PRO PATRIA AD MORTEM

A kibertér védelme

KOVÁCS LÁSZLÓ

Dialóg Campus

Kovács László

A kibertér védelme

Vákát oldal

Kovács László

A KIBERTÉR VÉDELME

Dialóg Campus Kiadó ❖ Budapest

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosító számú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében jelent meg.

Szakmai lektor
Munk Sándor

Tartalom

Előszó **9**

Bevezetés **11**

A könyvben használt legfontosabb fogalmak **17**

1. Kibertér a mindennapjainkban **19**

1.1. Digitális ökoszisztéma 22

1.1.1. A mesterséges intelligenciáé a jövő? 25

1.2. Digitális gazdaság és társadalom 26

1.2.1. Internethasználat: mit mutatnak a számok? 41

1.2.2. Mobilkommunikáció 57

1.2.3. Kereskedelem a kibertérben 59

1.2.4. Vállalatok a kibertérben: üzlet és digitalizáció 65

1.2.5. Állampolgárok a kibertérben 67

1.2.6. Közösség, hálózat, média 76

1.3. Digitalizált környezetünk és otthonunk 80

1.3.1. Számítógépet mindenhova és mindenre, avagy a dolgok internete 82

1.3.2. Okosautók 98

1.3.3. Okosvárosok 106

1.3.4. Okosotthonok 112

1.4. Kibertér és politika 115

2. A kibertér veszélyei **119**

2.1. Sérülékenységek, módszerek, eszközök 119

2.1.1. Malware-ek, avagy a szoftverek, amelyek rosszat akarnak 120
2.1.2. Túlterhelés mint támadási módszer 141
2.1.3. APT és egyéb támadási formák 148
2.2. Támadók, avagy a kibertér (egyéni és csoportos) szereplői 169
2.2.1. Hacktivisták, avagy az internet szabadságharcosai 174
2.2.2. Kiberbűnözők és kiberbűnözés 183
2.2.3. Terroristák a kibertérben 197

3. A kiberbiztonság megvalósítása 205

3.1. A kiberbiztonság tulajdonságai és kapcsolatai 206
3.2. Kiberbiztonság a kritikus infrastruktúrákban 212
3.2.1. Kritikus infrastruktúrák és kritikus információs infrastruktúrák meghatározása 213
3.2.2. Kritikus infrastruktúrák és kritikus információs infrastruktúrák támadhatósága 224
3.3. Kiberbiztonság Magyarországon 236
3.4. Kiberbiztonság az Európai Unióban 246
3.4.1. A NIS-direktíva 254
3.4.2. A GDPR-irányelv 257
3.4.3. A HORIZONT 2020 260
3.4.4. A kiberbiztonság európai uniós szervezetei 264
3.5. Kiberbiztonság a NATO-ban 271
3.6. Nemzetközi kiberbiztonsági szabványok és ajánlások 274
3.6.1. Common Criteria (ISO 15408) 275
3.6.2. ISO/IEC 27001 277
3.6.3. A NIST kiberbiztonsági kiadványai 279
3.6.4. COBIT 281
3.6.5. ITIL 282
3.6.6. Hazai információbiztonsági ajánlások 283

3.7. A kiberbiztonság gyakorlati megvalósításáról 284
3.7.1. Kockázatok felmérése és kezelése 286
3.7.2. Korai előrejelzés a kibertérben 289
3.7.3. Biztonság a fizikai térben 292
3.8. A kiberbiztonság humán oldala 293
3.8.1. Oktatás, képzés, kutatás 294
3.8.2. Tudatosítás 300

Rövidítések jegyzéke 307

Illusztrációk jegyzéke 315

Táblázatok jegyzéke 321

Irodalomjegyzék 323

Vákát oldal

Előszó

A mai modern, technológiaorientált társadalmunkban szinte megkerülhetetlen, hogy kapcsolatba kerüljünk a kibertérrel. Az emberek napi tevékenységük során szinte folyamatosan valamilyen információtechnológiai eszközt használnak, amelyeknek döntő hányada már az interneten, illetve egyéb hálózaton keresztül kapcsolódik más készülékekhez. A számítógép, táblagép, okostelefon és más infokommunikációs eszközök használatát ma már teljesen természetesnek vesszük. Ezekkel a nap bármely szakában, bárhonnan, folyamatosan információhoz jutunk, munkát végzünk, mindennapi ügyeinket intézzük, illetve a közösségi médiának köszönhetően kapcsolatba kerülhetünk családtagjainkkal, munkatársainkkal, barátainkkal, ismerőseinkkel. A dolgok internetének (*Internet of Things* – IoT) és más új, feltörekvő technológiáknak köszönhetően pedig már például az autónk és az otthonunk is részévé válik a kibertérnek.

A kibertér meghatározásában és értelmezésében bár eltérő álláspontok és nézetek tapasztalhatók, abban az e területtel foglalkozó szakértők mindegyike megegyezik, hogy a kibertér a hálózatok és benne az internet, valamint a hálózathoz vezetéken vagy vezeték nélkül csatlakozó eszközök működési tartománya. A kiberteret ma már egyre többen tudatosan használják, de sokan a létezésének tudtán kívül élvezik az általa nyújtott szolgáltatások előnyeit. Fontossága a legtöbb ember számára általában csak akkor tűnik fel, ha valamely kibertéri szolgáltatás nem elérhető: nem tudunk az internetre csatlakozni, nem tudunk e-mailt küldeni, banki tranzakciót végezni, esetleg online formában magán- vagy közügyeket intézni.

A kibertértől való nagymérvű függőségünk azonban magában hordozza az azon keresztüli sebezhetőségünket is. Minél inkább támaszkodunk a kibertér nyújtotta hálózatos lehetőségekre, annál

inkább számolni kell olyan új típusú fenyegetésekkel is, amelyek jelentősen befolyásolhatják a mindennapi tevékenységünket, a létfontosságú infrastruktúrák működését, a különféle szolgáltatásokhoz való hozzáférést.

A jelen könyv – a legújabb infokommunikációs technológiai trendeket figyelembe véve – a kibertérben megjelenő fenyegetések és a védelem kérdéskörét tárgyalja – az átlagolvasó számára is – közérthető formában. Bemutatja a mindennapjaink kibertéri környezetét, a dolgok internete technológiáját, az okosautó-, okosotthon-, okosváros-alkalmazásokat, valamint a digitalizáció gazdaságra és a társadalomra gyakorolt hatását. Számos támadási példán és azok elemzésén keresztül felvillantja az egyének és az egész társadalom biztonsága szempontjából legfontosabb kibertéri fenyegetéseket, illetve bemutatja a kibertér negatív szereplőit. A kötet második felében a fenyegetésekre adható válaszokat ismerteti részben az eljárások és gyakorlati módszerek, részben pedig a különféle szabályzók oldaláról. Az EU, a NATO és hazánk gyakorlatában alkalmazott jogszabályok, irányelvek, szabványok és ajánlások alapján bemutatja a kiberbiztonság megteremtésére irányuló törekvéseket, a gyakorlati megvalósítás lehetőségeit, valamint külön hangsúlyozza a biztonságtudatosság szerepét a kibertér védelmében.

A könyv jó szívvel ajánlható mindazoknak, akik számára a kibertér mindennapi használatán túl fontos annak biztonsága is. Hasznos olvasmányként forgathatják mindazok, akik érdeklődnek a kibertérben megjelenő újfajta veszélyek és fenyegetések iránt, illetve akik kíváncsiak a lehetséges kiberbiztonsági megoldásokra, az EU, a NATO és a nemzetek, köztük Magyarország stratégiai és jogszabályi erőfeszítéseire.

Budapest, 2017. december 21.

Haig Zsolt

Bevezetés

Az internet és az infokommunikációs eszközök egymással párhuzamos, nagyon sokszor egymásra is kölcsönösen hatással lévő fejlődése azt okozta, hogy ma már nem, vagy csak nehezen tudunk ezek nélkül az eszközök és szolgáltatások nélkül élni. Ezek az eszközök és rendszerek, valamint az általuk nyújtott szolgáltatások, ha nem is észrevétlenül, de részei lettek mindennapjainknak.

Az internet ma már nemcsak egyszerű szórakozási, információszerzési eszköz vagy a tudományos eredmények megosztására szolgáló hálózatok összessége, hanem a gazdaság, a politika, a kultúra és végső soron mindennapjaink teljes egészének meghatározója. Az internet és a hozzá kapcsolódó számtalan eszköz alkotta kibertérben éljük mindennapjaink jelentős részét.

Az infokommunikációs (röviden csak IKT) eszközöktől és rendszerektől való függőség egyre inkább konvergens módon jelentkezik, ráadásul nemcsak egy, hanem sok, egymástól látszólag független eszközzel és rendszerrel szemben alakul ki egyre inkább feloldhatatlan függőségünk.

Könyvünk a biztonság aspektusából vizsgálja ezt a függőséget és a mögötte lévő összefüggéseket. A biztonság a kibertérben összetett módon jelentkezik, hiszen a biztonság egyrészt a használt eszközök és rendszerek sérülékenysége és sebezhetősége, másrészt miattunk felhasználók miatt sem teljes. Ugyanakkor hatalmas társadalmi igény van arra, hogy az infokommunikációs eszközök és rendszerek zavartalanul működjenek. Mindezeket a tényezőket kell tehát egyensúlyba hozni, azaz meg kell teremteni annak a feltételeit, hogy a kibertér védelme megvalósuljon.

Ez a feladat azonban már az összetettségénél fogva is rendkívül nehéz, hiszen számítógépeket találunk az élet minden területén.

Néhány évtizeddel ezelőtt, de még akár 15 évvel ezelőtt is nagyon nagy jövőbe látó képességgel kellett rendelkeznie annak, aki előre akarta jelezni, hogy a háztartásokon keresztül a mindennapi élet legapróbb részletéig mindenhol olyan eszközöket találunk, amelyek számítógépek által vezéreltek. Olyan okostelefonokkal kommunikálunk, amelyekben már helyet kap a mesterséges intelligencia, számítógép-vezérelt autóban utazunk, otthonainkat robotporszívók takarítják, és sokáig folytathatnánk a sort tovább, hiszen a gazdaság, az oktatás, a kultúra minden területén számítógépekre támaszkodunk.

A kérdés az, hogy mit hoz a jövő. Ha az elmúlt évtizedek exponenciális technikai fejlődését prognosztizáljuk a közeljövő évtizedeire, könnyen belátható a Ray Kurzweil által lefestett technológiai szingularitás bekövetkezése. Ekkor a számítógépek önmagukat tervezik és gyártják, olyan nyelven és olyan sebességgel kommunikálnak egymással, amelyet ember nem ért és nem tud követni. Robotok gyártanak robotokat emberi közbeavatkozás nélkül. Ez egyelőre beláthatatlan jövőt vázol elénk. (Kurzweil 2013)

Ennek analógiáján, ha ma nehéz a biztonságot megteremteni a kibertérben, akkor a jövőben ez még inkább igaz lesz, mert bár már ma is intelligens, sokszor öntanuló eszközöket használunk mindennapjainkban, az előbb említett kurzweilli kép alapján ez a továbbiakban fokozódni fog.

Persze ennek a fejlődésnek sokan az árnyoldalaira figyelmeztetnek, amely elsősorban abban jelentkezik, hogy néhány évtizeden belül a számítógépek – ha egyáltalán így fogjuk őket akkor még hívni – a mai korlátozott intelligenciájuknál várhatóan sokkal okosabbak lesznek, így már nem is biztos, hogy a megalkotásukhoz szükség lesz az emberre. Legalábbis ezt állítja Kurzweil. (Galeon–Reedy 2017) Ugyanakkor az is elképzelhető, hogy a gépek másfajta – esetleg a mainál sokkal tökéletesebb – biztonságot teremtenek majd.

A robottechnológia előretörése már a mindennapi ember számára is kézzelfogható. Az elmúlt évtizedben a katonai célú robotok száma a sokszorosára nőtt, és ugyanez igaz a hétköznapi életre is. De az előbb

említetteknek megfelelően a robotok irányításában nagy szerepet játszó mesterséges intelligencia a jövőben akár veszélyt is jelenthet ránk nézve. Erre utal nyilatkozataiban Stephen Hawking, illetve egy kicsit más szempontból Elon Musk is. (Cellan–Jones 2014)

Ma a digitális társadalom építése során alapelvnek számít, hogy az internet és a hálózat nyújtotta előnyöknek mindenki számára elérhetővé kell válniuk. Ugyanakkor ez csak abban az esetben lesz valóban előny, ha ezt az elérést, illetve a hálózaton működő számtalan szolgáltatást biztonságosan tudjuk használni. Az online tartalomszolgáltatás, az elektronikus ügyintézés, az elektronikus banki szolgáltatások vagy akár az internetalapú kommunikáció csak akkor fog valóban mindenki számára előnyt hordozni, ha ezeket a lehető legnagyobb biztonság mellett tudjuk igénybe venni.

Azonban ez a biztonságos internethasználat ma még csak egy elképzelt jövőbeni állapot, és nyugodtan kijelenthetjük, hogy ma még csak álom, amelynek megvalósulására komolyan kell törekednünk. Számtalan buktatója van ma a kibertérnek a biztonság szempontjából. Egyfelől a humán összetevők (például mindig van valaki, aki jogosulatlan előnyt akar szerezni, akár mások kárára), illetve a másik oldalról technikai összetevők nehezítik a biztonság megvalósítását.

A humán összetevők esetében gyakran hallhatjuk, hogy a rendszerben a leggyengébb láncszem az ember. A fejlesztők, a szoftver- és hardvergyártók hiába hoznak létre maximális biztonsággal ellátott rendszert, ha a felhasználó a legalapvetőbb biztonsági protokollokat sem tartja be. Persze a másik – az egyszerű felhasználó – oldaláról is megkérdezhetjük, hogy miért is bízzák a biztonságot a gyártók a felhasználókra. Miért nem gyártanak olyan rendszereket, szoftvereket és eszközöket, amelyek valóban teljesen biztonságosak, és így azok függetlenek a felhasználó életkorától, illetve felkészültségétől? Hiszen már szakmai terminológia is van a biztonságtudatos fejlesztésre: *security by design.* Ennek alapján a tervezés és gyártás során a lehető legnagyobb figyelmet kell kapnia a biztonságnak, és amíg az adott szoftver vagy hardver nem esik át egy komoly auditon, addig az nem kerül(het) forgalomba.

Komoly kérdések, amelyekre ma még nincs és egyelőre nem is lehet uniformizált válasz.

A információtechnológia és információtechnika robbanásszerűen bekövetkezett fejlődése nagyon sokszor háttérbe szorította a biztonság kérdését. Ha belegondolunk, 30 évvel ezelőtt még csak néhány jó matematikai vagy műszaki képességgel megáldott ember sajátja volt a mindennapi számítógép-használat. Ma már viszont a legfiatalabbtól a legidősebb generációig mindenki kapcsolatba kerül a számítógéppel, a számítógép-hálózatokkal, az okoseszközök ezernyi megnyilvánulásával, ráadásul naponta akár többször is. A Föld népessége jelenleg közel 7,5 milliárd ember, amelynek majdnem a fele – több mint 3 milliárd ember – hetente legalább egyszer használja az internetet. Ha valamit „forradalmi" fejlődésként értelmezhetünk az emberiség történetében, akkor ez a kibertérben megvalósuló haladás joggal számíthat erre a jelzőre.

Napjainkban egyre nagyobb igény mutatkozik arra, hogy az eddig viszonylag jól elkülöníthető és egymástól elhatárolható területek – mint például az információbiztonság, a kritikus információs infrastruktúrák védelme, az informatikai eszközök biztonsága – egy átfogó területként, a kiberbiztonságban jelenjenek meg. Ma már sokszor nemcsak egyszerű információbiztonsági szakértőt keresnek a vállalatok, hanem kiberbiztonsági szakembert, aki nemcsak komplex módon képes kezelni a vállalatokat fenyegető veszélyeket és kihívásokat, hanem érti és biztonságosan menedzselni is képes a kibertérben zajló folyamatokat.

Amikor könyvünkről kell szólnunk, ki kell jelentenünk azt a nyilvánvaló tényt, hogy ma már a kibertér, illetve az ott megvalósítani kívánt biztonság leírása nem fér el egy könyvben. Egy könyv keretei nem teszik lehetővé a teljes kibertéri biztonság, az ott meglévő kihívások és veszélyek teljes körű bemutatását, legyenek azok humán vagy technikai veszélyek. Ráadásul ott van az ezekkel szembeállítani és megvalósítani kívánt védelem minden részlete is, amelynek bemutatása nemcsak terjedelmi, hanem időbeli korlátok miatt szintén

nem lehetséges, hiszen havonta, hetente, sőt egyes esetekben naponta újabb és újabb kihívások jelennek meg, gondoljunk csak a rosszindulatú programok tömegére, de akár a másik oldalon az online védelem különböző újabb és újabb megoldásaira.

Ezért aztán marad a nem túl ígéretes vállalás: egyes, a szerző számára érdekesnek, illetve bemutatásra érdemesnek vélt tényezőt villantunk fel és elemzünk. Természetesen a teljesség igénye felmerülhet az olvasóban, de a könyv szubjektív válogatás a legfontosabbnak vélt kiberbiztonsági tényezőkből, trendekből, eseményekből. A könyv tehát egy pillanatképet, egy aktuális állapotot mutat be a dinamikusan változó kibertér egyes szegmenseinek (de valóban korántsem mindegyik) bemutatásával.

Könyvünk felépítése a jól bevált gyakorlatot követi. Az első részben, azaz első fejezetben és a hozzá kapcsolódó alfejezetekben általános áttekintést adunk azokról a tényezőkről, amelyeket a legfontosabbnak gondolunk napjaink kiberterében. Ezt követi azoknak a veszélyeknek a feltárása, amelyek az első részben ismertetett tényezőket veszélyeztetik. Majd az utolsó rész mintegy a drámai hatás kifejtése érdekében elvezeti az olvasót a veszélyekkel szembeni védekezés egyes elemeiig, ami alapján mindenki eldöntheti, valóban biztonságos-e ma, és ami talán még fontosabb: a jövőben biztonságos lesz-e a kibertér? Választ keresünk arra, hogy megteszünk-e mindent annak érdekében, hogy megvédjük azt a teret, amely akarva-akaratlanul életünk meghatározó tényezőjévé vált.

Minden egyes rész bemutatása során törekszünk arra, hogy olyan forrásokat állítsunk egymás mellé, amelyek lefedik a kibertér (vagy annak egyes részeinek) biztonságát, azaz akár referenciaként is szolgálhatnak a kutatásokhoz, illetve, hogy jobban el tudjunk igazodni ebben a látszólag nem egyszerű világban és annak sokszor labirintusszerű útvesztőiben.

Mindezek mellett könyvünk egy filozófiai alapot kíván nyújtani ahhoz, hogy megértsük azt, ami persze ma már nyilvánvaló: a kibertér jelen van a mindennapjainkban, ennélfogva védelme olyan esszenciális

érdekünk, mint minden más biztonságot befolyásoló tényező a világon. De talán pont ezért nem tekintjük eléggé fontosnak annak biztonságát.

Ehhez kíván kisebb-nagyobb példákon keresztül támpontokat nyújtani e könyv.

A könyvben használt legfontosabb fogalmak

A kibertér biztonsága számos olyan fogalmat és meghatározást takar, amelyek ugyan naponta használatosak, de sokszor mégsem tudjuk, hogy azok alatt pontosan mit is kell értenünk. Ezért mielőtt belevágnánk a kibertér közepébe, összegyűjtöttük azokat a legfontosabb fogalmakat és meghatározásokat, amelyeket könyvünkben a későbbiekben az egyes fejezetekben és alfejezetekben használunk. Rögtön le kell szögeznünk, hogy ezek a fogalmak, illetve az azokat magyarázó meghatározások nem szabványok, nem ajánlások és nem örök érvényű igazságok, mégis szükséges megadni ezeket, legalább általánosságban. Ezért reményeink szerint a kiválasztott néhány fogalom nemcsak a könyv további részeinek megértéséhez ad némi támpontot, hanem talán a későbbiekben is – akár kiegészítésekkel, kisebb módosításokkal – alkalmazhatóak és használhatóak lesznek az olvasók számára.

Biztonság: az eszközök, rendszerek és hálózatok olyan megkívánt állapota, amelyben a veszélyek megfelelő szintű kezelése megtörténik.

Digitális ökoszisztéma: nagy sávszélességű infrastruktúra, képzett felhasználók, digitális szolgáltatásokat használó és azokra épülő üzleti szféra, fejlett és intenzív K+F+I ipar, digitális szolgáltató állam, online elérhető kereskedelmi szolgáltatások, digitális archívumok olyan összessége, amely a tudásalapú társadalom meghatározó tényezőjeként értelmezhető.

Infokommunikáció: az informatika és a kommunikáció konvergenciája révén létrejövő technológia, eszközök és rendszerek gyűjtőfogalma.

Infrastruktúra: létesítmények, hálózatok, rendszerek és üzemeltető szakemberek összessége, amelyek hozzájárulnak a társadalom alapvető szükségleteinek kielégítéséhez.

Internet: az internet egy olyan globális kiterjedésű számítógép-hálózat, amelyben számítógép-hálózati protokoll kapcsolja össze a felhasználókat és a szolgáltatásokat.

Kiberbiztonság: a biztonságot meghatározó eszközök, politikák, koncepciók, technológiák, irányelvek, kockázatkezelési módszerek, tevékenységek, képzések, valamint a legjobb gyakorlatok összessége, amelyek arra irányulnak, hogy megvédjék a számítógépes környezetet, az ezt használó szervezetek és felhasználók eszközeit, rendszereit.

Kibertér: felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek gyűjtőfogalma, amelyek közvetlenül vagy közvetett módon számítógép-hálózathoz vannak kapcsolva.

Kritikus infrastruktúra: olyan eszköz, létesítmény vagy rendszer, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.

Kritikus információs infrastruktúra: olyan hálózatszerű, fizikai vagy virtuális rendszereket, eszközöket és módszereket (eljárások, szolgáltatások) foglal magában, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban kritikus rendszerek vagy más azonosított kritikus rendszer működéséhez nélkülözhetetlenek.

Védelem: olyan tevékenységeket takar, amelyek a biztonság megteremtésére és fenntartására irányulnak.

1. Kibertér a mindennapjainkban

A kibertér varázslatos dolog. Ugyanakkor megfoghatatlan is. Amikor valakinek feltesszük a kérdést, hogy *„mi is az a kibertér?”,* akkor a válaszok túlnyomó többsége a következő: „a kibertér az internetet jelenti.”

Ez a válasz azonban csak részben igaz, hiszen az internet önmagában még nem azonos az egész és teljes kibertérrel. Számos más eszközt, szolgáltatást találunk az interneten kívül is a kibertérben, bár az kétségtelen, hogy ezek az eszközök is akkor válnak a kibertér részévé, ha hálózatba kapcsolva működnek. A kibertér értelmezése nagyon sok nézőpontból történhet, emiatt nagyon sok meghatározás létezik a fogalom tisztázására.

A válasz más értelmezésben azonban teljesen igaz, mert abban a pillanatban, hogy bármely olyan eszközt, amelyet az átlagos felhasználó alkalmaz és azt a hálózathoz kapcsolja, abban a momentumban az az internet részévé is válik. A dolgok internete, azaz az IoT *(Internet of Things)* nagyon jól mutatja ezt az álláspontot, hiszen ma már az informatikai és elektronikai eszközök jelentős részét hálózatba, és így az internetre is tudjuk kapcsolni.[1]

A kibertér meghatározására, valamint határainak körbeírására nagyon sok teória és elgondolás született az elmúlt évtizedekben. Magára a kibertér fogalmi meghatározására is számos példát találunk. Egységesen elfogadott definíció azonban nem létezik még, hiszen

---

[1] Ez azonban magával hozza azt a kérdést, amely alapvetően biztonsági oldalról jelentkezik. Mennyire és milyen módszerekkel (milyen filozófia mentén) tudjuk ennek a nagy tömegű, hálózatba kapcsolt, így a világ bármely pontjáról elérhető eszköznek a biztonságát megvalósítani. Könyvünk későbbi részeiben erre részletesebben kitérünk.

minden egyes meghatározás alaposan tükrözi az azt megalkotó álláspontját és sokszor azzal való viszonyát is.[2]

Az így született meghatározások közül természetesen többet is ki kellene emelni. Az egyik az ITU, azaz a Nemzetközi Távközlési Egyesület[3] alkotta fogalom. E szerint a kibertér nem más, mint a felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek összessége, amelyek közvetlenül vagy közvetett módon hálózathoz vannak kapcsolva. (ITU 2008)

A 2013-as hazai Nemzeti Kiberbiztonsági Stratégia megfogalmazása szerint: „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti." [1139/2013. (III. 21.) Korm. határozat]

Nagyon érdekes és figyelemre méltó, ugyanakkor számos vitát is kiváltó folytatással rendelkezik a kibertér meghatározása a Nemzeti Kiberbiztonsági Stratégiában. Ez a magyar kibertér vagy más olvasatban Magyarország kiberterének meghatározása. Az említett stratégia szerint „Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon talál-

---

2 A „kibertér" kifejezés megalkotását W. Gibsonhoz kötik, aki a *Neurománc* című cyberpunk novellájában használta ezt a kifejezést először, persze nem feltétlenül a ma használatos értelemben, de utalva arra a hálózatok alkotta térre, amelyben különböző digitális szolgáltatások valósulhatnak meg. (Gibson 1992; Haig 2015) Gibson e novelláját, amelynek az eredeti angol címe *Neuromancer* volt, egy trilógia első részeként 1984-ben jelentette meg, majd ezt követte a másik két rész: a *Számláló nullára* és a *Mona Lisa Overdrive*.

3 ITU: International Telecommunication Union, azaz Nemzetközi Távközlési Egyesület az ENSZ távközlésre szakosodott szervezete. Fő feladata a távközlés (ma egyre inkább az IKT) nemzetközi szintű koordinációja. Jelenleg 193 ország és több mint 800 akadémiai és gazdasági szervezet számít tagjának. Az ITU három nagy szakmai részre tagozódik: ITU-R (ITU Radiocommunication Sector), azaz a rádiókommunikációért felelős szervezetre, az ITU-T (ITU Telecommunication Standardisation Sector), azaz a nemzetközi telekommunikáció egységesítéséért és szabványosításáért felelős szervezetre, valamint az ITU-D (ITU Development Sector), azaz a nemzetközi infokommunikációs fejlesztésekért felelős szervezetre. (ITU 2017a)

hatóak, 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". [1139/2013. (III. 21.) Korm. határozat]

Ez az első olvasatra valóban meglepő definíció azonban nagyon is reális igényeken alapul. Meglepő a megfogalmazás, hiszen hogyan lehetne a kiberteret Magyarországra vonatkoztatni, amikor annak – azaz a kibertérnek – nemcsak hogy lehetetlen meghatározni a határait, de azok valóban nem is léteznek?

Ugyanakkor például pont a kiberbűnözés vagy akár a kiberhadviselés lehetnek az okai annak, hogy szükséges hazánk vonatkozásában is megjelölni a kiberteret. A megfogalmazásban foglaltak alapján ugyanis lehetőség van arra, hogy majd később a védelem – azaz az incidenskezelés, bűnüldözés, támadások elhárítása, felderítés, esetleges megelőző támadások stb. – ne csak a hazai eseményekre, incidensekre, támadásokra irányuljanak, hanem a földrajzi határokat átlépve jóval szélesebb körben legyen lehetőség mindezeket megtenni.

A kibertér tehát egy olyan, a hálózatok és az elektronikai eszközök alkotta tér, amelyben az információ áramlása az egyik legfontosabb tényező.

Mindezeken túl a kibertér biztonságának tárgyalása során szükséges a gyakran használt „kiberbiztonság" kifejezés bővebb és átfogóbb meghatározása is, hiszen a legfontosabb fogalmak leírásánál csak egy rövid definíciót adtunk erről. A kiberbiztonság meghatározásánál szintén az ITU X.1205 ajánlásgyűjteményét használjuk kiindulópontként, amely szerint a kiberbiztonság nem más, mint „eszközök, politikák, biztonsági koncepciók, biztonsági garanciák, irányelvek, kockázatkezelési módszerek, akciók, a képzés, a legjobb gyakorlatok, a biztonsági technológiák összessége, amelyek célja, hogy megvédjék a számítógépes környezetet, az azt használó szervezet és felhasználók eszközeit. A szervezet és a felhasználói eszközök és rendszerek körébe tartoznak a hálózathoz csatlakoztatott számítástechnikai eszközök, személyek,

infrastruktúra, alkalmazások, szolgáltatások, telekommunikációs rendszerek, valamint a számítógépes környezetben küldött és/vagy tárolt információk összessége". (ITU 2008)

A kiberbiztonság hozzájárul a szervezet és a felhasználók biztonságának megteremtéséhez és annak fenntartásához a számítógépes környezetben megjelenő releváns biztonsági kockázatok kezelésével. Az így megjelenő biztonsági célkitűzések magukba foglalják a bizalmasság (angol megnevezéssel: *confidentiality*), a sértetlenség (angol megnevezéssel: *integrity*) és a rendelkezésre állás (angol megnevezéssel: *availability*) biztosítását.[4] (ITU 2008)

1.1. Digitális ökoszisztéma

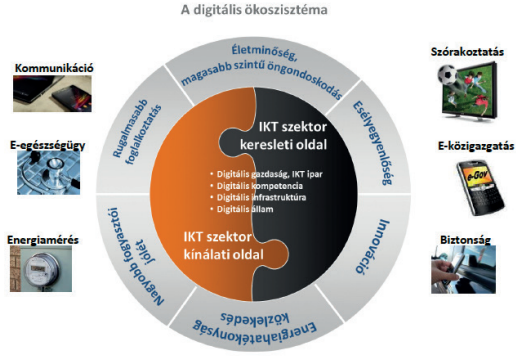
A digitális technológia innovációja, valamint a társadalom egyre nagyobb igénye az új digitális eszközökre és szolgáltatásokra azt eredményezte, hogy napjainkra egyre több országban alakult ki a digitális ökoszisztéma.

Ez a digitális ökoszisztéma a benne foglalt technológia révén hálózatba kapcsolja a felhasználókat, és a hálózatok segítségével eljuttatja számukra a legalapvetőbb digitális szolgáltatásokat is. Ezzel a társadalom is változik, amelyre korábban az egyik legtalálóbb kifejezés a *hálózatos társadalom* volt. A „hálózatos társadalom" fogalmát Manuel Castells spanyol szociológus adta meg, amely szerint az új társadalmat mint hálózatos társadalmat kell felfognunk. Castells szerint az információs társadalom „olyan hálózatos társadalom, ahol a kulcsfontosságú társadalmi rendszerek és tevékenységek elektronikus információs hálózatok köré szerveződnek". (Castells 2005)

[4] Ezekkel a biztonsági célkitűzésekkel jellemezni lehet az adott szervezet kiberbiztonságát (vagy akár a szűkebb értelemben vett információbiztonságát) is. Ennek megfelelően gyakran kiberbiztonsági jellemzőnek is hívják ezeket a tényezőket, amelyeket az angol szavak kezdőbetűiből sokszor CIA-elvnek is neveznek.

A különböző technológiákon alapuló eszközök, rendszerek és szolgáltatások között a határok eltűnnek. A számítógépek (hálózatba kapcsolva), az elektronikus távközlés és az elektronikus média egyre közelebb kerül egymáshoz. Nagyon éles határokat már korábban sem igazán tudtunk megjelölni az informatika és a kommunikáció között, így nem meglepő módon az informatikai és kommunikációs eszközök konvergenciája révén létrejött eszközöket és rendszereket már közel két évtizede „infokommunikációs technológiának" hívjuk. Ma már azonban a szolgáltatások, a felületek és a felhasználás módja is egyre inkább összemosódik. Digitális televíziót nézünk, amely internetelérést és telefont is jelenthet egyben. A mobiltelefonunk olyan „okos" eszköz, amely ma már tényleg egy „virtuális köldökzsinór", hiszen számos olyan funkciót egyesít magában ez az egyetlen eszköz, amely a klasszikus kommunikáción már jóval túlmutat. Ugyanígy azok a határok, amelyek eddig az ember és a technológia között nagyon élesen elkülöníthetőek voltak, szintén egyre inkább elmosódnak.

A társadalom legtöbb funkciója – legyen szó akár az oktatásról, a közlekedésről, az egészségügyről vagy a védelemről – digitális szolgáltatásokra épül. Nagyon gyakran még az emberek magánéletében is meghatározó szerepet kapnak ezek a szolgáltatások.

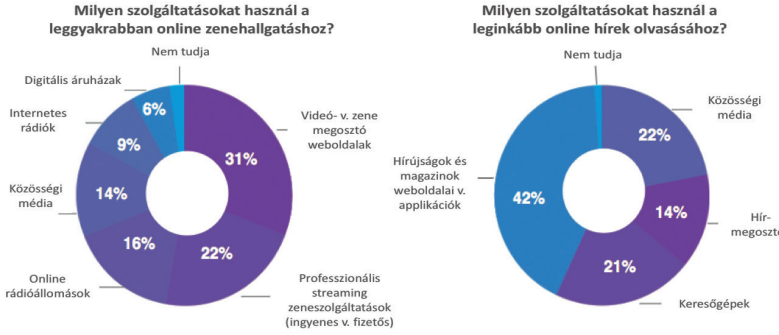


1. ábra
A digitális ökoszisztéma összetevői

Forrás: Nemzeti Infokommunikációs Stratégia (2014)

A 2014-ben megjelent hazai *Nemzeti Infokommunikációs Stratégia 2014–2020* a digitális ökoszisztémával kapcsolatosan így fogalmaz: „[a] digitális ökoszisztéma különböző összetevőinek (nagy sávszélességű elérést biztosító infrastruktúra, képzett és motivált felhasználók, az információs világ vívmányait kihasználó üzleti szféra, fejlett és intenzív K+F+I tevékenységet végző infokommunikációs és informatikai (IKT) ipar (amely ideális terület, a magyar gazdaság egyik fejlesztési fókusza), modern szolgáltató állam, online elérhető közés kereskedelmi szolgáltatások, digitális archívumok stb.) kiegyensúlyozott rendelkezésre állása jelentősen javítja az állampolgárok életminőségét, a vállalkozások versenyképességét és az állami működés hatékonyságát." (Nemzeti Infokommunikációs Stratégia 2014)

A digitális ökoszisztéma alapjaiban változtatta meg életünket.



2. ábra

A digitális forradalom társadalomra gyakorolt hatása: a zenehallgatás és a hírek forrása

Forrás: European Commission (2015a), a szerző szerkesztése

A technológiai fejlődésre az egyik legjellemzőbb példa az adatátviteli sebesség növekedése. Erre alapozva olyan szolgáltatások jöttek és jönnek létre folyamatosan, amelyek eddig elképzelhetetlenek voltak. Az online televízió vagy realtime (azaz valós idejű) videoközvetí-

tés, amely ráadásul full-HD minőségben áll rendelkezésünkre, ma már a mindennapok része.[5] Az IoT milliárdnyi eszközének összekapcsolását lehetővé tevő vezetékes és mobil hálózat teljes egészében lefedi azt a környezetet, ahol élünk.

1.1.1. A mesterséges intelligenciáé a jövő?

Nem mehetünk el szó nélkül a digitális ökoszisztéma tárgyalásakor a már ma is jelen lévő mesterséges intelligencia megemlítése, illetve legalább nagybani felvázolása mellett. Ugyanis ez az a terület, amely már a közeljövőben gyökeresen átalakíthatja az életünket.

Jelenleg a mesterséges intelligencia, röviden csak MI, vagy az angol *Artificial Intelligence,* azaz AI kifejezésekkel élve, ma már a hétköznapi életünk számos területén is egyre nagyobb helyet követel magának. A mesterséges intelligencia egyes elemei ma már nemcsak a gyártásban – például az ipari folyamatokat vezérlő számítógépekben vagy az ipari robotokban –, hanem a közlekedéstől elkezdve (gondoljunk csak az önvezető autók egyre növekvő számára) a telekommunikáción át a logisztikáig, számos helyen megtalálhatóak.

A mesterséges intelligencia területe hatalmas anyagi befektetéseket könyvel el évről évre, hiszen az MI egy olyan verseny, amely számos iparágra meghatározó jelentőségű lesz a jövőben. Az internetes közösségi oldalak és a hozzájuk kapcsolódó szolgáltatások fejlesztésében már ma is az MI-é a vezető szerep, de így van ez a járműgyártásban és akár az egészségügyben is.

Ugyanakkor a mesterséges intelligencia számos árnyoldalára és veszélyére is egyre több figyelmeztetés hangzik el. A bevezetőben már utaltunk Elon Musk, Stephen Hawking, illetve Ray Kurzweil

[5] Ugyanakkor egy nagyon komoly kérdés a különböző rendszerek együttműködési képessége, amely már korábban is számos alkalommal felmerült. Az együttműködés már az információ interoperabilitásában is jelentkezik (Munk 2007), amely megvalósítása nélkül nehéz elképzelni a hatékony digitális ökoszisztémát.

figyelmeztetéseire. Az azonban vitathatatlan, hogy a mesterséges intelligencia rohamos fejlődésének lehetünk tanúi, amely rendkívül izgalmas távlatokat nyit. Már ma is olyan eszközöket és rendszereket használunk, amelyek néhány évtizede elképzelhetetlennek tűntek, és az MI ugyanezt okozhatja a jövőre, ráadásul a közeli jövőre vonatkoztatva.

1.2. Digitális gazdaság és társadalom

20. század végének, illetve a 21. század elejének társadalmára korábbról már számos kifejezés használatos. Olyan kifejezéseket használunk, mint tudástársadalom, információs társadalom,[6] hálózatos társadalom.[7] Ugyanakkor mára egyre inkább a *digitális társadalom* kifejezés az elterjedtebb, amely bár egy szűkebb értelmezést jelent, alapvetően kifejezi a társadalom digitális technika és technológia iránti egyre inkább növekvő igényét, sőt a társadalom ezekkel az eszközökkel és rendszerekkel szembeni egyre nagyobb függőségét is reprezentálja.

Napjainkban a digitális gazdaság és társadalom fejlettsége különböző, az információtechnológiához kapcsolódó mérőszámokon keresztül megítélhető. Területi, illetve országonkénti lebontásban ezek a mérőszámcsoportok pedig viszonylag jó összehasonlítást is lehetővé tesznek. Ez azért fontos, mert ez alapján lehetséges a források megfelelő allokációja, a befektetések serkentése, illetve azokon a területeken, ahol erre szükség van, a versenyképesség eléréséhez és növeléséhez politikai, gazdasági, illetve társadalmi ösztönzés kiemelten fókuszálható.

---

6 Az információs társadalmat legtöbbször úgy jellemzik, mint „[a] tudomány eredményeinek intenzív és folyamatos felhasználására alapozott, új típusú termelési és társadalmi alapmodell, amelyet tartalma alapján intenzív tudásgazdaságnak és tudástársadalomnak neveznek". (Haig–Kovács 2012)

7 A már korábban említett M. Castells jellemzése és meghatározása rendkívül jól illik napjaink társadalmára. A hálózatok sokasága nemcsak technikai értelemben vett fejlődést jelent, hanem átalakítja a társadalom nagyon sok funkcióját is.

