolatban. Ezek felülvizsgálatára 10 évvel később került sor a 2002-ben kiadott *Irányelvek az információs rendszerek és hálózatok biztonságáról – Egy biztonsági kultúra felé* címmel.[44] A 2002. július 25-én elfogadott tanácsi dokumentum jelenleg is hatályban van, felülvizsgálatára még nem került sor.[45]

Az irányelvek kiadásának szükségességét az indokolta, hogy a 2000-es évekre már olyannyira összekapcsolódtak az információs rendszerek és hálózatok, hogy egymástól való függőségük s ezért sérülékenységük is soha nem látott méreteket öltött, ez pedig új biztonsági kérdéseket vetett fel. Az irányelvek az új információs társadalom valamennyi szereplőjére vonatkoznak, és megalkotásuk célja az volt, hogy a biztonságnak egy olyan kultúrája alakuljon ki, amelyben a szereplők elővigyázatosan teszik meg lépéseiket nagyobb biztonságuk elérése érdekében. Ez csak egy olyan megközelítés mentén érhető el, amelyben a résztvevők érdekeinek szem előtt tartása mellett hasonlóan fontos vezérlő elv a hálózatok, rendszerek és kapcsolódó szolgáltatások természetének figyelembevétele.

[44] OECD (2002).

[45] 2012-ben már kezdetét vette a felülvizsgálat folyamata, amely még jelenleg is tart. Lásd: OECD Reviewing Its Security of Information Systems and Networks Guidelines (2013).

Az OECD kilenc irányelvet rögzít, amelyeket egymástól nem elválasztva, egységesen kell kezelni, valamennyi biztonsági szereplőre vonatkoztatva. Az elvek három csoportba sorolhatók:

- a politikai-szervezeti elvek körében a tudatosság[46], a felelősség[47] és a reakcióképesség[48];
- a technológiai elvek között a kockázatok értékelése[49], a biztonság megvalósítása[50], biztonságmenedzsment[51] és az újraértékelés[52]; valamint
- a társadalmi jellegű elvek közt az etika[53] és a demokrácia.[54]

Ezen irányelveket alapul véve a szervezet az alábbi ajánlásokat fogalmazta meg:

- Az államok dolgozzanak ki új vagy dolgozzák át a már meglévő dokumentumaikat, gyakorlatukat, eljárásaikat.
- Az irányelvek megvalósítása érdekében mind nemzeti, mind nemzetközi szinten konzultáljanak egymással, egyeztessenek és működjenek együtt.
- Terjesszék az irányelveket a köz- és magánszektor szereplői között.
- A nem OECD országok számára is tegyék elérhetővé az irányelvek megismerését.
- Az együttműködés előmozdítása érdekében szükséges az irányelvek ötévenkénti felülvizsgálata.

Az irányelvek felülvizsgálatának folyamatában mérföldkőnek számít az a 2012-ben kiadott tanulmány[55], amely a nemzeti kiberbiztonsági stratégiák összehasonlító elemzésére vállalkozik. Az OECD 10 önkéntes országot[56] vont be vizsgálódása körébe – köztük az általam kutatott három államot is –, melynek során egyértelműen megállapítást nyert, hogy az országok nemzeti prioritássá emelték a kiberbiztonság kérdését, amelyet csak valamennyi kormány-

[46] A biztonsági szereplőknek tisztában kell lenniük azzal, hogy szükséges az információs rendszerek és hálózatok biztonságának megteremtése, s tudniuk kell, hogy a biztonság növelése érdekében pontosan mit tudnak megtenni.

[47] A rendszer valamennyi szereplője felelős a biztonság megteremtéséért.

[48] A szereplőknek gyorsan és egymással együttműködve kell cselekedniük, hogy a biztonsági incidenseket meg tudják előzni, vagy ha azok már bekövetkeztek, fel tudják deríteni őket és megfelelő válaszokat tudjanak rájuk adni.

[49] Minden esetben szükséges, hogy a rendszer szereplői a kockázatokat értékeljék, feltárva ezáltal a leselkedő fenyegetéseket és a rendszer sérülékeny pontjait.

[50] Az információs rendszerek szerves, elengedhetetlen eleme a biztonság kérdése; ennek megfelelően kell a rendszereket és hálózatokat felépíteni, működtetni és összehangolni.

[51] Olyan átfogó, a kockázatok értékelésére épülő megközelítésre van szükség, amely dinamikus és a rendszerben résztvevők tevékenységének valamennyi szintjét és aspektusát átöleli.

[52] Szükséges a rendszer biztonságának felülvizsgálata, a kockázatok újraértékelése, s ez alapján a stratégiák, szakpolitikák, eljárásrendek felülvizsgálata.

[53] A rendszer szereplőinek mások jogos érdekeit tiszteletben kell tartania.

[54] Az információs rendszerek és hálózatok biztonságának megteremtése és fenntartása során tett lépéseknek a demokratikus társadalmak alapvető értékeivel összhangban kell lenniük.

[55] OECD (2012).

[56] Ausztrália, Egyesült Államok, Egyesült Királyság, Finnország, Franciaország, Hollandia, Japán, Kanada, Németország, Spanyolország.

zati szektor bevonásával lehet és kell kezelni. Elengedhetetlen a terület központi vezérlése, mert olyan nemzeti érdekről van szó, amely biztosítása valamennyi állam számára elsődleges a gazdasági prosperitás és a társadalmi fejlődés garantálása érdekében.

A szervezet megvizsgálta az államok kiberbiztonsági stratégiáját, s ez alapján feltárta azon közös vonásokat, amelyek valamennyi állam stratégiáját jellemzik.[57] Ezek a következők:

- széles körű kormányzati koordináció politikai és műveleti szinten egyaránt: A kezdeti, több szervezetet magába foglaló koordinációt felváltó kormányzati szervezetek közötti együttműködés megköveteli egy erős központi irányítás létét a párhuzamosságok elkerülése és a világos feladatelhatárolások érdekében.
- a köz- és magánszféra együttműködésének bátorítása: Valamennyi stratégia elismeri, hogy a kibertérben a magánszféra játssza a döntő szerepet és a felhasználóknak is hasonlóan jelentős szerep jut, ugyanakkor az egyes stratégiák a konzultációk eltérő szintjét rögzítik, más-más részletezettséggel.
- a nemzetközi együttműködés további fejlesztése: Ezzel kapcsolatban azonban a nemzeti stratégiák kevés rendelkezést tartalmaznak (ez alól csak az Egyesült Államok[58] és az Egyesült Királyság[59] képez kivételt).
- az alapvető értékek tisztelete: Valamennyi stratégia nevesíti a magánélet tiszteletben tartását, a szólásszabadság érvényesülését és az információ szabad áramlásának szükségességét a kiberpolitika kialakítása és gyakorlása során.

A közös vonásokon túl csokorba gyűjthetők olyan jellemzők is, amelyek bár nem feltétlenül jelennek meg valamennyi stratégiában, de a fejlődés új irányvonalait vetíthetik előre. Ezek a következők:

- a szuverenitás kérdésköre, amely más-más megvilágításba kerül stratégiai, szervezeti és műveleti szinten;
- rugalmas, reagálni kész kiberpolitika gyors döntéshozatali folyamattal, gyors visszacsatolásokkal és változásra kész hozzáállással, amely képes biztosítani a nyílt internetet és az információ szabad áramlását;
- a kiberbiztonság gazdasági dimenziójának fontossága, hiszen a digitális világ a gazdasági fejlődés mozgatórugója;
- a sokszereplős párbeszéd adta előnyök, elsősorban a nem kormányzati szereplők bevonásával;
- a kiberstratégiák részeként kiadott vagy azt követően elfogadott akciótervek, amelyekben megjelenik az állami intézményrendszer biztonságának kérdése, a kritikus információs infrastruktúrák védelme, a kiberbűnözés elleni küzdelem, a tudatosság növelése és az oktatás fontossága, a reagálóképesség fejlesztése (kiemelve a CSIRT[60]-ek fontosságát), valamint a K+F kérdések.

---

[57] Megjegyzem, hogy a tanulmány ugyan 2010-2012-es adatokra épül, azonban figyelemre méltó, hogy az akkor hatályban lévő első generációs kiberbiztonsági stratégiák is már bírtak a felsorolt jellemzőkkel. Azóta természetesen az országok új stratégiákat fogadtak el, ami azonban ez nem jelenti a közös jellemzők körének megváltozását.

[58] Az Egyesült Államok önálló nemzetközi kibertér stratégiával rendelkezik, amelyet még 2011-ben az Obama. elnökség alatt fogadtak el „International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World" címmel (International Strategy for Cyberspace… [2011]).

[59] 2011 óta minden évben Londonban kerül megrendezésre a „London Conference on Cyberspace" nemzetközi konferencia.

[60] Computer Security Incident Response Team – gyorsreagálású kibervédelmi szakértői csapat.

Ezek a kérdések a fejlett államok kiberstratégiáinak általában már részét képezik, sőt, a legújabb stratégiák már kiegészülnek olyan újabb elemekkel, mint például a határokon átnyúló kibergyakorlatok kérdése, az internetszolgáltatókkal való kapcsolatok vagy a speciális online gyermekvédelmi politika.

Az OECD-elemzés tartalmaz egy olyan egységes szempontrendszert, amely segítségével elvégezhető az egyes államok kiberstratégiáinak összehasonlító elemzése. A következő rész ennek alapulvételével készül s végighalad a három vizsgált állam, az Egyesült Királyság, Németország és Franciaország vonatkozásában a stratégiaalkotási és szervezeti kérdéseken, valamint megjeleníti a nem kormányzati szektor által tett javaslatokat is.

3.2. ÖSSZEHASONLÍTÁS AZ ALAPVETŐ STRATÉGIAI KÉRDÉSEK MENTÉN

A stratégiaalkotás alapvető kérdései körében a stratégiaalkotás folyamatát, a mögötte meghúzódó mozgatórugókat és a főbb tartalmi elemeket kell vizsgálni, amelyet az alábbi öt területen végzek el:

1.Új, dinamikus tendenciaként jelentkezik az új, második és harmadik generációs nemzeti kiberbiztonsági stratégiák megalkotása.

Az általam megvizsgált három állam már ún. második, illetve harmadik generációs kiberbiztonsági stratégiával rendelkezik. Az Egyesült Királyság 2009-ben fogadta el első dokumentumát, amelyet két évvel később, 2011-ben megújított, deklaráltan ötéves időintervallumra vonatkozóan rögzítve a prioritásokat, célokat.[61] A legújabb dokumentum 2016-os keltezésű, szintén ötéves tervezéssel készült.[62] Németországban az első stratégia 2011-ben született meg[63], jelenleg pedig a 2016. évi változata van hatályban.[64] Franciaország 2011-ben kiadta első kiberbiztonsági stratégiáját[65], majd a 2013-ban elfogadott *Fehér könyv*ben[66] foglaltak alapján 2015-ben adták ki *Digitális stratégia* elnevezéssel a hivatalos kiberbiztonsági dokumentumukat.[67] (Franciaországban egyébként több, az információs rendszerekkel kapcsolatos stratégiai dokumentum is született[68], de elnevezését tekintve egyik sem viseli a kiberbiztonsági stratégia nevet.)

A dinamizmus a stratégiákban is fellelhető. A brit dokumentum a *Védelmi felülvizsgálat*ban rögzítetteknek megfelelően rugalmas kiberbiztonsági reagálást említ, míg a német és a francia stratégiákban is hangsúlyosan jelenik meg az aktív politikaformálás igénye. A francia stratégia esetében egyenesen a miniszterelnök az, aki a stratégia előszavában abbéli reményének ad hangot, hogy az új stratégia egy olyan dinamizmust indít útjára, amely

61 The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world (2011).

62 The UK Cyber Security Strategy 2011–2016. Annual Report (2016).

63 Cyber Security Strategy for Germany (2011).

64 Cyber Security Strategy for Germany 2016 (2016).

65 Défense et sécurité des systèmes d'information. Stratégie de la France (2011).

66 Livre blanc sur la défense et la sécurité nationale (2013).

67 Stratégie nationale pour la sécurité du numérique (2015).

68 Stratégie du lutte contre les cybermenaces (2017), Stratégie internationale de la France pour le numérique (2017).

egyidejűleg biztosít nagyobb védelmet és szabadítja fel az energiákat. A dinamikus reagálás iránti igénynek egyik mutatója lehet az is, hogy a stratégiák deklaráltan ötéves időtávra készültek, jelezve ezzel is azt, hogy ennyi idő alatt kellőképpen megváltozhat a biztonsági környezet ahhoz, hogy a dokumentumokat felül kelljen vizsgálni. A dinamikus politikaformáláson kívül az új stratégiák kiadása egyúttal azt is jelzi, hogy a kiberbiztonság egyre jelentősebb nemzetbiztonsági kérdéssé válik.

2.Valamennyi vizsgált kiberbiztonsági stratégia a megnövekedett számú és intenzitású kiberfenyegetések felismeréséből született meg.

A kiberfenyegetések egyre előkelőbb helyen jelennek meg a stratégiai dokumentumokban. A 2015-ös brit nemzeti biztonsági stratégia a „Tier I" típusú fenyegetések közé sorolja, tehát öt éven belül reálisan számolni kell a bekövetkezésével.[69] Ráadásul a brit fő kiberbiztonsági szerv, a Nemzeti Kiberbiztonsági Központ vezetője szerint a kérdés nem az, hogy a legnagyobb volumenű, ún. C1-es kategóriájú kibertámadással számolniuk kell-e, hanem az, hogy mikor. Véleménye szerint kicsi még arra is az esély, hogy két éven belül ez ne következne be.[70] Ezzel szemben Franciaországot már ért ilyen C1 kategóriájú kibertámadás, ezért nem véletlen, hogy az ország külön stratégiával rendelkezik a kiberfenyegetések elleni harcról is.[71] A francia *Fehér könyv* már 2013-ban a harmadik helyen nevesítette a kiberfenyegetéseket, amelyek jelentősége azóta csak tovább nőtt.