Kezdjük rögtön az Európai Unió mérőszámrendszerével. Az Európai Unió álláspontja szerint az infokommunikációs technológiák már nem külön ágazatot alkotnak, hanem napjaink gazdasági rendszereinek meghatározó alapját képezik. Az Európai Unió 2015-ben kiadott *Európai digitális egységes piaci stratégiájában* az Európai Bizottság elnöke így fogalmaz: „Az internet és a digitális technológiák a gazdaság és a társadalom valamennyi szektorába való intenzív beágyazódás révén minden szinten átalakítják életvitelünket és munkamódszereinket: egyénenként, az üzleti világban és a közösségben is." (European Commission 2015b)

Mindezek alapján nyilvánvaló, hogy a társadalom, illetve a gazdaság digitalizációjának, azaz azoknak a tényezőknek, hogy az adott ország társadalmi és gazdasági feladatai, illetve funkciói mennyiben integrálják, mennyiben épülnek a digitális technikára és technológiára, a mérése szükséges.

Egy ilyen mérési módszer az Európai Unió digitális gazdaság és társadalom indexe (Digital Economy and Society Index – DESI). Ez egy többelemű, összetett (kompozit) index, amely összefoglalja Európa digitális teljesítményét, és nyomon követi az EU tagországainak fejlődését, valamint digitális versenyképességét. (European Commission 2017)

A DESI öt eltérő, de nyilvánvalóan a digitalizációval összefüggő területen méri a gazdaság és a társadalom fejlettségét. Ezekkel a számokkal természetesen egy jelenlegi állapotot tudunk bemutatni, valamint az elmúlt évek számsorait egymás mellé téve tudunk a fejlődés trendjeire következtetéseket levonni. Ugyanakkor a fejlődés várható mértékére, illetve ütemére ezek a múltbeli trendek nagy biztonsággal eligazítást adnak, de nem biztos, hogy valós és teljes lesz a kép, hiszen számos olyan tényezőt is figyelembe kell, illetve kellene vennünk, amelyek előre nem, vagy csak nagy bizonytalansággal jelezhetőek. Az egyik ilyen tényező az, hogy a technológiai fejlődés különböző ütemekben valósul meg. Azaz csak látszólag exponenciális a fejlődés íve, de ez korántsem mentes a kisebb-nagyobb zökkenőktől, kilengésektől.

Az egyik oldalon ott vannak a változó felhasználói igények, amelyek bár előre jelezhetőek, mégsem mindig pontosak ezek a predikciók (gondoljunk csak a 2000-es évek WAP[8] szolgáltatására, illetve annak kudarcára), a másik oldalon pedig a gyártástechnológia fejlődésének kisebb-nagyobb egyéb – általában műszaki és technikai okokra visszavezethető – kilengései okozzák azt, hogy nem lehet mindig pontos az előrejelzés.

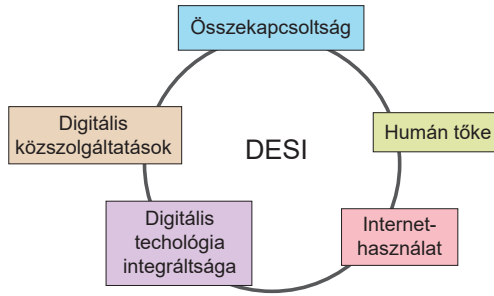
Az említett 5 fő terület, azaz indikátorcsoport – az összekapcsoltság, a humán tőke, az internethasználat, a digitális technológiák integráltsága és a digitális közszolgáltatások – több, mint 30 további indikátort tartalmaz. Egy ország átlag DESI-a a fő területek pontszámainak és a részterületek pontszámainak egyedi súlyozott átlagából tevődik össze. A számítást alapvetően az Európai Bizottság szakértői végzik az adott ország Eurostatnak szolgáltatott adatsorai alapján. A kapcsolati sebesség és a digitális készségek az adott ország átlagos pontszámának 25%-át, a digitális technológia integrációja 20%-át, az internethasználat és a digitális közszolgáltatások pedig 15%-át adják.

A DESI 0 és 1 között osztályozza az adott ország, illetve az Európai Unió fejlettségét. Minél jobb egy ország teljesítménye, azaz a mutatószámok alapján minél fejlettebb az adott ország digitális gazdasága és társadalma, az eredmény annál közelebb áll az 1-hez. (European Commission 2016a)

Az *összekapcsoltság-indikátorcsoport* méri többek között a szélessávú internetes infrastruktúrát és annak minőségét. A gyors és szélessávúinternet-alapú szolgáltatások az Európai Unió álláspontja szerint szükséges feltételek a gazdasági és társadalmi versenyképesség

[8] WAP: azaz Wireless Application Protocol, a vezeték nélküli adatátvitel egyik nyílt nemzetközi szabványa. Az 1990-es évek legvégén a hordozható eszközökhöz (mobiltelefonok, PDA-k) fejlesztették ki. A protokollcsalád fő célja a webalapú böngészés támogatása, de csökkentett funkciókkal. Ugyanakkor az okostelefonok *(smartphones)* 2007-től tartó robbanásszerű elterjedése miatt azok közel teljes értékű webböngészést, valamint egyéni internetes szolgáltatást és tartalmat elérhetővé tevő jellemzői miatt, ha nem is halt ki, de igazi fénykora sohasem alakult ki, és nem is igazán terjedt el olyan széles körben, mint ahogy azt várták a megalkotásakor.

eléréséhez. Ebben az indikátorcsoportban a legmagasabb pontszámot 2016-ban Hollandia érte el, majd Luxemburg és Belgium következett a sorrendben. Ezen indikátor tekintetében a leggyengébben Horvátország, Bulgária és Lengyelország teljesített 2016-ban. A vezetékes szélessávú internet az európaiak 98%-a számára elérhető, és 76%-uk számára a nagy sebességű, azaz legalább 30 Mbps vagy a fölötti sebesség is rendelkezésre áll. A 4G mobilhálózatok átlagosan az EU lakosságának 84%-ához eljutnak. Ezen felhasználók 74%-a szélessávú kapcsolatot, és több mint egyharmada nagysebességűinternet-előfizetést is választ a szolgáltatáshoz. (European Commission 2017a)



3. ábra
A DESI fő mérőszámcsoportjai

Forrás: European Commission 2016b, a szerző szerkesztése

A *humán tőke indexe,* azaz a humán készségek indexe azokat a mutatókat méri, amelyek azt értékelik, hogy az egyén vagy társadalmi csoport mennyire tudja a digitális társadalom által nyújtott lehetőségeket kihasználni. Ezek a készségek az alapvető felhasználói ismereteket jelentik, amelyek lehetővé teszik az egyénnek, hogy az online térben eligazodjon, a digitális termékeket és szolgáltatásokat megvegye vagy használja, illetve azokat a fejlett készségeket is idesorolják, amelyek képessé teszik a munkaerőt arra, hogy a technológia révén fokozzák a termelékenységet és a gazdasági növekedést. A DESI szerint ezen mutató alapján Dánia, Luxemburg, Finnország, Svédország

és Hollandia szerezte a legmagasabb pontszámot 2016-ban, ugyanakkor Románia, Bulgária, Görögország és Olaszország kapta a legalacsonyabb értékeket. A DESI szerint az európaiak 44%-a még mindig nem rendelkezik alapvető számítógépes ismeretekkel. Ugyanakkor pozitív hír lehet Európa számára, hogy – bár csak közvetve tartozik ehhez az indexhez – az úgynevezett természet- és mérnöki tudományokban (Science, Technology, Engineering and Mathematics, STEM), 1000 emberre vetítve a 20−29-es korosztályból már 19-en szereztek diplomát 2014-ben, amely előrelépés a 2012-es 12 fős számhoz képest. Ez a mutató szintén hozzájárulhat Európa versenyképességéhez, hiszen a technológiai szektorban tanult diplomások komoly hatással lehetnek a fejlődésre, és így közvetlenül vagy közvetve a társadalom egészére pozitív hatást gyakorolhatnak. (European Commission 2017a)

A DESI-csoport következő tagja az *internethasználatot* méri. Az index nemcsak azt mutatja meg, hogy egy adott országban hányan használják az internetet, hanem azt is, hogy milyen tevékenységeket végeznek a felhasználók az interneten vagy annak segítségével. Ilyen tevékenységek például az online tartalmak – videóletöltések, zenehallgatás, online játékok stb. –, illetve a korszerű kommunikációs módok vagy az online vásárlás és e-banki szolgáltatások igénybevétele. Az internethasználat-index esetében 2016-ban a legaktívabb Dánia, Svédország, Luxemburg és Hollandia volt. Ebben a mérőszámban szintén Románia, Bulgária és Olaszország teljesített a leggyengébben a 28 EU-tagországon belül. Az unió országainak internethasználat-számainak és -szokásainak indexálása alapján a tagországokban az online hírolvasás (70%), a videó és/vagy audiokommunikációs hívások (39%), a közösségi hálózatok használata (63%), az online vásárlás (66%) vagy az online bankolás (59%) kismértékben növekedtek az elmúlt néhány évben. (European Commission 2017a)

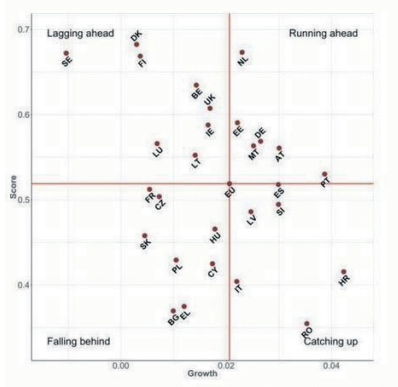
A *digitális technológia integrációs index* a vállalkozások digitalizációját, illetve az abban rejlő olyan lehetőségek kiaknázását, mint például az online értékesítési csatornák igénybevétele, méri. Ahogy korábban utaltunk rá, a digitális technológia széles körű alkalmazása,

valamint annak az üzletmenetbe való integrációja növeli a vállalkozások hatékonyságát, csökkenti a költségeket, ösztönzi és növeli a munkatársak, továbbá az üzleti partnerek aktivitását. Mindezeken túl egy üzleti vállalkozás számára az online kereskedelmi felület szélesebb körű piaci hozzáférést biztosít, valamint magában hordozza a növekedési potenciált. Ennek az indexnek a vonatkozásában Dánia, Írország és Finnország vállalkozásai teljesítettek a legjobban, illetve Románia, Lengyelország és Bulgária a leggyengébben 2016-ban. Összességében az index alapján megállapítható, hogy az európai vállalkozások egyre jobban alkalmazkodnak a digitális technológiákhoz, amely többek között az üzleti szoftverek, az elektronikus információmegosztás, az elektronikus számlázási területeken vagy az ügyfelekkel és partnerekkel a közösségi médiumokon való kapcsolattartásban is megnyilvánul. Az e-kereskedelem a kis- és közepes vállalkozások (KKV-k) esetében is nőtt európai átlagban (2014-ben a korábbi éves 15%-ról 17%-ra). Ugyanakkor az Eustat adatai alapján a KKV-knak csak kevesebb mint a fele értékesít egy másik uniós tagállamban is. (European Commission 2017a)

A *digitális közszolgáltatások indexe* elsősorban az e-kormányzati eszközöket, rendszereket, illetve azok használatát méri. A korszerű digitális közszolgáltatások növelik a közigazgatás hatékonyságát, aminek haszonélvezői elsősorban természetesen az állampolgárok, illetve a vállalkozások. Európa éllovasai a digitális közszolgáltatások terén Észtország, Finnország és Hollandia, a leggyengébb teljesítményt ezen a területen Románia, Magyarország és Horvátország nyújtotta 2016-ban. Európai uniós összesítésben a digitális közszolgáltatások kismértékű javulást, illetve fejlődést mutatnak (az EU-tagállamok összesített digitális közszolgáltatások indexe a 2015-ös 75-ről 2016-ban 82-re nőtt). (European Commission 2017a)

Ezeket az indexeket az Európai Unió – figyelembe véve az előző évek fejlődését (néhány esetben visszafejlődését) – összegezte, majd összevetette a tagországok teljesítményét az európai átlaggal. Az összegzés szerint 2016-ban digitális társadalom és gazdaság

tekintetében kiemelkedően fejlett[9] országok Ausztria, Észtország, Németország, Málta, Hollandia és Portugália, mert ezeknek az országoknak a (DESI alapján kapott) pontszáma meghaladja az uniós átlagot, és ez a pontszám gyorsabban nőtt, mint az EU-s átlag az elmúlt évben. Ráadásul ezekben az országokban a fejlődés olyan ütemű, hogy az lehetővé teszi számukra az EU-átlag fölötti teljesítést továbbra is.



4. ábra
Az Európai Unió tagországainak DESI alapján elfoglalt helye 2016-ban

Forrás: European Commission 2016b

Az éllovas országoktól kissé lemaradva, de még mindig az élmezőnyben található[10] Belgium, Dánia, Finnország, Írország, Litvánia, Svédország és az Egyesült Királyság. Ezeknek az országoknak a pontszáma még mindig meghaladja az EU átlagát, de a pontszámuk már lassabban növekedett, mint az EU-átlag. Ezek tehát jól teljesítő országok, de a digitális gazdaság és társadalom fejlesztési üteme már lassabb, mint az éllovas országoké.

9 Az EU ezeket az országokat az angol *running ahead* kifejezéssel illeti.
10 Az EU ezeket az országokat az angol *lagging ahead* kifejezéssel jellemzi.

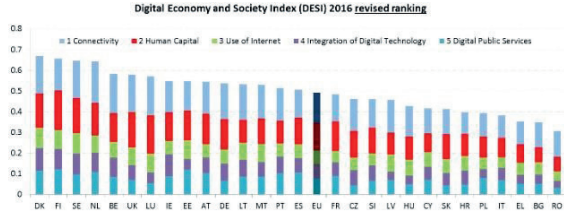
Az Európai Unió a felzárkózó jelzővel[11] illeti Horvátországot, Olaszországot, Lettországot, Romániát, Spanyolországot és Szlovéniát, mert ezek az országok már EU-átlag alatt teljesítenek a DESI által mért területeken. Ugyanakkor ezen országok pontszáma még mindig gyorsabban nőtt, mint az EU-átlag. Összességében ezekben az államokban a digitális gazdaság és társadalom fejlődése gyorsabb, mint az EU-átlag, és így megvan a lehetőségük az uniós átlaghoz való felzárkózásra.

Ezt követően találhatjuk a lemaradó országokat, nevezetesen Bulgáriát, Ciprust, a Cseh Köztársaságot, Franciaországot, Görögországot, Magyarországot,[12] Lengyelországot és Szlovákiát. Ezeknek az országok-

[11] Az EU ezekre az országokra az angol *catching up* kifejezést használja, a lemaradó országokra pedig az angol *falling behind* kifejezést használja.

[12] Magyarország teljesítménye főleg annak tükrében tűnik gyengének, hogy hazánk már több, mint másfél évtizede deklarálta elkötelezettségét az információs társadalom építése mellett. Először 2001-ben alkotta meg az akkori kormány a Nemzeti Információs Társadalom Stratégiát (NITS), amely több programmal – Infrastruktúra-fejlesztési Program, Gazdaságpolitikai Program, Kultúra Program, Oktatási Program, Társadalompolitikai Program, Elektronikus Kormányzati Program, Önkormányzati Program – volt hivatott fejleszteni az ország információs (digitális) képességeit. Ráadásul ezt a stratégiát 2003-ban egy újabb stratégia – a *Magyar Információs Társadalom Stratégia* (MITS) – követte. (Haig–Kovács 2012)
E stratégia fő céljai – tudásalapú gazdaság, információs társadalom létrehozása, valamint ezeken keresztül az egyének és a közösség életminőségének javítása – visszaköszönnek a 2010-ben megszületett Európai Digitális Menetrend céljai között. Világosan látszik tehát, hogy Magyarország stratégiai elképzelései és tervei közel egy évtizeddel megelőzték az európai közös gondolkodást, de ez mégsem vezetett oda, hogy hazánk a terület éllovasa legyen hosszú távon. Ugyanakkor meg kell jegyezni, hogy a magyar kormány 2016-ban Digitális Jólét Program (DJP) névvel a digitális gazdaság és társadalom fejlesztése érdekében számos stratégiát magába foglalva átfogó koncepciót dolgozott ki. A DJP keretében eddig elkészült stratégiák: Magyarország Digitális Gyermekvédelmi Stratégiája, (Digitális Jóléti Program 2017a), Magyarország Digitális Exportfejlesztési Stratégiája (Digitális Jóléti Program 2017b), Magyarország Digitális Oktatási Stratégiája (Digitális Jóléti Program 2017c), Magyarország Digitális Startup Stratégiája (Digitális Jóléti Program 2017d). A DJP magába foglalja a Digitális Magyarország programot is, amely célja olyan átfogó infokommunikációs fejlesztés, amely alapján minden háztartás számára lehetőség lesz gyors internet elérésének igénybevételére. A DJP számos olyan pályázati lehetőséget is takar, amely hátrányos helyzetű társadalmi rétegek vagy elmaradottabb, fejletlenebb régiók számára nyújt digitális eszközökhöz és szolgáltatásokhoz való hozzáférést.

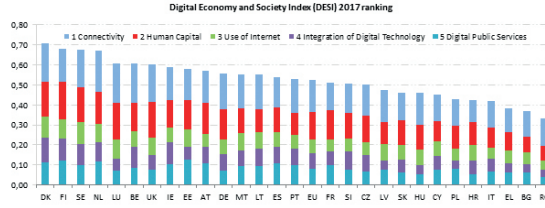
nak a digitális gazdaság és társadalom területein mutatott teljesítménye az uniós átlag alatt van, és a vizsgált területeken az elmúlt években lassabb volt a fejlődés, mint az EU egészében, ráadásul ez a lassú növekedés gátolja az EU-átlaghoz való felzárkózást is. (European Commission 2016b)



5. ábra

Az Európai Unió tagországainak DESI index alapján elfoglalt helye 2016-ban

Forrás: European Commission 2016c



6. ábra

Az Európai Unió tagországainak DESI index alapján elfoglalt helye 2017-ben

Forrás: European Commission 2017a

Magyarország DESI indexe

2016-ban Magyarország összesített eredménye a DESI alapján 0,43 volt, amellyel a 20. helyet foglalta el a 28 uniós tagállam között. Magyarország az internethasználat szempontjából az uniós átlag fölötti szintet ért el, viszont az összekapcsoltság és a humán tőke tekintetében pedig kevéssel átlag alattit. A legnagyobb lemaradás – hasonlóan a korábbi évekhez – a digitális technológiák üzleti integráltsága, valamint a digitális közszolgáltatások területén volt. Ugyanakkor a nagy sebességű széles

sávú szolgáltatások elérhetősége és terjedése, valamint a közösségi oldalak használata meghaladja az európai átlagot.

Összességében Magyarország eredménye az uniós átlagnál alacsonyabb volt, ráadásul az elmúlt évek során lassabb ütemben növekedett az európai uniós átlagnál. Így Magyarország a lemaradó országok csoportjába tartozott 2016-ban. (European Commission 2016a)

2017-ben hazánk az előző évi helyezéséhez képest egy helyet rontva a 21. helyen állt a DESI alapján összehasonlított uniós országok ranglistáján. Az ország DESI-eredménye 0,46 volt, amely magasabb pontszám, mint a 2016-os eredmény, de időközben az EU-s DESI-átlag értéke is emelkedett (0,49-ről 0,52-re). Magyarország 2017-ben is jól teljesített az összekapcsoltság területén, köszönhetően a nagy sebességű vezetékes széles sávú és a 4G-s mobilrendszerek elterjedtségének. Az előző évihez képest Magyarország javított a digitális készségek területén, bár kismértékben csak, de továbbra is elmarad az átlagos szinttől. Ugyanakkor ebben az évben is a legnagyobb kihívás és így a legnagyobb lemaradás a vállalkozások IKT-eszközök, rendszerek és szolgáltatások használatának csekély mértékében, valamint az e-government (digitális közszolgáltatások) alacsony fejlettségében keresendő. (European Commission 2017b)

Mindezek fényében a bemutatott számokból és a fenti tényekből (akár a százalékos arányokból, akár az egyes tagországok EU-s átlaghoz viszonyított helyzetéből) világosan látható, hogy Európa korántsem egységes a digitális gazdaság és társadalom tekintetében. Ennek megfelelően az Európai Bizottság egy európai *Digitális Egységes Piaci Stratégia*[13] megalkotása és végrehajtása mellett döntött 2015-ben. A stratégia egyik, az Európai Bizottság által megfogalmazott jelmondata: „Bontsuk le a korlátokat, hogy feltárjuk az online lehetőségeket!”[14]

[13] A stratégia angol címe: *Digital Single Market.*

[14] A stratégia jelmondata angolul: *“Bringing down barriers to unlock online opportunities.”* (European Commission 2017c)

A stratégia legfontosabb célja a digitális gazdaság kiterjesztése, amely magában hordozza annak a lehetőségét, hogy a fogyasztók kedvezőbb áron jussanak – ráadásul a versenyre kényszerített szolgáltatók által nyújtott – egyre színvonalasabb szolgáltatásokhoz. Ezzel a kis- és középvállalkozások növekedési potenciálja is nőhet. A stratégia egyik legfontosabb alkotóeleme a digitális szabad piac mellett a biztonság, amelyet a későbbiekben részletesen is elemezni fogunk. Mindezek mellett a stratégia a fogyasztók és a vállalkozások számára meg kívánja könnyíteni, hogy Európa-szerte egységes elvek mellett és könnyebben jussanak hozzá a termékekhez és szolgáltatásokhoz. A terv javítani kívánja a digitális hálózatok és szolgáltatások növekedési és terjeszkedési feltételeit, valamint természetszerűleg a stratégia egyes lépéseinek megvalósításával markánsan hozzá kíván járulni az európai digitális gazdaság növekedéséhez. (European Commission 2015b)

A stratégiában megfogalmazott célkitűzéseket számos olyan intézkedésen keresztül kívánja az Európai Unió elérni, mint amilyen a határokon átnyúló online értékesítési szabályok megreformálása. Ennek elérése érdekében az Európai Bizottság a digitális tartalmak – például alkalmazások, elektronikus könyvek – vásárlására vonatkozó uniós szabályokat, a fizikai termékek határokon átnyúló online értékesítésével kapcsolatos jogokat, illetve a fogyasztói jogokat is egységesíteni kívánja az EU-tagországokban. Az Európai Bizottság által javasolt intézkedéscsomag tartalmazza a határokon átnyúló csomagküldés fejlesztését, illetve a területi alapú tartalomkorlátozás megszüntetését, amellyel azt a korlátozást szüntetnék meg, ami akadályozza, hogy a fogyasztók elérjenek más uniós tagállamban működtetett honlapokat, illetve – a fogyasztók tartózkodási helyétől függően – eltérő árat kelljen fizetniük. Nagyon fontos intézkedések közé tartozik az európai szerzői jogi szabályozás reformja is, amely magában foglalja a tartalomszolgáltatások – például a videószolgáltatások – határokon átnyúló igénybevételének szabadabbá tételét, azaz hogy egy tagországban megvásá-

rolt film vagy zene korlátozás nélkül legyen nézhető, illetve hallgatható egy másik országban. (European Commission 2015b)

Az Európai Bizottság a digitális hálózatok és szolgáltatások növekedési és terjeszkedési feltételeinek javítása érdekében az uniós távközlési szabályok reformját is előirányozta. Ez magában foglalja a rádióspektrum kiosztásának és felhasználásának egyszerűbbé és könnyebbé tételét, a terület koordinációjának elősegítését, valamint a nagy sebességű széles sávú számítógép-hálózati infrastruktúrába való beruházások ösztönzését, amellyel a szabályozási intézményi keret fejlesztése is együtt jár.

A bizottság az audiovizuális média szabályozásának felülvizsgálatát is tervbe vette, amely kiterjed az audiovizuális médiaszolgáltatások irányelveire, a különböző európai műveket (film, zene, kép, egyéb művészeti tartalom) támogató intézkedésekre, valamint a kiskorúak védelmét szolgáló és a reklámokra vonatkozó szabályokra. Az intézkedéscsomagban helyet kap az online platformok szerepének értékelése is, amely során például az online platformok által gyűjtött adatok felhasználását is elemzik.

A biztonsággal is kapcsolatos egyik nagyon fontos intézkedés a felhasználók személyes adatainak a digitális szolgáltatások keretében végzett kezelése, annak biztonságosabbá, megbízhatóbbá és a felhasználók számára megnyugtatóbbá tétele, ami azonban az uniós adatvédelmi szabályozás áttekintését is magával kell, hogy hozza.[15] A bizalom fokozása a kiberbiztonság növelését is igényli. A kiberbiztonság javítása számos más stratégiát és intézkedést jelent uniós szinten.

[15] Ez meg is valósult, hiszen elfogadták az úgynevezett GDPR-irányelvet, azaz az EU általános adatvédelmi irányelvét, amelyet később részletesen is elemzünk.

Ezek közül talán a legfontosabbak az *Európai Digitális Menetrend*[16] részét képező *EU kiberbiztonsági stratégia*[17] (2013), valamint az úgynevezett *NIS-irányelvek*[18] (2016).

Európai Digitális Menetrend
Az Európai Digitális Menetrend az Európa 2020 stratégia részét képezi, ezen belül is az abban megfogalmazott hét pillér egyike. A 2010-ben kiadott digitális menetrend legfontosabb célja, hogy az unió tagországai számára egységes digitális piac révén fenntartható gazdasági és szociális előnyöket teremtsen. Mindezek alapfeltétele a nagy sebességű internet és az interoperabilitás kialakítása. A menetrend feltárja az Európai Unió meglévő gazdasági és társadalmi hiányosságait (például digitális piac szétaprózottsága, az interoperabilitás hiánya, számítógépes bűnözés terjedése, hálózati beruházások hiánya, nem megfelelő K+F tevékenység, digitális írástudás alacsony szintje), majd ezek kiküszöbölésére, illetve az uniós digitális területek fejlesztésére intézkedéseket határoz meg. Ilyen intézkedéseknek minősülnek például az egységes digitális piac létrehozása, a könnyebb tartalomhozzáférés, a nemzetközi tranzakciók

16 A 2008-as gazdasági világválság rámutatott arra, hogy az európai gazdaság nemcsak tagállami, hanem uniós szinten is komoly kitettséggel és sérülékenységgel rendelkezik. Ezt felismerve az Európai Bizottság 2010-ben *Európa 2020* címmel stratégiát hirdetett meg. Maga a stratégia öt fő célkitűzést fogalmaz meg a foglalkoztatás, a kutatás és fejlesztés, éghajlat-politika és ezzel kapcsolatosan az energiaügy, az oktatásügy, a társadalmi befogadás és szegénység elleni küzdelem területeken. Mindezeken túl a stratégia hét kiemelt kezdeményezést, úgynevezett pillért és alpillért tartalmaz. Az első pillér a kiemelt növekedés, amely magában foglalja az *Európai Digitális Menetrendet,* az *Innovatív Uniót* és a *Mozgásban az ifjúság* kezdeményezést. A második pillér a fenntartható növekedés, amely az *Erőforrás-hatékony Európa,* valamint az *Iparpolitika a globalizáció korában* című terveket határozza meg. A harmadik pillér az inkluzív növekedés, amely integrálja az *Új készségek és munkahelyek menetrendjét,* illetve a *Szegénység elleni európai platformot.* (Europe 2020 Strategy 2010)

17 Az EU kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér. (Cybersecurity Strategy of the European Union 2013)

18 Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. (NIS Directive 2016)

egyszerűsítése, a távközlési szolgáltatások egységes piacának erősítése, a közös szabványok kialakítása, a bizalomerősítés a digitális szolgáltatásokkal kapcsolatosan, a nagy sebességű internet és hálózati szolgáltatások létrehozása, valamint aktívabb és hatékonyabb K+F támogatása.

Ahogy korábban már utaltunk rá, mind az EU kiberbiztonsági stratégiáját, mind a NIS-irányelveket külön, részletesen is bemutatjuk, majd elemezni is fogjuk. Ugyanakkor ehelyütt már csak a téma relevanciája miatt is, talán nem érdemtelen felvillantani e stratégiáknak a legfontosabb alapvetéseit.

Az EU kiberbiztonsági stratégiája

Az Európai Unió a 2013-ban született kiberbiztonsági stratégiájában nem vállal kevesebbet, mint azt, hogy a digitális gazdaság biztonságos fejlődésének lehetővé tétele érdekében létrehozza a világ legbiztonságosabb internetes környezetét. Maga a stratégia az EU hivatalos megfogalmazása szerint az európai telekommunikációs rendszerek meghibásodásának és az azok ellen indított támadásoknak a megelőzésére, illetve az ilyen esetekre kidolgozott válaszlépésekre vonatkozó egységes uniós stratégiai elképzeléseket tartalmazza. A javaslatot 2013 februárjában két részben tették közzé, amelyből az első rész az Európai Bizottság, valamint a külügyi és biztonságpolitikai főképviselő közleménye az EU kiberbiztonsági stratégiájáról. A második rész az Európai Bizottság irányelvjavaslata a hálózat- és az információbiztonsággal kapcsolatban. (Cybersecurity Strategy of the European Union 2013)

A stratégia öt alapelvre épül, amelyek prioritásként jelennek meg az Európai Unió kiberbiztonsággal kapcsolatos jövőbeli elképzeléseiben. Ez az öt alapelv a kibertámadásokkal szembeni ellenálló képesség megteremtését, a kiberbűnözés drasztikus visszaszorítását, a kibervédelmi politika kidolgozását és annak a közös biztonság- és védelem-

politikába való beágyazását, illetve a tagállamok kibervédelmi képességeinek fejlesztését, a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtését, az EU által képviselt, a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozását, valamint az alapvető uniós értékek terjesztését célozza meg. (Cybersecurity Strategy Of The European Union 2013)

Mindezeken túl az Európai Unió 2017 őszén az európai kiberbiztonság átfogó reformját kezdeményezte, amely magában foglalja a stratégia felülvizsgálatát is.

Ez a reform – a NIS-irányelvet mint az egyik legfontosabb rendezőelvet szem előtt tartva – három pillérre támaszkodva kívánja megteremteni az új európai kiberbiztonságot. A pillérek pedig a következők: ellenálló képesség *(resilience)* megteremtése, elrettentés *(deterrence)* és védelem *(defence).* A javaslatcsomag magában foglalja az ENISA-ra épülő új Európai Uniós Kiberbiztonsági Ügynökség felállítását, valamint egy olyan új európai tanúsítási rendszer kialakítását, amely a digitális termékek és szolgáltatások biztonságos használatát hivatott garantálni. (European Commission 2017d)

NIS-irányelv

Az EU korábban említett kiberbiztonsági stratégiájának fontos része a hálózat- és információbiztonságra vonatkozó irányelv (NIS Directive – Network and Information Systems Directive, azaz hálózati és információs rendszerek irányelve). Az irányelv tervezetét már 2013-ban, azaz az EU kiberbiztonsági stratégia elfogadását követően napirendre tűzte mind az Európai Parlament, mind az Európai Bizottság. Az eredeti elképzelés szerint az Európai Unió előírta volna a tagállamok számára egy saját NIS-stratégia kialakítását (nyilvánvalóan az EU NIS-irányelvének alapjaira építve), valamint egy olyan nemzeti NIS-hatóság kijelölését is megcélozták, amelynek megfelelő erőforrásokkal kell rendelkeznie a kockázatok és incidensek megelőzé-

séhez, az azokra adandó válaszlépések megtételéhez és kezeléséhez. Mindezeken túl a NIS-irányelv javaslata a tagállamok és a bizottság közötti együttműködési mechanizmus kidolgozását is tartalmazta, amely alapján lehetővé válna az incidensekre vonatkozó adatok korai riasztással történő megosztása, az információcsere és a hálózatokkal, illetve informatikai rendszerekkel szembeni fenyegetésekkel és eseményekkel szembeni közös fellépés. Az eredeti irányelvjavaslatnak fontos eleme volt, hogy egyes informatikai vállalatok és szolgáltatók számára előírják speciális kockázatkezelési eljárás kidolgozását, valamint a jelentősebb informatikai biztonsági események bejelentését az illetékes nemzeti hatóságnak. Ugyanakkor közel hároméves tárgyalássorozat eredménye lett, hogy magát az irányelvet 2016 nyarán mind az Európai Parlament, mind az Európai Bizottság végül elfogadta. (European Commission 2017e)

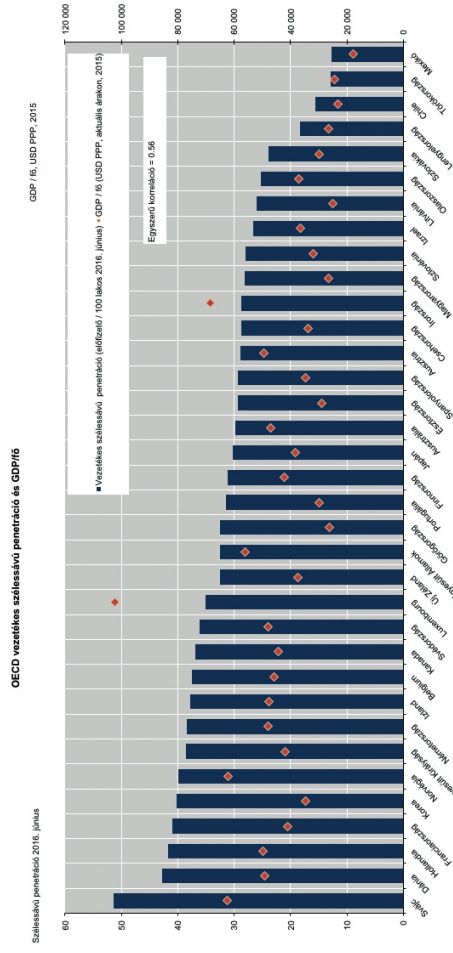
1.2.1. Internethasználat: mit mutatnak a számok?

Ahogy a korábbiakban bemutatott, a digitális gazdaságot és társadalmat átfogó módon értékelő DESI-nál utaltunk rá, szoros összefüggés mutatkozik egy adott ország gazdasági teljesítőképessége, valamint a szélessávúinternet-elérés mértéke között. A digitális gazdaság, illetve a digitális ökoszisztéma egyik megnyilvánulása tehát pozitív módon abban jelentkezik, hogy minél nagyobb a digitális technológia társadalomba, illetve az adott ország gazdaságába történt integrációja, annál inkább érzékelhető a gazdaság növekedési képessége. Ha vetünk egy pillantást a legnagyobb gazdasági telesítőképességgel rendelkező országokra, és megvizsgáljuk az adott ország szélessávúinternet-elérésének teljes lakossághoz viszonyított arányát, szoros korrelációt figyelhetünk meg a két tényező között. Ennek megfelelően nagy biztonsággal kijelenthetjük, hogy abban az országban, ahol magas a szélessávúinternet-elérés aránya, ott a gazdaság teljesítőképessége, illetve az erre mérőszámként használt GDP is magasabb.

Ugyanakkor a szélessávúinternet-elérés, valamint az ehhez szorosan kapcsolódó széles sávú technológiák lehetősége és annak elérése a gazdasági teljesítőképesség növekedése mellett (vagy annak részeként), számos más helyen is pozitív hozadékkal jár. A rövid idő alatt nagy mennyiségű adat továbbítása (le- és/vagy feltöltése), illetve az ilyen adattranszfer mellett, azzal párhuzamosan más szolgáltatások megbízható elérése a felhasználók számára mindenképpen pozitív eredményt ígér, hiszen ez teszi lehetővé az e-kereskedelem, a távmunka vagy akár az online távoktatás (e-learning vagy blended learning) egyre szélesebb körű elterjedését.

Mindezek alapján érdemes megvizsgálni, hogy egy-egy országban hogyan alakul az internetpenetráció, azaz milyen az internetfelhasználók százalékos aránya a teljes lakossághoz viszonyítva, majd arra is érdemes néhány pillantást vetnünk, hogy hogyan alakulnak a szélessávúinternet-elérés lehetőségei, valamint ezzel összefüggésben, milyen arányú azoknak a száma egy adott országban, akik nem használják az internetet.

Részletes vizsgálatainkat a visegrádi országokra (V4-ek) – Csehország, Lengyelország, Magyarország és Szlovákia –, valamint Ausztriára korlátozzuk, ugyanakkor mielőtt ezeket az országokat megvizsgálnánk, általános kitekintést teszünk az európai térségre és a világ országaira.



7. ábra
Néhány fejlett ország (vezetékes) szélessávúinternet-elérésének és az adott ország GDP értékének viszonya

Forrás: OECD 2015/2016, a szerző szerkesztése

A világ internethasználata számokban

A világ népessége megközelíti a 7,5 milliárd embert 2017-re, és ez a szám feltételezhetőleg el is éri vagy talán meg is haladja a 7,5 milliárdot 2018-ra. Egyes adatok szerint a világ népességének majdnem a fele rendszeresen használja az internetet, hiszen a 2016-os év végi statisztikai adatokból kiderül, hogy a világon közel 3,7 milliárd ember számít internetfelhasználónak. A 2000-től eltelt időszakban ez a szám, azaz azinternetet rendszeresen használók száma megtízszereződött.

A régiónkénti eloszlás azonban nem homogén. Óriási különbségek vannak a kontinensek, illetve a különböző régiók között a felhasználók számának alakulásában. Amíg Ázsiában több, mint 55%-os az internetpenetráció (miközben ebben a régióban tizenötszörösével nőtt az internethasználók száma az elmúlt 7 évben), addig Afrikában ez az arány csak 16% körüli.

1. táblázat
A világ internetpenetrációja

Régiók	Népesség (2017-es becslés) *millió fő*	Népesség %-a	Internet-használók száma (2016. 12. 31) *millió fő*	Internetpe-netráció ará-nya (népes-ség %-ában)	Növekedés (2000–2017)
Ázsia	4148	55,2%	1856	44,0%	1523%
Európa	822	10,9%	630	76,7%	500%
Latin-Amerika	647	8,6%	384	59,4%	2%
Afrika	1246	16,6%	335	26,9%	7%
Észak-Amerika	363	4,8%	320	88,1%	196%
Közép-Kelet	250	3,3%	141	56,5%	4%

Régiók	Népesség (2017-es becslés) *millió fő*	Népesség %-a	Internet-használók száma (2016. 12. 31) *millió fő*	Internetpe-netráció ará-nya (népes-ség %-ában)	Növekedés (2000−2017)
Óceánia, Ausztrália	40	0,6%	27	68,0%	261%
Összesen	7519	100%	3696	49,2%	923%

Forrás: Internet World Stats 2017, a szerző szerkesztése

Az nyilvánvaló, hogy az internethasználók növekedési aránya a jövőben nem lesz ilyen intenzív és ennyire robbanásszerű, mert ez a szám lassan eléri a teljes lakossághoz viszonyított maximális értéket, de még mindig igen jelentős növekedés prognosztizálható a következő 3−4 évben, azaz 2020-ig.