2.a. A kiberfenyegetések természete, céljai, szervezettsége és összetettsége tovább nő.

A fenyegetések természetében bekövetkező változás annak köszönhető, hogy az államok is megjelentek az új szereplők körében mint elkövetők a már meglévő egyének és csoportok mellett. A nemzetállamok politikai céljai és az államok közötti konfliktusok is incidensekhez vezethetnek a kibertérben, amelynek csak kedvez az internet határokat nem ismerő jellege és a legújabb technológiákhoz való könnyű hozzáférés. Az elkövetők köreit legtisztábban a brit stratégia mutatja be, megkülönböztetve az államokat, a terroristákat, a bűnözői csoportokat és a képzetlenebb elkövetőket („script kiddy"-k). A francia digitális stratégia további új szereplőként nevesíti az üzleti világ nagyvállalatait, amelyek az ügyfeleik manipulálása céljából erős pozíciójuk kihasználásával képesek akár gazdasági destabilizációt is előidézni. A francia hozzáállás érdekessége, hogy stratégiai dokumentumban rögzíti azt az egyébként köztudott tényt, hogy a kibertérben akár a szövetséges államok is kémkedhetnek egymás ellen – utalva ezzel az Egyesült Államok adatgyűjtési gyakorlatára.

A támadások szervezettsége is jelentősen javult, amely részben annak tudható be, hogy az elkövetők a való világban alkalmazott módszereket sikeresen ültették át a kibertér viszonyaira.[72] Még az egyéni elkövetők is laza

[69] National Security Strategy and Strategic Defense and Security Review 2015. A Secure and Prosperous United Kingdom (2015).

[70] A közepesen erős, az Egyesült Királyság elleni C2-es kibertámadások száma eddig 34, míg a gyengébb C3-as kategóriájú támadásoké 763. MACASKILL (2018).

[71] Stratégie du lutte contre les cybermenaces (2017).

[72] Az okok között említhető még a rendszerek összetettebbekké (és ezáltal sérülékenyebbé) válása, a rendelkezésre álló erőforrások (mind személyi, mind anyagi) megnövekedése, különleges backdoor alkalmazások (például a fizikai chipekbe építik be azokat, illetve a szoftvergyártók már régóta alkalmazzák azokat), és külön iparággá vált a bűnözőknek „gyártott" infokommunikációs eszközök előállítása, például speciális BlackBerry telefon, amelyet bűnözők előszeretettel használtak, lehallgathatatlansága miatt.

hálózatokat formálva vagy decentralizált online közösségekként együttműködnek egymással, ezáltal fokozva tevékenységük sikerességét és hatását (lásd „Anonymus").

Általánosságban megállapítható, hogy az újabb nemzeti kiberstratégiák a szándékos fenyegetések jelentette fejlődést követik le és azokra adnak válaszokat, a véletlenszerűen jelentkező fenyegetésekre nem helyeznek különösebb hangsúlyt. A stratégiák a fő különbséget a motivációk és célok tekintetében jelölik meg, a támadások célpontjai és elkövetési módszereik azonosak.

2.b. Az államok sérülékenysége és az infokommunikációs technológiáktól való függése olyan szintre emelkedett, amely a kiberbiztonság kérdését nemzeti prioritássá tette.

A 2000-es évek elején 10 év leforgása alatt az internet az egyének és szervezetek hasznos kommunikációs eszközéből a gazdaság és társadalom számára nélkülözhetetlen digitális infrastruktúrává nőtte ki magát. Jól mutatja a változást a kritikus infrastruktúrák megnövekedett digitális függősége. Ezt a változást követték le a kiberstratégiák is. A vizsgált államok első, 2010 körül megjelent stratégiái még az online bizalom megteremtését tűzték ki célul, mert a társadalmi biztonság és gazdasági prosperitás ezáltal volt növelhető. Ezzel szemben mára a kiberbiztonság az egész társadalom vonatkozásában nemzeti prioritássá vált, ezért a legújabb, második és harmadik generációs, stratégiai dokumentumok már holisztikus szemléletet követve a társadalom egésze és valamennyi biztonsági szektor vonatkozásában rögzítik a célokat, prioritásokat.

A brit stratégia kiemeli, hogy míg korábban elegendő volt az infokommunikációs rendszerek biztonságára nagy hangsúlyt helyezni, mára e rendszerek szövevényes hálózatai alakultak ki mind a lakosság[73], mind a kritikus infrastruktúrák[74] vonatkozásában, s ezek megvédése vált elsődleges prioritássá. A stratégiák egységesek a tekintetben, hogy rögzítik: a hálózatok egymástól való függése miatt egy esetleges kibertámadás következményei nem csak a kibertérben érezhetők, hanem a magában a fizikai világban (ha például nincs víz-, gáz-, áram-, telefonszolgáltatás vagy akadozik a bankkártyás fizetés).

3. A kiberstratégiák célrendszere kettős: a kibertértől egyre függőbbé váló társadalmak megvédése a kiberfenyegetésekkel szemben, valamint az internetgazdaság további fejlesztéséhez elengedhetetlenül szükséges a kiberbiztonság szintjének további növelése.

3.a. Az új kiberbiztonsági stratégiák a nemzeti biztonság megváltozott értelmezéséből fakadnak.

Mindhárom ország esetében alapvető különbség az első generációs stratégiákhoz képest, hogy a felülvizsgált változatok már közvetlenül a nemzeti biztonsági stratégiákból eredeztethetők. Az Egyesült Királyság 2015-ben adta ki új nemzeti biztonsági stratégiáját, amely alapján egy évvel később elkészítették az új kiberbiztonsági stratégiát is. Németország esetében a 2013. évi *Fehér könyv*ben rögzítettek alapján készült el a kiberbiztonsági stratégia új változata 2016-ban. A *Fehér könyv* a kiberfenyegetéseket az ország előtt álló kihívások körében nevesíti mint legmagasabb fokú (top tier) nemzetbiztonsági kockázatot, és rögzíti, hogy a kibertámadások akár a fegyveres támadások hatásával is vetekedhetnek. Franciaország esetében a 2015. évi digitális biztonsági stratégia is a 2013-as *Fehér könyv*ből eredeztethető, összhangban a holisztikus szemléletmóddal.

[73] Ez az Internet of Things (IoT) – a Dolgok Internete sokat emlegetett jelensége.

[74] Industrial Internet of Things.

3.b. A kiberbiztonság az internetgazdaság fejlődésének nélkülözhetetlen eleme.

Félrevezető volna azt állítani, hogy a vizsgált országok a kiberbiztonsági politikájuk alakítása során a gazdasági és szociális célokat nem tartják szem előtt. Ehelyett inkább az a helyes megfogalmazás, hogy az új stratégiák kettős cél által vezéreltek: egy prosperáló internetgazdasághoz szükséges feltételeket megteremteni képes kiberbiztonság kiépítése úgy, hogy eközben a társadalom egészét sikerüljön megvédeni a kiberfenyegetésektől.

A brit stratégia úgy fogalmaz, hogy az internet a gazdasági növekedés motorja, amely támogatja a nyílt és erős társadalmak működését. A német stratégia a gazdasági és társadalmi fejlődést helyezi előtérbe és a kiberbiztonságot mint a nemzetállamok, a nagyvállalati világ és a társadalmak számára alapvető fontosságú kérdését és a 21. század központi kihívását nevesíti. A francia stratégia is ezen elemekre helyezi a hangsúlyt, amikor az ötös célrendszerének körében nevesíti az állampolgárok és az üzleti világ digitális értelemben vett életének védelmét és a fejlődés fontosságát, amelyek alapja a digitális technológiába vetett bizalom.

4. Mindennek eredményeként a kiberbiztonság egyik fő kormányzati prioritássá vált és a kormányzati koordináció is magasabb szintre emelkedett.

A kiberterület vezető prioritássá válását jól mutatja az is, hogy a hivatalos dokumentumokat milyen magas szinten adják ki. Az Egyesült Királyság esetében mindhárom kiberbiztonsági stratégiát a Miniszterelnöki Hivatal adta ki, jelezve ezzel azt, hogy a szigetország a kezdetektől fogva kormányzati prioritásként kezeli a kiberbiztonságának kérdését. Németországban az eddigi két stratégiát a Szövetségi Belügyminisztérium jegyzi, tehát ez esetben is a kezdetektől fogva adott a kiberkérdések kiemelt kezelése. A kiberterület felemelkedését leginkább a francia példán tudjuk nyomon követni: az első stratégiát 2011-ben még a miniszterelnök közvetlen irányítása alatt működő védelmi és nemzetbiztonsági főtitkár jegyezte, a 2015-ös stratégiát azonban már maga a miniszterelnök adta ki.

Érdekes megfigyelni azt is, hogy ezeket a legmagasabb szintű kiberbiztonsági dokumentumokat milyen elnevezésekkel illetik. Általánosan elfogadott terminológia a stratégia kifejezés használata – ahogyan azt a brit és német esetben is láthatjuk –, ugyanakkor Franciaország például nem kiberstratégia néven fogadta el legújabb stratégiáját, hanem a kiberkérdéseket tágabb kontextusba helyezve digitális stratégiának nevezi azt.[75]

A stratégiákban megfogalmazott célkitűzések végrehajtása egyéb döntések és akciótervek segítségével zajlik. A brit stratégia maga tartalmazza az igen részletes végrehajtási tervet úgy, hogy mérőszámokat rendel a célok teljesítéséhez és rögzíti a felülvizsgálat részleteit is. A francia stratégia a felállított célrendszeréhez kapcsoltan már a végrehajtás részleteit is tartalmazza.

A kiberbiztonság formálásában és garantálásában részt vevő szervek köre országonként eltérő, a kormányformától és a stratégiai kultúrától függően. Azonban általánosságban igaz, hogy a kibervédelmi koordináció a politika magas szintjén valósul meg: vagy a miniszterelnökhöz rendelten (ahogyan az Franciaországban történik), vagy a Miniszterelnöki Hivatalhoz rendelten (mint az Egyesült Királyság esetében).

A kiberbiztonságért felelős szervek is országonként eltérnek. Vannak országok, amelyek esetében valamely minisztérium működik mint kiberbiztonságért felelős fő szerv – ahogyan az Németországban a Szövetségi Belügy-

[75] Bár az európai országok többségében a stratégia kifejezés használata terjedt el a kiberterület relációjában is, Ausztráliában például előszeretettel használják a fehér könyv kifejezést – jelezve ezzel a terület erős politikai-katonai meghatározottságát.

minisztérium. Ugyanakkor több ország esetében kizárólag a kiberbiztonságuk garantálása céljával állítottak fel egy új szervezetet. Ilyen az Egyesült Királyságban a Nemzeti Kiberbiztonsági Központ (NCSC)[76] vagy Franciaországban az Információs Rendszerek Biztonságáért Felelős Nemzeti Ügynökség (ANSSI)[77]. A kiberterület működtetéséhez elengedhetetlenül szükséges a megfelelő koordináció mind a kormányzati szervek, mind a köz- és magánszféra szervezetei között. Az előbbi vonatkozásában több ország azt a megoldást választotta, hogy önálló, a koordinációért felelős szervezetet hoz létre (ahogyan az a briteknél a Kiberbiztonsági Műveleti Központ[78] vagy Németországban a Nemzeti Kiberreagálási Központ[79]). A köz- és magánszféra közti koordináció pedig gyakran speciális fórumok keretében zajlik; ilyenek a szigetországban felállított innovációs központok vagy a német nemzeti kiberbiztonsági tanácsok. Egyes esetekben a magánszektorral folytatott konzultációk jelentősége olyan nagy, hogy az nemcsak hogy a stratégiák kiadása előtt kötelező, hanem a stratégiák is azt említés szintjén tartalmazzák. A brit stratégia kiemeli, hogy a társadalom egésze számára készült, mert a kiberbiztonság megteremtése minden szereplő együttes feladata. A német stratégia úgy fogalmaz, hogy a legszélesebb körű konzultációkra van szükség, összhangban a dinamikus kiberpolitika-formálás követelményével. Végezetül a francia stratégia az, amelyik már a miniszterelnök szavait idéző előszóban rögzíti, hogy mindannyiuk feladatáról van szó, és a kormányzat, a közigazgatás, a helyi közösségek, a vállalatok és valamennyi honpolgár részvétele mellett szükséges a nemzetközi együttműködés is.

5. A „kiberbiztonság" és „kibertér" kifejezéseket nem feltétlenül használja mindegyik stratégiai dokumentum, habár a stratégiákban foglaltak általában vonatkoznak valamennyi információs rendszerre és hálózatra, beleértve az internethez nem kapcsolódó kritikus információs infrastruktúrákat is.

A „kiberbiztonság" és „kibertér" kifejezések használata nem szükségszerű, ugyanakkor általánosságban elmondható, hogy amelyik ország ezen kifejezéseket használja, az rögzíti az általa megalkotott definíciót is. Ez problémák forrása lehet és ellene hat azon törekvésnek, hogy egy nemzetközileg elfogadott, egységes kibertérfogalom alakuljon ki.

A stratégiák felelősségi köre általában kiterjed valamennyi információs rendszerre, függetlenül attól, hogy az kapcsolódik-e a világhálóhoz vagy sem. Ez alól kivételt képez a német stratégia, amely úgy véli, hogy az IT-rendszerek egy elszigetelt virtuális teret alkotnak és nem képezik a kibertér részét. A német kibertér az internetet és az infokommunikációs eszközöket foglalja magában, ez alapján pedig Németországban kibertámadásnak minősül az IT-rendszerek elleni olyan támadás is, amely az információs rendszerek elérhetőségét, megbízhatóságát és integritását veszélyezteti.[80]

A fogalomhasználat vonatkozásában az egyik végletnek az Egyesült Királyságot tekinthetjük, amely mindkét fogalmat használja, és a kiberteret az infokommunikációs rendszerek összekapcsolt hálózataként értelmezi. A másik véglet pedig a francia példa lehet, ahol a 2011-es stratégiában a „létfontosságú információs rendszerek bizton-

[76] National Cybersecurity Centre.