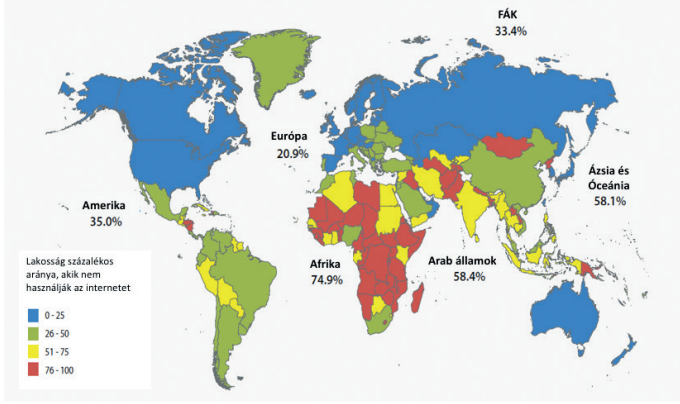
Ugyanakkor, ha megvizsgáljuk az internetet nem használók arányát, akkor az előbbi viszonylag pozitív kép máris árnyaltabban jelenik meg. Az ITU adatai alapján 2016 végén 3,9 milliárd ember, azaz a világ népességének közel 53%-a nem használta az internetet. Az amerikai kontinensen és a Független Államok Közösségében a lakosság közel egyharmada offline volt, azaz nem használta a világhálót. Ez az adat természetesen nem teljesen igaz Észak-Amerikára, mert ott a lakosság csak kevesebb mint egynegyede nem használta az internetet. Mindeközben Afrikában ez az arány majdnem 75%-os, amely óriási szám összehasonlítva a többi kontinenssel, illetve régióval. Ugyanakkor Európában csak az emberek 21%-a tartozik azokhoz, akik sohasem használták a világhálót. Ázsiában, illetve az arab országokban ez az arány kevéssel, de átlagban meghaladta az 58%-ot. (ITU 2016)

2. táblázat
A világ internetpenetrációjának előrejelzése 2030-ra

	2017	2030
Népesség*	7,6 milliárd	8,6 milliárd
Internethasználók száma**	3,9 milliárd	6,2 milliárd
Számítógépek száma	14 milliárd	100 milliárd

* Forrás: UN DESA 2017.
** Forrás: Internet World Stats 2017.

Forrás: a szerző szerkesztése



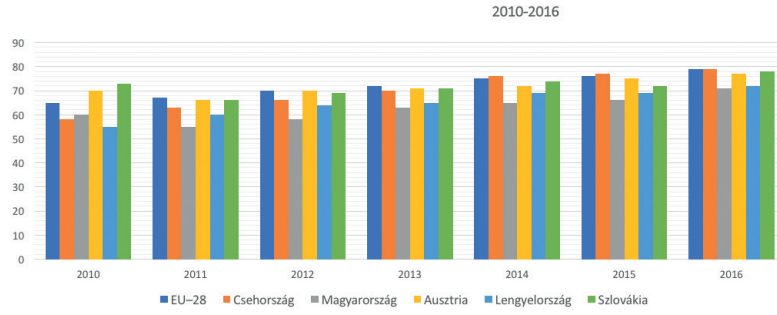
8. ábra
Az internetet nem használók aránya a világon

Forrás: ITU 2016, a szerző szerkesztése

A visegrádi országok és Ausztria internethasználata

A V4-ek és Ausztria esetében az internetfelhasználók száma a teljes lakossághoz viszonyítva 70% és 82% közé esik. 2016-ban ezek az értékek számszerűen a következőképpen alakultak: Ausztria 82%, Lengyelország 70%, Magyarország és Szlovákia egyaránt 78%, míg Csehország 79%-os internetfelhasználói aránnyal rendelkezett.

Amennyiben megnézzük az elmúlt hat év, azaz a 2010 óta eltelt időszakban az internethasználók növekedési arányát, látható, hogy Ausztriában 12%-kal, Lengyelországban 15%-kal, Magyarországon 18%-kal, Csehországban 19%-kal, míg Szlovákiában csak 5%-kal nőtt ez az arány. A növekedés Szlovákiát kivéve igen jelentős, bár Szlovákia esetében ehhez az alacsony növekedési arányhoz rögtön hozzá kell tennünk, hogy 2010-ben már eleve 73%-os volt az internethasználat.[19] (Eurostat 2017a)



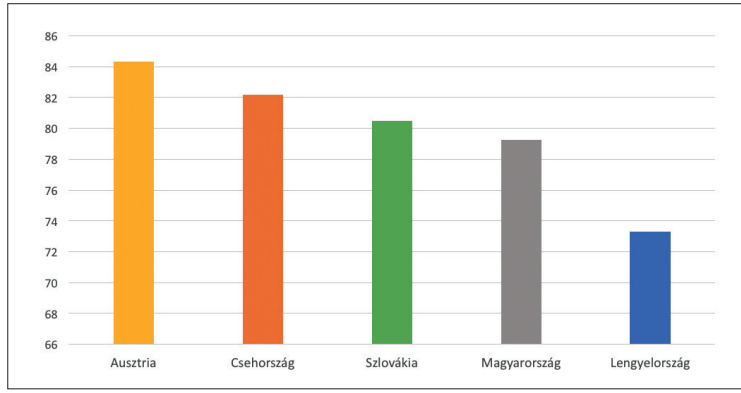
9. ábra
A V4-ek és Ausztria internetpenetrációja 2010–2016 között

Forrás: Eurostat 2017a, a szerző szerkesztése

Amennyiben közelebbről megvizsgáljuk ezeket az értékeket, és egészen pontos képet szeretnénk kapni a 16–74 éves korosztály körében azoknak a számáról, akik a felmérést megelőző 3 hónapban hetente legalább egyszer használták az internetet, viszonylag kiegyensúlyozott képet – közel 80%-os átlag körüli értékeket – kapunk a V4-ek és Auszt-

[19] A mérés az egyéni, rendszeres internethasználat alapján rögzíti százalékos arányban a 16 és 74 éves kor közötti korosztály körében végzett felméréssel az internepenetrációt. A rendszeres internethasználat: legalább egyszer egy héten (például mindennap, vagy majdnem mindennap, vagy legalább egyszer egy héten, de nem mindennap) internetezők átlagos száma a felmérést megelőző három hónapban. A mérés nem vizsgálja külön, így nem különíti el a magáncélú vagy munka- és/vagy üzleti célú internethasználatot. (Eurostat 2017a)

ria összehasonlításában (Lengyelország kivételével, ahol ez az érték jóval alacsonyabb).



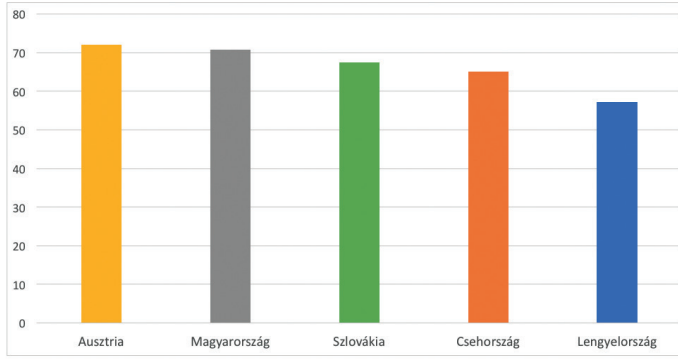
10. ábra

Ausztria és a V4-ek internethasználóinak teljes lakossághoz viszonyított százalékos aránya 2016-ban

Forrás: Eurostat 2016a, a szerző szerkesztése

A számokból jól látszik, hogy Ausztriában 84,3%, Csehországban 82,2%, Szlovákiában 80,5%, Magyarországon 79,3%, Lengyelországban pedig 73,3% használta az internetet a felmérést megelőző 3 hónapban.

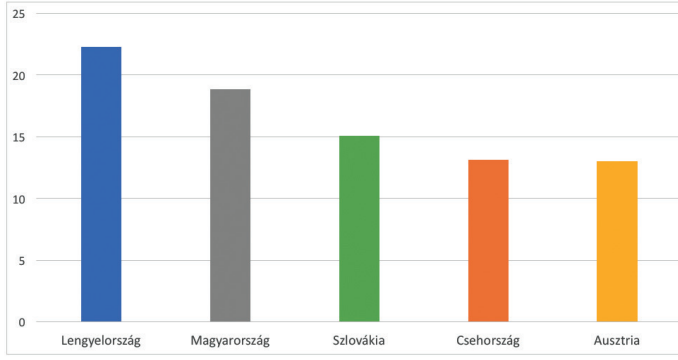
Ugyanakkor, ha megvizsgáljuk a napi rendszerességgel internetet használók számát, kissé más képet kapunk. A naponta vagy majdnem mindennap internetet használók számában is Ausztria vezet (72%), de második helyet már Magyarország éri el (70,7%), harmadik Szlovákia (67,5%), majd Csehország (65,1%) és végül Lengyelország (57,2%) következik.



11. ábra
Ausztria és a V4-ek napi internethasználóinak teljes lakossághoz viszonyított százalékos aránya 2016-ban

Forrás: Eurostat 2016b, a szerző szerkesztése

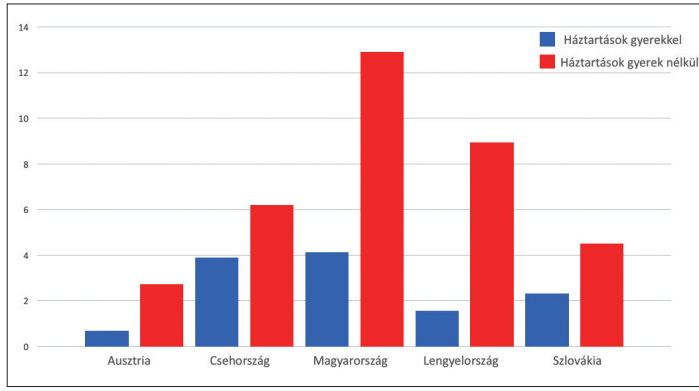
A statisztikai adatokat tovább vizsgálva az is látszik, hogy melyik vizsgált országban vannak nagyobb számban olyanok a 16 és 74 éves korosztályba tartozók közül, akik még sohasem használták az internetet. Ez a szám meglehetősen magas Lengyelországban (22,3%), illetve Magyarországon (18,9%), valamivel kisebb Szlovákiában (15,1%), majd ezt követi Csehország (13,1%) és Ausztria (13%).



12. ábra
Ausztria és a V4-ek olyan lakosainak teljes lakossághoz viszonyított százalékos aránya, akik sohasem használnak internetet 2016-ban

Forrás: Eurostat 2016c, a szerző szerkesztése

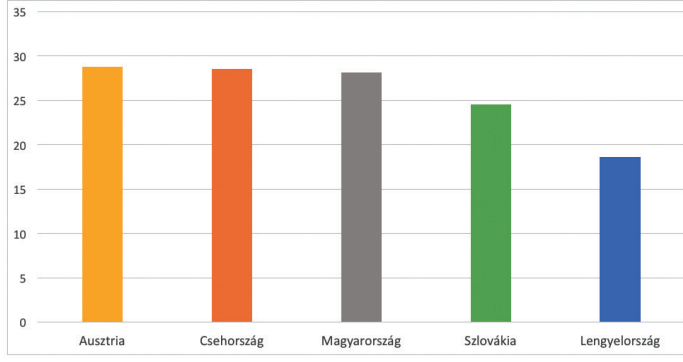
Nagyon tanulságos annak vizsgálata is az említett országok összehasonlításában, hogy hogyan alakul azoknak a háztartásoknak a száma, amelyek az internet-előfizetés magas ára miatt nem használnak internetet. Az Európai Unió adatai alapján Magyarországon közel 13% (12,9%) azoknak a háztartásoknak a száma, ahol nincs eltartott gyermek, ugyanakkor a magas internet-előfizetési ár miatt nem jutnak a szolgáltatáshoz, és kevéssel több mint 4% (4,13%) az eltartott gyermekkel rendelkező háztartások száma, akik ugyanazen ok miatt nem jutnak internethez. Ez a 4% hasonló arányt mutat, mint Csehországban (3,98%), de több mint kétszerese a lengyelországi (1,55%) és több mint négyszerese az osztrák (0,68%) adatnak.



13. ábra
Ausztria és a V4-ek olyan lakosainak teljes lakossághoz viszonyított százalékos aránya, akik a magas ár miatt nem használnak internetet 2016-ban

Forrás: Eurostat 2016d, a szerző szerkesztése

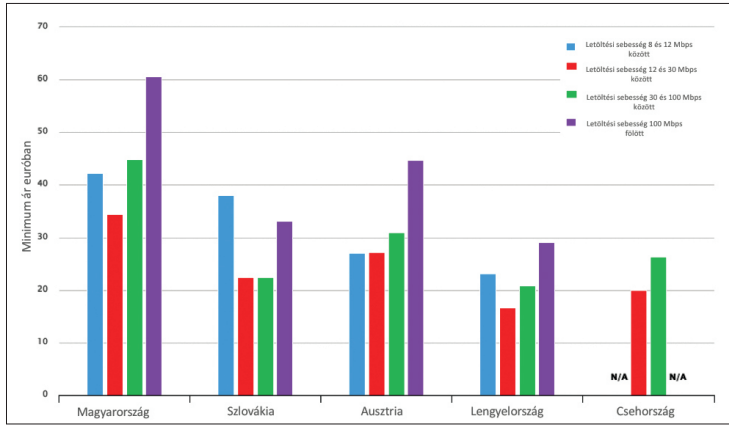
A lakossági szélessávúinternet-elérés tekintetében Ausztria, Csehország és Magyarország szintén kiegyensúlyozott – közel 30%-os – arányt mutat. Szlovákiában a lakosság 24,5%-a, Lengyelországban 18,6%-a fért hozzá a széles sávú internethez 2016 közepén.



14. ábra
Ausztria és a V4-ek szélessávúinternet-előfizetéseinek száma 100 lakosra vetítve 2016-ban

Forrás: Eurostat 2016e, a szerző szerkesztése

Ugyanakkor az internetelérés árában, különösen a szélessávúinternet-előfizetés árában nagy eltéréseket találunk a vizsgált országok vonatkozásában.

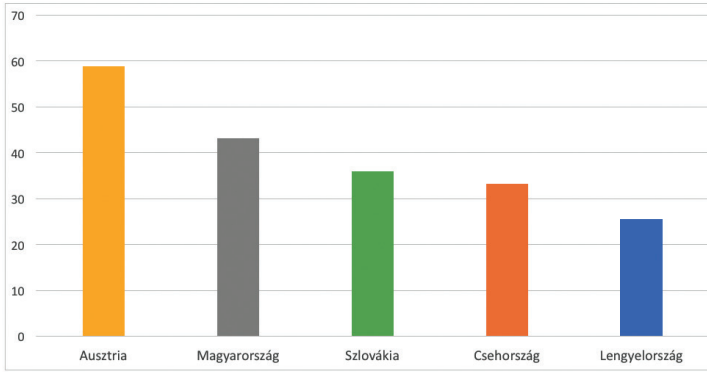


15. ábra
Ausztria és a V4-ek szélessávúinternet-előfizetéseinek sávszélességenkénti ára 2015-ben

Forrás: Eurostat 2016f, a szerző szerkesztése

A 100 Mbps fölötti sávszélességű internet-előfizetés ára Magyarországon volt a legmagasabb 2015-ben. Hozzá kell tenni, hogy a vizsgált 5 ország közül itt kiemelkedően magas az internet-előfizetés ára, és nemcsak ebben a kategóriában, hanem gyakorlatilag minden letöltési sebességű előfizetés tekintetében. Magyarországot Ausztria, majd sorrendben Szlovákia és Lengyelország követi az árak szerint.

A vizsgált 5 országban a mobiltelefonnal történő internetelérés nagy fejlődésen ment keresztül az elmúlt években. Amíg Magyarország esetében 2013-ban a lakosság alig több mint 25%-a érte csak el mobiltelefonon keresztül az internetet, ez a szám 2016-ban már meghaladta a 43%-ot. Ausztriában a 2013-as 49%-ról 59%-ra, Szlovákiában 25%-ról 36%-ra, Csehországban 21%-ról 33%-ra, Lengyelországban viszont 19%-ról csak 25%-ra nőtt ez az érték.

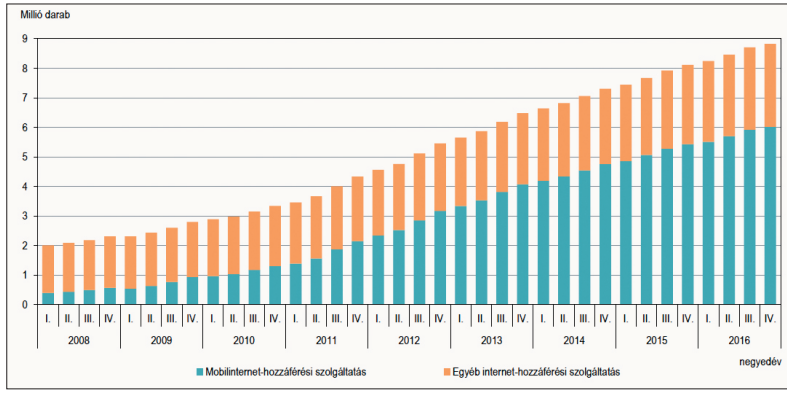


16. ábra
Ausztria és a V4-ek mobiltelefonon keresztüli interneteléréseinek száma 2016-ban a teljes internetelérések százalékos arányában

Forrás: Eurostat 2016g, a szerző szerkesztése

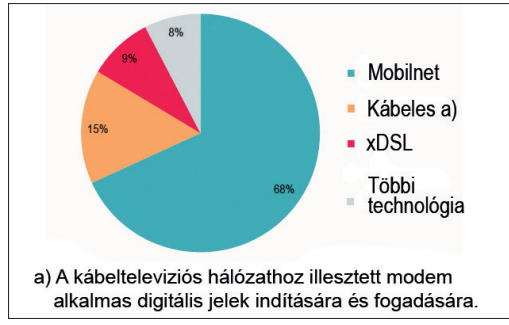
Magyarország vonatkozásában, megvizsgálva az internet-előfizetések számát,[20] azokat technológia szerinti részletesebb bontásban elemezve megállapítható, hogy a mobilinternet a teljes internet-előfizetések csaknem 68%-át adja. Itt rögtön meg kell jegyezni, hogy az elmúlt években az internethasználat teljes lakossághoz viszonyított arányának növekedésében (például 2010-ben a naponta internetet használók aránya csak 60% volt, addig ez 2016-ban már 71% volt) a mobilinternet hatalmas fejlődése alapvető szerepet játszott. A kábeles, tehát a kábeltelevíziós hálózatba integrált (általában külön erre a célra kialakított modemmel történő) internet-előfizetés 15%, míg az xDSL 9% arányt képviselt a teljes internet-előfizetések számából. (KSH 2017)

[20] Az internet-előfizetések száma nem feltétlenül egyezik meg a naponta (hetente, havonta) internetet használók számával. Ezért eltérő arányokat találunk a teljes lakosságra vonatkoztatva az előfizetések, valamint a használók számában.



17. ábra
Internet-előfizetések száma Magyarországon 2008 és 2016 között

Forrás: KSH 2017



18. ábra
Az internet-előfizetések megoszlása technológia szerint Magyarországon 2016. év végén

Forrás: KSH 2017

Ugyanakkor a mobiltelefonon keresztüli internetelérés önmagában kettős hatással jár. Egyrészt természetesen örvendetes, hogy a lakosság egyre növekvő része számára nyújt lehetőséget az internet, és így a különböző szolgáltatások elérésére a mobiltelefon, a másik oldalról azonban az eszköz jellegéből adódóan ez mégis egyfajta korlátozottabb

alkalmazást tesz csak lehetővé, mint egy asztali számítógép, notebook vagy akár egy nagyobb tablet.

Mindezeken túl azonban pont a mobil eszközök mérhető módon járulnak hozzá a digitális gazdasághoz. Egyrészt a mobil eszközökkel kényelmesen és helytől függetlenül lehetséges bármilyen online szolgáltatás elérése, és pont ez a tényező az egyik legnagyobb előny, amikor az e-kereskedelemről beszélünk.

Természetesen a mobiltelefonos internetelérés esetében azt is érdemes megvizsgálni, hogy mekkora olyan lefedettséggel rendelkezik az adott ország,[21] amely használható adatátvitelt tud biztosítani a felhasználók számára. Ebben a tekintetben a vizsgált országok közül Lengyelország áll az élen (88,68%), majd Magyarország (85,31%), Ausztria (80,93%), Szlovákia (74,26%) és Csehország (68,69%) a sorrend. (OpenSignal 2016)

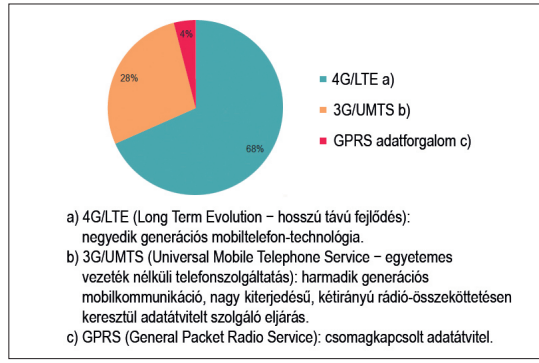
A hálózati lefedettség azonban csak egy része a jellemző adatoknak. A másik jellemző tény a hálózat (3G vagy magasabb technológia) nyújtotta átlagos adatátviteli sebesség. E tekintetben a világon a leggyorsabb mobilinternet nyújtotta hálózati sebességgel Dél-Korea rendelkezik (41,34 Mbps), de meglepő módon Magyarországot a világon a harmadik helyen találjuk (26,15 Mbps) ebben az összehasonlításban. A korábban vizsgált országok közül Szlovákia (16,69 Mbps), Csehország (16,21 Mbps) és Ausztria (15,48 Mbps) szintén az élmezőnyben van, míg Lengyelország (11,89 Mbps) kissé lemaradva következik.[22] (OpenSignal 2016)

Magyarország vonatkozásában a mobilhálózatok adatforgalmának közel 68%-a már a 4G/LTE hálózaton keresztül történt 2016. év végén, míg a mobil-adatforgalom 28%-a zajlott 3G/UMTS hálózaton. (KSH 2017)

---

21 Itt a vizsgálat a 3G vagy magasabb (4G, azaz LTE) hálózatok lefedettségét jelenti.

22 A felmérés és az összehasonlítás azonban csak a hálózati adatátviteli sebességre vonatkozik. A teljes képhez hozzátartozna az előfizetéshez tartozó adatmennyiség is, azaz annak az összehasonlítása, hogy egységnyi (például 1 GB) adatmennyiség használatának mennyi az ára.



19. ábra
A magyarországi mobilhálózati adatforgalom megoszlása hálózati technológia szerint 2016. év végén

Forrás: KSH 2017

Mindezeket összefoglalva egy táblázatba gyűjtöttük azokat az adatokat, amelyek Ausztria és a V4-ek gazdasági teljesítményét (GDP-vel jellemezve), a széles sávú internetet használók (teljes lakosságra vetített százalékos arányát bemutatva), a mobiltelefonos internetelérés arányát (szintén a teljes lakosságra vetített százalékos arányában kifejezve), valamint az internetet sosem használók (teljes lakosság %-ában kifejezett) arányát mutatja be.

3. táblázat
Ausztria és a V4-ek GDP-adatainak, internet- és mobiltelefon-felhasználóinak összehasonlítása (GDP 2015-re, többi adat 2016-ra vonatkoztatva)

	GDP (US$/ fő/2015)*	Széles sávú internet (a 16−74 éves lakosság %-os aránya)*	Mobiltelefonos internetelérés (a 16−74 éves lakosság %-os aránya)***	Internetet nem használók (a 16−74 éves lakosság %-os aránya)****
Ausztria	49 480	28,9	59,9	13
Csehország	33 780	28,8	33,2	13,1
Magyarország	26 468	28,1	43,1	18,9
Lengyelország	26 635	18,3	25,5	22,3
Szlovákia	29 939	23,8	36	15,1

* *Forrás:* OECD 2015. Megjegyzés: GDP-adat nominális értékben megadva.
** *Forrás:* Eurostat 2016e.
*** *Forrás:* Eurostat 2016g.
**** *Forrás:* Eurostat 2016c.

Forrás: a szerző szerkesztése

1.2.2. Mobilkommunikáció

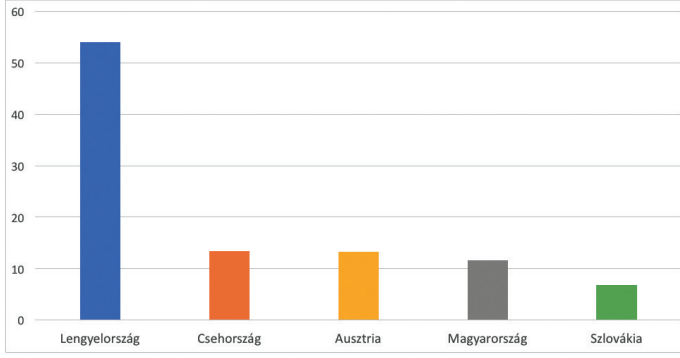
Az ITU 2016-os adatai alapján a Föld népességének közel 95%-a, azaz közel 7 milliárd ember él olyan területen, ahol van mobiltelefon-hálózati lefedettség. A mobil széles sávú hálózatok (3G vagy az ennél még újabb mobiltechnológia) lefedettsége eléri a világ népességének 84%-át, de a vidéki lakosság 67%-hoz jut csak el.[23]

Az LTE-hálózatok gyorsan terjednek az elmúlt években, és ma megközelítőleg 4 milliárd ember tudja használni ezt a technológiát, amely a világ népességének 53%-át jelenti. Ez a széles sávú internethez való hozzájutást nagyban elősegíti. (ITU 2016)

[23] Meg kell jegyezni, hogy a világ népességének több, mint 53%-a városokban él. (UN 2017)

A mobiltelefonos internetelérés bemutatásakor korábban megállapíthattuk, hogy az elmúlt évek során ez a terület mind Ausztriában, mind a V4-ek országaiban sokat fejlődött. Ebből következően érdemes egy pillantást vetni magára a mobilkommunikációra is az említett országokban.

Lengyelországban több mint 54 millió mobiltelefon-előfizetés volt 2015-ben. Csehországban közel 13,5 millió, míg Ausztriában 13,3 millió, Magyarországon 11,5 millió, Szlovákiában pedig 6,7 millió mobiltelefon-előfizetést regisztráltak ugyanebben az évben.[24] Ha összehasonlítjuk a 2010-es adatokkal ezeket a számokat – Lengyelországban 43,6 millió, Csehországban 13,3 millió, Ausztriában 11,9 millió, Magyarországon 10,8 millió, Szlovákiaban 6,1 millió – jól látszik, hogy a legnagyobb fejlődés ezen a területen Lengyelországban volt 2010 és 2015 között. (Eurostat 2016h; Eurostat 2016j)

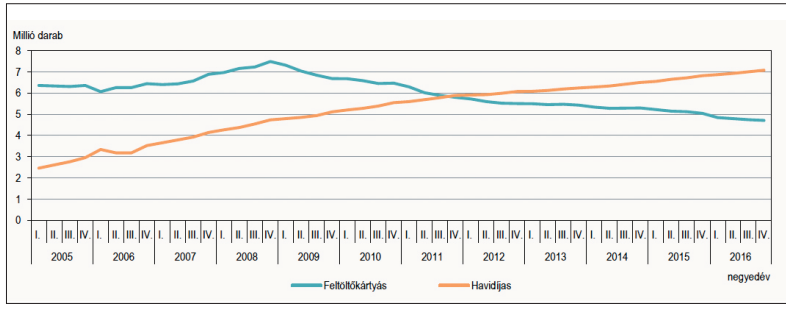


20. ábra
Ausztria és a V4-ek mobiltelefon-előfizetéseinek száma 2015-ben (millió darab)

Forrás: Eurostat 2016j, a szerző szerkesztése

[24] Természetesen ezekkel az adatokkal össze kell vetni az adott ország népességét is. Az ENSZ adatai szerint 2015-ben Lengyelország 38,612 millió, Magyarország 9,855 millió, Csehország 10,543 millió, Szlovákia 5,426 millió, Ausztria pedig 8,545 millió fő lakossággal rendelkezett. (UN DESA 2017)

Részletesebben megvizsgálva Magyarországot a következő képet kapjuk a mobilkommunikáció tekintetében. Az említett 10,8 millió mobiltelefon-előfizetés, amely 2015-re vonatkozó adat a következő év végére, azaz 2016. IV. negyedévére már 11,8 millió volt. (KSH 2017)



21. ábra
A magyarországi mobiltelefon-előfizetések számának alakulása 2005 és 2016 között

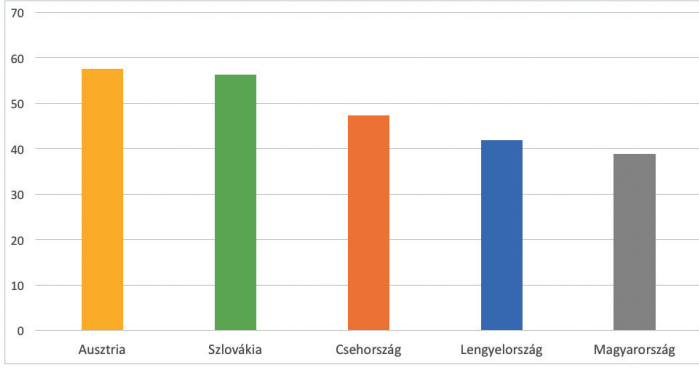
Forrás: KSH 2017

1.2.3. Kereskedelem a kibertérben

Ahogy korábban utaltunk rá, a digitális gazdaságon belül az elektronikus kereskedelem fejlesztése és növelése stratégiai cél nemcsak az egyes tagországokban, hanem európai uniós szinten is.

Szintén a V4-ek és Ausztria összehasonlításában megvizsgálva az e-kereskedelem különböző adatait a következőket állapíthatjuk meg.

Azon állampolgárok számát (illetve azok százalékos arányát) tekintve, akik valamilyen terméket, illetve szolgáltatást már rendeltek az interneten, Ausztria az első (57,6%), őt szorosan követi Szlovákia (56,3%), kissé lemaradva Csehország (47,4%) és Lengyelország (41,9%) következik, végül Magyarország (39,8%) zárja a sort.



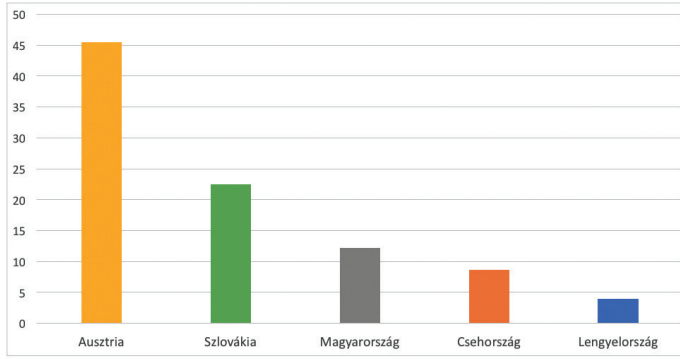
22. ábra
Ausztria és a V4-ek lakosainak teljes lakossághoz viszonyított százalékos aránya, akik már rendeltek árut vagy szolgáltatást az interneten 2016-ban

Forrás: Eurostat 2016k, a szerző szerkesztése

Ahogy korábban láthattuk, az Európai Unió Digitális egységes piac stratégiája az egyik legnagyobb kihívásként a határokon átnyúló termékek és szolgáltatások elektronikus kereskedelmét azonosította, így e terület fejlesztését és növelését stratégiai célnak tekinti.

Az e-kereskedelemi szegmens a vizsgált országok között a következőképpen néz ki. Azok száma, akik már rendeltek más országból valamilyen terméket vagy szolgáltatást, szintén Ausztriában a legmagasabb (45,5%). Ausztriát Szlovákia követi (22,5%), majd Magyarország (12,2%), Csehország (8,65%) és Lengyelország (3,94%). A százalékos arányokból nagyon jól látszik,[25] hogy Ausztriát leszámítva valóban szükséges az országokon átívelő elektronikus kereskedelem fejlesztése és ösztönzése.

[25] Ugyanakkor a digitalizáció ilyen megjelenése korántsem új dolog a vállalatok életében, hiszen már közel egy évtizede jelen vannak – akár már a kis- és középvállalkozásoknál is – a vállalatirányítási rendszerek. Ezek feladata és így egyben legnagyobb előnye pont a vállalaton (szervezeten) belüli folyamatok optimalizálása, legyen szó beszerzésről, tervezésről, gyártásról vagy akár kereskedelemről.



23. ábra
Ausztria és a V4-ek lakosainak teljes lakossághoz viszonyított aránya, akik már rendeltek árut vagy szolgáltatást másik EU-s országból az interneten 2016-ban

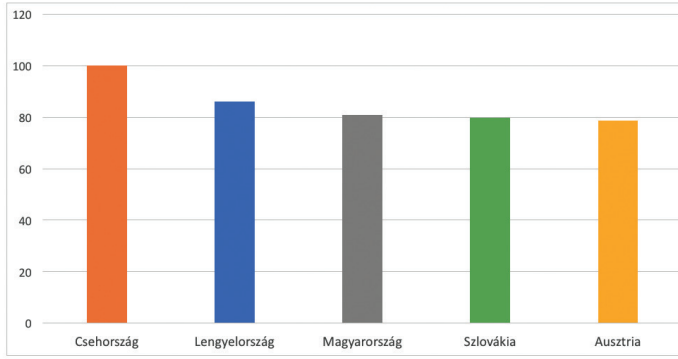
Forrás: Eurostat 2016m, a szerző szerkesztése

Amennyiben megvizsgáljuk a vállalkozások[26] e-kereskedelmi tevékenységét, a vizsgált országokban viszonylag kiegyensúlyozott képet kapunk. Ugyanakkor Csehország kiemelkedik ebből a kiegyensúlyozott képből, hiszen ebben a mutatóban messze megelőzi a V4-ek országait és Ausztriát, mivel a csehországi vállalkozások e-kereskedelmi mutatója csaknem 100%-os.

A legalább 10 főt alkalmazó azon vállalkozások aránya, amelyek valamely e-kereskedelmi megoldással[27] éltek az elmúlt időszakban, Ausztriában 78%-os, ami egyébként a vizsgált 5 ország közül a legalacsonyabb érték. Szlovákia és Magyarország esetében közel azonos értékekről – 79,7% és 81% – beszélhetünk, míg Lengyelország ebben a mutatóban igen jól szerepelve 86,1%-os arányt ért el 2016-ban.

26 A vizsgálatban a pénzügyi szektor vállalkozásai nem szerepelnek.

27 Ezek az értékek magukban foglalják mindazon vállalatok adatait, amelyek a teljes vállalati bevételük legalább 1%-át valamely elektronikus szolgáltatáson keresztül vagy annak segítségével szerezték. Ilyen elektronikus szolgáltatás: bármely számítógép-hálózaton, weblapo(ko)n keresztüli kereskedelmi tevékenység vagy egyéb elektronikus adattranszfer, ideértve az egyszerű e-mailt is.

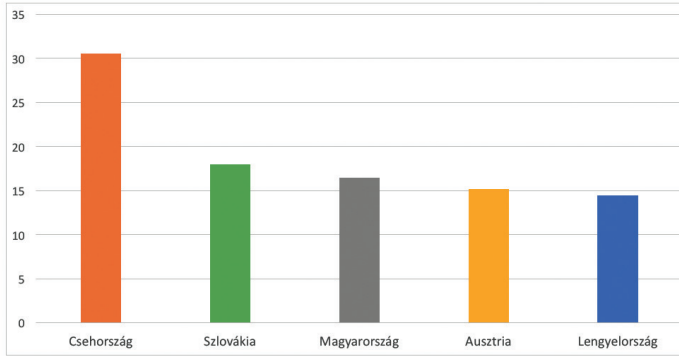


24. ábra
Ausztria és a V4-ek vállalkozásainak aránya, amelyek használták ez e-kereskedelem valamilyen formáját 2016-ban

Forrás: Eurostat 2016n, a szerző szerkesztése

Mindezek alapján azt is érdemes megvizsgálnunk, hogy azon vállalkozásoknak, amelyek élnek az e-kereskedelem különböző módszereivel, mekkora bevételük származik ebből a tevékenységből vagy ezen keresztül.

Az elektronikus kereskedelem által generált bevétel aránya a teljes vállalati bevételhez viszonyítva nem meglepő módon Csehországban a legmagasabb (30,5%), hiszen láthattuk, itt a vállalkozások közel 100%-a él valamilyen elektronikus kereskedelmi módszerrel. Csehországot Szlovákia (18%), majd Magyarország (16,5%), Ausztria (15,2%) és végül Lengyelország (14,4%) követi.



25. ábra
Ausztria és a V4-ek vállalkozásainak e-kereskedelemből származó bevétele a teljes bevétel százalékos arányában 2016-ban

Forrás: Eurostat 2016o, a szerző szerkesztése

Az e-kereskedelem – csakúgy, mint számos más online szolgáltatás – része lett az életünknek, mindennapjainknak.

Hazánkban 2015-ben készült először olyan nyilvános elemzés, amely az online kereskedelem szereplőit rangsorba állította.[28] A felmérés 2016-ban megismétlődött, alkalmat teremtve az egy évvel korábbi adatokkal való összevetésre és összehasonlításra. Ugyanakkor érdemes megjegyeznünk, hogy ezekben az elemzésekben alapvetően csak a webáruházak kereskedelmi tevékenységét hasonlították össze. Az elemzésből kiderül, hogy a tíz legnagyobb hazai webáruház online értékesítésből származó árbevétele elérte a 92 milliárd forintot, ami a teljes online kiskereskedelmi forgalom 34%-át jelentette. Ugyanakkor ezeknek az adatoknak az összevetése az egy évvel korábbi adatokkal azt mutatta, hogy a legnagyobb 10 webáruház 70%-os forgalomnövekedést ért el egy év alatt. Ez hatalmas szám, főleg annak tükrében, hogy korábban ez a növekedés csak 16% volt. (GKI Digital 2016a)

[28] A felmérést a GKI Digital Kft. készítette.

A növekedés egyik kulcsa nyilvánvalóan a piaci környezethez való alkalmazkodás volt, amelybe beletartozik például a logisztikai lánc optimalizálása, amely jelenti egyrészt a beszállítóktól egészen az áruk vásárlókig történő gyors, hatékony és alacsony költséget jelentő eljuttatását, másrészt a vásárlókkal való hatékony és nem utolsósorban interaktív kommunikációt[29] is. Természetesen ez egy gazdasági verseny is a szolgáltatók között, amelynek azonban vannak a kibertérben megjelenő, a biztonságot komolyan befolyásoló tényezői is. Napjainkban ugyanis ezen a területen már számos elvárás jelentkezik az ügyfelek, azaz a vásárlók részéről. Az egyik ilyen elvárás nyilvánvalóan pont a biztonság, amely a bizalommal közösen jelentkezik meghatározó tényezőként.

Ezzel párhuzamosan a vásárlók részéről megjelenik a kényelmes felhasználás igénye is, amely például a vásárlás menetének minél könnyebb áttekinthetőségét, vagy akár az automatikus felhasználóazonosítás lehetőségét is jelenti. Az automatikus felhasználói azonosítás mellett a vásárlók vagy a potenciális vásárlók azt is elvárásként fogalmazzák meg, hogy a vásárlási szokásaikat és nem utolsósorban igényeiket, az online kereskedelmi térben történő tevékenységüket az adott kereskedő felismerje, majd ezek alapján különböző ajánlatokat vagy célzott vásárlási tippeket adjon a számukra.

Mindezek azonban komoly biztonsági kérdést is jelenthetnek mind az e-kereskedelmet folytató vállalat, mind az ügyfél számára. Az egyik ilyen biztonsági kérdés a mobil eszközökön mint platformon keresztüli vásárlás. Ahogy korábban utaltunk rá, az internethasználat növekedésének egyik motorja pont a mobiltechnológia, ezért értelemszerűen az e-kereskedelem egyik meghatározó eleme is a mobil eszközökkel vagy azokon keresztüli minél egyszerűbb online vásárlás támogatása, amelyben meg kell jelennie az elvárható biztonságnak.

[29] Itt az interaktív kommunikáció a vásárlói szokások és a vásárlók online tevékenységének a feltérképezését is jelenti.

1.2.4. Vállalatok a kibertérben: üzlet és digitalizáció

A vállalatok számára egyértelmű előnyt – és így versenyelőnyt is – jelent a digitalizáció. Persze csak akkor, ha ezt az előnyt felismeri a vállalat vezetése, menedzsmentje.

Napjainkra az egyik jellemző trend, hogy a digitalizáció a vállalatok számára elsősorban az üzletmenetben jelent hatékonyságnövelést, azaz a digitális eszközök és rendszerek alkalmazásával nő az egyes vállalati folyamatok összehangolása, optimálisabbá válnak az egyes tevékenységek.[30] A vállalatok fejlődésének következő fázisa lehet, amikor nemcsak a vállalkozás működési folyamatainak hatékonyabbá tételében nyújt segítséget a digitalizáció, hanem maga a vállalkozás üzleti modellje épül a digitalizációra. (Microsoft 2017a)

Ezt a véleményt támasztja alá a GKI Digital Kutató és Tanácsadó Kft. és a Siemens Hungary 2016-ban készült közös felmérése is, amely egy digitalizációs helyzetképet kívánt bemutatni a magyar vállalatok körében. (GKI Digital 2016b)

A kutatás során közel 2000 hazai céget vizsgáltak és kérdeztek meg digitalizációs szokásaikról. A cégek alapvetően az ipar (ezen belül is a gyártás), a közlekedés és szállítás, az egészségügy, az ingatlanfejlesztés és az energiaszektor különböző területein működő közepes és nagyvállalatok voltak. A vizsgált vállalatok szerint hat olyan terület van, amelyeken egyértelműen megjeleníthető a digitalizáció, mivel ezeken a területeken nyújt(hat) egyértelmű hatékonyságnövelést a digitális technika és technológia. Ezek a területek: a működés hatékonyságának jobb átláthatósága, illetve annak ellenőrizhetősége; a vállalat elektronikus rendszereinek bővítése; adatok gyűjtése és azok elem-

[30] Ugyanakkor a digitalizáció ilyen megjelenése korántsem új dolog a vállalatok életében, hiszen már közel egy évtizede jelen vannak – akár már a kis- és középvállalkozásoknál is – a vállalatirányítási rendszerek. Ezek feladata és így egyben legnagyobb előnye pont a vállalaton (szervezeten) belüli folyamatok optimalizálása, legyen szó beszerzésről, tervezésről, gyártásról vagy akár kereskedelemről.

zése; komplex szemlélet a szervezet egészének működésére vonatkoztatva; a vállalat különböző szoftvereinek összekapcsolása; valamint az analóg folyamatok kiváltása. (GKI Digital 2016b)

A vizsgált vállalatok több mint fele már öt éve vagy annál régebben alkalmaz olyan fejlesztéseket, amelyek egyértelműen a digitalizációt jelentik, ugyanakkor a jelentés megállapítja, hogy bár a digitalizáció 60%-ot meghaladó mértékben van jelen a nagyvállalatok életében, a közepes vállalkozások csak 40%-a foglalkozik a digitalizáció kérdéseivel 5 évnél régebben. (GKI Digital 2016b)

A vizsgálat megállapította, hogy a megkérdezett vállalatok digitalizáció mellett szóló érvei legmarkánsabban a különböző folyamatok nyomonkövethetőségében, legkevésbé pedig az energiahatékonyság növelésében jelentkeztek. Ugyanakkor a vizsgált nagyvállalatok több mint 70%-ának az volt a véleménye, hogy egyértelmű versenyelőnyt jelent számukra a digitalizáció. Ezzel szemben a közepes vállalkozások csak 40%-a érezte úgy, hogy ez előny lenne a számukra. (GKI Digital 2016b)

Ez mindenképpen elgondolkodtató tény, hiszen ahogy korábban bemutattuk, például Csehországban az e-kereskedelem a vállalkozások közel 100%-a esetében van jelen. Ha továbbmegyünk, világosan látható, hogy egyenes arány mutatkozik (ahogy szintén utaltunk erre korábban) a gazdasági fejlődés és a digitalizáció között egy adott országban.

Természetesen a vállalatok számára is csak akkor jelent előnyt a digitális technika alkalmazása, ha az biztonságos. Ezt támasztja alá az a felmérés is, amelyet a Microsoft Magyarország készített az Informatikai Vállalkozások Szövetségével (IVSZ), és amely a vállalatok – elsősorban a vállalatvezetők – digitalizációval, ezen belül is kiemelten a felhőszolgáltatásokkal kapcsolatos ismereteit (és nem utolsósorban félelmeit) volt hivatott áttekinteni. E felmérés szerint a vállalatvezetőknek csak a fele rendelkezett valamilyen ismeretekkel a felhőszolgáltatásokról (mindamellett, hogy természetesen a vállalat informatikai vezetőinek több mint a 85%-a rendelkezett ilyen tudás-

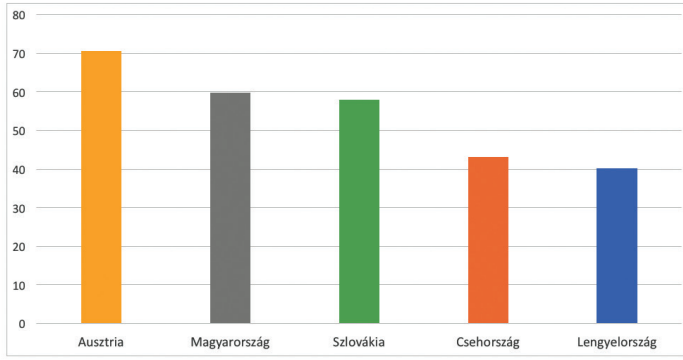
sal). Ugyanakkor a felhőszolgáltatással, illetve az ezzel a technológiával szemben megfogalmazott elvárások – jogi megfelelés, megfelelő költséghatékonyság stb. – mellett bizony az adatok biztonsága az egyik legfontosabb vezetők által megfogalmazott szempont. (DigitalHungary 2017)

1.2.5. Állampolgárok a kibertérben

A kibertér egyértelmű előnyt hordoz magában az állampolgárok és az állam interakcióinak viszonyában is. Az elektronikus közigazgatás – vagy napjaink divatos kifejezésével élve az e-government – számos olyan szolgáltatást nyújt, amelyek egyszerűbbé, átláthatóbbá és nem utolsósorban mind az állam, mind az állampolgár számára sokkal gyorsabbá teszik a különféle ügyek intézését.

Az e-közigazgatás különböző szolgáltatásai hozzájárulnak a hatékony közigazgatáshoz. (Kaiser 2016). Olyan szolgáltatások találhatóak meg ezen a területen, amelyek az állampolgárok mindennapi ügyeiben viszonylagos automatizmussal intézhetőek. Ugyanakkor talán ezen a területen is, hasonlóan a banki és egyéb pénzügyi szolgáltatások területeihez, a biztonság elengedhetetlen és alapvető elem. Ez elengedhetetlen ahhoz, hogy a felhasználók, azaz az állampolgárok bizalma e szolgáltatások mellett kialakuljon. Amennyiben nem megfelelően, akadozva, szolgáltatáskiesésekkel járó módon vagy nem biztonságosan működnek ezek a szolgáltatások, a felhasználók azonnal elfordulnak ezektől, és más megoldásokat keresnek. Ugyanakkor ezen a területen a biztonsági incidensek hatalmas károkat okoznak az állam számára is, hiszen egy-egy incidens esetében azonnal bizalomvesztés léphet fel az állammal szemben, amely kivetül más kormányzati területekre is.

Mindezek alapján érdemes egy kis kitekintést tennünk, hogy a korábban is vizsgált országok – Ausztria, valamint a V4-ek országai – hogyan teljesítenek az e-közigazgatás területén.

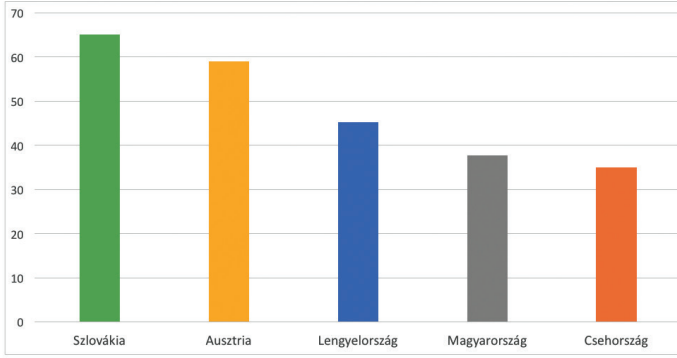


26. ábra
Ausztria és a V4-ek internethasználóinak aránya, akik legalább egy alkalommal használtak e-közigazgatási szolgáltatást 2016-ban

Forrás: Eurostat 2016p, a szerző szerkesztése

Az Eurostat adatait összehasonlítva látható, hogy az adott országban az internethasználók (16–74 éves korosztály) közül 2016-ban Ausztriában 70,5%, Magyarországon 59,8%, Szlovákiában pedig 57,9% használt valamilyen e-közigazgatási szolgáltatást. Ugyanakkor meglepő, hogy Csehországban ez az arány csak 43,1%, pedig Csehország korábban elemzett mutatói sokkal jobb eredményt mutattak. Lengyelország esetében ez az adat még alacsonyabb, egészen pontosan 40,2%.

Amennyiben megvizsgáljuk, hogy az elemzéseink és vizsgálataink alá vont országok közül az e-közigazgatási szolgáltatásokon belül melyikben és milyen arányban nyújtottak be az állampolgárok valamilyen űrlapot (azaz indítottak el legalább egy ügyet), akkor az előző statisztikától eltérő képet kapunk.



27. ábra

Ausztria és a V4-ek internethasználóinak aránya, akik legalább egy alkalommal használtak e-közigazgatási szolgáltatást, és ott legalább egy elektronikus ügyiratot ki is töltöttek 2016-ban

Forrás: Eurostat 2016q, a szerző szerkesztése

Ebben a mutatóban[31] Szlovákia áll az élen 65,1%-kal, majd Ausztria 59,1%-kal és némileg meglepő módon Lengyelország következik 45,3%-kal. Ez azért meglepő, mert a teljes e-közigazgatási szolgáltatásokat igénybe vevők számának, illetve arányának elemzésekor láthattuk, hogy Lengyelország messze lemaradt a másik négy vizsgált ország mögött. Magyarország 37,8%-ot, míg Csehország 34,9%-ot ért el ebben az összehasonlításban.

[31] Itt is a 16–74 éves internethasználók aránya a vizsgált mutatószám.

E-közigazgatás Magyarországon

Hazánkban az e-közigazgatás jogszabályi alapját és jogi feltételeit a 2004. évi CXL törvény *a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól* teremtette meg.[32] (EUGO 2017)

Az elmúlt években sok fontos fejlesztési program indult, elsősorban európai uniós finanszírozással.[33] Ilyen programok voltak az Elektronikus Közigazgatás Operatív Program (EKOP), Államreform Operatív Program (ÁROP), illetve a Közigazgatás- és Közszolgáltatásfejlesztési (KÖFOP) projektek. Többek között ezeknek is köszönhető, hogy számos e-közigazgatási megoldással bővült az állampolgárok által igénybe vehető szolgáltatások száma.

Fontos lépés volt 2015-ben az e-kártya bevezetése. Ez a kártya egy több funkciót magába foglaló elektronikus kártya, amely integrálja a személyi igazolvány, az adókártya és a társadalombiztosítási igazolvány szerepét. (EUGO 2017)

Magyarországon az egyik legfontosabb e-közigazgatási szolgáltatás az Ügyfélkapu.[34] Az Ügyfélkapu egy olyan központosított azonosítási szolgáltatás, amely egy azonosítással több mint száz[35] e-közigazgatási szolgáltatás elérését és használatát teszi lehetővé a felhasználó számára. Többek között olyan szolgáltatások elérését teszi lehetővé ez a megoldás, mint például a gépjármű-ügyintézés, személyi okmányokkal kapcsolatos ügyek intézése, anyakönyvi ügyintézés, egyéni

---

32 2011 decemberében ezt a törvényt módosította az Országgyűlés a 2011. évi CLXXIV. törvénnyel, amelynek címe *A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény és egyes kapcsolódó törvények, valamint a miniszteri hatósági hatáskörök felülvizsgálatával összefüggő egyes törvények módosításáról.* (2011. évi CLXXIV tv.)

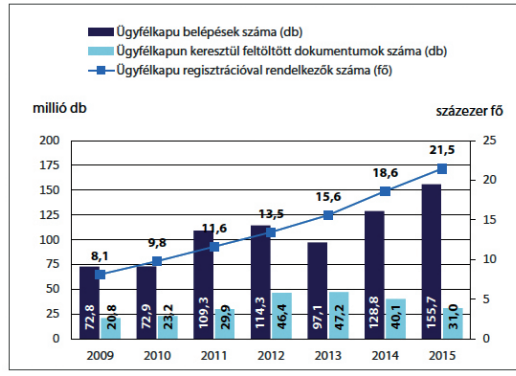
33 A közigazgatás fejlesztésére, illetve ezen belül infokommunikációs fejlesztésre a 2007 és 2013 közötti időszakban 441 milliárd forintot fordítottak, ami jelentős részben EU-s kohéziós és strukturális alapok ffelhasználásával finanszíroztak. (Nemeslaki 2014)

34 Az Ügyfélkaput a 100%-os állami tulajdonban lévő Nemzeti Infokommunikációs Szolgáltató Zrt. (NISZ Zrt.) üzemelteti számos más, kormányzati infokommunikációs rendszerrel együtt.

35 Forrás: Kaiser 2016.

vállalkozói ügyintézés, adózással kapcsolatos ügyek, valamint egyéb ügyek vagy akár tájékoztatás és információk kérése a különböző hivataloktól.

Az Ügyfélkapunak több mint 2 millió regisztrált felhasználója van, akik évente több mint tíz és fél millió belépést generálnak a rendszerben. (EUGO 2017)



28. ábra
Ügyfélkapu-belépések száma 2009–2015 között

Forrás: NISZ, idézi: Kaiser 2016

Önkormányzati feladatellátás – ASP

Természetesen az állampolgárok ügyeinek elektronikus úton történő intézése helyi, azaz önkormányzati szinten is azt igényli, hogy a megfelelő rendszereket építsék ki és működtessék.

Magyarországon korábban ezen a területen a nagyobb, erőforrásokban gazdagabb települések önkormányzatai voltak sikeresebbek. Ugyanakkor, központi – az egész országra kiterjedő – fejlesztési koncepció hiányában az e-közigazgatás helyi szintű szolgáltatásai jellemzően az önkormányzat saját honlapjának fejlesztésében, és ezen keresztül elérhető e-közigazgatási szolgáltatások létrehozásában merültek ki.

Így szigetszerű, egymástól elkülönült megoldások jöttek létre, amelyekben a közigazgatás egyes szakrendszerei közötti integráltság nem jelentkezett megfelelő módon. (Belügyminisztérium 2017)

Mindezek annak a megfogalmazásához vezettek, hogy ezen a területen az önkormányzati fejlesztéseket egységes elvek mentén, egymással összehangoltan célszerű megvalósítani. A fejlesztések összehangolásán túl az anyagi megfontolások és a források hatékony felhasználása is alapvető szempontként merült fel. Így született meg az alkalmazásszolgáltatási modell (Application Service Provider, ASP) megvalósításának koncepciója. (Belügyminisztérium 2017)

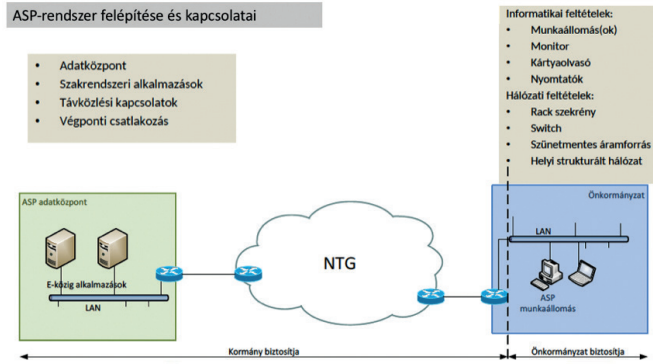
Az ASP lényege, hogy a felhasználók – azaz az önkormányzatok és különböző állami hivatalok dolgozói mint ügyintézők – egy egyszerű webböngésző segítségével internetes felületen keresztül vehetik igénybe a távoli szolgáltató központtól a tevékenységük támogatásához szükséges szoftvereket, illetve alkalmazásokat. E modell kétségtelen előnye, hogy a szolgáltatások kiépítése és működtetése, valamint azok biztonságának megteremtése költséghatékonyabb, mint a helyi végpontokra, azaz az önkormányzat vagy hivatal számítógépeire telepített programok és szolgáltatások esetén. (Belügyminisztérium 2017)

Az ASP-n alapuló rendszer kiépítése és bevezetése két lépcsőben valósult, illetve valósul meg. Az első lépcsőt, azaz az első fázist – az ASP1 projektet – az önkormányzatok önkéntes részvételével regionálisan, majd a második lépcső – az ASP 2.0 projektet – az önkormányzatok kötelező részvételével, országos szinten kerül vezetik be.

Az első fázisban megvalósítandó ASP projekt előkészítését a Nemzeti Fejlesztési Minisztérium megbízásából a Kormányzati Informatikai Fejlesztési Ügynökség 2011-ben kezdte meg, majd 2012-ben az *Önkormányzati ASP központ felállítása* projekt megvalósítására a Belügyminisztérium, a Magyar Államkincstár, a Kincstári Informatikai Nonprofit Kft., a Nemzeti Infokommunikációs Szolgáltató Zrt. (NISZ) és a Kormányzati Informatikai Fejlesztési Ügynökség konzorciumi együttműködési megállapodást írt alá. (Belügyminisztérium 2017)

E projekt keretében a közép-magyarországi régióban olyan ASP-központ kiépítése volt a cél, amely piaci – az e-közigazgatás területén használható – megoldásokra építve egységes és a kor követelményeinek megfelelő szolgáltatásorientált architektúra (Service-Oriented Architecture, SOA) alapú informatikai megoldásokat kínál az elsősorban kis és közepes önkormányzatok részére. Ez az ASP-központ olyan e-közigazgatási szolgáltatások elérését, illetve támogatását teszi lehetővé, mint például az önkormányzati adórendszer, az önkormányzati gazdálkodási szakrendszer, az ingatlanvagyon-kataszter szakrendszer, az ipar- és kereskedelem-szakrendszer, az iratkezelés-szakrendszer, az önkormányzati települési szakrendszer, valamint az elektronikus ügyintézésiportál-rendszer. Mindezen szolgáltatásokat az ASP hatékony forrásfelhasználás mellett biztosítja, így közvetlen módon az állampolgárok is a hatékonyabb önkormányzati feladatellátással és működéssel találkozhatnak. (Belügyminisztérium 2017)

Az ASP kiépítése és megvalósítása európai uniós támogatással valósult meg, amelyhez 2015 első felében már 55 önkormányzat csatlakozott a közép-magyarországi régióból. Ezt követően megszületett a 62/2015. (III. 24.) Korm. rendelet, amely alapján a Magyar Államkincstáron belül létrejött az Önkormányzati ASP Alkalmazásokat Támogató Főosztály (ASP-központ), amelynek fő feladata az ASP-rendszer működtetése és az alkalmazásokat igénybe vevő önkormányzatok támogatása lett. Az ASP-központ működését és üzemeltetését a Nemzeti Infokommunikációs Szolgáltató Zrt. kapta feladatul. (Belügyminisztérium 2017)



29. ábra
Az ASP-rendszer kapcsolatai

Forrás: Belügyminisztérium 2017b, a szerző szerkesztése

Az ASP-projekt második fázisa, az ASP 2.0 már a szolgáltatások országos szintű kiterjesztésével, de kötelező önkormányzati csatlakozással valósul meg, szintén európai uniós pénzügyi támogatással. Az ASP 2.0 szolgáltatásainak országos szintű kiépítése mellett főbb céljai közé tartozik az önkormányzati csatlakoztatások központi támogatása, az e-közigazgatási szolgáltatások fejlesztése, a szakrendszerek bővítése, illetve azok továbbfejlesztése, adattárházak megvalósítása, valamint a kapcsolódó hálózat és infrastruktúra – például a Nemzeti Távközlési Gerinchálózat, NTG – bővítése. (Belügyminisztérium 2017)

Elektronikus Egészségügyi Szolgáltatási Tér

2017. év elején kezdte meg működését – első körben próbaüzemben – az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT). A rendszer összeköttetést teremt az egészségügyi intézmények – legyen az háziorvosi vagy járóbeteg-ellátás, szakorvosi vagy kórházi kezelés –, a gyógyszertárak és a betegek adatai között. Ennek megfelelően

a kezelőorvos a beteg összes kórtörténeti adatát, addigi betegségeit, valamint azok kezelésére tett intézkedéseket – a felírt gyógyszereket, addigi terápiát, vizsgálatok eredményeit – láthatja.

A rendszer célja elsősorban a betegbiztonság növelése, hiszen a kórelőzmények és minden ehhez kapcsolódó információ rendelkezésre áll, csökkentve ezzel az információhiányból eredő esetleges kockázatokat. Nyilvánvalóan minden információ csak a jogosult személyek számára, csak az előre definiált jogosultságok mértékéig látható a rendszerbe belépők számára. Ennek megfelelően a kezelőorvos csak azokat az információkat láthatja, amelyek a beteg kezeléséhez szükségesek.

A betegeknek lehetőségük van a róluk szóló információkat szűrni, egyes esetekben az azokhoz való hozzáférést letiltani. Az EESZT-t mint alapvetően felhőalapú technológiára épülő szolgáltatást az Állami Egészségügyi Ellátó Központ vezette konzorciumon belül került fejlesztették ki.

A lakosság a szolgáltatáshoz ügyfélkapus azonosítást követően férhet hozzá, illetve egy lakossági portálon keresztül veheti azt igénybe. A belépést követően az ügyfél megtekintheti a számára felírt e-recepteket és e-beutalókat, valamint információkat kaphat a különböző egészségügyi vizsgálatokkal kapcsolatban. Visszamenőleg is lehetőség van az elvégzett vizsgálatok eredményeinek áttekintésére, letöltésére, legyenek azok laborvizsgálatok eredményei vagy képalkotó eljárással (röntgen, CT, MRI) készült vizsgálatok.

A sürgősségi ellátás számára lehetőség van úgynevezett e-profil létrehozására, amely felületen olyan fontos információkat tud megadni magáról az ügyfél (azaz a beteg), mint a vércsoportja, esetleges allergiája, egyéb allergén anyagok, gyógyszerérzékenysége, krónikus betegségei. Adott esetben ezekhez az adatokhoz a sürgősségi ellátást végzők nagyon rövid időn belül hozzáférhetnek, szintén növelve ezzel az ellátás biztonságát, végső soron a betegbiztonságot.

Az információkhoz való hozzáférésről, azok lekérdezéséről, azaz hogy ki, mikor és milyen információkat kért le róla, értesítést kaphat. A rendszert a Nemzeti Adatvédelmi és Információszabadság Hatóság

a megfelelő jogi környezet, az adott adatkezelési tevékenységhez tartozó konkrét cél, időtartam és a lehető legszűkebb adatkör, valamint a felhasználók tájékoztatása kritériumai alapján megvizsgálta, kisebb módosítások elvégzését követően pedig hitelesítette. (Kormány 2017; 39/2016. EMMI rendelet)

1.2.6. Közösség, hálózat, média

A közösségi oldalak térnyerése vitathatatlan, hiszen a társadalom legszélesebb rétegei számára ezek a szolgáltatások a mindennapok szerves részévé váltak.

A Facebook, a Twitter, a Youtube, az Instagram, a LinkedIn és más közösségi oldalak naponta több tízmillió embert vonzanak. Ráadásul ma már számos olyan közösségi médium van, amelyek egy-egy szubkultúra részét alkotják, akár korosztályi alapon is elkülönülve, hiszen majdnem kizárólag csak egy-egy nagyon jól körülhatárolható korosztály használja például az olyan médiumot, mint például az Ask.fm.

A legnépszerűbb közösségi oldal azonban kétségkívül a 2003-ban világhódító útjára indult Facebook, amelynek 2017. év elején több mint 1,8 milliárd aktív felhasználója volt. (Statista 2017a)

Magyar felhasználók és a Facebook

Magyarországon több mint 4 millió (egészen pontosan 4,13 millió) aktív Facebook-felhasználó volt 2017 év elején. (Statista 2017b)

Ez a teljes magyar internetfelhasználók számával összehasonlítva (71%-os a naponta internetet használók teljes lakossághoz viszonyított aránya, amely közel 7 millió fő) 59%-os arányt jelent.

2015 novemberében tette közzé a Magyarországi Tartalomszolgáltatók Egyesülete és az NRC Kft. azt a közös jelentését, amelyben a hazai Facebook-használat különböző trendjeit és statisztikai adatait mutatták be.

A kutatás célja az volt, hogy általánosságban megvizsgálják a hazai felhasználói szokásokat, valamint fő célként jelentkezett, hogy feltérképezzék a tartalomfogyasztás, ezen belül is a fogyasztott tartalmak típusait. Ennek megfelelően a felmérés vizsgálta a felhasználók Facebookkal

kapcsolatos szokásait, az ott elérhető különböző funkciók használatát, valamint a közösségi oldalon eltöltött idő hosszát. Nem túl meglepő módon a kutatási jelentés szerint a magyarországi Facebook-felhasználók átlagosan napi 86 percet töltenek az oldalon. A legaktívabb felhasználók a nők, illetve a 30 év alatti korosztály. A felmérés kitért arra is, hogy milyen eszközön keresztül történik a közösségi oldal elérése. A felmérésből kiderül, hogy minél több időt tölt valaki az oldalon átlagosan, annál valószínűbb, hogy okostelefonját vagy más mobil eszközét is használja. A felhasználók kétharmada követ valamilyen internetes portált, amelyek között nagy számmal akadnak hírportálok, blogok. A legtöbb felhasználó által követett oldalak között akadnak hírportálok (például Index, Nők Lapja Café, HVG) és olyan oldalak is, amelyek külön a Facebookra specializálódtak. A felhasználók a leghitelesebbnek vélt oldalak között nem tesznek szignifikáns különbséget, hiszen az ebben a kategóriában első helyre sorolt Index (18%) mellett megjelenik az olyan blogoldal is, mint például a receptneked.hu (12%). (MTE 2016)

Ez a hatalmas felhasználói szám már önmagában is értékes. Ugyanakkor ha a felhasználók adatait tekintjük értéknek, ez az értékesség hatványozottan igaz. A Facebook ma már több mint 2 milliárd felhasználója azt is jelenti, hogy a világ internethasználóinak jóval több mint a fele csatlakozott, és használja ezt a felületet. Ebből az is következik, hogy a Facebook számtalan információval rendelkezik a világ internethasználóinak közel kétharmadáról. A cég ezt alapesetben a saját tevékenységének fejlesztése érdekében használja fel, de ezek közül az információk közül szép számmal el is ad jónéhányat.[36]

[36] Ezek az értékesített adatok nyilvánvalóan adatbázisokat, illetve azokkal való munkát jelentenek. Számos alkalommal kerül azonban napvilágra olyan eset, amikor ezekben vagy ezeken az adatbázisokon keresztül szereztek további információkat vagy az adatokat a fejlesztők, az adatokat megvásárló cégek vagy akár nemzetbiztonsági szolgálatok. Az egyik leghíresebb ilyen eset a *Geofeedia* nevű, alapvetően a helyadatok elemzését végző cég tevékenysége miatt robbant ki. A Geofeedia, illetve annak szoftverei nemcsak a Facebookon, hanem a Twitteren és az Instagramon gyűjtöttek adatokat tüntetőkről rendőrségi céllal. Ennek hatására a Facebook többször is hangsúlyozta, hogy az ilyen célzott információszerzés ellenkezik a cég irányelveivel. (Conger 2017)

Ráadásul a Facebook a közösségi oldalakhoz, valamint számos más kibertéri szereplőhöz – például a Google-hoz – hasonlóan a felhasználók legtöbb online tevékenységét rögzíti, azokat megőrzi, sőt azokból számos olyan következtetést is levon, amelyekkel még talán a felhasználók sincsenek mindig tisztában. Persze ezeket az adatokat a felhasználók önként adják át a Facebooknak, hiszen elfogadják a közösségi oldal adatkezelési szabályzatát. Ez a szabályzat pedig elég egyértelműen fogalmaz, amikor leírja a felhasználóknak, hogy milyen adatokat is gyűjt róluk. Ezek szerint az oldal rögzíti a műveleteket, amelyeket a felhasználó végrehajt, illetve az információkat, amelyeket a felhasználó megad; az olyan műveleteket, amelyeket mások hajtanak végre, illetve az információkat, amelyeket a felhasználók profiljuk beállítása során megadnak. A Facebook rögzíti a tagok közösségeit és kapcsolatait, valamint a fizetési műveletekkel kapcsolatos információkat is. Mindezeken túl minden olyan adatot és információt is eltárol a cég, amelyek a felhasználók különböző – Facebookkal nyilvánvalóan valamilyen interakcióba kerülő eszközeinek (például mobiltelefon vagy egyéb mobil eszköz) – technikai adataival kapcsolatosak. A rögzített adatok között vannak a szolgáltatásokat használó által meglátogatott webhelyekről és alkalmazásokból származó információk is. (Facebook 2017)

Mindezekből nem nehéz levonni azt a következtetést, hogy a Facebook nagyon-nagyon sok mindent tud rólunk, felhasználókról. Ismeri a szokásainkat, érdeklődési körünket, barátainkat, tudja, hogy milyen eszközöket használunk, azokat milyen gyakran cseréljük, sőt még azt is nyomon tudja követni, hogy hol vagyunk. Ennek tükrében természetszerűleg következik az, hogy a felhasználóknak megfelelő biztonságtudatossággal kell vagy kellene rendelkeznie nemcsak a Facebook, hanem más közösségi médium használata során is. A közösségi oldalak használatával összefüggő kockázatokat nagyon sokszor ma már a biztonságtudatossági oktatások részévé is teszik, amelyek során természetesen elsősorban nem a közösségi oldal üzemeltetői által jelentett

kockázatokra, hanem a felületen megadott és nem megfelelően kezelt adatokkal és információkkal visszaélőkre hívják fel a figyelmet.

2017. év elején tette közzé a hazai Társadalomkutató Kft. a *Magyar Ifjúság 2016: Az ifjúságkutatás első eredményei. Ezek a magyar fiatalok* című kutatási jelentését, amelyben nyolcezer magyar fiatalt kérdeztek meg többek között a digitálismédia-fogyasztási szokásaikról. A felmérésben résztvevők száma meglehetősen nagy, így akár reprezentatív felmérésnek is elfogadhatjuk a kutatási jelentést. A dokumentum rámutat, hogy a digitalizáció alapvető társadalmi változásokat hozott, amely változások nagyon sok esetben a fiatal generáció esetében mérhetőek a legmarkánsabban. (Bauer et al. 2017)

A jelentés adatai alapján a fiatalok (15–29 éves korosztály) 85%-a otthonában már megtalálható a számítógép, amíg ez az arány 2000-ben csak 29% volt. Interneteléréssel a fiatalok háztartásainak a 87%-a rendelkezik (2000-ben ez a szám még csak 9% volt). Okostelefonnal e korosztály szintén 85%-a rendelkezik. A felmérés szerint ebben a korosztályban a naponta internetet használók aránya 88%-os. (Bauer et al. 2017)

Ez a korábban bemutatott hazai átlagos 70,7%-os napi internethasználati aránynál lényegesen magasabb, azaz a fiatal generáció tagjai közül messze többen használják az internetet naponta, mint a lakosság más korosztályba eső tagjai.[37]

A felmérésből az is kiderül, hogy a magyarországi fiatalok 79%-a tagja valamelyik közösségi oldalnak. Ezeken belül is messze a Facebook vezet (a fiatalok 55%-a naponta többször is használja ezt a platformot), majd az Instagram (8%-a naponta többször is használja) és a Twitter (6%-a naponta többször is használja) következik. (Bauer et al. 2017)

[37] Korábbi statisztikai elemzéseinknél már utaltunk rá, hogy a mintavételek általában a 16–74 éves korosztály esetében történnek meg. Ennek oka elsősorban az, hogy az internetfelhasználók korosztályi ollója az elmúlt években alaposan szétnyílt. Amíg korábban a rendszeres internethasználók a 18–49-es korosztályba voltak tehetők, addig ma az olló szétnyílik, és a 16–74 éves korosztály tekintetében is viszonylag kiegyensúlyozott képet mutat. Ugyanakkor e fenti tényből, miszerint a vizsgált több ezer fiatal (15–29 évesek) körében jóval magasabb a naponta internetet használók száma, arra is következtethetünk, hogy ez az egyenletes kép még mindig nem teljesen homogén.

Nagyon beszédes a jelentés azon része, amely az internetes közösségi oldalak használati céljait elemezte.[38] Eszerint a fiatalok 30%-a szórakozásra, 22%-a tájékozódásra, 16%-a pedig a helyi hírekkel kapcsolatos információszerzésre használja a közösségi oldalakat. (Bauer et al. 2017)

Az nyilvánvaló tény, hogy az internetes közösségi oldalak ilyen magas felhasználói száma, illetve magas aránya számos nagyon előremutató társadalmi szolgáltatást (funkciót) is hatékonyabbá tehet. Önmagában a közösségi oldalak biztonságos használatának oktatása, illetve általában a biztonságtudatos felhasználói viselkedés legalapvetőbb szabályai rendkívül gyorsan és hatékonyan juttathatók el nagy tömegekhez. Így számos olyan kampány vezethet eredményre, amely ezen szolgáltatások nélkül, csak jóval nagyobb anyagi erőforrással és több idő alatt, nem utolsósorban kisebb hatékonysággal lenne kivitelezhető.

1.3. Digitalizált környezetünk és otthonunk

A korábban bemutatott elemzéseinkből is kiderül, hogy a világ népességének közel a fele használja az internetet. Számítógépből, illetve olyan eszközből pedig, amely képes a hálózati csatlakozásra, ennél hatványozottabban több van.[39]

---

38 Az Európai Unió Egységes Digitális Piaci Stratégiájának megalkotása után két évvel az Európai Bizottság egy jelentésében megállapítja, hogy a társadalom alapvető digitális fogyasztási szokásai is alakulnak. Az emberek a híreket már túlnyomó többségben nem a televízióból, hanem az internetről, ott is elsősorban a közösségi oldalakon keresztül szerzik. (European Commission 2015a)

39 Még megbecsülni is igen nehéz, hogy hány darab számítógép van a világon. Ugyanakkor éves lebontásban az eladott számítógépek száma nagy közelítéssel megadható. A Gartner szerint 2017-ben 2,32 milliárd új számítógép talált gazdára. Ebben benne vannak a hagyományos PC-k és az okostelefonok is. Gartner az eladott számítógépek számát 2019-re 2,38 milliárd darabban prognosztizálja. (Gartner 2017) Ezek a számok azonban nem tartalmazzák az egyéb olyan eszközöket, mint amelyeket az IoT kategóriába sorolunk.

Néhány éve jelent meg a kifejezés: „dolgok internete", valamint az ehhez nagyon hasonló olyan fogalmak (és természetesen az ezek mögött lévő tartalom), mint az okosvárosok.

Persze felmerül a kérdés, hogy a dolgoknak hogyan lehet internete, és vajon mitől okos egy város. Beszélhetünk-e ebben az értelemben arról, hogy azok a funkciók, amelyek egy város életét támogatják és kiszolgálják, valóban okosak?

A 21. század hajnalán – egészen pontosan 2014-ben – az emberiség 54%-a városban[40] él. Ez az arány 1950-ben még csak 30% volt, viszont az ENSZ[41] előrejelzése alapján már több mint 66% várható.[42] (UN DESA 2014b)

Ezeknek az adatoknak a birtokában (is) szükséges egy pillantást vetni azokra a szolgáltatásokra, amelyek jórészt a digitális technológia révén hozzájárulnak azoknak a funkcióknak az ellátásához, amelyek a városokban elengedhetetlenül szükségesek a viszonylag limitált földrajzi környezetben élő nagyszámú, ennélfogva nagyon sűrűn élő emberek kiszolgálásához, ellátásához. Az alapvető közművek városi környezetben nemcsak a villamosenergiát vagy a vezetékes vizet jelentik, hanem többek között a gyors információcserét lehetővé tevő széles sávú internetet, a városi forgalom digitalizáció révén létrejövő optimális és hatékony szervezését vagy akár a logisztikai ellátás zökkenőmentességét, illetve akár a parkolás minél hatékonyabb lebonyolítását is.

Mielőtt azonban ezt megtennénk, fontos áttekinteni, hogy mit is jelent a dolgok internete, hiszen az okosvárosokban vagy akár az okosotthonainkban is számos olyan eszközt használunk, amelyek hálózatba kapcsolva működnek, így kommunikálnak és gyűjtenek adatokat,

---

40 Az ENSZ-felmérés értelmezésében a városok azok az urbanizált területek, amelyekbe beletartoznak a városok agglomerációs területei is.

41 Az ENSZ Gazdasági és Szociális Szervezetének népességgel foglalkozó egysége (The Population Division of the Department of Economic and Social Affairs of the United Nations) 1988 óta minden évben kiadja és pontosítja a népesség várható alakulásáról szóló jelentését, illetve előrejelzését. (UN DESA 2014a)

42 Magyarország esetében 71%-os urbanizációs értéket jelentett az ENSZ 2015-ben. (UN DESA 2014c)

amelyeket szintén a hálózat segítségével továbbítanak, nem mellesleg ezek az eszközök akár a fizikai térben is végeznek valamilyen műveletet.

1.3.1. Számítógépet mindenhova és mindenre, avagy a dolgok internete

Az elmúlt években a széles sávú internet elterjedésének, valamint az egyre olcsóbb hálózati kapcsolódásra képes milliónyi eszköznek köszönhetően rohamosan terjed a dolgok internete, azaz az *Internet of Things* (IoT)[43] fogalom.