[77] Agence nationale de la sécurité des systemes d'information.

[78] Cyber Security Operations Centre – CSOC.

[79] National Cyber Response Centre.

[80] Ez egyúttal jelzi azt is, hogy Németországban az adatvédelmi kérdések milyen kiemelt helyen szerepelnek.

sága" kifejezést használták, 2015-ben pedig a „digitális biztonság" kifejezést, de egyik esetben sem a kiberbiztonság fogalmát – jelezve ezzel azt is, hogy az általában használt fogalmakhoz képest Franciaországban mennyivel tágabb határokat szabnak e terület értelmezésének.

3.3. ÖSSZEHASONLÍTÁS A KONCEPCIONÁLIS KÉRDÉSEK MENTÉN

1 A kiberbiztonsági stratégiák elvi, koncepcionális alapjai azonosak, még ha a megfogalmazott célkitűzéseikben eltérnek is egymástól.

Ezek a közös elvi alapok a következők:

a) *holisztikus, integrált, átfogó megközelítés erős vezetés mellett:*

Az átfogó megközelítés ez esetben jelenti egyrészt a probléma valamennyi aspektusának bevonását a vizsgálat körébe – úgymint a gazdasági, szociális, oktatási, jogi, végrehajtási, technikai, diplomáciai, katonai és titkosszolgálati aspektusokat –, másrészt mind a kormányzaton belül, mind azon kívül eső valamennyi szereplő bevonását egészen a külföldi partnerekig.

Már a 2011-es német stratégia úgy fogalmazott, hogy „a kiberbiztonságnak átfogó megközelítésen kell alapulnia" és „magas szintű kormányzati elkötelezettséget kíván meg". Hasonlóan fogalmaz a 2011-es brit stratégia is: „olyan sokoldalú megközelítést támogat, amelyben a kormányzat, valamennyi érintett szektor szervezetei, a közszféra és a nemzetközi partnerek is kiveszik a részüket".

Az olyan kérdések, mint a kritikus információs infrastruktúra védelme, a kiberbűnözés elleni küzdelem vagy az információs rendszerek és hálózatok védelme továbbra is helyet kapnak a stratégiákban, azonban már nem elkülönítetten, hanem olyan átfogó címszavak alatt, mint a kibervédelem (a 2011-es francia stratégia esetében) vagy a kiberbiztonság (a 2011-es brit stratégia esetében). A legújabb stratégia dokumentumok már gyakrabban élnek más jellegű szóhasználattal, mint ahogyan a 2016-os brit kiberbiztonsági stratégia az elrettentés címszó alatt szerepelteti a kiberbűnözés elleni küzdelmet.

b) *kormányzati koordináció:*

A holisztikus megközelítés jegyében valamennyi kormányzati szervnek együtt kell dolgoznia a kölcsönös előnyök mentén, kerülve a feladatkörök duplikációját a hatékonyság jegyében. A kormányzati együttműködés felöleli valamennyi érintett szektort: a gazdasági, a szociális, a rendőrségi, a nemzetbiztonsági, a hírszerzései, a katonai és a diplomáciai területeket. Ezen cél elérése érdekében a stratégiák pontosan meghatározzák a már meglévő vagy az új, a kiberbiztonsági koordinációban részt vevő szervek felelősségét politikai és műveleti szinten egyaránt.[81]

[81] Egyes esetekben (mint például Kanadában) még cizelláltabb a stratégia, és nem csak központi szinten, hanem az alsóbb közigazgatási egységek vonatkozásában is rögzíti a felelősségi köröket.

c) *a köz- és a magánszféra partnersége:*

A stratégiák többsége rögzíti, hogy a kibertér jelentős részét a magánszektor birtokolja és működteti, ezért a stratégiáknak a köz- és magánszféra együttműködésén kell alapulnia, az üzleti élet, a civil társadalom és az akadémiai szektor részvételével. Mindez azonban eltérő hangsúllyal jelenik meg a stratégiákban annak ellenére, hogy az együttműködés fontosságát valamennyi dokumentum hangsúlyozza. A brit stratégia úgy véli, hogy az elért eredményeket úgy lehet továbbfejleszteni, ha a kiberbiztonsági tevékenységbe bevonják a magánszférát is, mind az innovációk, mind a tudatosság terén.[82] Németországban az útjára indított „Industry 4.0" akcióterv kifejezetten azért jött létre, hogy a kis- és középvállalkozásokat fejlesztésekre ösztönözze az IoT terén.[83] Az összefogás pedig mára olyannyira sikeressé vált, hogy a világ legnagyobb együttműködési fórumává nőtte ki magát, amely kiemelt figyelmet fordít a kibertérbeli biztonságra. Ezt a kérdéskört egyébiránt a stratégia a négy kiemelt cselekvési terv egyikeként külön nevesíti is. A 2015-ös francia stratégia a negyedik célkitűzés körében nevesíti a magánszféra minél szélesebb körű bevonását és a köz- és magánszféra együttműködésének szükségességét – többek között az ország versenyképességének megtartása miatt.

d) *a nemzetközi együttműködés:*

A stratégiák többsége kiemelt hangsúlyt fektet a kiberbiztonság nemzetközi dimenziójára, valamint a hasonlóan gondolkodó államok és szövetségesek közötti szövetségi és partneri viszonyok szükségességére, amely segítségével a kevésbé fejlett államok képességei is fejleszthetők. Ugyanakkor az államok többsége az elsőgenerációs stratégiáikban még nem rögzíti az ezen cél eléréséhez szükséges lépéseket. Ez alól kivételt képez az Egyesült Államok[84] és az Egyesült Királyság. A 2011-ben (és azóta minden évben) megrendezett Londoni Kiberbiztonsági Konferencia révén a britek vezető szerepet vállaltak a többoldalú párbeszéd megteremtésében és hozzájárultak a kibertérre vonatkozó, nemzetközileg is elfogadott magatartási szabályok elfogadásához.

A nemzetközi szervezetek szerepével kapcsolatban a kezdeti stratégiák elég szűkszavúan fogalmaztak, és csak általánosságban tettek említést olyan szervezetekről, mint az Európai Tanács, a G8 vagy az OECD. A NATO-val kapcsolatban a kiberbiztonság katonai területhez való kötődését hangsúlyozták, az Európai Unió esetében pedig elsősorban az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA)[85] európai kiberbiztonság formálásában betöltött egyre hangsúlyosabb szerepét emelik ki.

A francia stratégia az Unióval kapcsolatban a fenntartható digitális fejlődés, az internetkormányzás és a személyes adatok védelme kapcsán tesz említést, és fontosnak tartja a kontinens stratégiai autonómiájának megteremtését, önkéntes állami részvétellel. A stratégia hangsúlyozza a kétoldalú kapcsolatok fontosságát, külön kiemelve a nagy európai partnert, Németországot, a felhőszolgáltatásokkal kapcsolatban. Németország pedig

---

82 A 2009-es brit kiberbiztonsági stratégia még úgy fogalmazott, hogy a Nemzeti Kiberbiztonsági Program sikere nagymértékben azon múlik, hogy a magánszektort mennyire sikerül bevonni.

83 A terv köré önálló platform is szerveződött. Az Industry 4.0. Platform már jelenleg is a világ legnagyobb együttműködési fóruma több mint 100 vállalat 250 delegáltjával és számos ország számára modellként szolgál. (A Platformról részletesebben lásd Industry 4.0. Platform.)

84 Visszautalok az amerikai nemzetközi kiberbiztonsági stratégiára.

85 European Network and Information Security Agency.

az információ-megosztás és a határokon átnyúló szolgáltatásokkal kapcsolatban felmerülő biztonsági kérdésekkel kapcsolatban szól a kétoldalú partneri kapcsolatok fontosságáról. A német stratégia emellett fontosnak tartja a fejlesztési együttműködést is, elsősorban olyan területeken, mint a kibertérben történő biztonság- és bizalomerősítő intézkedések a fejlődő államok vonatkozásában – összhangban a *Fehér könyv* szellemiségével, amely végig következetesen hangsúlyozza az ország Európában betöltött kulcsszerepét és globális felelősségvállalását a globális rend megteremtésében. A nemzetközi együttműködéssel kapcsolatban a stratégia kiemelten kezeli az adatbiztonság területét, de a korábbi stratégiában szereplő bűnügyi, rendőrségi és igazságszolgáltatási együttműködést is nevesíti. Az egyes nemzetközi szervezetek vonatkozásában a stratégia külön részletezi, hogy mely szervezet a kiberbiztonság mely területét érintően lát el különösen fontos feladatokat. Újszerű a német stratégia azon célkitűzése, amely a nemzetközileg elfogadott exportellenőrzési rendszer megerősítésére irányul azért, hogy a külföldi megfigyelésekkel eredményesen tudja felvenni a harcot. A francia stratégia önálló célkitűzés keretei között tárgyalja a nemzetközi együttműködést, kifejezetten európai fókusszal. Az *Európa, digitális szuverenitás, a kibertér stabilitása* című fejezetben a stratégia rögzíti, hogy Franciaország az európai digitális stratégiai autonómia motorja szándékozik lenni, aktív szerepet játszva a biztonságos, stabil és nyitott kibertér megteremtésében. E célkitűzés elérésében az ENSZ és az EBESZ támogatására számít.

e) *alapvető értékek:*

A legtöbb stratégia elismeri az olyan alapvető értékek tiszteletét, mint a véleménynyilvánítás szabadsága, a magánélet védelme vagy az információ szabad áramlásának elve – összhangban az OECD demokratikus megközelítésével. A brit stratégia tartalmazza továbbá a kormányzás nyitottságának és elszámoltathatóságának elvét és az alapvető jogállamisági garanciák megtartásának követelményét. Ezen is túllépve, az Egyesült Királyság szerint, az offline térben érvényes normák és a nemzetközi jog szabályai alkalmazandók az online térben is. Ezt a gondolatmenetet a francia stratégia is magáénak vallja, bár mindkét állam hozzáteszi, hogy a nemzetközi jogi keretek még több ponton vitatottak, s ez gátját képezi a biztonságos és az alapvető jogokat garantálni képes kibertér megteremtésének.

2. Olyan alapvető kérdések, mint a kiberbiztonság gazdasági aspektusai, a dinamikus politikaformálás szükségessége és a szuverenitás kiemelése egyes stratégiákban különös tartalommal bírnak.

a) *A kiberbiztonság gazdasági aspektusai:*

Az országok eltérő hangsúlyt helyeznek a kiberbiztonság gazdasági aspektusaira: néhány ország a gazdasági növekedési stratégiájában hivatkozik az információs biztonságra[86], van olyan ország, amely külön stratégiai dokumentumot készít a gazdasági aspektusok vizsgálatára[87], és a köztes megoldást választva több ország a kormányzati intézkedések részeként tekint a kiberbiztonság gazdasági kérdéseire. Ez utóbbi jellemzi többek között a szigetország által alkalmazott megközelítést is. Az Egyesült Királyság 2015. évi nemzeti biztonsági stratégiáján végig érezhető a gazdasági biztonságra helyezett nagy hangsúly, több ponton is kulcsterületnek

[86] Például Japánban.

[87] Például az Egyesült Államok.

nevezve azt. Ezt a megközelítést a kiberbiztonsági stratégia is átveszi[88], és a növekedés célkitűzését a kiberszektor vonatkozásában is rögzíti a fejlesztési (develop) fejezetben. A stratégia célul tűzi ki, hogy egy növekvő, innovatív kiberbiztonsági szektor jöjjön létre, amelyben az innovációt minden rendelkezésre álló eszközzel ösztönzik. Így felállítanak két innovációs központot, emellett a 165 millió font értékben létrehozandó Védelmi és Kiberinnovációs Alap segítségével ösztönzik a védelmi beszerzéseket, valamint támogatják a nemzetközi standardok elterjesztését. Mindennek köszönhetően a kiberbiztonsági szektor évről évre elért növekedése az átlagos globális növekedés mértékénél is nagyobb lesz. Igen hasonlóan fogalmaz a francia stratégia is, amely szintén kormányzati intézkedéseket vár, hogy az erős és versenyképes nemzeti és európai ipar megteremtésének célkitűzését (mint a stratégia negyedik átfogó célkitűzésének része) elérjék. Ez egyben a jövőbeli versenyképesség előfeltételét is jelenti. Mindkét stratégia végcélja egy gazdasági rendszer megteremtése, amely kedvez a K+F tevékenységnek és elősegíti a digitális biztonság megteremtését. A német stratégia a német ipar erősítésére kiemelt hangsúlyt helyez, és javasolj a „IT Security Made in Germany" termékek és szolgáltatások kiterjesztését a versenyképesség javítása és a nemzeti informatikai ipar megerősítése érdekében.

b) *A dinamikus politikaformálás szükségessége:*

A változó kihívásokhoz és biztonsági környezethez való alkalmazkodás igénye a stratégiák többségében megjelenik. A brit stratégia szerint a dinamizmus nem csak a kiberfenyegetések dinamikus természetével összefüggésben jelenik, meg, hanem az arra adott válaszok közt is úgy, mint a Kiberbiztonsági Központ hírszerzési tevékenysége során, a kutatói szektor és az új kiberbiztonsági vállalatok jellemzői közt.

c) *A szuverenitás értelmezése[89]:*

A második és harmadik generációs stratégiák talán legfeltűnőbb új vonása a szuverenitás fogalmának előtérbe kerülése és kiszélesedése. Míg korábban a stratégiák a szuverén szervekkel foglalkoztak, addig az új stratégiák már a szuverenitás gazdasági, innovációs, szervezeti és nemzetközi aspektusait is beemelik vizsgálódásuk körébe. A britek már a 2009-es stratégiában jelezték a civil és katonai képességek fejlesztésének szükségességét a kibertámadások kivédése céljából[90], ám ezen jóval továbbmegy a 2016-os stratégia, amely már támadó kiber- és kriptográfiai kapacitások kiépítéséről rendelkezik az ország szuverenitásának megvédésére. Az ország érdekeit és szuverenitását ugyanis a kibertérben is meg kell védeni. A stratégia továbbá a technológia terén is megemlíti, hogy a szuverenitáshoz szorosan kapcsolódik a brit IT-ipar, az oktatás és a K+F támogatása. A francia stratégia a digitális szuverenitás fogalmát használja azzal összefüggésben, hogy az ország az európai digitális autonómia megteremtésének élharcosává váljon és az európai rend részeként legyen képes a francia szuverenitás e szegmensének megvédésére. Ez a kijelentés egyúttal jelzi azt a tendenciát is, hogy kialakulóban van egy regionális szuverenitás: az azonos elveket valló és értékeket tisztelő államok közösen próbálják felvenni a har-

[88] Már a 2011. évi kiberstratégia is célul tűzte ki, hogy az ország vezető állammá váljon nemcsak európai, hanem világszinten is a technológia és az innováció terén, valamint hogy az országot vonzóvá tegye az érdekelt vállalkozások számára.