Az IoT-technológia rendkívül gyors ütemű fejlődése a számítási felhők által széleskörben elérhetővé vált adatok és elemzési képességek gyors növekedésének, az intelligens (okos) mobil eszközök számának és képességei gyors növekedésének, az ipari intelligens mobil eszközök közötti összekapcsolódás egyszerűbbé és hatékonyabbá válásának, valamint az ipari és vállalati hálózatok konvergenciájának köszönhető. Mindezen tényezők együtt járulnak hozzá az olyan szolgáltatások fejlődéséhez, amelyek konvergens módon tartalmazzák az intelligens mérőeszközök, az eszközkövetés, a digitális egészségügyi monitorozás vagy a biztonságtechnikai eszközök és egyéb ehhez hasonló rendszerek – nagyon sok esetben emberi beavatkozás nélküli – működését. (Cisco 2014)

A „dolgok internete” kifejezést először Kevin Ashton, a Procter & Gamble marketingmenedzsere használta 1999-ben, aki a cég egyik termékéért, nevezetesen egy rúzsért volt felelős. A termék azonban váratlanul elfogyott a boltok polcairól, és Ashton ennek okát kutatva

[43] A *dolgok internete,* azaz az *Internet of Things* kifejezés terjedt el. Ugyanakkor egy bővebb fogalommal, az *Internet of Everything,* azaz a *minden internete* fogalommal is gyakran találkozunk. Ez azonban az IoT-nél bővebb tartalommal bír, amelybe a hálózatba kapcsolódó emberek, adatok, dolgok, valamint kapcsolódó eljárások is beletartozhatnak.

az ellátási láncban azonosított egy problémát. E probléma megoldásának keresése arra késztette, hogy megvizsgálja az RFID-technológia (Radio Frequency Identification, azaz rádiófrekvenciás azonosítás) alkalmazhatóságát ezen a területen. A történet az MIT-n, azaz Massachusetts Institute of Technology-n folytatódott, amikor az egyetem Ashtont kérte fel az RFID kutatásával és fejlesztésével foglalkozó – Auto-ID Center – csoport vezetésére. (Maney 2014)

A különböző tárgyak az RFID-technológia segítségével egyedileg is azonosíthatóak, és innen már csak egy ugrás a dolgok internete. A dolgok internete ma azoknak az eszközöknek a gyűjtőfogalma, amelyek hálózatba kapcsolódnak, azaz olyan csatlakoztatott eszközök, amelyek lehetnek fizikai eszközök, épületek szenzorai, ipari vezérlőelemek, járművek elektronikai berendezései vagy akár a lakásunkban található elektronikai eszközök is. Ezek képesek emberi beavatkozás nélkül is egymással kapcsolatot teremteni és kommunikálni, ráadásul az adatok gyűjtésén és továbbításán kívül képesek a fizikai térben különböző interakciók kiváltására vagy a fizikai térben a folyamatokba való beavatkozásra.

Az eszközök egymás közötti, emberi beavatkozás nélküli kommunikációja az M2M kommunikáció, azaz a *machine-to-machine,* azaz gép-gép közötti kommunikáció. Ehhez a gép-gép közötti kommunikációhoz természetesen olyan (számító)gépek kellenek mindkét oldalon (azaz adó és vevő oldalon egyaránt), amelyek rendelkeznek a kommunikációhoz szükséges technológiával. Ez persze nyilvánvalónak hangzik, de ha belegondolunk kommunikációelméleti szempontból abba, hogy az adó-vevő, átviteli közeg, közös nyelv, kódolás, dekódolás, zavarszűrés stb. mindegyike – ráadásul egy rendszerbe integrálva – szükséges a sikeres és nem utolsósorban hatékony, azaz érthető kommunikációhoz, már nem is annyira egyértelmű a dolog. A technológia alapfolyamataiban szerepet kap az adatgyűjtés, az adattovábbítás, az adatfeldolgozás és értékelés, majd a beavatkozás, azaz a megfelelő folyamatok elindítása, illetve azok felügyelete

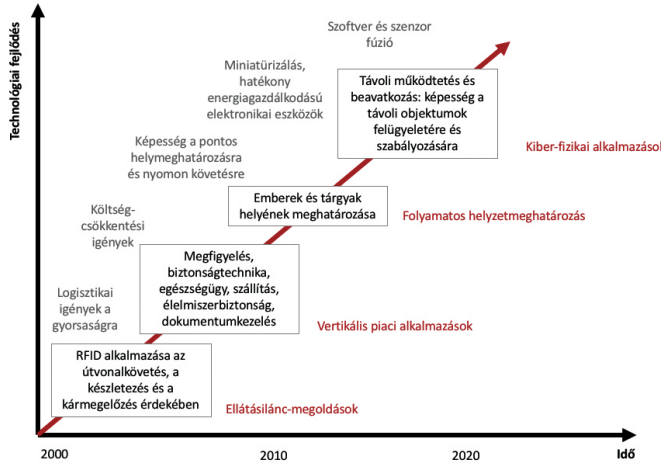
(a folyamatok sikerességének hasonló folyamaton keresztüli megítélése), mindez akár emberi beavatkozás nélkül.

Ugyanakkor ennek a folyamatnak nyilvánvalóan az egyik kulcsfontosságú eleme az adatok továbbítása lesz a hálózaton. Addig, amíg a vezetékes hálózatok voltak túlsúlyban, magától értetődően ezeket a hálózatokat (például telefonhálózatok kiépített vonalait) használták az adattovábbításra. Azonban a vezeték nélküli kommunikáció robbanásszerű elterjedése hatalmas lökést adott az M2M kommunikáció fejlődésének, mint ahogyan sok más közvetlen vagy akár közvetett szolgáltatásnak is. Mindezek alapján az M2M kommunikáció felhasználási területei ma már lényegesen szélesebb spektrumon mozognak, mint a tisztán vezetékes kommunikáció idejében, hiszen az ipar, a gépjárművek, a biztonságtechnika, a logisztika, de még akár a mezőgazdaság[44] is rendkívül hatékonyan tudja használni ezt a technológiát.

Az ITU Stratégiai és Politikai Egysége (Strategy and Policy Unit – SPU) elemzői 2005-ben készítettek egy jelentést, amelyben az IoT-jelenséget elemezték. Ebben a jelentésben áttekintették az olyan új technológiáknak, mint például az RFID, illetve azoknak az intelligens informatikai eszközöknek az akkori és várható jövőbeli helyzetét, amelyek összekapcsolt, azaz hálózatos eszközökként működnek, és amelyek releváns tartalmat és információt szolgáltatnak a felhasználó helyétől függetlenül. Ebben a jelentésben nagyon jól nyomon követhető, hogy az akkor még csak a fejlesztések elején tartó RFID-technológia alapján hogyan is jutunk el napjainkra a dolgok internetéig: „Minden, a gumiktól a fogkefékig, kommunikálni fog, ami egy

[44] Az M2M kommunikáció mezőgazdaságban való megjelenésére számos már működő gyakorlati példa létezik. Ilyenek például az automata öntözőrendszerek különböző funkcióiban szerepet játszó érzékelő-beavatkozó (például nedvességmérő, helymeghatározó) alrendszerek, a talajszerkezet változását érzékelő és elemző, majd a megfelelő szerves anyag kijuttatását végző rendszerek vagy akár a növényvédő szerek megfelelő dózisban és a megfelelő helyre való kijuttatásában szerepet játszó eszközök és rendszerek.

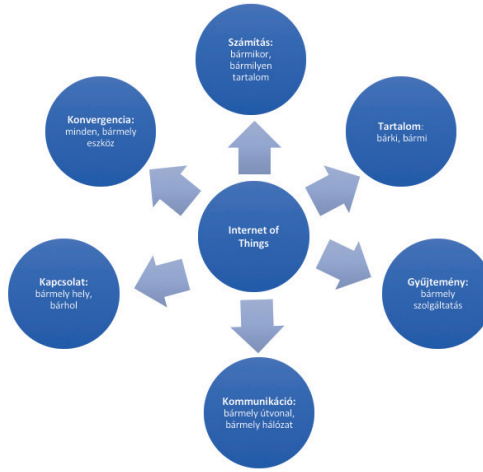
olyan új korszak kezdetét jelképezi, amelyben a ma internete (az adatok és az emberek közötti hagyományos internet) átalakul a holnap dolgok internetévé." (ITU 2005)



30. ábra
Az IoT-technológia fejlődése

Forrás: Sarwar 2012, a szerző szerkesztése

Az ITU-T Y.2060 (06/2012) ajánlásában egy többé-kevésbé jól megfogalmazott definíciót is adott az IoT-re, amely szerint „[a] dolgok internete az információs társadalom globális infrastruktúrája, amely lehetővé teszi a fejlett szolgáltatások összekapcsolását (fizikai és virtuális értelemben egyaránt), a már meglévő és a fejlesztés alatt lévő interoperábilis infokommunikációs technológiákra építve". (ITU 2012)



31. ábra
A dolgok internete és kapcsolatai

Forrás: Sarwar 2012, a szerző szerkesztése

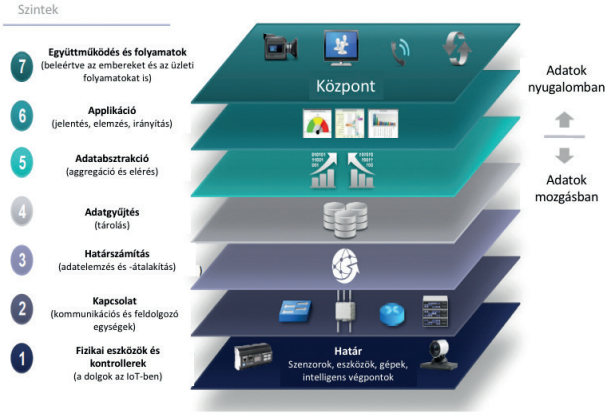
Nagyon sokszor a való világ leképezéseként vagy modellezéseként értelmezhetjük a „dolgok internete" kifejezést és a mögötte lévő tartalmat. Ez három tényezőn múlhat: nevezetesen olyan érzékelőkön, amelyek fizikai beavatkozásra is képesek; ezeket az érzékelőket összekötni képes hálózatokon; valamint olyan intelligens szoftvereken, amelyek segítségével a hálózatba kötött érzékelők adatait azok akár önállóan is fel tudják dolgozni, majd ezek alapján olyan döntéseket hoznak, amelyek az önálló fizikai beavatkozást eredményezik.

Az IoT-technológia robbanásszerű fejlődése, illetve az a tény, hogy ezeket az eszközöket az ipartól a háztartásokig mindenhol használjuk, felvetik egy olyan referenciamodell megalkotásának szükségességét, amely átláthatóvá teszi a technológiát és annak számos – főleg biztonsági – kérdését.

Az ITU kezdeményezésére létrejött egy a dolgok internetének globális szabványosítását célzó kezdeményezés (Global Standards Initiative on Internet of Things – IoT-GSI) is azzal a céllal, hogy elősegítse

az ITU-T egységes megközelítését a technikai szabványok fejlesztése érdekében. Legfőbb funkciója, hogy világszerte előkészítse a dolgok internete különböző szabványainak meghatározását és fejlesztését. Amennyiben ez a kezdeményezés sikeres lenne, az lehetővé tenné a globális szolgáltatók számára a technológia által várt széles körű szolgáltatások egységes kínálatát. (ITU 2015)

Ugyanezt tette meg a Cisco is, amikor egy tanulmányában felvázolta az IoT referenciamodelljét.



32. ábra
A Cisco „dolgok internete"-referenciamodellje

Forrás: Cisco 2014, a szerző szerkesztése

A Cisco szerint azért van szükség egy IoT-referenciamodellre, mert ez segítséget nyújthat az egyébként komplex rendszerek elemekre történő lebontásában, amivel az egyes részek kapcsolatainak és funkcióinak megértéséhez járulhat hozzá. A modell kiegészítő információkat nyújt a tárgyak internetes szintjének pontos meghatározásához, illetve egy közös terminológia létrehozásához. A referencia alapján meghatározható az adatfeldolgozás szintenkénti megvalósítása. Mindezeken túl a modell a gyártók számára – ahogyan az ITU hasonló referencia-

modellje – szabványos kialakítást is lehetővé tesz, amely megkönnyítené az eszközök egymáshoz való kapcsolódását, illetve azok interoperabilitási képességeinek javításához járulna hozzá. A modell valóságossá teszi az IoT-eszközöket és -rendszereket a koncepcionális vagy fogalmi meghatározások helyett. (Cisco 2014)

A hét egymást kiegészítő és egymást támogató réteg közül az első a fizikai réteg. Ez tartalmazza az eszközöket (ezek a dolgok internetéből a *dolgok*) és a vezérlőket. Az eszközök mérettől (amely méret lehet processzornagyságú, de akár járműméretű is), helytől és feladattól függetlenül helyet kapnak ebben a rétegben. Nagyon fontos hangsúlyozni, hogy a rétegek közötti kommunikáció nem egyirányú, hanem lentről fölfelé és onnan visszafelé is van adatáramlás, ráadásul a rétegeken belül (különösen igaz ez a fizikai rétegre) vertikálisan is van adatáramlás. Ugyanakkor fontos annak hangsúlyozása, hogy az eszközök nem mindegyike alkalmas adatfeldolgozásra, így ezek számára az adatfeldolgozás szabályozása nyilván nem értelmezhető, ugyanakkor az adatok ezen eszközökön is áthaladnak, ami azonban szabályozást igényel.

A második réteg a kommunikációt, illetve az összekapcsolást végzi. Mivel az IoT alapja a hálózatba szervezés és a kommunikáció, ezért ennek a rétegnek a legfontosabb feladata a megbízható és időbeni kommunikáció biztosítása az eszközök, a rétegek, valamint a hálózat és az eszközök között. Természetesen itt számos olyan technológia – elsősorban ma már vezeték nélküli kommunikációs kapcsolatot biztosító rendszer – elképzelhető, mint többek között a wifi, GSM, UMTS vagy akár a Bluetooth.

A harmadik réteg a számítási réteg. A réteg feladata a hálózati adatok nyers információvá[45] való átalakítása, ha kell, tárolása valamint ezek előkészítése a negyedik réteg számára.

A negyedik réteg az adatfeldolgozó réteg. Itt történik meg többek között az eszközök adatfeldolgozási képességeinek hiányában az adatok

[45] *Fog computingnak* nevezik azt az architektúrát és számítási folyamatot, amelynek fő feladata a nagy mennyiségű adatok nyers vagy előzetes feldolgozása, további információelemzésre történő előkészítése.

osztályozása, mert nem minden eszköz (vagy applikáció) igényel adatfeldolgozást. Eldöntendő kérdés ezeknek az adatoknak a tárolása vagy a hálózaton történő továbbítása, amelyet szintén ez a réteg szervez.

Az ötödik réteg az adatabsztrakciós réteg. Ez a réteg többek között egyezteti az adatformátumokat (a megfelelő formátumú adat megfelelő eszközhöz való eljuttatásának szem előtt tartásával), szemantikai szűrést végez az adatállományban, valamint megerősíti az adatok valódiságát magasabb szintű alkalmazásokhoz történő eljuttatás előtt, illetve bizonyos szintű autentikációt is végez. Az egyik legfontosabb feladat ebben a rétegben a különböző forrásokból származó adatok egyesítése és egyszerűsítése az applikációk számára történő eljuttatáshoz.

A hatodik réteg az alkalmazási réteg. Talán ez az egyike a legkomplexebb szinteknek, hiszen számos – gyökeresen eltérő – alkalmazást használnak az IoT-technológia során. Ennek megfelelően a réteg feladata az adatok elemzése, azokból jelentések összeállítása, valamint a mind az öt előző rétegre hatással lévő vezérlés.

A hetedik réteg az együttműködés és a folyamatok rétege. Itt markánsan jelenik meg a felhasználó, mert egy alkalmazást, vagy az abban megjelenő adatot akár különböző célokra is használhatnak (például üzleti, ipari), valamint számos olyan interakció születhet az ember részéről, amely új adatigénnyel vagy új adatfeldolgozással jár a modell többi rétegét is érintve. Ebből következik az IoT-technológia egyik filozófiai alapvetése is: nem az alkalmazás számára dolgozzák fel az adatokat, hanem valamilyen – alapvetően – emberi tevékenység segítése vagy akár kiváltása érdekében. (Cisco 2014)

A dolgok internete, illetve még inkább az azok által nyújtott szolgáltatások, adatok és információk összessége alaposan átalakítja a társadalmat. Ezek nemcsak kényelmi szolgáltatások, hanem nagyon sokszor más módon hasznos és a társadalom számára nagyon is értékes funkciók. Gondoljunk csak bele az okosotthonokban található intelli-

gens érzékelőkre és kiber-fizikai[46] eszközökre, amelyek például csökkentik az energiafelhasználást, vagy akár a gépjárművekben található olyan elektronikai rendszerekre, amelyek a biztonságot növelik akár azzal, hogy a sávelhagyásra figyelmeztetik az autó vezetőjét. Az IoT-technológia mégis talán az iparban és a gyártási folyamatokban jelenti a legnagyobb fejlődést.

Nagyon sok olyan vélemény is megfogalmazódik, amelyek szerint a dolgok internetén keresztül lehetővé válik a különböző fizikai jellemzők távolról történő érzékelése, azok ellenőrzése, ráadásul ehhez elegendő a meglévő hálózati infrastruktúra használata. A valós fizikai tér tehát integrálódik a kibertérbe, ami azzal az előnnyel jár, hogy jóval kevesebb humán beavatkozás szükséges a folyamatokba, ráadásul a számítógépek jóval pontosabbak (hiszen sosem hibáznak, sosem fáradnak el) és jóval hatékonyabban képesek még a legunalmasabb, illetve a legmonotonabb munkát is elvégezni.

Az IoT fogalomkörébe tehető eszközök számát csak megbecsülni lehet, hiszen eltérő adatokkal[47] találkozhatunk. Néhány elemzés már 2015-ben közel 50 milliárdra tette ezeknek az eszközöknek a számát (Cisco 2016), ugyanakkor más elemzések 2020-ra csak 24 milliárd ilyen eszközt prognosztizálnak. (Gubbi et al. 2013)

Az IoT, valamint a mögötte lévő M2M technológia meglehetősen új keletű, és mint ilyen természetszerűleg magával hozza a biztonság kérdését is. Általánosan elterjedt nézet ma, hogy az egyik legnagyobb információbiztonsági kihívást már ma is az IoT-technológia jelenti.

Az M2M technológia esetében „[p]roblémát jelenthet a mobileszközök, kommunikációs interfészek beágyazottsága, illetve az ennek következtében jelentkező szervizelési, hibajavítási, fejlesztési nehézségek felmerülése". (Bocsok et al. 2015)

---

[46] A *kiber-fizikai* jelző itt olyan eszközökre utal, amelyek mechanikai, elektronikai és informatikai elemek alkotta hálózatba vannak kötve. A hálózati kommunikációra képes eszközök a fizikai dimenzióban interakcióra – például mozgás kiváltására – képesek.

[47] Ahogy a világon megtalálható számítógépek (desktop, laptop, notebook, tablet stb.) számát is igen nehéz megadni, az IoT-eszközök számát sem tudjuk csak becsléssel felmérni.

A kommunikációs interfészek beágyazottsága, valamint az eszközök sokszor emberi beavatkozás nélküli – M2M-alapú kommunikáció szerinti – önálló azonosítása további problémát jelent, hiszen így az autentikációt gépek végzik. Ez történhet a már említett RFID-val vagy valamilyen tanúsítvánnyal. Ezek kompromittálás elleni védelme azonban jelenleg nem kielégítő.

Ugyanakkor pont a fent említett nagyszámú eszköz az, amely egyrészt magában hordozza akár az eszköz, akár a kommunikáció szintjén a sérülékenységeket és így a biztonsági kihívásokat, másrészt pedig mágnesként vonzza a támadókat. Ennek oka többrétű. Az IoT-technológia alkalmazásával, főleg, ha abban újabb és újabb sérülékenységek vannak, a támadók számára kaput is nyit a rendszereinkben tárolt adatokhoz való hozzáféréshez.

A rendkívül gyors ütemű IoT-eszköztelepítés és rendszerbe integrálás óhatatlanul azzal jár, hogy egységes és átfogó biztonsági szemlélet hiányában – akár hardver-, akár szoftveroldalról – sérülékenységet tartalmazó eszközök is bekerülnek a rendszerbe. Ez az IoT-eszközök és a hozzá kapcsolódó szoftverek és alkalmazások rendkívül felgyorsult – sokszor a piac által generált – fejlesztése miatt is bekövetkezhet. A rendelkezésre álló rövid idő alatt nem lehetséges az eszközök tervezése és gyártása során az alapvető információbiztonsági elvek figyelembevétele, ráadásul a gyors piaci ciklus nem teszi lehetővé az eszközök későbbi támogatását.

Biztonság nélkül, avagy támadás az IoT-n keresztül

A dolgok internete jelentette biztonsági kihívások és veszélyek egyik leglátványosabb és egyben legsokkolóbb példája 2016 október közepén történt. Ekkor DNS-szolgáltatásleállás következett be először az USA keleti partján, majd az Egyesült Államok más területein is, amely egyben komoly internetszolgáltatás-kiesést is eredményezett. Ráadásul,

mivel nagyon sok ázsiai IP-cím is ezeken a szolgáltatásokon keresztül érhető el, a támadás hatása jóval túlmutatott az Egyesült Államokon.

A szolgáltatások leállásának oka az volt, hogy a New Hampshire székhelyű Dyn nevű DNS-szolgáltatást nyújtó nagyvállalat szervereit masszív, nagyon erős DDoS-támadás érte. Ez önmagában még nem szokatlan, hiszen naponta érik ezen szolgáltatásokat is ilyen támadások, de annak volumene és nagysága teljesen új volt a Dyn esetében.

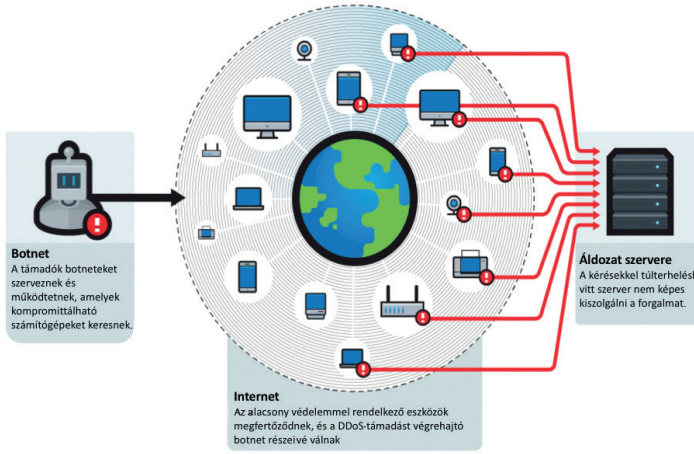
A támadás három hullámban történt. Az első, két órán keresztül tartó támadás 2016. október 21-én reggel hét órakor kezdődött, majd a második támadás ugyanezen a napon kicsit később, a délelőtti órákban kezdődött. A Dyn délután négy óra után jelentette a támadások harmadik hullámát. A támadások elsősorban a Dyn internetes címtárszolgáltatásait célozták. Az eredmény katasztrofális volt: az Egyesült Államokban – többnyire a keleti parton, de később az ország más területein is – leállt a DNS-szoltáltatás, aminek következményeként több tízmillió IP-cím vált elérhetetlenné. (Newman 2016)

Az első jelentések után nyilvánvalóvá vált, hogy a támadás egy jól felépített DDoS-támadássorozat volt. Ebben a túlterheléses támadásban alapvetően IoT-eszközökre épülő botnet(ek) vettek részt. Az elemzések alapján nagy bizonyossággal kijelenthető, hogy a támadásban nagy szerepe volt a Mirai[48] néven ismert malware-nek, amelyet alapvetően hálózatba kötött IoT-eszközökre fejlesztettek ki.

A Trend Micro elemzése szerint közel százezer Mirai által megfertőzött IoT-eszköz vett részt a támadásban. (Trend Micro 2017a)

Ugyanakkor ez a szám – összehasonlítva a támadások volumenét – valószínűleg meglehetősen alulbecsült.

[48] A Mirai egy olyan rosszindulatú program, amely a hálózati eszközöket távvezérelt botnettagokká alakítja, így azok nagyszabású hálózati támadásokban használhatókká válnak. A Mirai elsősorban olyan online eszközöket céloz meg, mint az IP-kamerák vagy a háztartásokban használt routerek. (Herzberg–Bekerman–Zeifman 2016)



33. ábra
A Mirai által fertőzött IoT-eszközökkel elkövetett támadás vázlata

Forrás: Trend Micro 2017a, a szerző szerkesztése

Mégis van IoT-biztonság?

A fenti eset is rávilágít az IoT egyre növekvő biztonsági problémáira. A ma már több milliárdra tehető IoT fogalomkörébe tartozó eszköz jelentős része gyakorlatilag semmilyen védelmi megoldással nem rendelkezik. Bár ezek az eszközök gyakorlatilag számítógépek, még sincs hálózati védelmük, gyakran hiányzik a hozzáférés védelme is, nem beszélve a sérülékenységek javítási lehetőségeinek teljes hiányáról.

Az OWASP (Open Web Application Security Project) alapítvány IoT Sérülékenységek Projektje[49] (IoT Vulnerabilities Project) folyama-

[49] Az OWASP IoT-projekt célja, hogy segítse a gyártókat, a fejlesztőket és a felhasználókat abban, hogy jobban megértsék a dolgok internetével kapcsolatos biztonsági kérdéseket, valamint hogy a felhasználók, legyen szó bármilyen környezetről is, biztonsági szempontból jobb döntéseket hozhassanak az IoT-technológiák építése, telepítése és értékelése során. (OWASP 2017A)

tosan értékeli a dolgok internete területén meglévő biztonsági kihívásokat és sérülékenységeket. Ezek közül a legfontosabbakat és a legtöbbször előforduló sérülékenységeket egy adatbázisba rendezve, a támadási felületek alapján is kategorizálva nyilvánossá is teszi.

Az OWASP adatai alapján az IoT legfontosabb sérülékenységeit foglalja össze a következő táblázat.

4. táblázat
IoT-sérülékenységek az OWASP alapján

Sérülékenység	Támadási felület	Összegzés
Felhasználónév-számlálás	Felügyeleti interfész Készülék webes felülete Felhőfelület Mobilalkalmazás	Valós felhasználónevek gyűjtésének képessége a hitelesítési mechanizmussal kölcsönhatása kihasználásával
Gyenge jelszavak	Felügyeleti interfész Készülék webes felülete Felhőfelület Mobilalkalmazás	A fiók jelszavait például „1234” vagy „123456”-ra állíthatja. Előre programozott alapértelmezett jelszavak használata
Fiók kizárása	Felügyeleti interfész Készülék webes felülete Felhőfelület Mobilalkalmazás	Lehetőség a hitelesítési kísérletek továbbküldésére 3−5 bejelentkezési kísérlet után
Titkosítatlan szolgáltatások	Eszközhálózati szolgáltatások	A hálózati szolgáltatások nem megfelelően vannak titkosítva, így nem akadályozzák meg, hogy a támadók lehallgassák vagy manipulálják a hálózatot/adatokat.
Kétfaktoros hitelesítés	Felügyeleti interfész Cloud webes felület Mobilalkalmazás	Kétszeres hitelesítési mechanizmusok hiánya, például token- vagy ujjlenyomatszkenner

Sérülékenység	Támadási felület	Összegzés
Gyenge titkosítás	Eszközhálózati szolgáltatások	A titkosítás végrehajtása helytelenül van beállítva, vagy nem megfelelően frissül, például az SSL v2 használatával.
A frissítés titkosítás nélkül	Frissítési mechanizmus	A frissítések TLS használata vagy a frissítési fájl titkosítása nélkül kerülnek továbbításra.
Frissítés írható helyre	Frissítési mechanizmus	A frissítési fájlok tárolási helye bárhonnan írható, ami lehetővé teszi a firmware módosítását és az összes felhasználó számára terjesztését.
DoS	Eszközhálózati szolgáltatások	A szolgáltatás megtámadható túlterheléses támadással.
A tárolóeszköz eltávolítása	Készülékfizikai interfészek	Az adathordozó fizikailag eltávolítható az eszközből.
Nincs kézi frissítési mechanizmus	Frissítési mechanizmus	Nincs lehetőség az eszköz frissítésének kézi ellenőrzésére.
Hiányzó frissítési mechanizmus	Frissítési mechanizmus	Az eszköz frissítésére nincs lehetőség.
Firmware verzió megjelenítése és/vagy utolsó frissítés dátuma	Eszköz firmware	A jelenlegi firmware verzió nem jelenik meg, és/vagy az utolsó frissítési dátum nem jelenik meg.
Firmware és tároló extrakció	Szerviz interfész Labormérés OTA-frissítés lehallgatása Letöltés a gyártó weboldaláról eMMC lehallgatás Az SPI Flash/eMMC chip törése és adapterben való olvasása	A firmware sok hasznos információt tartalmaz, például a forráskódot és a futó szolgáltatások bináris kódjait, előre beállított jelszavakat, SSH-kulcsokat stb.

Sérülékenység	Támadási felület	Összegzés
A készülék kódvégrehajtási folyamatának manipulálása	Szerviz interfész Oldalsócsatorna-támadások	Különböző csatlakozásokon keresztül módosíthatjuk a készülék firmware-jének végrehajtását, és szinte az összes szoftveralapú biztonsági vezérlőt megkerülhetjük. Az oldalcsatornás támadások módosíthatják a végrehajtási folyamatot is, vagy információkat szerezhetnek meg az eszközről.
A konzol elérése	Soros interfészek	Soros interfészhez való csatlakozás esetén teljes konzolhozzáférés szerezhető egy eszközhöz Általában a biztonsági intézkedések magukban foglalják az egyéni rendszerindító eszközöket, amelyek megakadályozzák a támadó egyetlen felhasználói módba való belépését, de így azt is megkerülhetik.
Nem biztonságos külső gyártók	Szoftverek	Elavult Open SSL, SSH, webszerverek stb.

Forrás: OWASP 2017b, a szerző szerkesztése

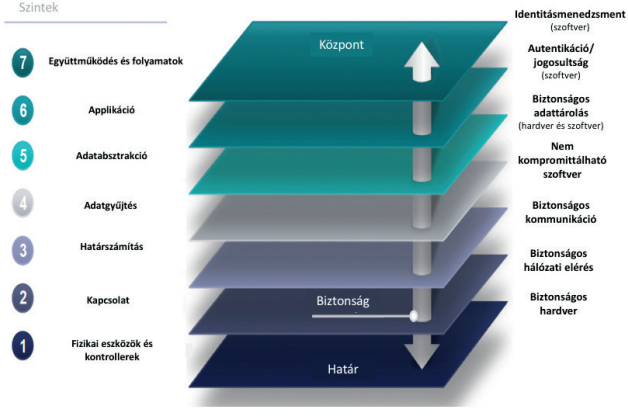
Pedig a védelem az IoT-k esetében is megvalósítható, hiszen a sérülékenységek jelentős része már ismert.

A védelem ezen a területen is – mint ahogy a későbbiekben többször is utalni fogunk rá – legalább két szereplőre bontható. Egyrészről megjelenik a gyártók felelőssége. Természetesen ennek nemcsak üzleti kérdésnek kell lennie, hanem ahogyan a felhasználóktól elvárjuk a biztonságtudatos eszköz- és szolgáltatáshasználatot, úgy a gyártókkal szemben is természetes módon kellene megjelennie. Persze a kérdés nem ennyire egyszerű, hiszen a piaci verseny és annak szabályai (vagy

szabálytalanságai) nagyon sokszor felülírják ezt a biztonságtudatos fejlesztést, programozást és végső soron a gyártást is. Mindezek mellett a folyamatos, tehát az eszközök és rendszerek teljes életciklusára kiterjedő kockázatértékelés, a kommunikációs protokollok, valamint a szoftvertámogatás (Software Development Kits – SDKs) biztosítása az IoT-eszközöket gyártókra is igaz kellene, hogy legyen.

A másik oldalról viszont valóban felmerül a felhasználók felelőssége is. Technikai segítséget mindenesetre kapnak az IoT-felhasználók, hiszen számos olyan eszköz-, rendszer- és szoftverkomponens létezik már ma is, amelyek elsődleges célja az IoT-rendszerek biztonságának növelése. Ugyanakkor ha a felhasználó biztonságtudatossága a gyári felhasználónevek jelszavainak megváltoztatását sem éri el, akkor az IoT-eszközökkel elkövetett, a Dynhez hasonló támadásokat kell feltételeznünk a jövőben is.

A biztonság Cisco referenciamodelljét felhasználva tehát mind a hét rétegben – komplex módon – kell megvalósulnia.



34. ábra
A dolgok internetének biztonsági modellje

Forrás: Cisco 2014, a szerző szerkesztése

Az első rétegben, azaz a fizikai rétegben biztonságos eszközöket kell használni. Itt mindenképpen a hardvergyártók felelőssége merül fel elsőként. A második rétegben, azaz a kapcsolati rétegben a hardverre és a különböző protokollokra alapuló biztonságos hálózati kapcsolat elérését kell megvalósítani. A következő rétegben – azaz a számítási rétegben – el kell végezni a titkosítást, hiszen itt már feldolgozott adatok találhatóak. Az adatfeldolgozói rétegben az adatok konzisztenciája és azok integritása a védendő cél, azaz szoftveres védelem szükséges az adatok módosítása ellen. Az absztrakciós rétegben a biztonságos adattárolást kell megvalósítani. Az alkalmazási réteg komoly autentikációt és jogosultság-ellenőrzést igényel. Az együttműködés és folyamatok réteg pedig identitásmenedzsmentet igényel. (Cisco 2014)

Pedig az IoT felhasználási területei egyre nőnek. A dolgok internete különböző helyeken jelenik meg. Ott van az ipari folyamatokban, a közlekedésben, akár az autóinkban, az épületeinkben, amelyek így egyre okosabbak lesznek, vagy akár a városokban, ahol a különböző társadalmi szolgáltatásokban játszanak egyre inkább nélkülözhetetlen szerepet.

1.3.2. Okosautók

A 21. századi autók esetében egyre több olyan eszközzel találkozhatunk, amelyek számítógép-vezérlésűek, vagy valamilyen számítógép-hálózati csatlakozással, ezen belül is egyre gyakrabban vezeték nélküli hálózati hozzáféréssel, illetve erre épülő adatátvitellel rendelkeznek. Ezek egyrészt a biztonságot növelő, másrészt a kényelmi funkciókat emelő eszközök és rendszerek megjelenésének köszönhetők. Egy mai gépjárműnek már alapvető tartozéka az elektronikus indításgátló, a keréknyomás-ellenőrző vagy akár az ABS-rendszer, de a korszerűbb autókban ugyanígy megtaláljuk a vezeték nélküli szórakoztató rendszereket, amelyekhez az okostelefonjainkat szintén

vezeték nélkül tudjuk csatlakoztatni, vagy akár az olyan rendszereket is, amelyek a jelzőtáblák felismerését végzik, az intelligens navigációról már nem is beszélve.[50] A szenzorok árának drasztikus csökkenésével egyre több rendszer vezeték nélkül kapcsolódik a fedélzeti számítógéphez, azaz vezeték nélkül szolgáltatja a funkciójának megfelelő adatokat.

Így a dolgok internete az autók esetében is megjelenik, hiszen azok a rendszerek, amelyek az autóinkban egyre nagyobb számban és egyre inkább kiterjesztett funkciókkal jelennek meg, már egymással is képesek kommunikálni, és képesek a fizikai térben is különböző beavatkozásokra.[51]

Mindezek mellett a közúti forgalomban is megjelentek az – egyelőre még korlátozott mértékben ugyan, de – önvezetésre is képes autók. Ennek talán első és egyben leghíresebb példája a Tesla. Ez az autó már

[50] Természetesen ezeken kívül is találunk számos olyan elektronikai vagy számítógépes megoldást, amelyek a biztonságot vagy a kényelmet szolgálják. Némelyek, mint az OBU City GPS-alapú, automatikus parkolást nyújtó szolgáltatása, már túlnyúlnak az autón, és inkább az okosváros-koncepcióval mutatnak komoly átfedést. Ez a szolgáltatás egy, a gépjárműbe beépített eszköz segítségével, akár az okostelefonunktól függetlenül is, mindig pontosan meg tudja határozni, hogy mikor és hol parkolunk az autónkkal, mikor kezdtük és mikor fejeztük be a parkolást, így csak addig fizetjük a parkolást, amíg azt valóban igénybe vesszük. (ObuCity 2017)

[51] Ezek a kiber-fizikai rendszerek (cyber-physical systems – CPS), amely rendszerek a kibertérben megjelenő utasítás vagy vezérlés hatására a fizikai térben, például egy aktuátor vagy manipulátor segítségével valamilyen fizikai változást (például mozgást) tudnak előidézni. A NIST (National Institute of Standards and Technology, azaz az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete) megfogalmazásában a CPS: „A kiber-fizikai rendszerek vagy az 'intelligens' rendszerek a fizikai és számítási komponensek együttműködő interaktív hálózatai. Ezek a rendszerek szolgálnak alapjául a létfontosságú infrastruktúráinknak, amelyek a feltörekvő és jövőbeni intelligens szolgáltatások alapját képezik, és sok területen javítják az életminőségünket." (NIST Cyber-physical Systems 2017)

önmagában a teljesen elektromos meghajtása miatt[52] is rendkívül innovatív, de a szoftveres komponensei révén nevezhető igazán úttörőnek.

A Tesla berobbanása az autópiacra egy olyan versenyhelyzetet teremtett az iparágban, amelyet a nagy – és természetesen, ha egy kis időbeni késéssel is, de a kisebb – autógyártók sem hagyhattak figyelmen kívül. A Tesla – és nem utolsósorban annak gyártó tulajdonosa, feltaláló üzletembere, Elon Musk – valóban számos olyan, az autóiparban addig szokatlan újítást hozott a köztudatba, amelyek elsősorban az információtechnológián alapulnak. A Tesla különböző modelljeinek fejlődése során nemcsak a gépjármű belső és külső megjelenésére, a dizájnra, hanem az elektromos meghajtás hatékonyabbá tételére törekedtek. Az elektromos meghajtás egyik legnagyobb kihívása, és tegyük hozzá rögtön, hogy egyik legnagyobb hátránya maga az elektromos meghajtás energiaforrása, az akkumulátor. Ezek kapaci-

[52] Az elektromos meghajtás gyorsabb elterjedése akkor várható, ha a ma még csak korlátozott hatótávolságot lehetővé tevő akkumulátortechnológiát sikerül olyan mértékűre fejleszteni, amely már összemérhető hatótávolságot és nem utolsósorban ár-érték arányt fog jelenteni a belső égésű motorok meghajtásával. Az azonban elgondolkodtató, hogy nagy valószínűséggel a belső égésű motorokkal hajtott gépjárműveket leváltó olyan elektromos járművek, amelyek akkumulátorokat használnak az elektromos áram tárolására, valószínűleg csak egy átmeneti fejlődési szakaszt jelentenek a közlekedésben, illetve a szállításban. Az ilyen járműveket minden bizonnyal az olyan üzemanyagcellás energiaellátással rendelkező járművek követik majd, amelyek például hidrogént használnak az elektromos áram előállításához. Ehhez természetesen szükséges az üzemanyagcella-technológia áttörése, hiszen jelenleg ezek hatásfoka és így alkalmazhatósága rendkívül kicsi. Ugyanakkor az elektromos gépjárművek jelenlegi fejlesztésében megfigyelhető az a trend, amely a hibrid vagy a teljes elektromos meghajtás fejlesztése mellett számos fedélzeti elektronikai rendszer beépítését is jelenti a gépjárművekbe.

tása[53] a jelenlegi technológiával csak nagyon lassan növelhető, ráadásul ezek ár-érték aránya nagyon rossz, valamint a kapacitás növelés jelenleg ezeknek a celláknak a tetemes súlygyarapodásával érhető csak el.

Ugyanakkor mindezek mellett a Tesla Modell 3 2017 év közepén meginduló gyártásával Elon Musk azt is megcélozta, hogy emberi kéz beavatkozása nélkül, azaz csak robotok segítségével kerüljön le – ha még nem is ez a modell, de a közeljövőben a következő széria – a gyártósorokról.

Nyilvánvalóan az autógyárak által diktált elektronizálási verseny nem öncélú. A biztonság és a kényelem mellett olyan szempontok is jelentkeznek a gyártók oldaláról, amelyek a szenzorok által gyűjtött és akár közvetlenül az autógyártónak küldött adatokban keresendők. Ezen adatok alapján a meghibásodások, a szervizigény vagy az optimálisabb futásteljesítmény mind-mind nyomon követhető és tervezhető, ami versenyelőnyt jelenthet az adott gyártónak. Ugyanakkor ez a folyamat óriási adattovábbítási és adatfeldolgozási igénnyel is jár.

[53] A Tesla által közzétett adatok alapján a Model X 100 KWh-ás modellje közepes átlagsebesség (körülbelül 100 km/h) és közepes hőmérséklet (21 °C) mellett körülbelül 340 mérföld, azaz körülbelül 544 km maximális távolságot tud megtenni töltés nélkül. (Tesla 2017) Ugyanakkor a megtehető távolság nagyban függ a sebességtől, sebességváltozások intenzitásától, valamint a külső hőmérséklettől. Mindezeken kívül még egy komoly hátrány jelentkezik az elektromos meghajtású autókkal szemben, ez pedig az akkumulátorok töltési ideje. A Tesla esetében az előbb említett 544 km megtétele után még az úgynevezett szupertöltővel (Supercharger 120 KW) is 1 óra 15 perc a töltési idő, amely lényegesen több, mint egy belsőégésű motorral szerelt jármű átlagos üzemanyagtöltési ideje. (Tesla 2017)

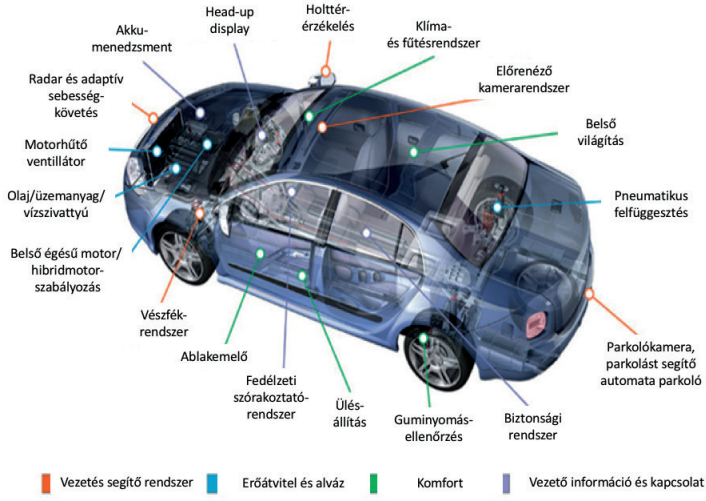
Napjaink korszerű, egyre több elektronikai eszközzel és rendszerrel felszerelt autói a számítógépeknél már megszokott busztopológiát[54] használják a különböző rendszerek összekapcsolására. Az egyik legelterjedtebb ilyen busztopológia a vezérlőhálózat-busz (Controller Area Network – Bus, CAN-BUS), amelyet a Bosch az 1980-as évek közepén fejlesztett ki elsősorban az autóipar számára.[55] Az így felépített hálózat megkönnyíti a diagnózist és a hibakeresést is, mivel az autóban lévő összes elektronikus rendszer, illetve azok vezérlőegységei egy központi csatlakozón, azaz porton keresztül érhetők el.[56] Ma ez a port jellemzően a már-már szabványosnak tekinthető OBD-II (On-Board Diagnostic, azaz fedélzeti diagnosztika) port. (Walz 2016)

---

54 Számítógépes hálózatban busztopológiának nevezzük, amikor az összes hálózati vagy adatátviteli eszköz egyetlen kábelen keresztül csatlakozik egymáshoz. Az alapvető cél az egyszerűség és a hatékonyság a különböző eszközök csatlakoztatására. Így a hálózat összes eszközének kommunikációja egy (vagy több) központi buszon keresztül érhető el. Ez azt az előnyt jelenti, hogy nem szükséges minden eszközt minden eszközzel külön-külön kábellel összekötni, mert az adatok a buszon belül bármelyik irányba áramolhatnak. Ennek megfelelően a busztopológia további előnye a költséghatékonyság. Természetesen a buszon történő kommunikáció megfelelő protokollt, illetve szoftveres vezérlést (címzést) igényel, amely alapján az adott egység el tudja dönteni, hogy egy üzenet neki szól-e, vagy sem. A zökkenőmentes adattovábbítást szolgálja a buszon történő adatcsomagok priorizálása is. Ez alapján a magasabb prioritású adatcsomag a vezérlőegység döntése alapján valós időben jut el a megfelelő elektronikus rendszerbe. Ilyenek lehetnek az autók esetében a veszélyelhárítást (például vészfékezést vagy a fékerőelosztást) jelentő adatcsomagok is.

55 1993-ban a CAN szabvánnyá is vált az autóiparban, amikor a Nemzetközi Szabványügyi Testület *ISO 11898 Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signalling* címen azt kiadta mint nemzetközi ajánlást, illetve szabályozást. Jelenleg ennek a 2015-ös változata számít a legfrissebbnek. Az ISO 11898–1:2015 leírja és meghatározza a CAN általános felépítését, amelyet az OSI, azaz az ISO/IEC 7498–1 szabvány szerinti nyitott rendszerösszekötők (OSI) ISO referenciamodell alapján határoz meg. A CAN adatkapcsolati réteget az ISO/IEC 8802–2 és az ISO/IEC 8802–3 szabvány határozza meg. (ISO 11898–1:2015)

56 Amikor egyre több és több elektronikai rendszert kezdtek az autógyártók a különböző modelljeikbe beépíteni, egy idő után felmerült az igény, hogy ezeket az eszközöket ne külön-külön kábelekkel kelljen összekötni, amelyek önmagukban nemcsak hatalmas energiaigényt jelentettek, hanem komoly súlyt, és nem utolsósorban sokba is kerültek, hanem legyen egy olyan közös adat- és/vagy elektromos összeköttetés a rendszerek között, amely kiváltja a súlyos kábelkötegeket.



35. ábra
Korszerű személyautó elektronikai rendszerei

Forrás: Walz 2016, a szerző szerkesztése

Van azonban egy probléma az autókban található egyre több elektronikai és számítógépes rendszerrel kapcsolatban. Ez a probléma paradox módon pont a biztonság kérdése, hiszen az említett elektronikus rendszerek legtöbbje pont a vezetés biztonságát hivatott növelni. Ugyanakkor a biztonság problémája nem a vezetés biztonsága területén, hanem a kiberbiztonság dimenziójában jelentkezik.

2014-ben két fiatal kutató – Charlie Miller és Chris Valasek – megvizsgáltak közel húsz darab, 2006 és 2014 között gyártott különböző típusú autót, amely során azok vezeték nélküli kapcsolatait elemezték. A kutatók autónként minimum húsz, de egyes típusoknál közel száz olyan adatátviteli kapcsolatot (elektronikai vezérlőegységet és azok összeköttetéseit), illetve megoldást azonosítottak, amelyeket a vizsgált gépjárművek a különböző funkcióikhoz vezeték nélkül használtak. (Valasek–Miller 2014)

A két kutató elemezte és a gyakorlatban meg is vizsgálta azokat a megoldásokat, amelyekkel ezeken a vezeték nélküli kapcsolatokon keresztül az autó különböző rendszerei vagy akár kiber-fizikai alrendszerei elérhetőek és manipulálhatóak.[57] A szerzők ezeket a támadásokat három szakaszra, illetve hozzáférési megoldásra osztották. Az első szakaszban a támadó távoli hozzáféréssel éri el a gépjármű rendszereit. Ez lehetővé teszi a támadó számára, hogy üzeneteket küldjön az autó különböző hálózataiba, így közvetlenül vagy közvetve irányítani tudja az adott elektronikai vezérlőegységet. Ugyanakkor ez a fajta beavatkozás is sok esetben valamilyen rendszer sérülékenységét kihasználva lehet csak sikeres. Ilyen lehet például a Bluetooth egyik ismert sérülékenysége, amely segítségével már korábban a Washington Egyetem és a kaliforniai San Diego Egyetem kutatói távoli hozzáféréssel egy jármű telematikai egységeibe jutottak be. (Checkoway et al. 2011, idézi Valasek–Miller 2014)

Ugyanakkor az említett vizsgálat eredményeit összefoglaló tanulmány megállapítja, hogy egy kiber-fizikai támadás általában egy második lépést is szükségessé tesz, mert az első lépésben említett távoli hozzáféréssel elérhető elektronikus vezérlőegységek nem képesek a fizikai beavatkozó egységek közvetlen vezérlésére. Ennek megfelelően szükség van az autó belső hálózatába olyan kódok bejuttatására, amelyek közvetlenül az olyan kritikus rendszereket irányító elektronikai vezérlőegységekkel teremtenek kommunikációs kapcsolatot, mint például a kormányzásért, a fékezésért, a távolságtartásért vagy a gyorsulásért felelős rendszerek. A harmadik lépés pedig nyilvánvalóan a hamis vezérlőparancsok bejuttatása a kritikus rendszerekbe, amely csak látszólag egyszerű feladat, mert a különböző gyártók különböző adat-

[57] Ezeket a biztonsági hiányosságokat támasztja alá az a tény is, hogy naponta találnak szakértők sérülékenységeket ezekben a rendszerekben. 2017 júliusában több ilyen sérülékenységre való figyelmeztetés is napvilágot látott. Ezek közül az egyik a CAN olyan sérülékenysége, amelyen keresztül a fedélzeti hálózat DoS-támadásnak lehet kitéve. (ICS-CERT 2017)

struktúrákat használnak, így először azok elemzése szükséges a sikeres beavatkozáshoz, illetve kódfuttatáshoz. (Valasek–Miller 2014)

A tanulmány természetesen lehetséges védelmi megoldásokat is megfogalmaz. Az első ilyen védelmi megoldás nyilvánvalóan a támadási pontok, például a távvezérlésre használható szolgáltatások csökkentése, illetve lezárása. Ugyanilyen fontos védelmi kérdés a kapcsolódó szolgáltatások, mint például az említett Bluetooth sérülékenységeinek javítása vagy a hálózati adatforgalom megfelelő titkosítása, megnehezítve a támadók számára az egyszerű kódfuttatást. A hálózati architektúra megfelelő kiépítése, amelynek a különböző kritikus rendszerek szegmentálását is magában kell hordoznia, szintén sikeres védelmi megoldás lehet. (Valasek–Miller 2014)

A korábban említett Tesla elektronikus rendszerei is komoly biztonsági kockázatokat rejtenek. 2016-ban négy kínai kiberbiztonsági kutató – Samuel LV, Sen Nie, Ling Liu és Wen Lu – látványos demonstráció keretében bizonyította be, hogy a Tesla rendszereibe akár több kilométeres távolságból is be lehet avatkozni. A teszt során a kutatók 12 mérföldről (körülbelül 20 km) a Tesla S modelljének CAN buszán keresztül képesek voltak többek között az autó elektromosan állítható üléseinek mozgatására, a napfénytető és a csomagtartó felnyitására vagy akár a műszerek vezérlésére, miközben az autó drive (azaz vezetés), illetve parking (azaz parkolás) üzemmódban volt. Mindezeken kívül a távoli beavatkozás képes volt az autó fékrendszerének vezérlésére is, amely messze túlmutat a napfénytető kinyitásának problémáján. A Tesla hivatalos válaszában természetesen próbálta a kérdést elbagatellizálni, mert szerintük az ilyenfajta távolirendszer-elérés csak akkor lehetséges a Tesla járművei esetében, amikor annak fedélzeti számítógépe a webböngészőt futtatja, és az autó közel van egy olyan wifi hotspothoz, amely korábban kompromittált, azaz feltört volt, és amelyen keresztül a támadás így kivitelezhető. (Solon 2016)

A kínai mérnökök hackelését bemutató Guardian-cikk is idézi, hogy nem ez volt az első eset, amikor a Tesla elektronikus rendszerét távolról manipulálták. 2016 májusában a University of South Carolina,

a kínai Zhejiang University és a Qihoo 360 kínai biztonsági cég a Tesla Autopilot, azaz az autó automatikus vezetését lehetővé tevő elektronikus rendszerébe avatkozott be úgy, hogy ott nem létező akadályokat hoztak létre, amelyeket az Autopilot valóságosnak vélt. (Greenberg 2016)

Mindezek alapján nem túlzás kijelenteni, hogy a hálózati csatlakozásra és internetelérésre képes autók területén a kiberbiztonság hasonlóan fontos terület, mint a gépjárművek különböző fizikai biztonságot megteremtő és az azt növelő rendszerei. Az autókban kötelező biztonsági övhöz hasonlóan a kiberbiztonságnak is kötelezőnek kell lennie gépjárműveinkben.

Ha egy kicsit a jövőbe tekintünk, akkor a biztonságnak annál is inkább előtérbe kell kerülnie ezen a területen, mert az már most prognosztizálható, hogy a nem is olyan távoli jövőben olyan autókon fogunk utazni, illetve a közúti áruszállításban olyan teherautókon fog eljutni az áru egyik helyről a másikra, amelyeket nem emberek, hanem beépített – mesterséges intelligenciával támogatott – számítógépek, ha tetszik: robotok fognak vezetni.

1.3.3. Okosvárosok

Ahogy korábban is utaltunk rá, a világ népességének több mint fele városokban él, sőt ez az arány az európai lakosságra vetítve még magasabb, hiszen Európában az emberek 75%-a él városokban, illetve erősen urbanizált területeken. (UN DESA 2014b)

Mindezeknek megfelelően nyilvánvaló, hogy szükségessé válik az egyre inkább túlzsúfolttá váló városokban olyan megoldások felkutatása, amelyek hozzájárulnak az ott élő és dolgozó emberek életminőségének javításához. A világon számos helyen folynak kutatások és különböző fejlesztések, amelyek arra irányulnak, hogy az információtechnológiát használják fel e probléma részbeni vagy teljes megoldására. Ezek a kezdeményezések kapták az *okosváros* nevet.

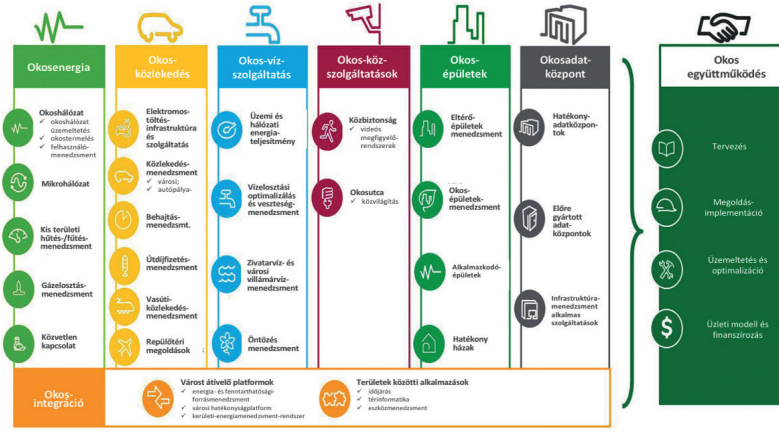
Technológiai oldalról megközelítve az okosváros, azaz a *smart-city-koncepció* az infokommunikációs technológia által nyújtott szolgáltatásokat és rendszereket a lehető leghatékonyabban integrálja. Az elgondolás célja, hogy az egyre inkább túlzsúfolt városi környezetben jelentkező problémákra adjon hatékony válaszokat. Számos egymással összefüggő, komplex kérdést kell minél hatékonyabban és lehetőség szerint integráltan megoldani a városi környezetben. Ehhez nyújt segítséget az infokommunikációs technológia, hiszen ez kézenfekvő módon nemcsak a különböző szolgáltatásokban található meg, hanem ott van a városi ember zsebében, otthonában vagy akár a korábban említett autójában is.

Az okosváros-koncepció legfontosabb célja tehát a város működőképességének és ezen belül is az adott urbanizált térben zajló társadalmi funkciók minél hatékonyabb összehangolása, azok együttműködésének a növelése. Ehhez az összehangolt működéshez szükséges a közszolgáltatásokban, ezen belül akár a közműszolgáltatásokban, azaz a villamosenergia-szolgáltatásban, a víz-, a csatorna-, a gáz- és az egyéb szolgáltatásokban meglévő érzékelők (levegő hőmérsékletét, páratartalmát mérő eszközök) együttes – nyilvánvalóan hálózatba kötött – működésének kialakítása.

Ezeknek a rendszereknek, eszközöknek és érzékelőknek az adatai, kiegészítve a városban élő lakosság digitális adataival (például mobiltelefon, vezeték nélküli eszközök helyadatai) valós képet adnak a város pillanatnyi állapotáról. Ez alapján monitorozható egy sor olyan dolog, amely akár azonnali beavatkozást igényelhet az adott szolgáltatás vagy funkció ellátásában, de akár az élhetőbb és hatékonyabb város irányába történő fejlesztést is lehetővé teheti. Mérhető a zsúfoltság vagy éppen az adott szolgáltatás kihasználatlansága, feltérképezhető a zaj- vagy a környezeti szennyezés. Megannyi – akár valós idejű – adat gyűjthető, amely alapja lehet a hatékonyság megtervezésének és kivitelezésének.

Mindezek hozzájárulhatnak az életminőség javításához, a város átalakítása vagy egy-egy régebbi városrész újjáépítése során az élhe-

több tér létrehozásának megtervezéséhez, a környezetvédelemhez, a klímavédelemhez, de segítséget nyújthatnak az olyan gazdasági vagy akár közigazgatási funkciók hatékonyabb megtervezéséhez és kialakításához, amelyek szintén a mindennapjaink részei. Ezen feladatok során modellezhető a város és az abban élő emberek számos tevékenysége, funkciója. Ezek alapján olyan értékelések végezhetők, amelyek korábban csak jóval nagyobb energiabefektetéssel vagy egyáltalán nem voltak kivitelezhetők. Gondoljunk csak bele, például a vezeték nélküli kapcsolatok – például wifi, mobiltelefon stb. –, illetve azok használatának monitorozásával nagyon egyszerűen feltérképezhető, hogy melyik városi tér melyik időszakban mennyire zsúfolt, az emberek ott mennyi ideig tartózkodnak. Ezeket az adatokat akár a légszennyezettséggel, akár a zajtérképpel összevetve egészen más megoldásokat lehet javasolni egy-egy funkcióra, mint korábban.



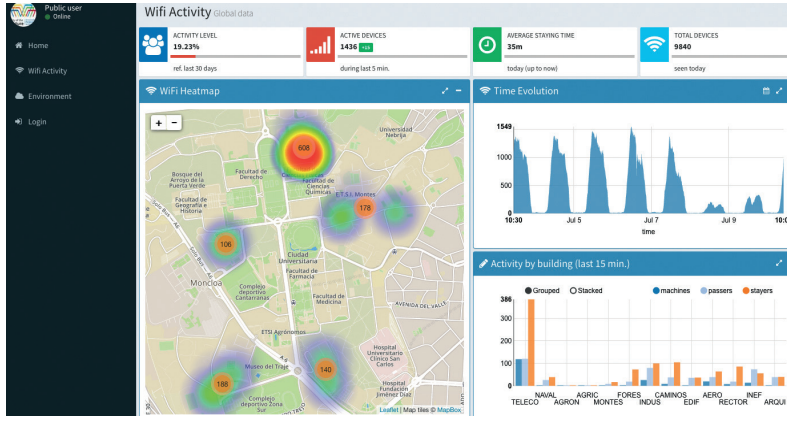
36. ábra
Az okosváros lehetséges összetevői

Forrás: Schneider–electric 2015, a szerző szerkesztése

Nagyon előremutató okosváros-kutatás folyik a Madridi Műszaki Egyetem (Universidad Politécnica de Madrid – UPM) vezetésével.

Az egyetem a madridi Moncloa Campusán egy úgynevezett Smart City Experimentation Platformot telepített. A Campus mintegy 5,5 négyzetkilométernyi területen fekszik Madrid központjában. A Campus területén – amely egyébként szerves része a városnak – számos oktatási épület, kutatóközpont és hallgatói kollégium, valamint három nagy sportkomplexum és hatalmas zöldterületek is találhatók. A Campus területén lévő utakon több tízezer autó halad át naponta, de a Campus nagyon jó tömegközlekedéssel – közte két metrómegállóval és 13 buszjárattal – is rendelkezik. Mindezek alapján a Campus és az ott lévő okosváros-platform reprezentatív adatokat szolgáltat a kutatásokhoz. (Mella–Marquez–López–López–Mella–Lopez 2014)

A még kísérleti fázisban lévő kutatások egyes – valós idejű adatai – egy úgynevezett *dashboardon,* azaz adatmegjelenítőn keresztül nyilvánosan is nyomon követhetők. Olyan adatokat jelenítenek meg a különböző szenzorok által gyűjtött adatok feldolgozása után, amelyek későbbi tudományos elemzések alapjai lehetnek. Ilyen adatok például a vezeték nélküli hálózatokat használók számának mérése vagy akár a különböző környezeti adatok: hőmérséklet, páratartalom, zaj, napfény erőssége stb. (Smart CEI Moncloa 2017)

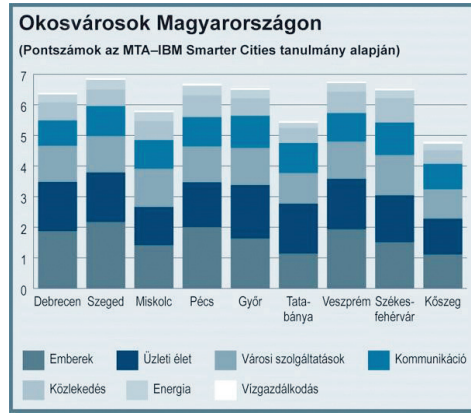


37. ábra

A Madridi Műszaki Egyetem okosvárosprojektjének pillanatnyi adatai

Forrás: Smart CEI Moncloa 2017

Hazánkban is igen élénk érdeklődés mutatkozik az okosváros-koncepciók iránt. Számos hazai nagy és közepes városban kezdődtek el különböző projektek a koncepció egyes elemei mentén.



38. ábra
Magyarországi okosvárosok és azok rangsora[58]

Forrás: Schopp 2014

Természetesen a fővárosunkban is létezik számos olyan megoldás, amely az okosváros-koncepcióba illik. 2017 januárjában jelent meg a *Smart Budapest: Budapest okos város jövőképe* című ezeket a megoldásokat egy egységes stratégia mentén összefoglaló koncepció.

Ez az elgondolás azokat az elveket követi, amelyek alapján egy nagyváros a 21. században nemcsak fenntarthatóvá, hanem a jövőben fejleszthetővé is válik. A dokumentum és az abban foglaltak illeszkednek a Budapest 2020 integrált településfejlesztési stratégiához, valamint a főváros által 2013-ban elfogadott Budapest 2030 hosszú távú városfejlesztési stratégiához is. (Finta–Barta–Balogh 2017)

[58] Az ábrán látható területek pontszámításának forrása Lados (2011) tanulmánya.

39. ábra
Budapest okosváros-kapcsolatai és céljai

Forrás: Finta–Barta–Balogh 2017

A koncepció a térségben vezető tudásközpontként képzeli el Budapestet, amely a környezetében a fenntartható erőforrásokra, a mobilitásra és az élhető városi környezetre támaszkodik. Természetesen ehhez szükség van a társadalom támogatására is, amely társadalmi partnerséget és tudatos lakosságot feltételez. Mindezek erős – az információtechnológián alapuló –, fenntartható és versenyképes gazdaság nélkül elképzelhetetlenek. Olyan programok valósulhatnak így meg, amelyek – mint például Budapest egyik legneuralgikusabb problémáját: a közlekedést – proaktív módon tudják orvosolni. Ez nemcsak a lakosság életminőségét javíthatja, de ezzel megvalósítható a költséghatékonyság, és akár a környezeti terhelések csökkentéséhez is mérhető módon járulhat hozzá. (Finta–Barta–Balogh 2017)

Ezek persze így leírva rendkívül jól hangzanak és egy jól szerkesztett prospektusban még szépen is néznek ki. Ugyanakkor a koncepció a célrendszer mellé a főváros számára olyan feladatokat is meghatároz, amelyek mentén valóban létrejöhet egy élhetőbb, *okos* város.

Az okosváros-koncepció azonban, köszönhetően a nem mindig biztonságos infokommunikációs és egyéb elektronikus rendszereknek, komoly biztonsági kockázatot rejt magában a világon mindenhol. Az első – és talán az egyik legnagyobb – biztonsági kérdés a függőség. Függőség az infokommunikációs rendszerek és az azok nyújtotta szolgáltatásoktól.

Abban a pillanatban, ha egy városi térben, amely egyébként is túlzsúfolt, és amelynek működőképesége csak az információs rendsze-

reken keresztül tartható fenn hatékonyan, az okos szolgáltatások nem vagy csak akadozva működnek, hatalmas káosz alakul ki.

A közlekedésszervezéstől kezdve a logisztikán át a közművek szolgáltatásáig minden rendszer egyre inkább egymástól is függ, egymásra is hatással van. Ebben a helyzetben egy jól megválasztott – informatikai vagy információs – támadással a város működésképtelenné tehető. Nincs szemétszállítás, akadozik a közösségi közlekedés, nincs áruszállítás, nincs kommunikáció, nincsenek még arról sem hírek, hogy mi is történt.

Persze ez csak fikció egyelőre, és az okosvárosoknak sincs alternatívája. Ebből következően a biztonság és a biztonságos rendszerek az egyetlen lehetséges megoldás, amelyben a jövő nemzedéke érdekében gondolkodhatunk.

1.3.4. Okosotthonok

Az okosvárosokban lévő otthonainkra is egyre inkább illik az „okos" jelző. De mitől is „okos" egy lakás, egy otthon? Nyilvánvalóan azoktól az „okos" eszközöktől, amelyeket az otthonainkban egyre nagyobb számban használunk.

Természetesen ez még mit sem érne anélkül, hogy ezeket az eszközöket hálózatba ne kapcsolnánk, hiszen azok funkcionalitása csak ebben az esetben válik teljessé. Ennek megfelelően vissza is jutunk a dolgok internete fogalomkörhöz, hiszen a háztartásokban használt megannyi elektronikus eszköz nemcsak hálózatba kapcsolható, hanem ezek jelentős része önállóan kommunikál más ilyen eszközzel, ráadásul ezek zöme valamilyen kiber-fizikai tevékenységre is képes.

A hálózatba kapcsolt otthoni elektronikus és különböző infokommunikációs eszközök az okosváros-koncepcióhoz hasonlóan az otthonokra érvényes okosotthon-elgondolást indukálták. Ez nem jelent mást, mint az otthonokban élők igényeinek minél magasabb szinten történő kielégítését, és végső soron életminőségük javítását.

Az épületekben használt különböző szenzorok és valamilyen szintű automatizálást lehetővé tevő eszközök jelenléte persze nem új keletű dolog, hiszen az épületautomatizálásban az elmúlt három évtizedben hatalmas fejlődés ment végbe. Ez a fejlődés a lakásokban használt egyéb olyan eszközökre is igaz, amelyek szoftveresen – akár távolról is – vezérelhetők. Az okosotthon-koncepció tehát e két fejlődési trendet ötvözi. Az okosotthon ráadásul nagyon sok olyan dologra meg is tanítható, amelyek a felhasználók – legyenek azok lakók vagy irodában dolgozók – igényeihez a legjobban és a leghatékonyabban igazodnak. Az okosotthonokat nagyon sokszor egy mobiltelefonhoz szokták hasonlítani. Ráadásul egy olyan mobiltelefonhoz, amely ismeri a tulajdonosa szokásait, igényeit, ehhez mérten nyújt a számára szolgáltatásokat, ehhez igazítja az eszköz különböző paramétereit.

Az okosotthon, akárcsak az okosváros egyik legnagyobb innovatív előnye pont abban van, hogy a felhasználói igények testre szabásával energia és erőforrás takarítható meg, hiszen csak azokban a terekben kapcsolja fel a világítást, ahol tartózkodunk, az intelligens világítótest – a környezeti mintavételezésnek köszönhetően – akár a külső fényviszonyoknak megfelelően változtatja a kibocsátott fény intenzitását, csökkentve ezzel a lakás vagy egyéb helyiség villamosenergia-fogyasztását. Az okos-vízmelegítő csak akkor kapcsol be és állít elő kellő hőfokú vizet, amikor arra szükség van, és az okos vezérlő csak azokat a fogyasztókat kapcsolja be, amelyeket valóban szükséges működtetni, valamint csak ott biztosítja az optimális hűtést vagy fűtést – akár a külső hőmérséklet figyelembevételével – ahol tartózkodunk. Ha nem vagyunk otthon, az intelligens zár segítségével bezárja a lakás ajtaját, és némán ügyel a biztonságra.

40. ábra
Az okosotthon összetevői

Forrás: Okosotthon összetevői, a szerző szerkesztése

Az okosotthonok funkcionalitásához természetszerűleg tartozik hozzá a távvezérlés, illetve a távoli elérés és ellenőrizhetőség lehetősége. A különböző mobil alkalmazásokkal egyre szélesebbé válik azoknak az eszközöknek és rendszereknek a száma, amelyek távolról elérhetőek és vezérelhetőek. Ráadásul sok gyártó kínál olyan eszközt, amelyek integráló és funkcióelosztó eszközként működnek. Ezek az eszközök a lakáson belül lévő különböző okoseszközökkel kapcsolatba lépnek, és képesek azokat vezérelni. A felhasználó számára érintőképernyős vagy akár hangvezérléses funkciót nyújtanak, azaz egy központi helyről tudjuk a lakás összes elektronikus eszközét érintéssel vagy hanggal vezérelni.

Az okosotthon és azok az elektronikus eszközök, amelyek hálózatba kapcsolva segítik otthon töltött mindennapjainkat, ma már egyre inkább realitássá válnak, és egyáltalán nem futurisztikus álmok csupán. Az „okos” jelző valóban illik ezekre az otthonokra, hiszen az épületautomatizáláson jóval túlmutatva ezek az otthonok valóban

megtaníthatók a szokásainkra, viselkedési mintáink alapján akár az igényeinkre is. Szoftvereiknek köszönhetően akár tanácsokat is tudnak adni az energiatakarékosság fokozásához vagy akár napi bevásárlási szokásaink optimalizálásához.

1.4. Kibertér és politika

Az internet és a korábban említett közösségi oldalak komoly szerepet játszanak a politika alakításában is. Egyre inkább nyilvánvalóvá válik, hogy a kibertér is jó terep a politikai küzdelmekhez, és hogy ez a dimenzió annyira fontos lett, hogy aki itt sikereket ér el például egy választási kampányban, mert meg tudja szólítani a választók vagy a potenciális választók tömegeit (és ez a kibertérben hatványozottan könnyebben történhet, mint más dimenziókban, legyen szó akár a hagyományos elektronikus médiumokról is), az befolyásolni tudja a választókat és végső soron akár a választások eredményeit is.

Már a 2008-as amerikai elnökválasztás is bizonyította, hogy a közösségi oldalakon keresztül elérhető tömegek és az így számukra eljuttatható üzenetek egyre inkább felveszik a versenyt a televízióval.[59]

A 2016-os amerikai elnökválasztás eseményeiben is nagy szerepet játszottak az internetes támadások. A támadások körül azóta is nagy a bizonytalanság, de egyre nyilvánvalóbb tény, hogy ezek nagymértékben befolyásolták a végeredményt.

Azt korábban is megállapítottuk, hogy a „politikai viszonyok formálására a média, esetünkben az internet és a segítségével igénybe vett közösségi médiumok hatalmas lehetőséget rejtenek magukban". (Kovács–Krasznay 2017)

[59] Az 1960-as amerikai elnökválasztási kampány volt az első olyan esemény, amelyben a televízió alkalmazhatósága és mi több hatalma a politikai küzdelemben is nyilvánvalóvá vált. Ez volt az első olyan elnökválasztási kampány, amelyben a két elnökjelölt – Kennedy és Nixon – között tv-vitára került sor. (Webley 2010)

Ugyanakkor csak a legújabb elemzések után válik világossá, hogy egy olyan nagy formátumú politikai esemény alakításában, mint amilyen az amerikai elnökválasztás (vagy ezt követően a 2017-es francia elnökválasztás), milyen mértékben is játszott szerepet a kibertámadások egész arzenálja.

Az már korábban is köztudott volt, hogy Oroszország hatalmas nyomás alatt tartja Ukrajnát, illetve a balti országokat, de nem kíméli Kelet-Európát sem. Ez a nyomás alapvetően a média különböző eszközeivel történik. Ennek célja például a balti országokban folyamatos (média)jelenlét fenntartásával alapvetően a lakosság befolyásolása. Azokkal a nagyon jól szerkesztett hírekkel operálnak ezek a műveletek, amelyek alkalmasak lehetnek arra, hogy az orosz fél támogatására biztassák a lakosságot, ezen belül is nyilvánvalóan az orosz nemzetiségű helyi lakosságot. Másik oldalról a cél a bizonytalanság megteremtése és fokozása, mert ilyen politikai, gazdasági és társadalmi helyzetben (vagy legalábbis az azokról szóló hírek fényében) sokkal könnyebb különböző olyan akciókat végrehajtani, amelyek így rejtve maradnak.

A 2016-os elnökválasztási kampány során történt kibertámadásokat, majd az azt követő érzékeny információk kiszivárogtatását az USA Belbiztonsági Minisztériuma, valamint az FBI közös elemzése egyértelműen Oroszországhoz kötötte. (US DHS–FBI 2016; idézi: Kovács–Krasznay 2017)

A hírszerző szervezetek információi alapján készült jelentés szerint a támadók célzott adatszerző támadásokat hajtottak végre kormányzati intézményekkel, kritikus infrastruktúrákkal, politikai szervezetekkel és a politikához köthető vállalatokkal szemben. Az említett

jelentés két támadó csoportot nevez meg: az APT[60] 29-et, azaz Cozy Beart, amely feltételezhetően az orosz SZVR-hez vagy az FSZB-hez köthető, illetve az APT 28-at, azaz Fancy Beart, amely az orosz katonai titkosszolgálathoz a GRU-hoz kapcsolható. (US DHS–FBI 2016; idézi: Kovács–Krasznay 2017)

A későbbi elemzések és az ezek alapján készült jelentések azt mutatják, hogy a korábban feltételezettnél sokkal nagyobb a baj. A vizsgálatok megállapították, hogy az USA legalább 39 államában voltak kibertámadások a választási rendszerrel szemben. Illinois-ban pedig arra is találtak bizonyítékokat, hogy a támadók a választási névjegyzéket manipulálták, illetve azokban adatokat töröltek. (Riley–Robertson 2017)

Mindezek ellenére, vagy éppen a fentiek miatt figyelemre méltó az a tény, hogy egy kiberbiztonsági cég, az UpGuard a nyilvános interneten rábukkant a Republikánus Nemzeti Bizottság (RNC – Republican National Committee) által megrendelt választói adatbázisra. Ez az adatbázis mintegy 198 millió amerikai – választásra jogosult – állampolgár minden adatát tartalmazta. Az adatbázisban – amely összesen 1,1 terabájt méretű letölthető fájlokból állt – a választók neve, pontos születési ideje, lakcíme, telefonszáma és egyéb adatai is megtalálhatóak voltak. (O'Sullivan 2017)

[60] Az APT itt is az Advanced Persistent Threat, azaz magyarul „célzott támadás" kifejezésre utal. Az APT olyan nagyon komplex, nagyon fejlett technikákat használó támadások sorozata, amelyek feltételezik, hogy a támadó mögött nagyon nagy tudás és tapasztalat van a támadás megtervezése, kivitelezése és végrehajtása során. Ennek okán általában országokat, és nem egyszerű kibertámadókat feltételezhetünk egy-egy APT mögött. Erre utal nagyon sok esetben az APT-k célja is, amely alapvetően nem a károkozás vagy a rombolás, nem az üzleti vagy anyagi haszonszerzés, hanem az információszerzés. Ezt támasztja alá az is, hogy az APT-k célpontjai túlnyomó többségben az állami és/vagy közigazgatási informatikai rendszerek.

Nagyon beszédes a Trend Micro 2017. év eleji elemzése, amelyben az előző évek nagyszabású kiberkémkedési akcióinak,[61] valamint azok eredményeinek propagandacélú, azon belül is elsősorban politikára gyakorolt hatásait vizsgálták meg és elemezték. A jelentésben több tucat katonai védelmi, illetve külügyminisztériumi védelmi szektorban érdekelt vállalat, valamint médiacégek elleni phishing, spear phishing és malware támadások áldozatait azonosították és jelölték meg. (Trend Micro 2016; Trend Micro 2017b)

Az elemzés, valamint annak eredményei nagyon jól jellemzik, hogy ma már a politikai pártok, a közigazgatás legfelső szintje és akár a védelmi szféra nagyon jó terepe a kiberkémkedésnek, hiszen az ezektől a szervezetektől származó adatok és információk valóban felhasználhatóak a politika befolyásolására.

[61] Ezeket az akciókat összefoglaló néven a sakkból származó Pawn Storm kifejezéssel illetik. A kiberkémkedéssel és benne ezeknek az akcióknak a bemutatásával később részletesen is foglalkozunk.

2. A kibertér veszélyei

2.1. Sérülékenységek, módszerek, eszközök

„Sérülékenységek márpedig vannak" – szól az egyelőre örök érvényűnek tűnő igazság. Minden információs, infokommunikációs rendszerünk és minden számítógép-hálózatunk tartalmaz olyan sérülékenységeket, amelyeken keresztül ezek a rendszerek támadhatók, illetve kompromittálhatók. A kérdés persze az, hogy ezek a sérülékenységek mennyire ismertek,[1] mennyire nyilvánosak, létezik-e már ezekre valamilyen védelmi megoldás, azaz valamilyen biztonsági javítás,[2] valamint hogy ezeken keresztül milyen mértékben lehet az adott rendszerben kárt okozni. Mivel rendszereink általában nem egymástól függetlenül működnek, egy rendszer kiesése vagy működésképtelensége egy vagy több másik rendszerre is nagy hatással lehet. És akkor még nem beszéltünk arról, hogy egy ilyen összekapcsolt rendszeregyüttesben is a leggyengébb láncszemen, azaz a legsebezhetőbb vagy legsérülékenyebb rendszeren keresztül egy egyébként jól védett másik rendszer is kompromittálható, támadható.

---

1 A sérülékenységek nyilvánosságra kerülése és ismertté válása esetében mindenesetre elgondolkodtató, hogy évek óta a támadók által legtöbbször kihasznált sérülékenység az Adobe Flashben (ráadásul ebben az esetben nem is egy ilyen került napvilágra az elmúlt években), a Microsoft Silverlightban, valamint az Internet Explorerben található. Ezeket a sérülékenységeket évről évre nyilvánosságra is hozzák a biztonsági cégek, a szoftvergyártók – ha némi késéssel is, de – javításokat adnak ki ezekre a hibákra, a felhasználók jelentős része azonban mégsem ismeri vagy telepíti ezeket a javításokat. Ez ugyanúgy igaz az egyszerű „átlagfelhasználóra", valamint a kisebb-nagyobb vállalati rendszereket üzemeltetőkre egyaránt. (Garnaeva et al. 2016)

2 A sérülékenység javítására használt *patch* (magyarul „folt") angol megnevezésből használatos a sérülékenységek javítására alkalmazott *patch management* kifejezés.