[89] E fogalom alatt értjük például a nemzetbiztonsági, hírszerzési, katonai-védelmi kérdéseket.

[90] Ennek megfelelően megkezdték többek között az önálló katonai kibervédelmi intézményrendszer felállítását.

cot a kibertérben jelentkező fenyegetésekkel szemben az európai biztonság és szuverenitás megőrzése érdekében. A stratégia kiemeli a diplomácia fontosságát mint egyedi jellemvonást a nemzetközi kapcsolatokban. A német stratégia a szuverenitással kapcsolatban szintén tartalmazza az önálló nemzeti ipar megteremtésének igényét a kiberbiztonságért felelős szervek említésén túl, emellett pedig a stratégia újításának tekinthető az, hogy a kiberbiztonság katonai dimenzióját külön is nevesíti, és azt elkülönülten kezeli a civil kiberbiztonsági kérdésektől.

3.4. ÖSSZEHASONLÍTÁS A MENEDZSMENTSTRUKTÚRÁK ÉS AKCIÓTERVEK MENTÉN

1. A stratégiák többsége erősebb kormányzati koordinációs mechanizmusokat és vezetést említ, bár általános recept nem létezik.

A stratégiák célkitűzései közt általában szerepel a kiberbiztonsággal foglalkozó szervezetrendszer racionalizálása és a terület koordinációjának elősegítése. A modellek azonban eltérők. A politikai koordinációs feladatokat az Egyesült Királyságban a miniszterelnök látja el, míg Németországban a Szövetségi Belügyminisztérium, Franciaországban pedig egy önálló szervezet, az ANSSI tölti be a koordinációs hub szerepét. Műveleti szinten általában van egy központi szervezet. Franciaországban ezt a szerepet is a kormányzati szervként is működő ANSSI látja el, amely közvetlenül a miniszterelnöknek jelent. Németországban a Kiberbiztonsági Reagáló Központ a felelős szervezet, míg a briteknél a Kabinetirodán belül felállított Kiberbiztonsági és Információvédelmi Iroda[91] (OCSIA) szolgál stratégiai iránymutatásokkal.

2. Az országok többségében a szuverenitás garantálásában szerepet játszó szervek meghatározó kiberbiztonsági szereppel bírnak.

E közös jellemző lényege, hogy a védelmi minisztériumok és titkosszolgálatok egyre kiterjedtebb szerepet töltenek be az államok kiberbiztonságának megteremtésében. Jól tükrözi ezt a szerepet az is, hogy a kiberköltségvetést milyen arányban allokálják ezen szervek felé. A britek esetében 2011-ben a 650 millió fontos tervezett négyéves kiber költségvetés 14%-át szánták a Védelmi Minisztériumnak és 59%-át a titkosszolgálatoknak.[92] Ez az összességében 73%-os részesedés kimagasló és jelzi, hogy az állami szuverenitás garantálásához elengedhetetlen a kiberbiztonság megteremtése és fenntartása.

[91] Office of Cyber Security & Information Assurance.

[92] The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world (2011).

3. A 2000-es évek elején a korábbi kiberstratégiákban megfogalmazott prioritások még hangsúlyosabban jelennek meg az új stratégiákban.

A következőkben ezen prioritások fejlődéstörténetét mutatom be röviden.

a) *A kormányzat biztonságának növelése és a kritikus információs infrastruktúrák védelme:*

Ezek a területek kibertámadás esetén kiemelt célpontok lehetnek, ezért magasabb fokú szervezettségre és gyorsabb válaszadási képességre van szükség. Minden állam tett lépéseket kormányzatának megvédése érdekében – ilyenek például a kriptográfia használatának elterjesztése, a kormányzati hálózatok korszerűsítése, a kormányzati rendszerek ellenálló képességének növelése, a civil alkalmazottak azonosításának megkövetelése, támadást előrejelző és megelőző kapacitások kifejlesztése, a CICO[93] tisztségek számának megtöbbszörözése, standardok és audit technikák felállítása vagy a biztonsági alkalmazottaknak karrierutak megtervezése. Az országok többségében felállították a kormányzati incidenskezelő központot, ahol pedig már létezett, ott jobban megszervezték annak működését. Sok esetben a stratégiákban is megjelenítik a kormányzati szintek közötti koordináció szükségességét és fontosságát (ahogyan Németországban is), míg máshol (ahogyan az Egyesült Királyságban) a kormányzat online szolgáltatásainak használatába vetett bizalom fontosságát hangsúlyozzák („digital by default" elv[94]).

A kritikus információs infrastruktúrák védelme általában a kiberbiztonsági stratégiák részét képezik, bár gyakran külön is szabályozzák e fő prioritást jelentő kérdéskört. A szabályozás nagyban függ adott állam fejlettségi szintjétől, és általában a köz- és magánszféra közötti együttműködés képezi az alapját. Beletartoznak olyan előkészítő intézkedések, mint a megelőző intézkedések, a válságkezelő tervek, gyakorlatok szervezése, gyorsreagáló képesség kifejlesztése, az egyes szereplők közötti információmegosztás és hatékony koordináció, a jogi keretek kidolgozása és a nemzetközi szövetségek felállítása. E tárgykörben az Egyesült Királyság nem rendelkezik külön jogszabállyal, ami annak köszönhető, hogy a kritikus infrastruktúra-kapacitások jelentős részben magánkézben vannak. A kiberstratégia néhány nem kritikus infrastruktúrát ugyan nevesít (mint például a média, az adatkezelők), de az őket érő esetleg támadás is a nemzet egészére nézve negatív hatással járhat, ezért szükséges a kormányzati szervek segítségnyújtó és tanácsadó tevékenysége az incidensek bekövetkezése esetén. Németországban külön törvény rendelkezik ezekről a kérdésekről és az ország célja, hogy a köz- és magánszféra együttműködésén alapuló rendszert továbbfejlesszék. A francia stratégia lényegében egy teljes fejezetet szentel ennek a kérdéskörnek: az első célok közt ugyanis az alapvető érdekek mellett a kritikus információs infrastruktúrák biztonságát és megvédését nevesíti a dokumentum.

b) *A kiberbűnözés elleni harc fejlesztése:*

Az államok többsége a bűnmegelőzési kapacitások fejlesztésére törekszik. Az Egyesült Királyságban felállították a Csalás elleni akciócsoportot (Action Fraud), amely a Kibervédelmi Központtal is kapcsolatot tart, és folyamatosan érkezhetnek hozzá bejelentések a kibertérben elkövetett bűncselekményekről. Az országban már

[93] Chief Information Security Officer – Információbiztonsági vezető.

[94] A cél, hogy a kormányzati szolgáltatások online elérhetők és intézhetők legyenek, s a papíralapú ügyintézéssel szemben az online ügyintézés váljék a főszabállyá.

regionális szinten is kialakulóban van a kiberbűnözés elleni szervezetrendszer, amelyet regionális egységek felállításával[95] építenek ki. Emellett a stratégiákban akad példa a jogi szabályozás fejlesztésére (például Franciaországban és az Egyesült Királyságban), a nemzetközi együttműködés megerősítésére (a francia és német szabályozás esetében), és valamennyi megvizsgált ország támogatja a kiberbűnözés elleni *Budapesti egyezmény*t.[96] A korábbi francia stratégia kifejezetten szólt az egyezményről, mellyel kapcsolatban megfogalmazta a normák egységesítésének és az uniós tagállamok közötti egyszerűsített jogi együttműködés igényét.

c) *A tudatosság növelése és az oktatás fejlesztése:*

A *tudatosság növelését* célzó kezdeményezések célközönségét a társadalom egésze alkotja, olyan kiemelt célcsoportokkal, mint a gyermekek (az Egyesült Királyságban is), az üzleti élet, a kormányzati szervek vagy a kritikus infrastruktúrákat üzemeltetők. A lakosság oktatása terén tett lépések között található az általános kibertudatosság oktatása minden oktatási szinten vagy a közösségi média használata (a brit stratégiában rögzítettek szerint). A britek a piacok szegmentálására tanúsított biztonsági címkékkel látnak el termékeket és szolgáltatásokat.

Egyre növekvő problémát jelent a szakképzett *kibermunkaerő hiánya*, amely a kormányzatok előtt álló legnagyobb kihívássá kezdi kinőni magát. A britek felismerték a probléma jelentőségét, de megoldását reálisan csak mintegy húsz év távlatában látják. Ennek elősegítése érdekében a kiberképzést iskolai programok segítségével, minőségi közép- és felsőoktatással, tanárképzéssel és Védelmi Kiberakadémiák[97] mint kiválósági központok felállításával képzelik el. További lépések szükségesek a kibertudományok és a technológia területén is, amelyet megkönnyíthet az akadémiai és az üzleti szféra közötti szorosabb együttműködés. Ennek sarokpontjait a 2017. november 30-án kiadott *Kiberbiztonsági tudományos és technológiai stratégia* is rögzíti.[98] A fenti célkitűzések megvalósításában oroszlánrészt vállal a Nemzeti Kiberbiztonsági Központ. A központ *CyberFirst* programjának célja a terület megkedveltetése a fiatalok körében.[99] A programok közt található nyári kiberkurzus[100] a középiskolás korosztály részére, de évközben is rendszeresen szerveznek alapszintű tanfolyamokat.[101] A lányok toborzásával külön is foglalkoznak, számukra külön kiberversenyt is rendeznek.[102] Az egyetemi szinten pedig

95 Regional organised crime units.

96 Budapest Convention on Cybercrime (2001).

97 Defence Cyber Academy.

98 Interim Cyber Security Science&Technology Strategy: Future-Proofing Cyber Security (2017).

99 A nagyobb vonzerőt egyébiránt anyagi ösztönzőkkel is igyekeznek elősegíteni. A programban részt vevő egyetemi hallgatóknak évente 4000 font adómentes ösztöndíjat adnak, nyári diákmunka esetén heti 250 fontot fizetnek, a diploma megszerzését követően pedig garantálják, hogy három évig a kormányzati szférában e területen foglalkoztatják őket. CyberFirst.

100 2017 nyarán például 1060, 14 és 17 év közötti diák vett részt a nyári kurzusokon.

101 Ilyen kurzusok a CyberFirst Defenders kurzus (egynapos ingyenes oktatás a 14-15 éves korosztály számára), a CyberFirst Futures (öt napos emelt szintű tanfolyam a 15-16 éveseknek) és a CyberFirst Advanced kurzus (legmagasabb szintű kurzus, ötnapos, szintén ingyenes a 15-16 éves korosztály számára).

102 2017-ben a 13 és 15 éves lányok közül 8000-en vettek részt az első, lányok számára kiírt kiberbiztonsági versenyen.

az elmúlt években 28 partnerszervezet 2,8 millió font értékben fektetett be a kiberképzés támogatásába, s jelenleg már 14 Kiberbiztonság Kiválósági Központ működik egyetemi keretek között, ahol a legmagasabb elméleti szinten járulnak hozzá e terület fejlődéséhez. A szakemberek képzésének igényét mind a német, mind a francia stratégia rögzíti. Németországban felsőfokú kiberképzés indult a müncheni egyetemen és 50 millió eurós beruházással felállítják a Német Internet Intézetet is, amely a kibertér jogi, gazdasági és etikai kérdéseit vizsgálja.[103] A francia stratégiában is szerepel a szakemberképzés iránti igény, kiemelve a gyerekek kiberoktatásának szükségességét.

d) *K+F:*

A kutatás-fejlesztés terület jelentősen felértékelődött az első kiberstratégiák kiadása óta, és igen szorosan összekapcsolódik a köz- és magánszféra együttműködése kérdéskörével. Ez a szinergia elősegíti a kutatás terén tett erőfeszítések hatékonyabb összehangolását. Az Egyesült Királyságban 165 millió font áll rendelkezésre a kis- és középvállalkozások számára, hogy új, innovatív termékeket fejlesszenek és azokat terjesszék. A támogatást elsősorban olyan termékekre fordíthatják, amelyek már beépített védelemmel vannak ellátva (secure by default). Utalok a már említett *Kiberbiztonsági tudományos és technológiai stratégiá*ra, amely nevesíti napjaink tendenciáit, kihívásait és megfogalmazza a tervezett válaszlépéseket is. Németországban a 2011-es stratégiában megfogalmazott, a K+F szektor megerősítésére vonatkozó célkitűzés megvalósításaként Berlinben két big data központot is felállítottak[104], majd 2015-ben egy ötéves kormányzati program indult (*High-tech stratégia* néven) az adattitkosítási technológiák innovatív megújítása és a személyes adatok védelme érdekében.[105] A francia kiberstratégia szintén tartalmazza a K+F terület fejlesztésének célkitűzését a nemzeti és európai kiberönállóság megteremtésével összefüggésben: cél a digitális bizalmon és biztonságon alapuló európai térség kialakítása, amely részeként Németországgal már megindult az együttműködés a felhőszolgáltatások terén. Az ilyen és ehhez hasonló technológiák használatát azonban Franciaország szerint minden esetben alapos hatásvizsgálatnak kell megelőznie.