Nyilvánvalóan a védelem megvalósítása érdekében az egyik megoldás az lenne, ha a gyártók abszolút biztonságos vagy legalább biztonságosabb rendszereket gyártanának. Ez azonban egyrészt utópisztikus elképzelésnek tűnik, főleg a korábban már említett rendkívüli módon felgyorsított fejlesztési ciklusnak köszönhetően, másrész pedig az emberi tényezőt ekkor sem hagyhatjuk figyelmen kívül, hiszen a bármilyen motivációs háttérrel rendelkező rosszindulatú vagy ártó szándékú emberi tevékenység sajnálatos módon ekkor sem lenne kizárható.

A sérülékenységeket kihasználó különböző rosszindulatú szoftverek és az azokkal történő különböző támadási módszerek száma napról napra nő.

2.1.1. Malware-ek, avagy a szoftverek, amelyek rosszat akarnak

A Kaspersky 2016-os rosszindulatú szoftverekről készített jelentésében közel 70 millióra teszi azoknak a malware-eknek a számát, amelyeket a biztonsági cég csak ebben az évben azonosított. (Garnaeva et al. 2016)

A jelentés szerint az online támadások több mint 96%-áért húsz rosszindulatú program[3] volt a felelős 2016-ban.

[3] Az első helyen (első sor) szereplő rosszindulatú URL olyan linkeket takar, amelyeket elsősorban fertőzött weboldalakra történő átirányításhoz használnak. Ezeken a linkeken elért oldalak exploitokat, botnetvezérlő központokat, zsarolóoldalakat vagy egyéb rosszindulatú programokat tartalmaznak. (Garnaeva et al. 2016)

	Megnevezés	Az összes támadás %-a
1	Malicious URL	77.26
2	Trojan-Clicker.HTML.Iframe.dg	8.15
3	Trojan.Script.Generic	6.74
4	Trojan.Script.Iframer	3.14
5	Trojan-Downloader.Script.Generic	0.35
6	Exploit.Script.Generic	0.20
7	Packed.Multi.MultiPacked.gen	0.15
8	Trojan.JS.FBook.bh	0.13
9	Exploit.Script.Blocker	0.11
10	Trojan-Downloader.JS.Iframe.div	0.11
11	Trojan.JS.Redirector.ns	0.09
12	Trojan-Dropper.VBS.Agent.bp	0.08
13	Trojan-Downloader.JS.Agent.hjc	0.08
14	Trojan.JS.Iframe.ako	0.07
15	Trojan.Win32.Generic	0.06
16	Trojan.Win32.Generic	0.06
17	Trojan.JS.Agent.ckf	0.05
18	Trojan-Spy.HTML.Fraud.gen	0.05
19	Trojan.Win32.Invader	0.04
20	Exploit.SWF.Agent.gen	0.04

41. ábra
A 20 legjelentősebb rosszindulatú program 2016-ban

Forrás: Garnaeva et al. 2016, a szerző szerkesztése

Önmagában a *malware* kifejezés az angol *malicious software,* azaz „rosszindulatú számítógépes program" szavak összevonásából származik. Ahogy a Kaspersky fent idézett elemzése is mutatja, a rosszindulatú szoftverek száma ma már hatalmas, akár a több tízmilliót is elérheti, de egyes források ezek számát több százmillióra is becsülik. Korábban a malware-ek két nagy kategóriáját különböztettük meg: a programtípusú malware-ekre és a szövegtípusú malware-ekre oszthattuk ezeket a programokat. (Kovács 2006; Haig–Kovács 2012)

Ráadásul időre időre felbukkannak – akár szolgáltatásként is – olyan oldalak, ahonnan bárki kedve és természetesen pénztárcája szerint tölthet le rosszindulatú szoftvert előállító alkalmazást. Ezekkel gyakorlatilag szoftverfejlesztői vagy mélyebb programozói tudás nélkül is tud a felhasználó vírusokat írni – vagy csak egyszerűen már meglévő komponensekből azokat modulrendszerűen összeállítani –, majd azokat fel tudja használni különböző célokra.

Az áttekinthetőség érdekében a rosszindulatú programokat a következő táblázatokban foglaltuk össze nagyon rövid magyarázó, értelmező kiegészítésekkel ellátva.

5. táblázat
Programtípusú malware-ek és jellemzőik

Megnevezés	Jellemzők
Vírusok	A vírusok olyan rosszindulatú programok, amelyek saját programkódjukat egy másik programhoz hozzáfűzik, vagy azokba beépítik. Így biztosítják terjedésüket is. A gazdaprogramhoz való kapcsolódás módja különböző lehet: például a vírus saját programkódját beleírja a gazdaprogram kódjába, így módosítja azt. Korábban a vírusok egyik nagyon virulens és veszélyes fajtája a makrovírusok voltak. Ugyanakkor a ransomware-ek terjedése során látható, hogy ez ma újra igaz, hiszen egyes zsarolóvírusok újra a makróvírusokkal nyitnak utat az áldozat számítógépén.
Programférgek (worms)	A programférgek olyan önállóan futó, gazdaprogramot nem igénylő szoftverek, amelyek képesek saját maguk megsokszorozására. Másolataikat részben a megtámadott számítógép merevlemezén készítik el, részint pedig a hálózaton keresztül juttatják el a megfertőzni kívánt számítógépekre vagy hálózati elemekre.
Ransomware-ek	Zsarolóvírusok. A megfertőzött számítógépre jutva titkosítják a felhasználó fájljait. A titkosítás feloldását lehetővé tevő kódért váltságdíjat – pénzt vagy bitcoint – kér cserébe.
Trójai programok	A trójai programok látszólag hasznos szoftverekbe elrejtve fertőzik meg a számítógépet. Adatokat módosítanak, könyvtárakat, adatállományokat törölnek, backdoort nyitnak stb.

Megnevezés	Jellemzők
Backdoorprogram	A backdoor programok eredetileg a rendszeradminisztrátorok vagy rendszerfelügyeleti jogokkal rendelkező személyek részére nyitottak olyan lehetőségeket, hogy a kívánt számítógépet távolról is elérjék, és azon különböző javításokat, illetve beállításokat végezzenek. A rosszindulatú backdoorprogramok azonban jogosulatlanul próbálnak meg „hátsó ajtókat" nyitni a rendszerhez. Többségük e-mail-mellékletként, vagy egyéb letöltési „mellékletként" érkezik. Az igazi veszélye a backdoorprogramoknak az, hogy ezek remek megoldásokat nyújtanak a rendszer-adminisztrációs jogok megszerzésére.
Dropperek	A dropperek a trójai programok speciális fajtájának tekinthetőek, mivel hasonló elven kerülnek a számítógépbe. Ott azonban legyártanak kettő vagy több, az operációs rendszer által futtatható vírust, majd elindítják azokat. Mivel nem saját magát másolja a program, hanem új programot állít elő, ezért ezeket nem lehet a klasszikus vírus kategóriájába sorolni.
Spyware	A kémprogramok a rendszerbe juttatva, ott elrejtőzve, a háttérből figyelik a rendszer eseményeit, és ezekről jelentéseket, illetve adatokat küldenek.
Keyloggerek	A keyloggerek a háttérben települve a billentyűleütéseket – így akár a jelszavakat, bankkártyaszámokat, azonosítókat is – rögzítik, és kijuttatják ezeket az információkat a hálózaton keresztül.
Adware	Olyan programok, amelyek a felhasználó internetes szokásait figyelik és rögzítik, majd ezek alapján valamilyen szolgáltatást reklámoznak a számára hirdetési bannerekkel vagy pop-upokkal. Sok esetben spywareként is viselkednek.
Scareware	Hamis vírusirtó szoftver, amely úgy tesz, mintha egy felhasználó eszközét ellenőrizné, és ott rosszindulatú programokat vagy biztonsági fenyegetéseket keresne. Ehelyett titkosítja a merevlemezt, így a felhasználónak fizetnie kell annak eltávolításáért. Egyfajta ransomware-ként működik.

Forrás: Kovács 2006

6. táblázat
Szövegtípusú malware-ek fajtái (példák)

Megnevezés	Jellemzők
Spam	A spam kéretlen leveleket jelent. Ezek nagyon nagy számban érkeznek egy-egy számítógépre, így foglalva sávszélességet. A nagy szám miatt nemcsak sávszélességet, de komoly tárhelyet is foglalnak. A hasznos e-mailek közül történő kiválogatásuk rendkívül idő- és energiaigényes.
Hoax	A spam egyik speciális csoportja, amelyekben vagy valamilyen veszélyre (vírus, spam, csatolt fájl) figyelmeztetnek, vagy valamilyen nyereményt helyeznek kilátásba, ha meghatározott számú helyre továbbítjuk őket. Több veszélyt rejt magában, hiszen amennyiben sok helyre továbbítjuk ezeket, akkor sávszélességet és tárhelyet foglalunk le, ugyanakkor lehetnek ezek önmagukban például trójait tartalmazó melléklettel ellátottak is.
Holland/ spanyol lottónyeremény-levelek, nigériai csalások	Az emberek naivitására és gyanútlanságára építő e-mail alapú malware-ek. Vagy valamilyen lottónyereményt ígérnek, amely átvételéhez csak be kell fizetnünk néhány tíz dollárt, vagy valamilyen nigériai (általában olajjal foglalkozó) üzletember zárolt bankszámlájának a feloldásához kérnek tőlünk segítséget, természetesen részesedés fejében, amelyhez szintén csak át kell utalnunk néhány száz dollárt.
Phishing	Az utóbbi idők egyik legelterjedtebb csalásra, illetve az emberek hiszékenységére és megtévesztésére épülő eljárása. A *phishing,* azaz az „adathalászat” eljárása során látszólag a bankunktól érkezik egy e-mail, amelyben arra szólítanak fel, hogy adatainkat egyeztessük. Ehhez adnak egy linket, amely látszólag a bank oldalára mutat. Rákattintva erre a hivatkozásra a bankéval látszólag teljesen azonos oldalra kerülünk, ahol kérik a belépési nevünket, jelszavunkat és elektronikus azonosítónkat is. A csalók az eredeti banki oldalhoz a megtévesztésig hasonló oldalra navigálják a felhasználókat, ahol sokan megadják a kért adataikat. Ezeket az adatokat azután a csalók elektronikus vásárláshoz vagy pénzátutaláshoz használják saját céljaikra. A bankok és a média tömeges és látványos, a veszélyre figyelmeztető felhívásokat tesznek közre időről időre, de ennek ellenére még mindig több millió euróra tehető a phishinggel okozott veszteség Európában.

Megnevezés	Jellemzők
Pharming	Szofisztikáltabb megoldás az adathalászatra, amely a számítógépen található hosts-fájlba írja bele a meghamisított banki oldalak címét. Ennek megfelelően a megtámadott számítógépen a felhasználó hiába írja be a böngésző címsorába bankja URL-címét, a címfeloldás nem a megszokott DNS-szerveren történik, hanem helyben, az átírt hosts-fájl segítségével, és az ügyfél a hamis banki oldalon találja magát, ahol gyanútlanul megadja adatait.

Forrás: Kovács 2006

Általánosságban megfogalmazva a rosszindulatú szoftverek olyan programok – vagy azok egyes részei –, amelyek anélkül jutnak a felhasználó számítógépére (okoseszközére, hálózati eszközére vagy akár az IoT fogalomkörébe tartozó egyéb eszközre), hogy arról maga a felhasználó tudna, illetve arra engedélyt adott volna.

A malware-eknek mindegyike speciális és sajátos funkcióval bír. Egy közös azonban van bennük: akár információszerzésről, akár adatlopásról, vagy a rendszer működésének akadályozásáról van szó, ezek a programok kárt okoznak, ráadásul a primer káron felül közvetett kárként jelentkezik még a felfedésük is, mert az időt, energiát, hardver- és/vagy processzorteljesítményt igényel, nem beszélve az eltávolításukról. Az okozott kár azonban nem minden esetben azonosítható teljes egészében és teljesen egyértelműen. A későbbiekben utalni fogunk rá, hogy számos olyan támadási módszer létezik, amelyek bár malware-eket használnak, mégsem egyértelmű (legalábbis azonnal), hogy a rendszert valaki megtámadta. Ilyen támadási módszer például a korábban már említett APT (Advanced Persistent Threat), azaz célzott támadás, amely során a bekövetkezett károkat – például azt, hogy mennyi és milyen adatot loptak el – nagyon sokszor csak megbecsülni lehet.

A malware-ek fejlődésével a korábban ismertetett felosztást azonban ki lehet egészíteni egyéb alkategóriákkal. A vírusok esetében például a fertőzési mód alapján történő osztályozással is élhetünk, amely

alapján a rosszindulatú szoftverek terjedhetnek közvetlen fertőzéssel vagy rezidens módon. Maguk a vírusok is tovább osztályozhatók: bootvírus, programvírus, makrovírus, scriptvírus vagy akár a legújabb típus, a féregvírus. Ugyanígy a trójaikat is külön csoportokra lehet osztani, amely csoportok egyébként önálló rosszindulatú programkategóriákat is jelölhetnek: disk wiper (merevlemeztörlő), keylogger (belépési azonosítókat rögzítő), banki jelszólopó, spyware (kémprogram), backdoor (hátsó ajtót nyitó program), rootkit (rendszerfájlok fertőzése), ransomware (zsarolóprogramok). (Szappanos 2015)

A rosszindulatú szoftverek – ahogy a fentiekben bemutattuk – egész armadája lesi az áldozatokat. Ezek közül egyet – a zsarolóvírust, azaz a ransomware-t – emeljük ki és mutatjuk be részletesen. Ennek oka elsősorban az, hogy az elmúlt időben ez a malware okozta a legnagyobb pánikot világszerte, majd később arra is találunk utalásokat, hogy ezek egyes fajtái, illetve az azokkal elkövetett támadások jóval túlmutatnak az egyszerű pénzszerzési akciókon, azaz már régen nem, vagy nemcsak kiberbűnözésről, hanem olyan kibertámadásokról beszélünk, amelyek mögött országok állnak.

Ransomware-ek, avagy zsarolni jó üzlet?

A malware-ek közül 2017-től külön figyelmet kell szentelnünk a ransomware-eknek azaz a zsarolóvírusoknak. A korábban említett Kaspersky-féle elemzés már 2016-ban 62 fő zsarolóvírus-családot és ezeken belül közel 54 ezer mutánst azonosított. Ezek 1,5 millió, a Kaspersky biztonsági szoftvereit futtató felhasználót érintettek valamilyen mértékben. (Garnaeva et al. 2016)

A Trend Micro elemzése szerint 2016-ban a zsarolóvírusok legfőbb fajtáit jelentő családok száma közel 7,5-szeresére nőtt az előző évihez képest. (Trend Micro 2017a)

Mégis 2017 tavaszán keltett először világméretű pánikotés, nyugodtan kijelenthetjük, „hisztériarohamot" a WannaCry nevű zsaroló-

program. Persze ebben a hisztériakampányban nagyon nagy szerepet kaptak a különböző médiumok is, amelyek látványos képekkel sokkolták az embereket.

Még a kiegyensúlyozottságáról és rendkívüli hitelességéről híres *BBC* is hangzatos szalagcímekkel jelentkezett 2017. május 12-én, pénteken: „Massive ransomware infection hits computers in 99 countries", azaz szabad fordításban: „Masszív zsarolóvírus fertőzött meg számítógépeket 99 országban". (BBC 2017)

Már az első híradások is arról tudósítottak, hogy a korábban az NSA által felfedezett, a Windows operációs rendszer onnan ellopott sérülékenységeit kihasználó szoftver[4] továbbfejlesztett változata a *WannaCry* (vagy *WanaCrypt0r 2.0*) névre keresztelt vírus és annak mutánsai több tízezer számítógépet fertőztek meg. Ez a szám később több százezerre nőtt.

A zsarolóvírusok – ahogy a vírus történelmét röviden bemutató összefoglalásunkban is látható – nem új keletű eszközök. Ami unikálissá tette, és nem utolsó sorban valamennyire alátámasztotta a WannaCry okozta hisztériát, amely ráadásul nemcsak a médiában, hanem szakmai körökben és a szakmai sajtóban is jelentkezett, az a vírus terjedésének gyorsasága és intenzitása volt főleg azokban a hálózatokban (elsősorban vállalati környezetben), ahol nagyon sok számítógép volt megtalálható egy adott hálózaton belül.

A WannaCry első áldozatai az Egyesült Királyság, ezen belül is Anglia és Skócia különböző kórházai és egyes egészségügyi intézményei voltak. (BBC 2017)

---

[4] Egyes források ezt a szoftvert az *Eternal Blue* nevű exploittal azonosítják, amelyet korábban egy homályos hátterű hacker, vagy hackercsapat – a *Shadow Brokers* – tett közzé, és amelyet az NSA-től loptak el. (Goodin 2017) Mindazonáltal ez az eset is jól rávilágít arra, amikor egy nemzetbiztonsági szolgálat sérülékenységeket fedez fel, elkészíti az annak a kihasználását lehetővé tevő exploitot, anélkül hogy akár a sérülékenységről, akár annak támadási lehetőségéről az adott szoftvert gyártót értesítené. Különösen aggasztó ez egy olyan nemzetbiztonsági szolgálat esetében, mint az NSA, valamint az olyan cég relációjában, mint a Microsoft.

Az elektronikus médiumok a brit állami egészségügyi szolgálat (NHS – National Health Service) közleményét világszerte továbbították. Eszerint a vírus áldozatai első körben 19 angliai körzetben, köztük London, Blackburn, Nottingham, Liverpool és Manchester egyes kórházaiban jelentkeztek. A zsarolóvírus a számítógépek és számítógépes rendszerek mellett a telefonszolgáltatásokat is komolyan érintette. Az ügy súlyosságát mutatja, hogy az érintett kórházakban időlegesen felfüggesztették a sürgősségi ellátást nem igénylő betegek fogadását. (Bolcsó–Haász 2017)

Külön érdekesség, hogy az Egyesült Királyság egészségügyi rendszereiben működő MRI képalkotó berendezések közül számos még mindig Windows XP operációs rendszerrel működött a támadás idején. (Dorrans 2017; idézi: Hlács 2017)

A vírus kizárólag a Windows korábbi sérülékenységeit használta ki, első körben a Server Message Blockot (SMB), amely egy, az alkalmazásrétegben lévő protokoll. Ennek segítségével a vírus átvette az irányítást a megtámadott számítógép felett, ami után elindított sok olyan folyamatot, amelyekkel a fájlok hozzáférési jogait megváltoztatta. Ezt követően TOR-hálózaton elérhető szolgáltatásokkal lépett kapcsolatba, onnan várva vezérlést a fertőzött számítógéphez. Mindezek után titkosította a felhasználó fájljai közül a leggyakoribb kiterjesztésűeket (alapvetően Office alkalmazások fájljait), illetve igyekezett titkosítani egyéb fájlokat (virtuális gépek fájljai, tanúsítványok stb.) is. (ITMA Hungary 2017)

Mivel a WannaCry alapvetően Microsoft Windows operációs rendszerek sérülékenységeit érintette, a Microsoft a tömeges fertőzés hatására váratlanul és előre nem tervezetten frissítéseket adott ki a Windows 8 és Windows Server 2003 rendszereire, sőt a már évek óta nem támogatott Windows XP-re is. (Microsoft 2017b)

42. ábra
WannaCry képernyőkép

Forrás: HLÁCS 2017

A WannaCry egész világot bejáró támadási hullámai előtt már 2017. április elején Magyarországot is elérte egy zsarolóvírus-fertőzési hullám. Hazánkban is több kórházat ért ilyen támadás, köztük a veszprémi Csolnoky Ferenc Kórház informatikai rendszerét is. (BOLCSÓ 2016)

A kórházak és a közintézmények ideális célpontnak tűnnek a zsarolóvírus gazdái számára, hiszen itt olyan mindennapi használatban lévő adatokat tárolnak és kezelnek, amelyek időleges kiesése is nagyon komoly – akár emberéletekben jelentkező – következményekkel járhat. Így az azonnali váltságdíj fizetésére – esetlegesen más megoldás hiányában (például háttérmentésből az eredeti adatok visszaállításának lehetősége) – jó eséllyel nagyobb hajlandóságot mutatnak ezen intézmények. Másrészt ezek azok az intézmények, ahol a világon gyakorlatilag mindenhol a biztonságtudatosság, valamint a rendszereket használók információbiztonsági felkészültsége, annak naprakészsége sok kívánnivalót hagy maga után.

A ransomware történelme

A zsarolóvírusok története egészen 1989-ig nyúlik vissza. Ekkor egy úgynevezett *AIDS,* vagy más néven *Aids Info Disk* – amely arra a floppy lemezre utal, amelyen AIDS-cel kapcsolatos információkat ígértek a felhasználóknak – jelent meg. (Más források *PC Cyborg Trojannak* hívták ezt a vírust). Ekkor még nyilvánvalóan a vírus, illetve a trójai közvetítő közege az említett flopilemez volt. A vírus felülírta az AUTOEXEC.BAT fájlt, majd ezt követően a 90. bootolás után elrejtette a C: meghajtó könyvtárait, és titkosította a fájlokat. A titkosítás feloldásához 189 – egyes esetekben 378 – amerikai dollárnyi összeget kért, amelyet egy panamai postafiókcímre a PC Cyborg Corporation cég nevére kellett az áldozatnak elküldenie. A vírus szimmetrikus kulcsú titkosítást használt, így egy idő után a titkosított fájlok visszaállítása nem okozott túl nagy problémát.

Ezt követően azonban a kiberbűnözés is szintet lépett, és 2005-től sorra jelentek meg az olyan zsarolóvírusok, amelyek már RSA-titkosítást használtak, mint például Archiveus, GPcode, Krotten, Cryzip, MayArchive.

Amíg korábban a locker típusú zsarolóvírusok, azaz a felhasználót egyszerűen a rendszerből kizáró ransomware-ek addig ma elsősorban a cryptoware-ek, azaz az adatállományon titkosítást végrehajtó programok terjednek.

A WannaCry terjedése újszerűnek mondható, hiszen a fertőzéséhez nem szükséges a felhasználó közvetlen interakciója, azaz nem kell például egy fertőzött csatolmánnyal ellátott e-mailt megnyitnia, mert a vírus hálózati kapcsolat esetén az operációs rendszerek sérülékenységeit kihasználva terjed és fertőz. Természetesen ehhez a felhasználók közvetett segítsége mégis kell, hiszen a WannaCry által kihasznált sérülékenységek több hónappal korábban már ismertté váltak, sőt a Microsoft ezek többségére korábban javítást is kiadott. Ezeket azonban az áldozattá vált felhasználók nem telepítették, illetve nem engedélyezték az automatikus frissítési opciót.

A vírus terjedését sikerült egy időre visszaszorítani azzal, hogy egy információbiztonsági szakember – Darien Huss – egy, a vírus kódjában megtalálható teljesen értelmetlennek tűnő doménnevet regiszt-

rált. A vírus kódjában lévő algoritmus ezt a doménnevet kereste, és amennyiben ez működött, azaz elérhető volt, nem terjedt tovább. Ez azonban a WannaCry egyes mutánsaira nem feltétlenül volt igaz. (Khomani–Solon 2017)

A vírus a titkosítás feloldásáért első körben 300 dollárnyi, majd egyes esetekben 600 dollárnyi bitcoint kért.

A vírus nemcsak kórházakat, közintézményeket és egyszerű felhasználókat támadott, hanem minden olyan elérhető számítógépet, amely az említett operációs rendszereket futtatta az ismertetett sérülékenységekkel. Így egyetemek, iskolák, de ipari folyamatokat irányító rendszerek vagy közlekedésszervezést megvalósító számítógépek is áldozattá váltak.

43. ábra
A WannaCry hatása egy németországi vasúti pályaudvar utastájékoztató terminálján

Forrás: Graham 2017

Két hónap sem telt el 2017 májusa után, és máris egy újabb – de sokkal furcsább – zsarolóvírus keltett ismételten pánikot.

2017. június 27-én egy *NoPetya* (más néven *PetrWrap)* nevű ransomware kezdett terjedni és fertőzni óriási sebességgel elsősorban Európában, annak is keleti felében. A fő célpontok és a vírus első áldozatai Ukrajnában voltak.

A vírus szintén az SMB egyik sérülékenységét használta ki, de ellentétben a WannaCry-jal ez már e-mailek csatolmányaként is terjedt.

A hazai Kormányzati Eseménykezelő Központ azonnal egy részletes közleményt adott ki a ransomware-rel kapcsolatban. (Gov-CERT 2017)

A GOVCERT közleménye a NoPetya zsarolóvírussal kapcsolatban

„2017. 06. 27-én indult el a PetrWrap kampány, amely komoly károkat okozott Oroszországban, Ukrajnában és Európa több országában is. A PetrWrap ransomware egy Petya [1] alapú zsarolóvírus. A C-ben írt és MS Visual Studioban fordított program több egy újabb variánsnál. Mivel a Petya-t használja a fájlok titkosítására, ami egy jól ismert ransomware, ezért a PetrWrap saját kriptográfiai rutint használ ennek elrejtésére. Ezt a folyamatot a készítők az OpenSSL-ből emelték át. Így a PetrWrap eléri, hogy az áldozat gépét lezárja és titkosítja az NTFS partíciókat. Mindezt anélkül, hogy megjelenne a képernyőn a villogó koponya animáció, amiről a Petya ismert.

A PetrWrap a WannaCry-hoz [2] hasonlóan az SMBv1 sérülékenységet (EternalBlue) használja ki, emellett e-mail-ben, kéretlen adathalász levelekben is terjed, ahol álláshirdetésre való jelentkezésnek álcázza magát. Az elemzések szerint a csatolmányként érkező dokumentum tartalmazza azt parancsot, amely letölti a zsarolóvírust a számítógépre. A számítógép újraindítása után nem engedi bootolni a Windows-t, a saját bootloader-ét tölti be helyette, amely mutatja a titkosított fájlrendszer dekódolásához szükséges instrukciókat. A dekódoláshoz $300 értéknek megfelelő bitcoin fizetőeszközt várnak váltságdíjként.

Ha megfertőzött egy számítógépet, az alábbi módokon terjeszti tovább magát: MS17-10 sérülékenységet kihasználva (amit a WannaCry is használt) [3]; WMI (Windows Management Instrumentation) használatával [4]; PSEXEC vagy ehhez hasonló eszköz segítségével [5].

A következőket teszi a fertőzött számítógépen:

- törli a rendszer eseménynaplóját, hogy nehezebb legyen detektálni;
- felülírja és titkosítja a Master Boot Record (MBR) bejegyzést, majd újraindítja a számítógépet egy órán belül (feladatütemezőben hozza létre a feladatot);

- titkosítja a FAT táblát, vagy ha ehhez nincs hozzáférése, újraindítás nélkül is képes titkosítani következő kiterjesztésű fájlokat: 3ds, 7z, accdb, ai, asp, aspx, avhd, back, bak, c, cfg, conf, cpp, cs, ctl, dbf, disk, djvu, doc, docx, dwg, eml, fdb, gz, h, hdd, kdbx, mail, mdb, msg, nrg, ora, ost, ova, ovf, pdf, php, pmf, ppt, pptx, pst, pvi, py, pyc, rar, rtf, sln, sql, tar, vbox, vbs, vcb, vdi, vfd, vmc, vmdk, vmsd, vmx, vsdx, vsv, work, xls, xlsx, xvd, zip.

Az GovCERT a fertőzés elkerülése érdekében az alábbi javaslatokkal él a felhasználók irányába:

- telepítsék a Windows SMB sérülékenységét befoltozó javítást [3];
- ne látogassanak nem megbízható weboldalakat és ne kövessenek ilyen hivatkozásokat (linkeket) se;
- az ismeretlen feladótól kapott e-mail csatolmányaként érkező dokumentumokkal szemben legyenek elővigyázatosak;
- készítsenek biztonsági mentést a számítógépen tárolt fontos adatokról;
- kapcsolják le az SMB1-et [6];
- a fertőzés megelőzése érdekében az alábbi címek elérését érdemes letiltani a tűzfalon: french-cooking.com, benkow.cc, 185.165.29.78, upd.me-doc.com.ua, 95.141.115.108, 111.90.139.247, 84.200.16.242, 185.165.29.78, yadi.sk.
- részleges megoldások: készítsenek egy kiterjesztés nélküli „perfc” nevű fájlt a Windows telepítési mappájába (C:\Windows\), vagy blokkolják a „C:\Windows\perfc.dat” állomány írási/végrehajtási jogát [11], és ezáltal a ransomware semmilyen kárt sem fog okozni. Amennyiben bekövetkezett a fertőzés, az NKI nem javasolja a váltságdíj megfizetését. Többen fizettek már, de nem kapták vissza az adataikat [7], továbbá a támadók által használt postafiókot letiltotta a szolgáltató [8], így onnan válasz nem várható fizetés esetén sem. Ezért ilyen esetben a rendszer újratelepítése szükséges és az adatok visszaállítása a biztonsági mentésből.

Hivatkozások:

[1] http://tech.cert-hungary.hu/vulnerabilities/CH-13138
[2] http://tech.cert-hungary.hu/tech-blog/170513/az-smb-serulekenyseget-kihasznalo-wannacry-ransomware-kampany
[3] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

[4] https://msdn.microsoft.com/en-us/library/aa394582(v=vs.85).aspx
[5] https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx
[6] https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows
[7] https://motherboard.vice.com/en_us/article/new8xw/hacker-behind-massive-ransomware-outbreak-cant-get-emails-from-victims-who-paid
[8] https://posteo.de/en/blog/info-on-the-petrwrappetya-ransomware-email-account-in-question-already-blocked-since-midday
[9] www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know
[10] www.symantec.com/security_response/writeup.jsp?docid=2016-032913-4222-99
[11] https://twitter.com/HackingDave/status/879779361364357121

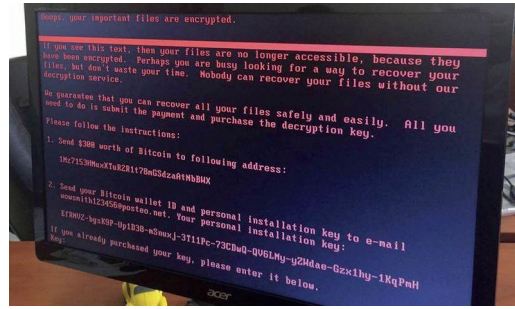
A NoPetya-vírus a WannaCry-jal ellentétben nem véletlenszerűen választott megfertőzni kívánt IP-címeket, hanem nagyon is tudatosan terjedt. Pont ez teszi érdekessé, és egy kicsit furcsává is. Egy másik nagyon elgondolkodtató tény, hogy a vírus alapvetően egy, a *MeDoc* nevű – elsősorban Ukrajnában használt – könyvelőszoftver automatikus frissítésével került az elsőként megfertőzött gépekre.[5] Ez felveti annak a veszélyét, hogy valóban megbízhatóak-e, azaz tényleg nem kompromittálhatók-e az automatikus frissítések? Ez azért is fontos kérdés, mert az információbiztonsági szakemberek elsődleges tanácsa pont az, hogy a felhasználó kapcsolja be az automatikus frissítés opciót, azaz ne a felhasználóra legyen bízva az esetleges biztonsági javítások időpontja, hanem az történjen meg automatikusan és a lehető legrövidebb idő alatt, legyen szó operációs rendszerről vagy akár egy egyszerű könyvelőprogramról.

[5] A Kaspersky elemzései megállapították, hogy a NoPetya-víruson kívül ezzel egyidőben legalább még egy vírus is megfertőzte a MeDoc-felhasználókat, amely az *ed.exe* nevet viselte. Nem meglepő módon ez is egy ransomware volt. (Ivanov–Mamedov 2017)

Itt egy kis kitérőt kell tennünk a történet folyamatában, mivel ez a probléma, azaz az automatikus frissítések biztonsági kérdései – ahogy láthatjuk a NoPetya esetében – igen jelentősnek tekinthetőek. Ennek analógiáján felmerül a kérdés, hogy mi történik, ha az adott szolgáltatást nyújtó nagy szoftvervállalat beszállítói nem megbízhatóak, vagy azok kompromittálódnak?

Egy ilyen esetről számolt be a szakmai sajtó 2016-ban. Az eset az Apple-nél, illetve annak egyik beszállítójánál a Supermicrónál történt. Ez a cég szállította az Apple által használt egyes szervereket. Ugyanakkor feltételezhető, hogy ezeknek a szervereknek a firmware-jei rosszindulatú programokkal voltak fertőzöttek, ráadásul ezeket a malware-eket az Apple belső fejlesztői környezetében, valamint az Apple App Store-ban is megtalálták. Ezt követően az Apple megszüntette a Supermicróval való együttműködését. (Gallagher 2017)

Visszatérve a NoPetya zsarolóvírus történetéhez, sok kiberbiztonsági szakértő annak a véleményének adott hangot, hogy bár oroszországi és egyéb európai szervereket is ért támadás, mégis Ukrajna volt a fő célpont, amiből feltételezhetően az következik, hogy Oroszország állhat a vírus hátterében. Azt, hogy a támadások elsősorban nem pénzszerzési céllal történtek, az is alátámasztja, hogy a vírus – ellentétben a WannaCry-jal, ahol egészen ötletes módokon lehetett a támadókkal kapcsolatba lépni – csak egyetlen olyan e-mail-címet adott meg kapcsolatnak, ahol a váltságdíjról tárgyalni lehet. Ezt az e-mail-címet azonban annak szolgáltatója rövidesen blokkolta, így gyakorlatilag más kontakt hiányában nem volt lehetséges a támadókkal kapcsolatba lépni.



44. ábra
A NoPetya képernyőképe

Forrás: MTI, Bolcsó 2017

Mindezek alapján feltételezhetjük, hogy ennek a támadásnak a pénzszerzés helyett több, sokkal komolyabb célja is volt.

Az első cél az információszerzés lehetett. Ha valóban igaz az a feltételezés, hogy a támadások mögött ilyen vagy olyan módon, de a hivatalos orosz politika állt, akkor a támadások hatásainak elemzése sok olyan információt szolgáltat a megcélzott rendszerekről az orosz szervezetek számára – legyenek azok nemzetbiztonsági szolgálatok vagy állami biztonsági vállalatok – amelyek alapján azok gyenge és támadható pontjait lehet nagyon nagy biztonsággal beazonosítani.

A másik cél egyértelműen egy nagyon masszív üzenet eljuttatása a világ, elsősorban az Egyesült Államok számára. Az üzenet már-már a kiberhadviselés irányába mutat: mi erre is képesek vagyunk!

A zsarolóvírusok elleni védekezés – hasonlóan a többi rosszindulatú program elleni védelemhez – meglehetősen összetett, de nyilvánvalóan itt is szükséges felsorakoztatni olyan specifikus biztonságot növelő tényezőket, amelyek elsősorban az adatállomány védelmét szolgálják.

A biztonság növelése azonban nagyon egyszerű, már-már triviálisnak tűnő intézkedések sorozatával nagyban növelhető. Ezek a védelmi lépések valóban nem igényelnek hatalmas befektetést, csak alapvető biztonságtudatosságot és figyelmet. Az első ilyen védelmi intézkedés

látszólag meglehetősen távolról közelíti meg a kérdést: ez az oktatás és a képzés. Ez ugyanakkor az egyik legjobban és talán a leggyorsabban megtérülő befektetés a biztonság megteremtése érdekében, hiszen a felhasználók biztonságtudatosságának növelése egy egyszerű oktatással vagy rendszeresen ismétlődő képzéssel nagyban növelhető.

Mivel a felhasználók jelentik minden rendszerben a biztonság leggyengébb láncszemét, értelemszerűen az ő felkészítésük és nem utolsósorban folyamatos képzésük ezen a területen nagyon gyorsan és nagyon látványosan hozhat eredményeket. Ennek az oktatásnak, illetve képzésnek az egyik legnagyobb előnye az lehet, ha az olyan egyszerű és életszerű biztonsági kérdéseket, mint például a kéretlen e-mailek, valamint azok csatolmányai esetén mit kell tennie a felhasználónak. Az oktatásnak ki kell térnie arra is, hogy melyek azok az áruló, a mindennapi élet különböző folyamataihoz nagyban hasonló, attól csak kis mértékben eltérő jellemzők, amelyek alapján ha nem is lehet felismerni a támadást vagy annak szándékát, de mindenesetre az erre irányuló gyanúnak fel kell ébrednie, amelynek alapján az incidenskezelési tervben foglaltak alapján már el lehet járni. Nyilvánvalóan az adott szervezet incidenskezelési tervének (ha van) ennek is részének kell lennie, de az is nyilvánvaló, hogy a felhasználókat ezzel a tervvel csak a számukra szükséges szintig és mértékig kell megismertetni.

A képzésnek sok esetben tréning, azaz gyakorlásrésze is kell, hogy legyen, hiszen így lehet egyrészt meggyőződni arról, hogy valóban a gyakorlatban is képes a felhasználó alkalmazni az elméletben megszerzett tudást, másrészt az incidenskezelési terv próbája is egy ilyen – ellenőrzött keretek között történő – gyakorlati próba.

A ransomware-ek elleni védekezés technikai oldala szintén olyan egyszerűnek tűnő tényezőket jelent, amelyek általánosságban az információbiztonság vagy a kiberbiztonság alapvetései is lehetnének.

Természetesen ezek az egyszerű tényezők csak komplex módon értelmezhetők, azaz minden megtett védelmi intézkedésnek és tevékenységnek egy cél érdekében, egymással összefüggésben kell történnie. Szükséges annak hangsúlyozása, hogy a megelőzés nagyon sok-

szor az egyetlen mód a károk elkerülésére. Egy-egy támadás esetén már nincs mód a védekezésre, maximum a károk enyhítésére. Ennek megfelelően a rendszereink, és ebbe bele kell érteni a korábban már említett felhasználókat is, lehető legnagyobb és teljes körű védelmére kell törekedni.

Az első lépés nyilvánvalóan a naprakész víruskereső alkalmazások futtatása a rendszerünkben, amelyek közül ma már a legtöbb valamilyen tűzfalat is tartalmaz. Összetettebb rendszerek esetében behatolásérzékelő rendszerek (Intrusion Detection System – IDS) alkalmazása szintén szükséges. Ezek bekapcsolása már egyfajta biztonságot jelenthet.

Minden információbiztonsági kézikönyv tartalmazza azokat az ajánlott, sőt kötelező tennivalókat, mint például a „Készíts másolatot, vagy még inkább másolatokat a legfontosabb adataidról!". Ez persze nem ennyire egyszerű, hiszen még egy átlagos felhasználó is sokszor abba a problémába ütközik, hogy az adatok háttérmentése sok időt és energiát igényel, nem beszélve arról, hogy bizony ez ma már valóban stratégiát is igényel. Minél nagyobb a szervezet, amelynek adatállományáról gondoskodnunk kell, annál nagyobb szükség van egy valóban működő adattárolási és adatmentési stratégiára. Az így mentett és természetesen folyamatosan aktualizált adatállományokat fizikailag több helyen – népszerű kifejezéssel: georedundáns módon – célszerű tárolni.

Az adatok háttérben történő mentésén kívül szintén egyszerű és a kiberbiztonságban mindennap elhangzó figyelmeztetés a rendszerek naprakészen tartása, azaz a biztonsági és egyéb szoftveres összetevők frissítése. Ez szintén egy külön stratégiát igényel: a korábban már említett *patch management,* azaz a biztonsági frissítések kezelésének stratégiáját.

Mindezeken túl szervezeti szinten szükség van üzletmenet-folytonossági tervre (Business Continuity Plan, BCP)[6], valamint katasztrófavédelmi tervre (Disaster Recovery Plan, DRP)[7] is.