4. A stratégiákban megjelenő új elemek.

Az újabb generációs stratégiákban számos új elem jelenik meg. Ilyenek például a gyermekek online védelme, a kiberbiztonsági gyakorlatok szervezésének igénye, az ellátási láncok biztonságával kapcsolatos megfontolások vagy az internetszolgáltatókkal való partneri kapcsolatok kialakítása. Kiemelem a digitális azonosítási keretrendszere létrehozásának igényét, amely mindhárom vizsgált állam vonatkozásában megjelenik. (Megjegyzem, hogy a több szempontból is kuriózumnak számító Észtország esetében ez már bő tíz éve megvalósult.) Németország hangsúlyozza az alapvető biztonsági funkciók állami bevezetésének fontosságát (mint például az e-személyazonosítás és a hitelesített e-mailek), Franciaország pedig már felvázolta az elektronikus azonosítórendszer

[103] German Internet Institute: Berlin-Brandenburg consortium wins bid (2017).

[104] Berlin Big Data Center.

[105] Self-determined and secure in the digital world 2015–2020. The German government's research framework programme on IT security (2015).

létrehozásának tervezett menetét is. Végezetül kiemelem a katonai kibervédelmi kapacitások fejlesztését mint új elemet, amelyet szintén tartalmaz mindhárom vizsgált stratégia. Legmesszebb a brit stratégia megy, amely megkezdte támadó kiberkapacitások kiépítését is az aktív kibervédelem eszközeként. A kibertámadások végrehajtása a brit fegyveres erő feladata, mert a kibertérben végrehajtott támadást a stratégia ugyanolyan támadásnak ítéli, mint a fizikai térben elkövetett támadást. A német stratégia csak a kibervédelem kérdéskörével foglalkozik történelmi okok és alkotmányossági korlátok miatt, s a hadsereg még kevésbé kész kibertámadások végrehajtására.

5. Erősebb nemzetközi együttműködési formák megteremtését valamennyi ország támogatja.
A nemzetközi együttműködés kezdetben a leghatékonyabb technikák és iránymutatások államok egymás közti megosztását jelentette, mára azonban sokkal szorosabb és erőteljesebb az államok interakciója. Az európai államok a regionális együttműködést külön is kihangsúlyozzák és erőltetik. Az együttműködés jelenlegi formái közt találjuk szövetségek felállítását (például az Egyesült Királyság és Franciaország esetében), nemzetközileg is elfogadott magatartási szabályok megalkotását, multilaterális tárgyalásokon való részvételt vagy nemzetközi kibergyakorlatok szervezését és az azon való részvételt. A nemzeti stratégiák nemzetközi dimenziója gyakran olyan problémákat is felvet, amelyek túlmennek a kibertér gazdasági és szociális hatókörén és a politikai (s néha katonai) biztonság érdekkörébe esnek (mint a fegyveres konfliktusok megelőzésének kérdése vagy a bizalomerősítő intézkedések köre).

3.5. ÖSSZEHASONLÍTÁS A SZERVEZETI KÉRDÉSEK MENTÉN

Mindaz, amit a nemzeti kiberbiztonsági stratégiák rögzítenek, csak egy jól strukturált szervezetrendszer keretei között valósítható meg, ezért a nemzeti kiberbiztonsági helyzet összehasonlítását a szervezetrendszerek közötti hasonlóságok és különbségek feltárásával zárom.

A nemzeti szervezetrendszerek több különálló, ám egymáshoz sok szállal kapcsolódó szervezeti elemből tevődnek össze. Ezen elemek között minden esetben megtalálható a politikai koordinációért és stratégiai irányvonalakért felelős kormányzati elem, a katonai kibervédelem elkülönült intézményei és a kritikus infrastruktúra védelméért felelős szervek köre, de országspecifikusan ezek további szervezetekkel egészülhetnek ki.

3.5.1. A politikai koordinációért felelős szervek

Az Egyesült Királyságban központi kiberbiztonsági szervként funkcionál a *Kabinetiroda* (Cabinet Office), amely teljes hatáskörrel bír a kormányzati koordináció és stratégiai irányvonalak kijelölése terén. A Kabinetiroda alegységeként működő Nemzetbiztonsági Titkárság[106] a nemzetbiztonságot érintő valamennyi kérdésben segítséget nyújt a Nemzetbiztonsági Tanácsnak és a miniszterelnöknek. A Titkárságon belül a Kiberbiztonsági és Információvédelmi

[106] National Security Secretariat – NSS.

Iroda[107] foglalkozik a kiberkérdésekkel, közvetlen iránymutatásokat nyújtva a Kabinetirodát vezető miniszternek és a Nemzetbiztonsági Tanácsnak.[108]

Németországban a Szövetségi Belügyminisztérium játszik központi politikaformáló szerepet, több tárcával együttműködésben. Már az első, 2011-es kiberstratégiát követően felállították a *Nemzeti Incidenskezelő K*özpontot (NCAZ)[109], melynek feladata a kormányzati szervek közötti kooperáció és IT-incidensek esetén a válaszlépések összehangolása lett. A központ feladatainak végrehajtásáért a Belügyminisztérium irányítása alá tartozó *Szövetségi Információbiztonsági Hivatal* (Bundesamt für Sicherheit in der Informationtechnik, a továbbiakban: BSI)[110]. A Hivatal felel a kiberbiztonsági stratégia végrehajtásáért és egyúttal nemzeti kiberbiztonsági hatóságként is funkcionál. Emellett incidens esetén a Szövetségi Belügyminisztériumot közvetlenül tájékoztatja és a kiberincidenseket is hozzá kell bejelenteni. A politikai koordinációért felelős szervek között még meg kell említeni a 2011-ben megalakult *Nemzeti Kiberbiztonsági Tanácsot*, amelynek feladata a tárcák, valamint a köz- és magánszféra közötti együttműködés erősítése és a legfelsőbb szintű vezetők számára javaslatok megfogalmazása stratégiai kérdésekben. A Tanács mellett működik egy 2012-ben alapított nonprofit szervezet, a *Kiberbiztonsági Szövetség* (Alliance for Cyber Security)[111], amely a legkiterjedtebb nemzeti együttműködési platform 100 partnervállalat mintegy 2000 résztvevőjével.

Franciaországban a kiberpolitika irányítója a miniszterelnök, akit munkájában az információs rendszerek biztonság**áért felelős stratégia**i bizottság[112] támogat. A szakterület szakmai felelőse a védelmi és nemzetbiztonsági főtitkár (SGDSN)[113], aki felel a vonatkozó szabályozás végrehajtásáért és jelentéstételi kötelezettséggel tartozik a miniszterelnök felé. 2009-ben hozták létre e feladatok támogatására az Információs Rendszerek Biztonságának Nemzeti **Ügynöksége**t (ANSSI)[114], amely hatóság a miniszterelnök és a főtitkár közvetlen felügyelete és szakmai irányítása alatt működik. Jelenleg elsősorban a minisztériumok közötti koordinációs feladatokat látja el.

3.5.2. A katonai kibervédelem szervei

Az Egyesült Királyság 2015 óta kezeli kiemelten a kibervédelem kérdéskörét. Központi intézményei a Védelmi Minisztérium, amely a kibertér katonai célú használatáért felelős, valamint a Fegyveres erők. A vezérkari főnök a holisztikus szemlélet jegyében az Egyesített parancsnokság alá rendelte valamennyi kiberegységet, jelezve, hogy a

[107] Office of Cyber Security and Information Assurance – OCSIA.

[108] Az iroda szoros munkakapcsolatban van a Védelmi Minisztériummal, a Kormányzati Kommunikációs Központtal (Government Communications Headquarters – GCHQ), a Nemzeti Infrastruktúra-védelmi Központtal (Centre for the Protection of National Infrastructure – CPNI) és a Külügyi és Nemzetközösségi Irodával (Foreign and Commonwealth Office).

[109] National Cyber Response Center.

[110] A BSI-t eredetileg 1991-ben hozták létre IT-biztonsági szolgáltatások nyújtására a köz- és a magánszféra számára.

[111] Alliance for Cyber Security.

[112] Comité Stratégique de la Sécurité des Systemes d'Information.

[113] Secretariat général de la défense et de la sécurité nationale.

[114] ANSSI – Agence Nationale de la Sécurité des Systèmes d'Information.

kiberbiztonság olyan, az ország egész védelmét átfogó terület, amely valamennyi szektort érinti.[115] 90 millió fontot allokáltak a Védelmi Kiberbiztonsági Programra, melynek keretében felállították a Védelmi kiberműveleti csoportot, mely 2013-ban már Egyesített kibercsoportként (JFCyG)[116] kezdte meg működését. Ennek keretében az egyik Egyesített kiberalegység éjjel-nappal a Védelmi Minisztérium hálózatait védi a kibertámadásoktól, a másik egység pedig új taktikákat, technikákat és terveket dolgoz ki, hogy az ország hatékony katonai válaszlépések megtételére legyen képes a kibertérben is.[117]

A katonai intézményrendszer keretét a Globális Műveletek és Biztonsági Ellenőrző Központ (GOSCC)[118] adja, amely a két központi szerv hálózatai biztonságáért felelős legfőbb intézmény. Napi 24 órában mintegy 200 000, a védelmi szférához tartozó elektromos eszközt monitoroz, de feladati közé tartozik a jövőbeni kibertámadásokra való felkészülés is.[119]

2013 szeptemberében újabb nagy előrelépés történt a katonai kibervédelem területén az Egyesített kibertartalékos egység[120] felállításával.[121] A cél, hogy olyan, speciális szaktudással rendelkezők[122] álljanak készen szolgálatra, akik kibertámadás esetén rövid időn belül „bevethetők".

Németországban a 2016-os kibervédelmi stratégia emelte legmagasabb szintre a kibervédelem kérdéskörét, amely vonatkozásában a Szövetségi Védelmi és Honvédelmi Minisztérium az illetékes tárca. A stratégiában foglaltakkal összhangban már 2016-ban felállították a *kiber- és információs parancsnokságot* (KCIR)[123], amely a katonai hírszerzési, geoinformációs, műveleti és kiberkommunikációért felelős. A parancsnokság a Bundeswehr kibertevékenységet végző egységeit olvasztotta magába. A Bundeswehr önállóságát megőrző egysége, a Stratégiai Hírszerző Egység[124] már támadó kapacitással is rendelkezik, de elsődlegesen a védelmi területen tevékenykedik.[125] A kibervédelem felértékelődését jelzi, hogy 2017 áprilisában felállították a bonni székhelyű német kibervédelmi parancsnokságot, amely a hadsereg valamennyi kiberegységének biztonságáért lesz felelős 2021-re, mire teljesen kiépül – beleértve a földi, légi, tengeri, orvosi alakulatokat és az egyesített erőket is.[126].

115 Defence and Cyber Security: Goverment response to the Committee's Sixth Report of Session 2012–13 (2013).

116 Joint Forces Cyber Group.

117 Defence Cyber Operations Group (2016).

118 Global Operations and Security Control Centre.

119 Global Operations and Security Control Centre (2013).

120 Joint Cyber Reserve.

121 New cyber reserve unit created (2013).

122 Három személyi körből verbuválják a tartalékosokat: a fegyveres erőknél korábban szolgálatot teljesítők közül, informatikai szaktudással rendelkező volt vagy még aktív tartalékosok közül és olyan speciális szaktudással rendelkező szakemberek köréből, akik korábban nem teljesítettek katonai szolgálatot.

123 Cyber and Information Space Command.

124 Strategic Reconnaisance Unit, Department of Information and Computer Network Operations.

125 Germany Reveals Offensive Cyberwarfare Capability. Atlantic Council (2012).

126 Kiberegységet állít fel a német hadsereg (2017).

Franciaország élesen elhatárolja egymástól a kiberbiztonságot és a kibervédelmet.[127] Míg az előbbi a kritikus infrastruktúra intézményeinek és a gazdaság biztonságának garantálását jelenti, addig az utóbbi a katonai és hírszerzési területeket öleli fel. Ezen elhatárolásnak megfelelően a 2013-as *Fehér könyv* a kiberbiztonság vonatkozásában az EU-val való kapcsolatokat hangsúlyozza, míg a kibervédelem területén a NATO-val való együttműködést nevesíti.

A katonai kibervédelmi feladatok ellátásért a Védelmi Minisztérium felel, ahol e tevékenység koordinálására 2011-ben létrehozták a Kibervédelmi Felelős tisztséget.[128] A Kibervédelmi Doktrína alapján a kibervédelmi tervezés a vezérkari főnök feladata.[129] A kibervédelem **műveleti irányítójaként a** kibervédelmi csoport vezetője tevékenykedik, a Tervezési és Műveleti Központ[130] pedig a műveleti tervezésbe illeszti a kiberműveleteket.

3.5.3. A kritikus infrastruktúra védelméért felelős szervek

Az Egyesült Királyságban a kritikus infrastruktúrák jelentős része magánkézben van, ezért az állam nem tud hatékony irányító szerepet közvetlen módon betölteni. Ennek köszönhető, hogy kritikus infrastruktúrákra vonatkozó általános jogszabály sem létezik, hanem egyes szektorokat külön-külön szabályoznak. A legfőbb szervként működő Nemzeti Infrastruktúra Védelmi Központot (CPNI) 2007-ben állították fel, majd 2016-ban a NCSC-be integrálták. A CPNI feladata elsősorban a biztonsággal kapcsolatos tanácsok nyújtása – legyen az humán biztonság vagy kiberbiztonság –, de részt vesz a politikaformálásban is.

Németországban több, a kritikus infrastruktúra intézményei üzemeltetését felügyelő hivatal is működik. Ezek az incidenskezelő központ keretei közt tudnak egymással együttműködni.

Franciaországban a „Plan Vigipirate"[131] eredetileg a terrorvédelemmel kapcsolatos dokumentum volt, majd továbbfejlesztették a fenyegetések értékelésére kiadott kormányközi dokumentummá. Bár a terület a Védelmi és Nemzetbiztonsági Főtanácsadó irányítása alá tartozik, a döntési jogkörök súlyos fenyegetés esetén a miniszterelnök kezében vannak. A terv titkos záradéka, a Piranet-terv[132], a környezeti és technológiai kihívások esetén életbe léptetendő intézkedéseket tartalmazza. 2006-ban rendeletben jelölték ki azt a 12 szektort, amely a gazdaság és a társadalom védelme okán kritikus infrastruktúrának minősül.[133] Ezen belül pedig a kritikus információs infrastruktúrák üzemeltetői számára külön is rögzítik a kötelezettségeket egyrészt a felülvizsgált védelmi törvénykönyvben, másrészt a katonai tervezési törvényben. Számukra az ANSSI nyújt iránymutatást és a kritikus infrastruktúrát ért támadás esetén az illetékes minisztérium felé jelentéstételi kötelezettséggel tartoznak.

---

127 VITEL–BLIDDAL (2016).

128 Officier Général Cyberdéfense.

129 BRANGETTO (2015).

130 Centre de planification et de conduite des opérations.

131 Le plan Vigipirate és Vigipirate: Objectifs de cybersécurité (2014).

132 Le plan Piranet.

133 Miniszterelnöki rendelet: Arrêté fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs (2006).

3.5.4. Országspecifikus jellemzők

Az Egyesült Királyságban hagyományosan kiemelt szerepet töltenek be a titkosszolgálatok, s ez a kiberbiztonság terén is érzékelhető. A Kabinetirodán belül működő Nemzetbiztonsági Titkárság összkormányzati stratégiai titkosszolgálati kérdések koordinálásért felelős központi szervként működik. Részét képezi az Egyesített Titkosszolgálati Szervezet[134], amely független értékeléseket készít nemzetbiztonsági vagy külpolitikai szempontból fontos kérdéseket illetően. Központi szervként mégis a Kormányzati Kommunikációs Központ, a GCHQ szolgál. Szoros munkakapcsolatban van olyan titkosszolgálati intézményekkel, mint az MI5 vagy az MI6, s szinte minden feladata közvetlenül kapcsolódik kiberbiztonsági kérdésekhez. A GCHQ legjelentősebb alárendelt szervezete a *Nemzeti Kiberbiztonsági* Központ[135] (National Cyber Security Centre, a továbbiakban: NCSC).[136] A Központot 2016. október 1-jén állították fel azzal a céllal, hogy az új kiberbiztonsági stratégiában lefektetett célokat megvalósítsa. A London központjában átadott új főhadiszállást hivatalosan 2017. február 14-én maga az angol uralkodó, II. Erzsébet királynő avatta fel, ezzel is szimbolizálva a kiberterület megnövekedett jelentőségét.[137] A Központ 2018 októberében publikálta az elmúlt egy évben elért eredményeket, amelyek igen impozánsak.[138] Működésének első két évében 1100 kibertámadást hárított el sikeresen, ami átlagosan heti 10 támadást jelent.[139] Végezetül említést kell tenni a Kiberbiztonsági Műveletek Központjáról[140] (CSOC), amely jelenleg a védelmi hálózatok és rendszerek biztonságáért felel (tehát átszervezésének köszönhetően immáron a katonai kibervédelem intézményei közé tartozik).[141]

Németországban a BSI működteti a *Nemzeti Információtechnológiai Szituációs Központot*[142], amely a nemzeti és globális IT-biztonság fejleményeit kíséri figyelemmel az IT-biztonsági incidensek gyors felderítése és elemzése érdekében. Súlyos IT-incidensek esetén Nemzeti Információtechnológiai Krízisreagáló Központtá alakul át, s így teszi meg a hatékony válaszlépéseket. Németországban emellett számos *CERT*[143] működik. Az 1994-ben a BSI által felállította első CERT (BSI-CERT) 2001-ben átalakult kormányzati CERT-té, és az elnevezése CERT-BUND-ra változott[144], manapság pedig már nemzeti CERT-ként üzemel, együttműködve mind az állami, mind a nem állami CERT-ekkel. A BSI emellett 2006-ban felállította az állampolgárok CERT-jét is, a Bürger-CERT-et.[145]

---

134 Joint Intelligence Organization.

135 A Központ tevékenységének bemutatásáról lásd MOLNÁR (2018).

136 A Központ magába olvasztotta a technikai megoldásokért felelős, korábban a GCHQ-nak alárendelten működő szervezetet, az Információbiztonsági Nemzeti Technikai Hatóságot (CESG), a 2014 óta működő brit hálózatbiztonsági reagáló csoportot (CERT-UK), a Kiberértékelési Központot (CCA) és a CPNI-t.

137 Her Majesty the Queen opening the new National Cyber Security Centre (2017).

138 Annual Review (2018).

139 NCSC deals with 1,100 cyber attacks in first two years (2018).

140 Cyber Security Operations Centre.

141 2016. április 1-jén született döntés arról, hogy 40 millió fonttal támogatják az új központ felállítását. Lásd: Defence Secretary Announces Ł40m Cyber Security Operations Centr (2016).

142 Nationales IT-Lagezentrum.

143 Computer emergency response team – feladatuk a hálózatbiztonsági incidenskezelés és az információ terjesztése.

144 CERT-Bund.

145 Bürger CERT.

Franciaországban 2012-ben hozták létre az állampolgári kibertartalékos rendszert[146], amely felállításának gondolatát először a Szenátus előtt a védelmi miniszter vetette fel 2012. július 18-án.[147] Működési elve némiképp eltér a brit rendszertől, ugyanis kizárólag civil szakemberekből áll, és a tartalékosokkal a kormányzat elsődleges célja az állampolgári tudatosságnövelés; ténylegesen műveletek végrehajtásában ők nem vesznek részt.

3.6. ÖSSZEGZŐ ÉSZREVÉTELEK

A kibertér szereplői között az állami intézményrendszeren kívül megtaláljuk a nem kormányzati szerveket, az üzleti élet szereplőit, a civil társadalmat és annak intézményeit, valamint az internet technikai értelemben vett közönségét. Mindannyian egyetértenek abban, hogy a lehető legszélesebb körű részvétellel zajló együttműködés kulcskérdés a hatékonyan működő kiberbiztonsági politika kialakításához. Szükséges továbbá az is, hogy a politika – amely kellőképpen erős legyen és a tények értékelésén alapuljon – rugalmasan tudjon reagálni az internet dinamikus működési jellemzőire.

Számos kérdés még megoldásra vár. A nemzetállamok félőn figyelik azt a tendenciát, ahogyan a kritikus infrastruktúra intézményei magánkezekbe vándorolnak, s ezáltal nő a szakadék a nemzeti biztonság és a gazdasági biztonság között. *Ez már szuverenitással összefüggő kérdéseket is felvet, ugyanis a kormányok úgy fogják alakítani kiberbiztonsági politikájukat, hogy az hatással legyen a gazdasági biztonságra és a gazdasági élet szereplőire is. Azzal párhuzamosan pedig, ahogyan a szuverenitás kérdései beszivárognak a kiberpolitikába, úgy szűkül le vagy esetleg tűnik el a civil társadalom részvételi lehető*sége a politika*formálás folyamataiban. Szerepüket a rendőrségi, titkosszolgálati, védelmi ipari érdekeket képviselő szervezetek veszik át, s ezáltal a kiberbiztonsági* kérdések erősen nemzetbiztonsági töltetet kapnak. Ezek a folyamatok ahhoz vezetnek, hogy a kiberbiztonsági kérdéseket sokkal inkább „hard" eszközökkel szeretnék megoldani, semmint az egyeztetéseket előtérbe helyező „soft" megközelítést alkalmaznák. Ezáltal a szuverenitás és a gazdasági-szociális megfontolások közötti szakadék még tovább szélesedik.

A technikusok alkotta internetközösség a kereskedelemmel és innovációkkal összefüggő nemzetközi kiberbiztonsági kérdésekkel kapcsolatban fogalmazza meg fenntartásait. A kereskedelem előtt tornyosuló egyre több technikai akadály, amelyeket az infokommunikációs technika eszközei rejtenek magukban, valamint a végfelhasználók eszközei, azzal járhat, hogy az internet különböző piacokra szegmentálódik, amelyekre eltérő szabályrendszerek fognak vonatkozni. Az üzleti élet szereplői számára létkérdés, hogy kialakuljon a kiberpolitikák egy nemzetközileg elfogadott egységes szintje globális, költséghatékony megoldások alkalmazása mentén – hozzátéve azt, hogy nyilvánvalóan nem várható el az, hogy a nemzeti kiberpolitikák közti különbségek megszűnjenek. A nemzetközi standardok további fejlesztése ösztönözheti ezen folyamatokat.

A technikusok alkotta internetközösség kiemeli saját független tanácsadó szerepét, de egyúttal elismeri azt is, hogy a kiberbiztonsági erőfeszítésekben vezető és koordináló szerepet a kormányzatoknak kell betölteniük.

[146] A kibertartalékosok (La réserve de cyberdéfense) a hagyományos tartalékos erők (La réserve citoyenne) mellett működnek. Lásd La réserve citoyenne és La réserve de cyberdéfense.

[147] Az erről szóló 7. sz. miniszteri ajánlást lásd: Rapport d'Information du Sénat No. 681. (2012).

Ezt megfelelő jogi reformok, valamint a köz- és magánszféra együttműködésével tudják megvalósítani, s ezáltal elhárulnak az akadályok az információmegosztás és a kialakult gyakorlatok ipari szereplők általi önkéntes alkalmazása előtt.

Az OECD által megfogalmazott javaslatok[148] tükrözik a kibertér szereplőinek észrevételeit. Mindenekelőtt a kiberpolitikákat, intézkedéseket, eljárásokat és a gyakorlatot kell úgy kialakítani vagy a már meglévőt átalakítani, hogy az összhangban legyen a fent ismertetett alapvető követelményekkel. Szükség van minél szélesebb körű hazai és nemzetközi konzultációkra és együttműködésre, csakúgy, mint az irányelvek lehető legszélesebb körű terjesztésére – beleértve valamennyi szektort és szereplőt, valamint a nem OECD tagállamokat is. Tekintettel a kiberfenyegetések igen gyorsan változó természetére, ötévente szükséges felülvizsgálni az irányelveket.

[148] OECD (2002).

4. KIBERDIPLOMÁCIA: A JÖVŐ ZENÉJE?

Az elmúlt években a kiberbiztonság fogalmával óhatatlanul összefonódott a kiberhadviselés fogalma.[149] Ez annak köszönhető, hogy egyre több az olyan, a kibertérben megvalósított támadás, amelyek hatása már a háborúk okozta szörnyűségekkel ér fel, s mindez gátját képezi az államok kiberbiztonságuk megteremtése érdekében tett erőfeszítéseinek.

A kibertér mára a negyedik hadszíntérré vált[150], ezen a hadszíntéren – szemben a hagyományosnak mondható másik három hadszíntérrel – azonban nincsenek általánosan elfogadott szabályok, amelyeket a nemzetközi közösség érvényre tudna juttatni. Míg a hagyományos fegyveres konfliktusokra vonatkozóan jól kialakult szabályrendszer van érvényben a hágai és genfi egyezmények alapján, a kiberháborúban még farkastörvények uralkodnak. Bár vannak kísérletek arra vonatkozóan, hogy a nemzetközi jog kialakult normáit átültessék a kiberterületre is, érdemi előrelépésről még nem beszélhetünk. A *Tallinni jegyzőkönyv* erre tesz kísérletet, azonban az ott lefektetett szabályok még nem bírnak kötelező érvénnyel, sokkal inkább mint követendőnek tartott magatartásminták vannak jelen az állami gyakorlatban.

A kibertérben zajló háborúval kapcsolatban sok alapvető kérdés még nem tisztázott, de a legproblematikusabb annak eldöntése, hogy ki támadott először. Úgy gondolom, hogy erre a kérdésre még jó ideig nem fogunk választ kapni, addig viszont aligha lehetséges egy, a nemzetközi közösség által teljes mértékben elfogadott kötelező érvényű szabályrendszer megalkotása.

A megoldás talán egy egészen más irány választása lehetne. A nagy klasszikust, Carl von Clausewitzet idézve a háború nem más, mint a politika folytatása más eszközökkel. Ez bár a kiberháború esetében is helytálló megfogalmazás lehet, sokkal inkább a „más eszközök" mibenlétében kellene a megoldást keresni. Ez a más eszköz mint megoldás lehet a kiberdiplomácia.

A diplomácia elsődleges eszköze a tárgyalás. A tárgyalás nem csak megoldási eszköz, hanem egyúttal a háború ellentéte is. Talán kijelenthető, hogy senkinek – legyen az magánszemély, üzleti vállalkozás vagy nemzetállam – sem érdeke az, hogy a kibertérben állandó jelleggel háborús viszonyok uralkodjanak, ezért az egyetlen megoldás csak az lehet, hogy a konfliktusban érintettek egy tárgyalóasztalhoz leülve rendezik a problémás kérdéseiket. A tárgyalások során azonban a diplomácia alapvető szabályait be kell tartani és bizonyos alapelveket követni kell – ez nem lehet másképp a kiberdiplomáciai tárgyalások során sem. A felek kölcsönös tisztelete mellett elsődleges

---

[149] A kiberbiztonság területén a kiberhadviselés fontosságához lehet hasonlítani a kiberbűnözést – mind volumenét, mind hatását tekintve, amellyel kapcsolatban hatalmas problémát jelent egyrészt az alanyi kör nem állami mivolta, másrészt pedig az egységes szankciórendszer hiánya.

[150] A NATO-terminológia szerint a kibertér a negyedik hadszíntér, ezzel szemben az Egyesült Államok már mint ötödik hadszínteret tartja nyilván a kiberteret.

vezérlő elv a jogegyenlőség elve. A kibertárgyalások résztvevőit azonos jogok illetik meg és azonos kötelezettségek terhelik, függetlenül alanyi mivoltuktól. Önmagában pedig már az is két alapelv igenlését jelenti, hogy a felek tárgyalóasztalhoz ülnek: az egyik az erőszak alkalmazásától vagy az azzal való fenyegetéstől való tartózkodás, a másik pedig a készség arra vonatkozóan, hogy a felmerült vitás kérdéseket békés úton rendezzék. A tárgyalás tehát az erőszakról való lemondás és a békés út választásának elismerését jelenti. Végül, de nem utolsósorban, a nemzetközi jog egyik vezérlő alapelve, a pacta sunt servanda elv, alapján a kiberdiplomáciai tárgyalások során kialkudott eredmények és kompromisszumok hosszú távú érvényesülése mindenképp várható.

A kiberdiplomácia újkeletű fogalom, de nem keverendő össze az e-diplomácia és a digitális diplomácia kifejezésekkel. Az e-diplomácia fogalmát 2007 óta használjuk, amikor a svéd diplomácia felállította az első „virtuális nagykövetségeket". A kezdeti lelkesedés, amikor az információs technológia új eszközeit még arra használták, hogy kapcsolatot alakítsanak ki a világ lakosságával, 2014-től kezdve (az ukrán eseményeknek köszönhetően) kezdett gyökeresen átalakulni és a cél már nem a kapcsolatépítés, hanem az információs befolyásolás lett. Az információ fegyverré vált, amely birtoklásáért küzdelem – ha úgy tetszik, háború – folyik a diplomácia világában is. A külügyi szervek szerte a világban digitális kapacitásaik növelésébe kezdtek, hogy a más államok irányából észlelhető dezinformációs tevékenységeket észlelni, felderíteni és megakadályozni tudják. Az Egyesült Királyságban például két digitális szervezeti egységet is felállítottak a Külügyminisztériumon belül: az egyik információkat gyűjt az ellenséges *bot*ok (emberi viselkedést szimuláló automatizált szoftverek) működését illetően, a másik a nyílt forrásokat elemzi (elsősorban a közösségi médiában található információk alapul vételével). Ezáltal a britek egy olyan erős digitális hálót építenek ki, amely segítségével – már a Brexit utáni érára készülve – továbbra is erős szálak kötnék a szigetországot Európához.[151]

Az e-diplomácia fogalmához képest a digitális diplomácia fogalma szűkebb, alatta elsősorban a közösségi média eszközeit, a Facebookot és a Twittert értik, nem is alaptalanul. A brit külügyminiszter már 2011-ben élőben válaszolt a twitterfiókján keresztül, de Izrael az az állam, amely a „Facebook-diplomáciáját" még magasabb szintre fejlesztette. 2011-ben kezdtek nagyszabású digitális fejlesztésbe, amikor elindították az „Izrael arabul szól" elnevezésű oldalt. Az oldal hirtelen nagyon közkedvelt lett az arab lakosság körében – beleértve a nem éppen Izrael-párti irániakat is –, s mára másfél millió követői közössége van. A sikeren felbuzdulva „Izrael – iraki arab dialektusban" névvel új oldalt indítottak, amellyel együtt már 1,6 milliót számlál az izraeli külügyminisztérium platformjainak követői köre.

Ha a digitális világ bármely szegmense szóba kerül, nem mehetünk el szó nélkül az Egyesült Államok mellett. A kiberszempontból is a világ vezető hatalmai között lévő észak-amerikai állam külügyi palettáján egyre hangsúlyosabban jelennek meg a kibertér szabályozásával és működtetésével kapcsolatos témakörök – ezek között is kiemelten a kiberbiztonság kérdése. Tárcaközi együttműködés keretében látják kezelhetőnek a kibertérben jelentkező hatalmas problémahalmazt, amely szervezeti keretéül a minisztériumon belül felállítandó Kiberdiplomáciai Iroda (Office of Cyber Issues) jelentené. A hivatalos amerikai véleményt pedig a nemzetközi fórumok előtt egy rendkívüli és meghatalmazott nagyköveti minőségben eljáró „digitális diplomata" képviselhetné a leghitelesebb-

[151] MANOR (2018).

ben.[152] Mindezt a világon is egyedülálló jogforrás, a 2018 júniusában elfogadott *Kiberdiplomáciai törvény* rögzíti.[153] A törvényt, amelyet a republikánus és demokrata képviselők egyaránt támogattak, megelőzte a 2018. május 11-én kiadott elnöki rendelet a kormányzat hálózatainak és a kritikus infrastruktúra kiberbiztonságának megerősítéséről.[154] Ezen intézkedések jól mutatják, hogy a kiberbiztonság kérdésköre a legfontosabb politikák egyikévé nőtte ki magát. Nincs ez máshogy Európában sem, ahol egy olyan kis állam, mint Észtország, a 2019-es évet a digitális és kiberdiplomácia évének nyilvánította.[155]

[152] BURWELL (2018).

[153] Az Egyesült Államok Kiberdiplomáciai törvényének tervezete (2017).

[154] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017).

[155] Minister says next year's budget helps strengthen Estonia's foreign service (2018).

ZÁRÓ GONDOLATOK

Mai világunk forrong. Számos kezeletlen és kezelni próbált törésvonal mentén feszülnek egymásnak az eltérő állami érdekek, amely csatározások színtere áttevődik a negyedik hadszíntérre, azaz a kibertérre. Napjaink fejleményei közül elég, ha a *Stuxnet 2* néven elhíresült, az iráni intézményrendszer ellen irányuló kibertámadásra gondolunk, de említhetjük a Donald Cook amerikai torpedóromboló elleni fekete-tengeri irányított rádióhullámos orosz támadást 2014-ből vagy a napjainkban (2018-ban) épp *Automata Harcos* néven zajló eddigi legnagyobb brit robothadgyakorlatot. Ezek az események egyértelműen állam és állam közötti, erődemonstráló vagy célzott támadások, felvillanások, ugyanakkor nem feledkezhetünk meg az állampolgári szintről sem. Ugyanis mindenki olyan kérdések megválaszolására vár még, mint a mesterséges intelligencia felhasználhatósági korlátainak és etikai határainak meghúzása például a GDPR által is részben szabályozott gépek általi profilalkotás esetén vagy az önvezető autók hamarosan beköszöntő korszakával együtt felmerülő olyan kérdéshalmazok kezelése, mint balesetek esetén a felelősség kérdése és az élethez való alapvető jog biztosításának garantálása.[156]

A kibertér védelme ugyanakkor közös érdek. Valamennyi állam, szervezet és magánszemély joga, hogy a kibertérben is biztonságban tudhassa magát, de ugyanakkor kötelessége e biztonság megteremtéséhez hozzájárulni. Az érdekközösség legszembetűnőbben a kritikus infrastruktúrák vonatkozásában – azon belül is különösen az energiaelosztó rendszerek esetében – érhető tetten: egy célzott kibertámadás ugyanis képes nem csak az adott államot, hanem teljes régiókat dominóelvszerűen megbénítani – ahogyan az Egyesült Államok nyugati partját érintő áramszünet esetén már 2011-ben bebizonyosodott.

Az általam vizsgált három állam vezető európai hatalmak, amelyek – eltérő mértékben ugyan, de – globális befolyással is rendelkeznek.[157] Mindhárom ország az elsők között ismerte fel a biztonság legújabb területének, a kiberbiztonság rohamosan növekvő fontosságát a rájuk leselkedő veszélyek okán, és igyekszik adekvát, gyors és nyílt válaszlépéseket tenni. Az államok tudják, hogy a kibertérben lehetetlen egy országot határokkal körülbástyázni és megvédeni, ezért összefogást sürgetnek, amelyet stratégiai szinten is valamennyien deklarálnak, ám annak megvalósítása már nehézségekbe ütközik. Addig, amíg nem születik konszenzus a kibertérben alkalmazandó alapvető kötelező érvényű szabályok tartalmát illetően, addig nehéz lesz felvenni a küzdelmet a kiberbűnözőkkel és lator államok kibertámadásaival szemben. Márpedig a szabályalkotás folyamata akadozik és a megoldás még nem körvonalazódik. A jövőben a brit–német–francia-tengely kulcsszerepet tölthet be az öreg kontinens, és egyben a világ, kiberbiztonsága alapjainak megteremtésében nem csak proaktív szerepet játszva a folyamatok generálásával,

[156] A Google alkalmazottai már odáig is elmentek, hogy petíció formájában fejezték ki tiltakozásukat az ellen, hogy az amerikai Védelmi Minisztérium megvásárolta az általuk fejlesztett képfelismerési algoritmust, amelyet azt követően egyértelműen haditechnikai célokra szándékoznak felhasználni.

[157] Itt elsősorban a brit katonai-politikai, a német gazdasági és a francia kulturális hatalmi mivoltra gondolok.

hanem azáltal is, hogy mint mintaállamok példaképül szolgálhatnak más államok számára. Különösen hangsúlyos lehet Franciaország szerepe, amely állam mindig is a diplomáciai megoldások híve volt. A kibertérben ugyanis a kiberdiplomáciáé lehet a jövő, hogy a kibertér véres eseményeit ne fegyverrel, hanem békés úton, tárgyalásokkal lehessen rendezni. Ha a nemzeti kiberstratégiákban megfogalmazott célkitűzéseket mindhárom államnak sikerül átültetnie a gyakorlatba, akkor megfelelő tudással felvértezve, a szükséges anyagi, technikai és szervezeti eszközök birtokában bizakodóan vághatnak neki a következő évtizednek, amely minden bizonnyal nem kevés meglepetést tartogat a kibertérben is.

FELHASZNÁLT IRODALOM

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, http://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf (Letöltés ideje: 2018.11.22.)

2016 Presidential Campaign hacking Fast Facts, (2018. július 18.), https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html (Letöltés ideje: 2018.10.10.)

Az EU globális kül- és biztonságpolitikai stratégiája – 2016 (2016), https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf (Letöltés ideje: 2018.09.30.)

Az Európai Biztonsági Stratégia – Egy biztonságos Európa egy jobb világban (2003), https://europa.eu/globalstrategy/en/european-security-strategy-secure-europe-better-world (Letöltés ideje: 2018.09.30.)

Az Európai Digitális Menetrend, 2010. augusztus 26. (2010), https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN (Letöltés ideje: 2018.09.30.)

Az Európai Parlament 2012. június 12-i állásfoglalása „A kritikus információs infrastruktúra védelme. Eredmények és következő lépése: a globális kiberbiztonság felé" című dokumentumról. 2013/C 332 E/03 (2012), http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1479216690655&uri=CELEX:52012IP0237 (Letöltés ideje: 2018.09.30.)

Az Európai Unió kiberbiztonsági stratégiája (2013), Brüsszel, 2013. február 8., http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=hu (Letöltés ideje: 2018.09.30.)

Alliance for Cyber Security https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/ACS_Broschuere_en.pdf?__blob=publicationFile&v=4 (Letöltés ideje: 2017.11.11.)

Annual Review (2018), NSCS https://www.ncsc.gov.uk/news/annual-review-2018 (Letöltés ideje: 2018.11.05.)

ANSSI – *Agence Nationale de la Sécurité des Systèmes d'Information* https://www.ssi.gouv.fr/en/ (Letöltés ideje: 2018.10.01.)

Arrêté fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs.(2006) Journal officiel de la République Française, 2006. június 2., http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20060604&numTexte=1&pageDebut=08502&pageFin=08502 (Letöltés ideje: 2018.10.01.)

Az Egyesült Államok Kiberdiplomáciai törvényének tervezete. (2017) https://docs.house.gov/meetings/FA/FA00/20171115/106637/BILLS-115-HR3776-R000487-Amdt-076.pdf (Letöltés ideje: 2018.10.31.)

BUZAN, Barry – WAEVER, OLE – WILDE, JAAP DE (1998): *SECURITY: A NEW FRAMEWORK FOR ANALYSIS*. LYNNE RIENNER PUBLISHERS, BOULDER (CO).

BERLIN BIG DATA CENTER, HTTP://WWW.BBDC.BERLIN/HOME/ (LETÖLTÉS IDEJE: 2018.10.23.)

BRANGETTO, Pascal (2015): *National Cyber Security Organisation: France.* CCDCOE, Tallinn.
https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_FRANCE_032015_0.pdf (Letöltés ideje: 2018.10.01.)

Budapest Convention on Cybercrime. Európai Tanács, 2001., https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Letöltés ideje: 2018.10.23.)

BURWELL, Frances G.: *State Department needs a makeover for the digital age*. 2018. október 6., https://thehill.com/opinion/cybersecurity/410096-state-department-needs-a-makeover-for-the-digital-age (Letöltés ideje: 2018.10.31.)

Bürger CERT https://www.buerger-cert.de/ (Letöltés ideje: 201711.11.)

CERT-Bund https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/cert-bund_node.html (Letöltés ideje: 2017.11.11.)

COM (2009) 149: Az Európai Gazdasági és Szociális Bizottság véleménye – A kritikus informatikai infrastruktúrák védelme – „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása. (2010/C 255/18) 2010. szeptember 22., https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52009AE1948&from=HU (Letöltés ideje: 2018.09.30.)

CORERA, Gordon: *How France's TV5 was almos destroyed by 'Russian hackers'*. 2016. október 10. https://www.bbc.com/news/technology-37590375 (Letöltés ideje: 2018.10.10.)

CyberFirst https://www.gchq-careers.co.uk/early-careers/cyberfirst.html (Letöltés ideje: 2017.10.11.)

Cyber Readiness Index 2.0. A plan for cyber readiness: a baseline and an index. Country Profiles. Potomac Institute for Policy Studies, November 2015., http://www.potomacinstitute.org/academic-centers/cyber-readiness-index (Letöltés ideje: 2018.10.11.)

Cyber Security Strategy for Germany. (2011) Federal Ministry of the Interior, 2011. https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile (Letöltés ideje: 2017.11.11.)

Cyber Security Strategy for Germany 2016. Federal Ministry of the Interior, 2016, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (Letöltés ideje: 2017.11.11.)

Defence and Cyber Security: Government response to the Committee's Sixth Report of Session 2012-13. United Kingdom House of Commons Defence Committee, 2013. március 22., https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/719/71904.htm (Letöltés ideje: 2017.10.11.)

Defence Cyber Operations Group: Finance: Written question – 26326. United Kingdom Ministry of Defence, 2016. február 8., http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-02-08/26326/ (Letöltés ideje: 2017.10.11.)

Défense et sécurité des systèmes d'information. Stratégie de la France. ANSSI, 2011. https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf (Letöltés ideje: 2018.09.01.)

Defence Secretary Announces £40m Cyber Security Operations Centre. 2016. április 1. https://www.gov.uk/government/news/defence-secretary-announces-40m-cyber-security-operations-centre (Letöltés ideje: 2017.10.11.)

eEurope Action Plan (1999) http://ec.europa.eu/idabc/en/document/70/5849.html (Letöltés ideje: 2018.11.26.)

FELEDY Botond: *A kibertér mindent felfalhat.* 2018. július 3., https://index.hu/tech/2018/07/03/kiberter_cyber_kiberhadviseles/ (Letöltés ideje: 2018.10.10.)

Gartner Says Worldwide Enterprise IT Spending to Reach $2.7 Trillion in 2012, Orlando, Fl, 2011. október 17., https://www.gartner.com/newsroom/id/1824919 (Letöltés ideje: 2018.09.15.)

Az EU 2016/679. sz. rendelete – GDPR (General data protection regulation) – általános adatvédelmi rendelet. 2016. április 27., https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN (2018.09.30.)

German Internet Institute: Berlin-Brandenburg consortium wins bid. 2017. május 23., https://www.fu-berlin.de/en/presse/informationen/fup/2017/fup_17_131-zuschlag-internet-institut/index.html (Letöltés ideje: 2018.10.23.)

Germany Reveals Offensive Cyberwarfare Capability. Atlantic Council, 2012. június 8., http://www.atlanticcouncil.org/blogs/natosource/germany-reveals-offensive-cyberwarfare-capability (Letöltés ideje: 2017.11.11.)

Global Cybersecurity Index 2017. International Telecommunication Union, Geneva, Switzerland, 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (Letöltés ideje: 2017.10.11.)

Global Operations and Security Control Centre (GOSCC). Defence Committee, Further written evidence from the Ministry of Defence. 2013. március 12. https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106we05.htm (Letöltés ideje: 2017.10.11.)

HANULA Zsolt (2018): A bizalom a legújabb olaj. 2018. október 8., https://index.hu/techtud/2018/10/08/a_bizalom_az_uj_olaj/ (Letöltés ideje: 2018.10.08.)

Hack attack causes 'massive damage' at steel works. 2014. december 22., https://www.bbc.com/news/technology-30575104 (Letöltés ideje: 2018.10.10.)

Her Majesty the Queen opening the new National Cyber Security Centre. 2017. február 15., https://www.gchq.gov.uk/her-majesty-queen-opening-new-national-cyber-security-centre (Letöltés ideje: 2017.10.11.)

i2010 – European Information Society for growth and employment. COM (2005) 299. Commission of the European Communities, Brüsszel, 2005. június 1., https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF (Letöltés ideje: 2018.11.26.)

ILASCU, Ionut: *New Stuxnet Variant Allegedly Stuck Iran*. 2018. október 31., https://www.bleepingcomputer.com/news/security/new-stuxnet-variant-allegedly-struck-iran/ (Letöltés ideje: 2018.11.18.)

Industry 4.0. Platform http://www.plattform-i40.de/I40/Navigation/EN/Home/home.html;jsessionid=07277181712612D1527839CB5A17D587 (Letöltés ideje: 2017.11.11.)

Interim Cyber Security Science&Technology Strategy: Future-Proofing Cyber Security. 2017. november 30. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663181/Embargoed_National_Cyber_Science_and_Technology_Strategy_FINALpdf.pdf (Letöltés ideje: 2018.10.23.)

International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. (2011) United States, May 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Letöltés ideje: 2018.10.10.)

ITU Recommendation X.1205., 2008.04.18. https://www.itu.int/rec/T-REC-X.1205-200804-I (Letöltés ideje: 2018.11.22.)

Kiberegységet állít fel a német hadsereg. 2017. április 6., http://hu.euronews.com/2017/04/06/kiber-egyseget-allit-fel-a-nemet-hadsereg (Letöltés ideje: 2017.11.11.)

KOVÁCS László: *A kibertér védelme*. Dialóg Campus Kiadó, Budapest, 2018.

La réserve citoyenne. http://www.lareservecitoyenne.fr/ (Letöltés ideje: 2018.10.01.)

La réserve de cyberdéfense. http://www.gouvernement.fr/risques/les-reserves-de-cyberdefense (Letöltés ideje: 2018.10.01.)

Le plan Piranet https://www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/ (Letöltés ideje: 2018.10.01.)

Le plan Vigipirate http://www.gouvernement.fr/vigipirate (Letöltés ideje: 2018.10.01.)

LEWIS, James*: Economic Impact of Cybercrime – No Slowing Down.* McAfee, February 2018., https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHdutm_source=Pressutm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21utm_medium=emailutm_term=0_7623d157be-bb9303ae70-194093869 (Letöltés ideje: 2018.09.30.)

Livre blanc sur la défense et la sécurité nationale. 2013, https://www.defense.gouv.fr/content/download/206186/2286591/file/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf (Letöltés ideje: 2018.09.01.)

MACASKILL, Ewen (2018): *Major cyber-attack on UK a matter of 'when, not if' –security chief.* 2018. január 23., https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin (Letöltés ideje: 2018.10.10.)

Major cyber attack on UK a matter of 'when not if' – security chief. 2018. január 23. https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin (Letöltés ideje: 2018.10.15.)

MANOR, Ilan (2018)*: Can digital diplomacy skills serve as opublic diplomacy resources? The case of the Brexit*, Exploring Digital Diplomacy; 2018. október 4., https://digdipblog.com/2018/10/04/can-digital-diplomacy-skills-serve-as-public-diplomacy-resources-the-case-of-brexit/ (Letöltés ideje: 2018.10.31.)

MCGUINNESS, Damien (2018): *How a cyber attack transformed Estonia.* 2017. április 27., https://www.bbc.com/news/39655415 (Letöltés ideje: 2018.10.10.)

Megkezdődött a legnagyobb robothadgyakorlat. 2018. november 13. https://index.hu/techtud/2018/11/13/megkezdodott_a_brit_hadsereg_tortenetenek_legnagyobb_robot-hadgyakorlata/ (Letöltés ideje: 2018.11.29.)

Minister says next year's budget helps strengthen Estonia's foreign service. 2018. szeptember 27., https://www.baltictimes.com/minister_says_next_year_s_budget_helps_strengthen_estonia_s_foreign_service/ (Letöltés ideje: 2018.10.31.)

MOLNÁR Dóra (2017a): Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése. *Hadmérnök*, XII. évfolyam 1. szám - 2017. március, 255-267. oldal http://hadmernok.hu/171_20_molnar2.pdf (Letöltés ideje: 2018.11.26.)

MOLNÁR Dóra (2017b*):* Kiberbiztonsági alapvetések – 2016-os kitekintéssel. *Nemzet és biztonság* 2017/3. szám, 16–24. o. http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_3_03_molnar_dora_-_kiberbiztonsagi_alapvetesek-a_2016-os_kitekintessel.pdf (2018.11.26.)

MOLNÁR Dóra (2018): Mérföldkövek a brit kiberbiztonság fejlődésében II. Intézkedések és a szervezeti keretek kiépülése. In: *Hadmérnök*, XIII évfolyam „KÖFOP" szám, 2018. január, 193–204. o.

MUHA Lajos: *Az információbiztonság fogalma*, Forrás: lmuha.hu (Letöltés ideje: 2017.01.02.)

National Information Technology Situation Centre Nationales IT-Legezenztum https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Aktivitaeten/IT-Lagezentrum/lagezentrum_node.html (Letöltés ideje: 2017.11.11.)

National Security Strategy and Strategic Defense and Security Review 2015. A Secure and Prosperous United Kingdom. HM Government, United Kingdom, 2015. november 23. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf (Letöltés ideje: 2017.10.11.)

New cyber reserve unit created. 2013. szeptember 29. https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit (Letöltés ideje: 2017. 10.11.)

NIS (Directive on security of network and information systems) – hálózat- és információbiztonsági irányelv. 2016/1148/EP-Tanácsi irányelv. 2016. július 6. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L1148&from=EN (Letöltés ideje: 2018.09.30.)

Norbert Wiener-idézetek: https://www.brainyquote.com/authors/norbert_wiener (Letöltés ideje: 2018.09.15.)

NCSC deals with 1,100 cyber attacks in first two years. 2018. október 16. https://www.ncsc.gov.uk/news/ncsc-deals-1100-cyber-attacks-first-two-years (Letöltés ideje: 2018.11.05.)

OECD (2002): *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Securiy.* 2002., http://www.oecd.org/internet/ieconomy/15582260.pdf (Letöltés ideje: 2018.09.20.)

OECD (2012)*: Cybersecurity Policy Making at a Turning Point. Analysing a new genartion of national cybersecurity strategies for the Internet economy*. 2012., https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf (Letöltés ideje: 2018.08.10.)

OECD Reviewing Its Security of Information Systems and Networks Guidelines. CCDCOE, 2013. április 8., https://ccdcoe.org/oecd-reviewing-its-security-information-systems-and-networks-guidelines.html (Letöltés ideje: 2018.08.10.)

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 2017. május 11., https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (Letöltés ideje: 2018.10.31.)

Rapport d'Information du Sénat No. 681., 2012. július 18., http://www.senat.fr/rap/r11-681/r11-6811.pdf (Letöltés ideje: 2018.11.06.)

Self-determined and secure in the digital world 2015–2020. The German government's research framework programme on IT security. Federal Ministry of Education and Research, Germany, March 2015. https://www.bmbf.de/pub/IT_Security.pdf (2018.10.23.)

STONE, Zara: *An Artificial Intelligence Ethics Committee*. 2018. június 11. https://www.forbes.com/sites/zarastone/2018/06/11/the-artificial-intelligence-ethics-committee/#4cd9ab61637d (Letöltés ideje: 2018.11.21.)

Stratégie du lutte contre les cybermenaces. Ministère de l'Intérieur, France, 2017. https://www.interieur.gouv.fr/Archives/Archives-des-actualites/2017-Actualites/Lutter-contre-les-cybermenaces (Letöltés ideje: 2018.09.01.)

Stratégie internationale de la France pour le numérique. France, 2017. december 15. https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf (Letöltés ideje: 2018.09.01.)

Stratégie nationale pour la sécurité du numérique. France, 2015. https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf (Letöltés ideje: 2018. szeptember 1.)

TAYLOR, Adam: *The Czech foreign minister says his email was hacked – and hints Russia could be behind it.* 2017. január 31. https://www.washingtonpost.com/news/worldviews/wp/2017/01/31/the-czech-foreign-minister-says-his-email-was-hacked-and-hints-russia-could-be-behind-it/, (Letöltés ideje: 2018.10.10.)

The UK Cyber Security Strategy 2011–2016. Annual Report, HM Cabinet Office, United Kingdom, 2016. április, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf (Letöltés ideje: 2017.10.11.)

The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. Cabinet Office, 2011. november, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (Letöltés ideje: 2017.10.11.)

Vigipirate: Objectifs de cybersécurité. ANSSI – SGDSN, 2014. február 27. https://www.ssi.gouv.fr/uploads/2014/10/20140310_Objectifs_de_cybersecurite_document_public.pdf (Letöltés ideje: 2018.10.01.)

VITEL, Philippe – BLIDDAL, Henrik: French Cyber Security and Defence: an Overview. In: *Information & Security: An International Journal*, 2015. Vol.32., https://connections-qj.org/system/files/3209_france.pdf (Letöltés ideje: 2018.10.01.)

ZETTER, Kim: *Everything we know about Ukraine's power plant hack*. 2016. január 6., https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ (Letöltés ideje: 2018.10.10.)

A Nemzeti Közszolgálati Egyetem kiadványa

Kiadó:
Nemzeti Közszolgálati Egyetem
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős kiadó:
Prof. Dr. Kis Norbert rektorhelyettes
Címe: 1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Zsoldos Sándor

Tördelőszerkesztő:
Mikes Vivien

ISBN 978-963-498-173-2 (elektronikus)