Nyilvánvalóan akár az adattárolásra, akár a BCP egyes elemeinek biztosítására lehetséges megoldás a felhőszolgáltatások igénybevétele, amennyiben erre lehetőség van (például ez engedélyezett, nincsenek minősített adataink, vagy ha vannak, akkor megfelelő magán-felhőszolgáltatást lehet alkalmazni stb.), mivel az azokba történő adatmentés, illetve az azokból történő adat-helyreállítás nagyon gyorsan megoldható.

A ransomware-ek esetében szükséges néhány – korábban említett specifikus – védelmi intézkedés megtétele. Szükség van azoknak a sérülékenységeknek a külön javítására vagy azoknak a szolgáltatásoknak az ideiglenes lekapcsolására, amelyeket ezek a vírusok kihasználnak a fertőzésükhöz. A WannaCry és a NoPetya esetében az SMB-protokoll által használt portok lekapcsolása lehet ilyen megoldás.

Amennyiben megtörtént a ransomware-támadás a rendszerben vagy a rendszer egyes elemeinél, akkor az egyik azonnali védelmi megoldás a rendszer, illetve a fertőzött rendszerelem elszigetelése, izolálása addig, amíg a rendszer többi elemének vizsgálata, illetve a fertőzött rendszerelemekből a vírus eltávolítása tart. Ezt követően a rendszer felhasználóit a bekövetkezett támadásról, annak következményeiről,

---

6 Az üzletmenet-folytonossági terv célja, hogy amennyiben valamilyen fennakadás történik a működésben, a lehető legrövidebb időn belül, a lehető legkisebb kár elszenvedése mellett legyenek helyreállíthatók az adott szervezet működése szempontjából legfontosabb folyamatok. Ebben a komplex tervben helyet kap a kockázatok azonosítása (legyen szó hagyományos, a szervezet működését befolyásoló olyan kockázatról, mint például a természeti csapások, illetve tűz vagy akár a kibertámadások jelentette kockázatok), ezek esetleges bekövetkezésének a szervezet működésére gyakorolt hatásainak elemzése, a védelmi tervek stratégiai szintű elkészítése, majd a terv működőképességének ellenőrzése, azaz a végrehajtás eredményességének ellenőrzése (szimulálás).

7 A katasztrófavédelmi terv gyakorlatilag egy olyan itiner, egy olyan sorvezető, amely lépésről lépésre tartalmazza azokat a tennivalókat, amelyeket egy váratlan és negatív, a szervezet működését alapjaiban befolyásoló esemény bekövetkeztekor végre kell hajtani annak érdekében, hogy a szervezet a normál működését mielőbb visszanyerje.

valamint a számukra szükséges mértékig a megtett védelmi intézkedésekről tájékoztatni kell.

Mindezeknek a védelmi terv részét kell képezniük. Nagyon fontos a jó dokumentálás, azaz minden tényezőt az incidens bekövetkezésétől, a felhasználók esetleges tevékenységén át a védelmi intézkedések megtételéig dokumentálni, rögzíteni kell. Ezek a későbbi elemzésekhez, valamint a későbbi oktatáshoz – legyen az akár egy egyszerű tudatosító kampány vagy szervezett tréning – felhasználhatóak.

A védekezés terén előremutató kezdeményezés a *No More Ransom,* azaz *Ne legyen több zsarolóvírus* című honlap és a mögötte lévő tartalom, illetve tevékenység. Az oldal a holland rendőrség Számítástechnikai Bűncselekmények Elleni Egységének (National High Tech Crime Unit – NHTCU), az Europol Európai Számítástechnikai Bűnügyi Központja (Europol European Cybercrime Centre – EC3), valamint két információbiztonsági nagyvállalat – a Kaspersky Lab és az Intel Security – támogatásával és hatékony közreműködésével jött létre. Fő célja, hogy hathatós segítséget nyújtsanak a ransomware-ek áldozatainak abban, hogy adataikat visszanyerjék, valamint hogy a hasonló fertőzések elkerülhetők legyenek. A célok közül természetesen ez utóbbi sokkal reálisabb, hiszen a zsarolóvírus-fertőzést elkerülni sokkal egyszerűbb, mint a fertőzések után az adatok visszaállítása. Az oldal fő mottója és általános érvényű tanácsa: „Don't pay the ransom", azaz „ne fizess a zsarolónak". Ennek érdekében az oldal gyűjti azokat a titkosítást feloldó kulcsokat, illetve az azok használatát leíró tenni- és tudnivalókat, amelyek egy-egy korábbi vagy akár aktuális zsarolóvírus esetén már működtek, és ezeket az áldozatok számára elérhetővé teszi. (No More Ransom 2017)

A kezdeményezéshez annak elindulását követően több tucat partner, számos ország – kiberbűnözésre szakosodott – rendőrsége, köztük a magyar Készenléti Rendőrség Nemzeti Nyomozóiroda Kiberbűnözés Elleni Főosztálya is csatlakozott.

2.1.2. Túlterhelés mint támadási módszer

A Denial of Service (DoS) támadásai – azaz szolgáltatásmegtagadással járó támadások vagy elterjedtebb szóhasználattal élve túlterheléses támadások – az egyik legnagyobb problémát és egyben a legnagyobb kihívást is jelentik a kibertér biztonságában.

A támadás alapvetése viszonylag egyszerű: olyan mennyiségű kérést (lekérdezést) kell intézni az adott célpont felé, amely azt már kapacitás hiányában nem tudja kiszolgálni. A nagy mennyiségű lekérdezés azonban egyrészt sok számítógépet, másrészt ezeknek a számítógépeknek az egyidejű és koordinált tevékenységét feltételezi.

A DoS-támadások sok fajtája és még több technikai kivitelezése létezik. Ugyanakkor nagy biztonsággal három főbb kategóriába lehet ezeket besorolni. (Gyányi 2012)

Az első fő kategória a hagyományos DoS-támadások kategóriája. Ebben a csoportban a támadó erőforrásai (lekérdezéseinek száma, sávszélesség, kiszolgálási folyamatok száma, idő stb.) meghaladják az áldozat, azaz a megtámadott számítógép erőforrásait.

A második kategória az úgynevezett *elosztott túlterheléses,* angol megnevezéssel *DDoS – Distributed Denial of Service* támadások kategóriája. Ebben az esetben a támadó nemcsak egy, hanem sok olyan eszközt használ a megcélzott számítógép erőforrásainak túlterhelésére, amelyek nem egy végpontban, hanem a világon bárhol lehetnek. Az összehangolt támadók erőforrásai egy irányba hatnak, azaz összeadódnak, így haladva meg a megtámadott számítógép erőforrásait.

A harmadik csoport a reflektív vagy felerősített elosztott túlterheléses támadás. A támadó ebben az esetben sok olyan számítógépet használ a célba vett számítógép vagy szolgáltatás túlterhelésének előidézésre, amelyek nincsenek teljesen az ellenőrzése alatt, mégis a kiszolgálási kéréseket továbbítják az áldozat felé. (Gyányi 2012)

Természetesen másfajta csoportosítás is elképzelhető. Abban az esetben, ha a támadás a célpont hálózati kapcsolatának vagy a célpont valamely – szolgáltatást nyújtó – alkalmazásának túlterhelésére

irányul, akkor vagy hálózati, vagy alkalmazási rétegben (utalva itt az OSI referenciamodelljére) végrehajtott DoS típusról beszélhetünk. (Gyányi 2009)

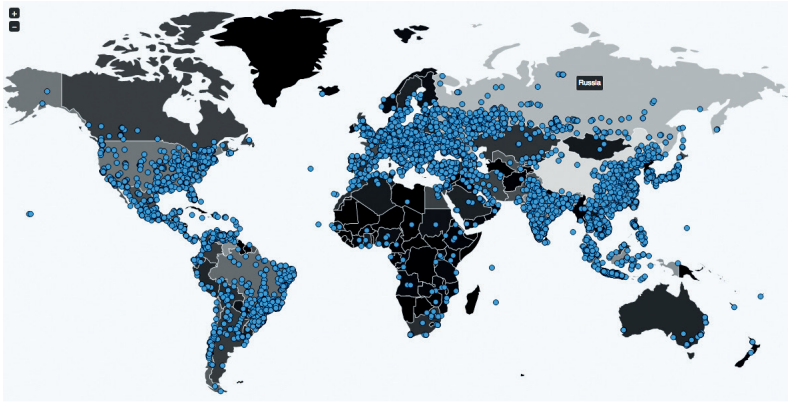
A DDoS-támadások trendjeit is kutató Akamai[8] cég adatai alapján 2016 harmadik negyedévében a legnagyobb sávszélességet elérő DDoS-támadás meghaladta a 623 Gbps-ot. Önmagukban a DDoS-támadások pedig 71%-kal nőttek 2016 végére az előző két év adatait figyelembe véve. Ezen felmérés szerint a DDoS-támadások kiindulópontjai között első helyen Kína áll 30%-kal, második az Egyesült Államok 22%-kal, és harmadik helyen szerepel az Egyesült Királyság 19%-kal. (Akamai 2016)

A DDoS-támadásokhoz, azaz az igazi károkozáshoz – főleg, ha azok olyan nagyságrendűek, mint a fent említett adatokban látszik – nagyon sok számítógép egyidejű tevékenységére van szükség. Ennek érdekében hálózatba szervezett, alapvetően[9] megfertőzött számítógépek kellenek. Ezek a gépek anélkül fertőződnek meg, és így anélkül lesznek ennek a hálózatnak a tagjai, hogy arról azok felhasználói tudnának. A szoftver robotokkal felderített sérülékeny és támadható számítógépeket valamilyen malware-rel kompromittálja, majd botnetbe (robotok segítségével összeállított hálózatba) szervezi. A megfertőzött számítógépeket korábban sok esetben *zombigépeknek* is nevezték. Így alakulnak ki a botnetek vagy a botnethálózatok.

---

8 Az Akamai céget a Massachusetts Institute of Technology (MIT), a Massachusettsi Műszaki Egyetem kutatói, Tom Leighton és Danny Lewin alapították 1998-ban. A cég alapötlete azokra a matematikai algoritmusokra épült, amelyek az elosztott hálózatok (szerverek) esetében az intelligens útvonalválasztásokat, valamint a tartalom ismétlését teszik lehetővé, biztosítva ezzel a lehető leggyorsabb lekérdezéskiszolgálást. (Akamai 2017)

9 Nem feltétlenül kell fertőzötteknek lenniük a DDoS-támadásokban rész vevő számítógépeknek, hiszen az lehet engedélyezett és tervezett közreműködés is. Ekkor azonban már inkább kiberhadviselésről beszélhetünk, hiszen egy ország például a közigazgatásában használt számítógépeket ilyen célra is használhatja.



45. ábra
A kép készítésének pillanatában működő botnetek

Forrás: MalwareTech 2017

Az *elosztott hálózatok elmélete* nem új keletű fogalom az internet világában, hiszen annak kezdetén a decentralizáltság volt az egyik igen nagy hozadéka a hálózatok összekapcsolásának. Számtalan előnnyel jár, ha az elvégzendő feladatokat olyan hálózatban osztjuk szét, amelynek kapacitása jóval meghaladja egy-egy nagy teljesítményű számítógép kapacitását is, hiszen az abban lévő gépek erőforrásai összeadódnak. Mindezeken túl az elosztott hálózatban nincsenek olyan korlátok, amelyek egyes gépek esetében az erőforrások növelésekor jelentkeznek: hűtés, áramellátás, sávszélesség biztosítása – hogy csak néhány tényezőt említsünk.

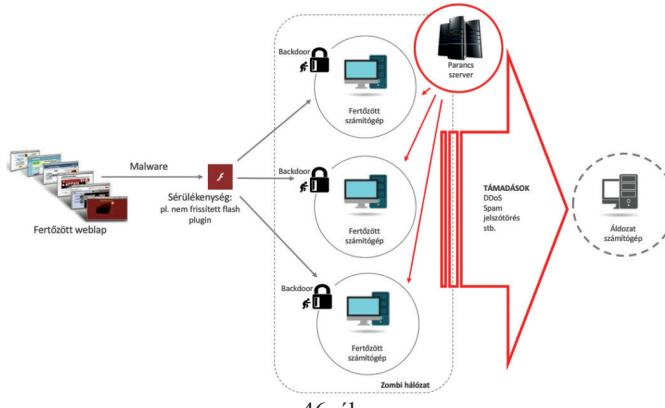
A botnetek az elosztott hálózatok filozófiájához hasonló elméleten alapszanak. Természetesen vannak legális botnetek is, amelyekben a felhasználók csatlakozása önkéntes és tudatos. Ilyen elosztott hálózat például a *SETI@home,* azaz *Search for Extra-Terrestrial Intelligence*, magyarul *földön kívüli intelligencia*[10] *keresése* projekt vagy a Stanford Egyetem 2000-ben indított *folding@home* nevű projektje, amely

[10] A SETI alapvetően a földön kívüli technikai civilizációt kutatja olyan jelek – elektromágneses vagy más kisugárzások – keresésével, amelyek bizonyítékok lehetnek arra, hogy nem az ember képviseli az egyetlen civilizációt a világegyetemben.

különböző orvosi kutatásokhoz használja fel az önkéntes módon csatlakozók számítógépkapacitásait elosztott hálózatként. (Almár 1999)

Mégis a botnetek az illegális tevékenységben kapják a legnagyobb szerepet, hiszen a túlterheléses támadások mellett számos más – nem feltétlenül legális – tevékenységet végeznek a segítségükkel, mint például spamküldés, jelszótörés stb.

A botnetek felépítése meglehetősen összetett, mégis négy jól elkülöníthető részre oszthatók. Ezek a szegmensek a következők: az első a botnet gazdája,[11] avagy tulajdonosa. Ő végzi az irányítást és a feladatok elosztását a botnetek tagjai, azaz a fertőzött számítógépek között. A második részbe a botnet tagjai tartoznak, ezek a megfertőzött számítógépek. A harmadik szegmens a botnet gazdája és a fertőzött gépek közötti kommunikációs csatorna, amelyet vezérlő vagy C2 (Command & Control) csatornának is neveznek. Itt listázzák általában a botnet tagjait (a megfertőzött számítógépek IP-címeit). A botnet negyedik fontos része az úgynevezett *dropszerver,* amely a botnet által összegyűjtött adatokat tároló számítógép. (Gyányi 2012)



46. ábra

A botnet általános felépítése (példa)

Forrás: a szerző szerkesztése

[11] A botnet gazdáját *botheldernek,* azaz pásztornak (mint aki a nyáját terelgeti) vagy *botmasternek* is nevezik.

DDoS akcióban, avagy az orosz–észt konfliktus

Ahogy korábban utaltunk rá, a DDoS-támadások hatalmas kihívást jelentenek napjainkban. Elosztott túlterheléses támadás naponta számtalan történik, amelyek motivációja és célpontjai rendkívül szerteágazóak.[12]

A kiberbűnözés mellett azonban megjelentek az olyan támadások is, amelyek a pénzszerzés helyett egészen más motivációval rendelkeznek. Az egyik ilyen legnagyobb támadás az *orosz–észt kiberkonfliktus* néven elhíresült eset volt.

2007. április végén járunk Tallinnban, a Baltikumban. Észtország fővárosában egy második világháborús, hősi szovjet felszabadító emlékművet távolít el a helyi önkormányzat. Ez hatalmas tiltakozást vált ki az egyébként hozzávetőlegesen 25–30%-ra becsült orosz nemzetiségű kisebbségből. Először csak Tallinnban, majd Észtország más városaiban, később pedig Oroszországban sok helyen kezdődnek tüntetések, amelyek elítélik ezt az észt akciót. Mindeközben az utcai megmozdulásokkal egy időben internetes támadások kezdődnek az észt közigazgatás kommunikációs rendszerei és különböző webes szolgáltatásai ellen.

A közvetlen kibertámadások mellett, a közösségi oldalakon és mobiltelefonos SMS-üzeneteken keresztül tüntetésekre, ellenállásra és további erőszakra szólítanak fel a támadók.

A kibertámadások közel három hétig tartanak, amelynek végére Észtország internetes hálózata már szinte teljes egészében megbénul.

---

12 Az itt bemutatott és elemzett Észtországot ért DDoS-támadások motivációja világos. Ugyanakkor hazánkat is számos ilyen támadás éri, ha nem is ilyen volumenben. Talán az egyik legnagyobb ilyen támadás, amely hatalmas szakmai visszhangot is kiváltott, 2016 áprilisában, majd májusában történt, és a kormányzati hálózatokat érte. A Nemzeti Kibervédelmi Intézet (NKI) akkori tájékoztatása szerint ennek a támadásnak, illetve támadássorozatnak fő célpontjai a Közigazgatási és Igazságügyi Hivatal honlapja, a *kormany.hu* és a Külgazdasági és Külügyminisztérium publikus szolgáltatásai voltak. (Belügyminisztérium 2016) A hazai rendszereket ért támadásokról azonban nem derült ki, mi volt azoknak az egyértelmű célja, illetve ezek mögött a támadások mögött lévő támadóknak mi jelentette a motivációt.

A kibertámadások több hullámban masszív, alapvetően az országon kívülről érkező DDoS-támadásokat jelentenek. A támadások célpontjai az észt parlament, a kormányhivatalok, valamint a bankok, pénzintézetek és az észt média informatikai központjai. A támadások volumenére jellemző, hogy az észt hálózaton az adatforgalom sokszor órákon át a megszokott közel ezerszerese. Mivel az ország internetes forgalmában kulcsszerepet játszó fő adat- és kapcsolóközpontok *(exchange)* naponta többször is leállnak, a közigazgatás számítógéphálózatait le kell kapcsolni az internetről.

A támadások hatására a banki rendszerek többsége megbénul, így a pénzügyi megbízások teljesítését a bankok nem tudják végrehajtani.

Május közepére a támadások elérték a maximális intenzitásukat, de számos hálózati rendszer még hetekig alacsonyabb teljesítménnyel volt csak képes üzemelni. Május 15-én az ország második legnagyobb bankja, a SEB Eesti Ühispank a támadások miatt kénytelen felfüggeszteni azokat a szolgáltatásait, amelyek a külföldről való banki rendszerekbe történő belépést biztosítják. Egy másik bank, a Hansabank nyilvánosságra hozott adatai szerint a támadások miatt elszenvedett vesztesége május 10-én több mint egymillió dollár volt.

Nyilvánvalóan a nemzetközi szervezeteknek is meg kellett szólalniuk az ügyben, hiszen ekkora kibertámadás még nem ért egy országot sem, főleg nem egy EU- és NATO-tagországot. Az Európai Parlament 2007. május 24-én állásfoglalást adott ki ez ügyben, a NATO pedig már május közepén szakértőket küldött Észtországba, hogy kivizsgálja a történteket, és segítsen a további támadások elhárításában. Ugyanakkor az óvatosság mind nemzeti, mind nemzetközi szinten megnyilvánult, mert sem az észt kormány, sem az EU, sem a NATO nem minősítette katonai támadásnak a történteket. Ráadásul a NATO nyilvánosan még abban sem foglalt állást, hogy kik voltak a támadók, és nem nevezték meg – egyértelmű bizonyítékok hiányában – Oroszországot mint támadót. A NATO hivatalosan csak azt jelentette be, hogy alaposan megvizsgálja, milyen hatásai lehetnek ezeknek az akcióknak.

Ugyanakkor ezt követően a NATO komoly lépéseket tett annak érdekében, hogy az ehhez hasonló kibertámadások teremtette helyzetet kezelje. 2008-ban a szövetség létrehozta egy kibervédelmi kiválósági központ alapjait Tallinnban. Az angol megnevezéssel *NATO Cooperative Cyber Defence Centre of Exellence (CCDCoE),* azaz *NATO Kibervédelmi Kiválósági Központ* egy olyan kutató- és koordináló szervezet, amely a kibertér jogi kérdéseitől kezdve a technikai védelem megvalósításáig ajánlásokat dolgoz ki a szövetség egészének és a tagálamoknak egyaránt. 2010 óta Magyarország is teljes jogú tagja a kiválósági központnak.

Mindezek mellett 2012 végére a NATO létrehozta a szövetség számítógép-vészhelyzeti eseménykezelő csoportját (Computer Emergency Response Team, CERT),[13] amely napi 24 órában, heti 7 nap végzi a NATO és a tagállamok katonai rendszereinek incidenskezelését. A NATO CERT sok ponton kapcsolódik a tagállamok ágazati vagy kormányzati CERT-jeihez.

A 2007-es észtországi DDoS-támadások világosan mutatják azokat a konzekvenciákat, amelyeket ebből és a hasonló kibertámadási módszerekből le kell vonnunk. Az összehangolt, masszív támadások, illetve azok indítéka közvetett bizonyítékként szolgál arra, hogy valószínűleg egy másik állam, nevezetesen Oroszország állt a támadások mögött. Bár néhány támadást sikerült egészen orosz szerverekig visszanyomozni,[14] sőt az Európai Parlament hivatalos állásfoglalásában is az szerepelt, hogy a támadások egy része az orosz közigazgatáshoz köthető IP-címekről érkezett, mégsem lehet egyértelműen kijelen-

---

13 A CERT szinonim fogalmaként gyakran használatos a *CSIRT,* azaz a *Computer Security Incident Response Team,* amely jelentésében és feladataiban is közel azonos: számítógép-vészhelyzeti reagáló csoportot jelent. Ugyanakkor a *CERT* kifejezés eredetileg a Carnegie Mellon University (USA) által bejegyzett védjeggyel ellátott név, amely az egyetemen 1988-ban indult CERT koordinációs központ (CERT Coordination Center) megnevezése. A CERT jelenleg is a Carnegie Mellon University szoftverfejlesztő intézetének (Software Engineering Institute) része. (CERT 2017)

14 A támadások megindulása után az egyik védelmi megoldás az Oroszország felől érkező IP-címek blokkolása volt, amely után töredékére esett vissza a túlterhelés sávszélessége, de ez csak egy ideig bizonyult hatásos védekezésnek.

teni, hogy orosz állami szándék és/vagy elkövetők álltak a támadások mögött. (Kovács 2014)

Mindenesetre az Észtország ellen végrehajtott túlterheléses támadássorozat is bizonyíték arra, hogy ma már messze más célokra is lehet használni a számítógép-hálózati támadásokat, így a DDoS-támadásokat is kiberbűncselekményekre. Az ezekkel az eszközökkel elkövetett támadások, valamint a mögöttük álló esetleges idegen állami szereplők óriási kockázatot jelentenek azon országokra, ahol fejlett kritikus információs infrastruktúrákra alapozott a társadalom működése. Különösen aggasztóvá teszi ezt az a tény – ahogy korábban többször utaltunk rá –, hogy ez gyakorlatilag a teljes fejlett nyugati világunk egészére igaz. Ennek megfelelően az informatikai eszközökkel elkövetett támadások nemzetbiztonsági kérdéssé is válnak.

2.1.3. APT és egyéb támadási formák

A fentiekben bemutatott támadási formák mindegyike valamilyen létező sérülékenységen keresztül éri el célját. Ezeknek a sérülékenységeknek a kihasználhatósága indukálja a rosszindulatú programok megjelenését, illetve rendszerint az azokkal elkövetett különböző támadási formákat. Természetesen léteznek olyan támadási formák, amelyeket a technika jelenlegi elégtelen volta szül (gondoljunk csak itt a hálózati rétegben elkövetett támadásokra), mégis nyugodtan kijelenthető, hogy a támadások jelentős része ma már az alkalmazási rétegben, és ott is elsősorban a felhasználókat megcélozva jelentkezik.

Ugyanakkor egyre gyakoribb a különböző támadási formák kombinációja. A védelmi megoldások fejlődésével a támadók is rákényszerülnek, hogy több, egymást támogató támadási módszert vessenek be, hogy kikerüljék a védelem különböző eszközeit és módszereit.

7. táblázat
Jellemző informatikai támadási módszerek

Megnevezés	Jellemzők
Sniffing	A hálózaton zajló információáramlás folyamatos nyomon követése, „hallgatózás, szimatolás”. Legális és nem legális formái is ismertek.
Spoofing	Alapvetően valaminek a meghamisítását jelenti. Leggyakoribb formája az IP-spoofing, amikor az IP-csomagokhoz tartozó IP-címet hamisítják. Más formái is lehetnek, például GPS-jelek hamisítása a GPS-vevők megtévesztésére.
Man-in-the-middle attack	Közbeékelődéses támadás. Két node közötti adatforgalmat a támadó úgy téríti el, hogy mindkét fél számára a másiknak adja ki magát. Ehhez szükséges a csatornákhoz való hozzáférés, az azon folyó adatforgalom lehallgatása, illetve annak megakadályozása, hogy az eredeti csomagok a címzetthez eljussanak.
IP fragmentation attack	A hálózati eszközök számára engedélyezett módszer az IP-csomagok kisebb méretűre történő feldarabolása. Ennek kihasználása, például hamis IP-csomagok bejuttatásával.
TCP Session Hijacking	A webszerverek a felhasználók TCP-kapcsolatainak azonosítására különböző megoldásokat használnak. Ezek a munkamenet-azonosítók, amelyeket a támadók „eltérítenek”, így jutva hozzá az adott kapcsolathoz a szerverrel vagy a felhasználóval. Módszerei a sniffing, a man-in-the-middle stb.
Information leakage	Az információ kiszivárgása, kikerülése vagy kinyerése egy zárt, akár titkosított rendszerből. Alapesetben nem szándékos, hanem tervezési vagy műszaki hiba miatt kerülnek ki szenzitív információk. Az ezzel a módszerrel elkövetett támadás a kiszivárgott adatokra épít.
Cross site scripting (XSS)	A támadók webalkalmazások esetén olyan kódot (HTML-kód vagy kliensoldali script) helyeznek el más felhasználók által is megtekintett weboldalakba, amelyek segítségével adatokat (például felhasználónév, jelszó) lopnak el.
SQL injection	Az SQL-adatbázis hibáit kihasználó támadás, amely során az adatbázis egyes lekérdezései segítségével lehetséges adatokhoz jogosulatlanul hozzáférni vagy az adatbázison keresztül a rendszerbe behatolni.

Forrás: a szerző szerkesztése

Ezek közül a támadási formák közül kiemelkedik a már többször említett Advanced Persistent Threat (APT). Az APT támadások együttesét jelenti, amelynek még nagyon jó és jól használható magyar megnevezése sincs. Magyarul talán a *nagyon fejlett támadás veszélye* megnevezés szolgálhat arra, hogy nevet adjunk ennek az egyébként összetett és sok támadási formát magába foglaló eljárásnak, de egyre gyakrabban *célzott támadásoknak* is hívják ezeket a magyar szakterminológiában.

Az egyik legjellemzőbb tényező az APT támadásokra, hogy ezek jelentős része nagyon sokáig felfedetlen, észrevétlen marad. A támadások másik jellemzője, hogy ezek nem véletlenszerű célpontokat támadnak, hanem tudatosan – jellemzően politikai, üzleti vagy ezek kombinációja mint motiváció által – választott rendszereket támadnak. A támadás önmagában nem egy egyszerű támadás, hanem támadások sorozata. Az APT harmadik jellemzője az, hogy ezek a támadások nagyon jól előkészítettek és nagyon sokáig fennállnak.

Az APT-k esetében tehát nem egyszerű szoftverrobotokról van szó, amelyek véletlenszerűen talált sérülékeny számítógépeket valamilyen malware segítségével megfertőznek, hanem nagyon tudatosan kiválasztott célpontokról, azok gyenge és sérülékeny pontjainak a kifinomult feltárásáról, majd ezeken keresztül a rendszerbe történő behatolásról, valamint az ott tárolt adatok észrevétlen ellopásáról beszélhetünk. Ez azt is jelenti, hogy emberi döntések sorozata szükséges az APT életciklusa egészének során,[15] hiszen az APT támadás mögött álló ember az, aki annak függvényében dönt a támadás folytatásáról, illetve az abban használt technikáról, hogy az adott rendszerben milyen

[15] Néhány forrás az APT-ket kritériumok alapján elkülöníthetőnek tartja más támadásoktól. Ilyen jellemzők: a célok; időbeniség, azaz mennyi ideig tart, illetve áll fenn a támadás; a támadások mögött lévő források és azok háttere; a kockázat elviselésének szintje; a támadók képességei és a támadások módszerei; a támadások kiindulópontjai; a támadásba bevont végpontok száma; a veszélyről szóló tudás megléte, azaz lehetséges-e például online információgyűjtéssel a veszélyről adatokkal rendelkezni. (Bodmer et al. 2012)

védelmi megoldásokkal találkozik, illetve hogy egyáltalán a rendszerben tárolt és kezelt adatokhoz milyen módon lehet hozzáférni.

Mindezeknek megfelelően kerültek a támadás megnevezésébe az *advanced* (fejlett), a *persistent* (perzisztens, azaz folyamatosan fennálló), valamint a *threat* (fenyegetés) szavak.

Az *advanced,* azaz a *fejlett* kifejezés egyrészt a támadók felkészültségére utal, másrészt arra a technikai eszközkészletre, amellyel a támadások kivitelezhetőek. Az APT támadás különböző – egymástól meglehetősen jól elkülöníthető – szakaszokból áll. Minden szakasz rendelkezik az arra a szakaszra jellemző támadási módszerrel vagy technikával. Mivel komplex rendszerek támadása és onnan adatok kinyerése a cél, a támadási módszerek skálája is igen széles: az egyszerű malware-ek alkalmazásától a social engineeringen át a telefonlehallgatásig, számos eszköz megtalálható egy-egy APT támadás során. Nyilvánvalóan ezek nem mindegyike érdemli ki a *fejlett* jelzőt, de az, ahogyan ezeket együtt alkalmazzák és kombinálják, már lehet igen fejlett támadás.

A *persistent,* azaz *folyamatosan fennálló* jelző arra utal a támadás megnevezésében, hogy a támadás egy konkrét célpont ellen irányul, egy-egy jól működő védelmi megoldás nem eredményezi a támadás befejezését, sokkal inkább újabb technika vagy támadási mód bevetését. Ez nyilvánvalóan valamilyen reakciót igényel a támadást koordinálók részéről. A *perzisztens* jelző szintén arra is rámutat, hogy ezek a támadások célzottak, és nem ad hoc módon kiválasztott célpontok ellen irányulnak. Másik megközelítésben a folyamatosság azt is sugallja, hogy a támadó annak függvényében folyamatosan változó eszközöket használ, ahogy a célpont védelme reagál az egyes támadási eszközökre. A cél: úgy fenntartani a hozzáférést a megtámadott célpont rendszeréhez, hogy az a lehető legtovább (vagy a megkívánt ideig) fennálljon.

A *threat,* azaz a *fenyegetés* jelző azt érzékelteti, hogy ezek a támadások mivel célzottak és nagyon is tudatosak, komoly fenyegetést (veszélyt) jelentenek a megtámadott rendszerre, ráadásul a fenyegetés azért is jelentős, mert a támadások mögött feltételezhetően olyan

erők állnak, amelyek erőforrásai (az erőforrások körébe beletartozik mind az anyagi, mind a technikai, mind a humán lehetőségek) nem limitáltak, céljaik pedig – legyen szó politikai vagy üzleti motivációról –, nemzetbiztonsági kockázatokat jelentenek. (Bodmer et al. 2012)

Mindezekből az is következik, hogy az APT támadások mögött – igaz sok esetben csak feltételezhetően – országok, azaz rendszerint idegen kormányok állnak a már említett erőforrásokkal. A célpontok nagyon vegyes képet mutatnak, hiszen a közigazgatás, a nemzetbiztonsági, a katonai, de a logisztikai vagy akár az egészségügyi rendszerek is szerepeltek már APT támadások áldozataiként, nem is beszélve kutatóintézetekről vagy egyetemekről. Ugyanakkor ahogy ezek a célpontok is vegyes képet mutatnak, ugyanúgy a támadások mögött lévő valódi célok is eltérőek, hiszen ezek jelenthetnek valóban adatokhoz való folyamatos hozzáférést és ezek a megtámadott rendszerből való kinyerését, de jelenthetik olyan rosszindulatú szoftverek elhelyezését is a célpontnál, amelyek aktiválása csak később történik meg.

Bár az APT támadások története meglehetősen homályos, egyes források az első publikált esetet 2005-re teszik, amelyben pont az a furcsa, hogy még nem is APT-nek hívták. Ebben az évben júniusban és júliusban az Egyesült Királyság Nemzeti Infrastrukturális Biztonsági Koordinációs Központja (United Kingdom National Infrastructure Co-ordination Center – UK NISCC) és az Amerikai Egyesült Államok CERT-je (US-CERT) technikai figyelmeztetéseket tett közzé olyan célzott social engineeringgel terjedő e-mailekre hívta fel a figyelmet, amelyek trójaiakat tartalmaztak, és amelyeknek alapvető célja az adatszerzés volt. Ezek a célzott e-mailekkel elkövetett támadások akkor már feltételezhetően régóta fennálltak, nagyon szofisztikált megoldásokat használtak, amelyek az akkori víruskeresőket és egyéb védelmi rendszereket megkerülve jutottak célba és szereztek adatokat. (US_CERT 2005; idézi: Hutchins–Cloppert–Amin 2011)

Magát az Advanced Persistent Threat kifejezést egyes források az amerikai légierő ezredeséhez, Greg Rattray-hez kötik, aki 2006-ban használta elsőként ezt a kifejezést. (Heise 2015)

Ahogy korábban utaltunk rá, az APT támadások száma ma már rendkívül nagy. Természetesen a felfedezett ilyen támadásokról van szó, és csak sejteni lehet, hogy a napvilágra került ilyen támadások nagyságrendjével megegyező, ha nem nagyobb számban vannak olyan APT támadások, amelyek egyelőre még rejtve vannak. A támadások célpontjai szintén széles skálán mozognak, hiszen gyakorlatilag a közigazgatáson és a védelmi szférán kívül is minden pénzügyi szervezet – legyen szó bankról, biztosítóról vagy akár tőzsdei cégről –, illetve minden olyan szervezet, amely a támadó számára fontos adatokat kkezel, ilyen támadás veszélyének van kitéve.

Az APT támadások életciklusa viszonylag jól feltérképezhető, bár, ahogy említettük, minden támadás más és más eszközöket használ, függően a megtámadott szervezet védelmi mechanizmusaitól. Sok esetben a támadások kivitelezéséhez olyan közvetett rendszereket használnak, amelyeket korábban kompromittáltak, és amelyeken keresztül a célba vett rendszerhez hozzáférés nyitható.

Az APT támadások életciklusa és eljárási módja *(modus operandi)* általában social engineering, illetve célzott phishing *(spear phishing)* támadásokkal kezdődik. Ezek egyrészt hozzáférést keresnek a célpont rendszereihez, másrészt például vírussal vagy nulladik napi sérülékenységeket kihasználó exploittal fertőzött e-mailekkel operálnak. A fertőzés másik népszerű módja, hogy a célba vett szervezet nagyon jól kiválasztott munkatársait olyan weboldalak meglátogatására veszik rá, amelyek rosszindulatú programokkal fertőzöttek.

47. ábra
Az APT életciklusa

Forrás: a szerző szerkesztése

Ezt követően a következő lépés egy vagy több olyan szoftver telepítése az áldozat rendszerében, illetve annak számítógépén, amelyek back-doorokat nyitnak. A backdoor segítségével a rendszerbe bejutott támadó igyekszik kiterjeszteni jogosultságait, azaz törekszik arra, hogy rendszergazdai jogosultságot szerezzen az áldozat számítógépén, illetve ha lehetséges, abban a hálózatban is, amelybe ez a gép tartozik.

Ezt követi az első körös, de már belső információszerzés. Ekkor a belső hálózat feltérképezése, a hierarchia, a kapcsolatok és rendszerben tárolt vagy kezelt adattípusokról szóló információk gyűjtése a cél.

Ezt egy vertikális hálózati felderítés követi, amely során a hálózat többi szegmensében keres a támadás információkat annak felépítéséről az abban tárolt vagy kezelt adatok milyenségével egyetemben.

A támadás itt nem ér véget, hanem igyekszik fenntartani a hozzáférést, illetve mindazokat a kommunikációs csatornákat, amelyeken

keresztül a vezérlés, illetve az adatok küldése megvalósul. Ez a jelenlét fenntartását jelenti.

Mindeközben a támadás a lehető legnagyobb rejtettséggel az áldozat rendszerében tárolt adatokat kijuttatja a hálózatból.

APT támadások: a legnagyobbak, amelyek megrázták a világot

Az APT támadásokra számos nyilvánosságra került példát találunk.

Az egyik ilyen példa a Stuxnet-féregvírus, amely Irán nukleáris programját, azon belül is az urándúsító centrifugákat vezérlő speciális számítógépeket támadta 2010-ben. Erről külön, részletesebben is szólunk a későbbiekben.

Ugyanakkor már jóval a Stuxnet előtt, az évtized elején, sőt a 90-es évek végén is kaphattunk híreket olyan támadásokról, amelyek az APT-kategóriába tartoztak, és amelyek fő célja a nagy mennyiségű – elsősorban állami szervezetektől történő – adatlopás volt.

Az első ilyen APT támadás, amely talán ki is érdemelhetné az évtized célzott támadásának címét, a *Moonlight Maze,* azaz a *Holdfény-labirintus* nevet kapta.

A Moonlight Maze támadásra utaló jeleket teljesen véletlenül fedezték fel 1999-ben. Maga a támadás valószínűleg 1998-ban indult, és célpontjai között olyan szervezetek voltak, mint az Egyesült Államok különböző kormányzati szervei: az Energiaügyi Minisztérium, a Pentagon, az USA légierő egyes bázisai, a NASA és egyéb, a különböző katonai kutatásokba bevont egyetemek és kutatólaborok. A támadásra, amely – ahogy arra korábban utaltunk – valójában egy egész támadássorozat, még 2003-ban is találtak jeleket.

Csak feltételezni, lehetett, hogy kik voltak a támadók, de nagy valószínűséggel a volt Szovjetunió valamely tagállamából érkeztek a támadások. Talán nem vagyunk messze az igazságtól, ha feltételezzük, hogy ezen belül is valójában Oroszország állhatott a támadás mögött. (Guerrero-Saade et al. 2017)

A támadók kilétéhez hasonlóan az ellopott adatok mennyiségét és azok mibenlétét is csak sejteni lehet, de nagy valószínűséggel az amerikai kormányzati szervektől katonai létesítmények térképeit, katonai alakulatok szervezeti felépítéseit, különböző doktrínákat és belső szabályzatokat, valamint katonai eszközök részletes adatait és azok tervrajzait lopták el.

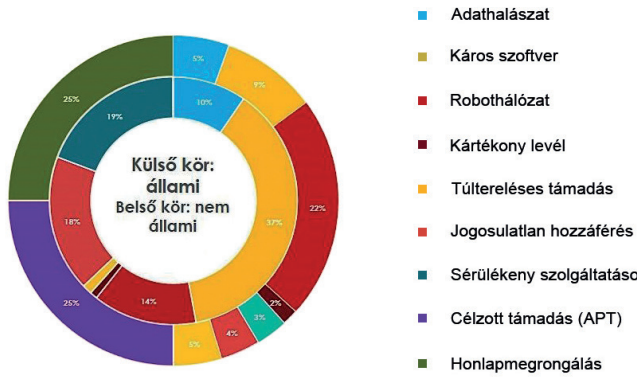
A „Holdfény árnya" azonban még a következő évtizedekre is, így a 21. századra is rávetül. A Kaspersky Lab és a Kings College London 2017-ben is talált olyan backdoorprogramot, ráadásul egy, az Egyesült Királyságban lévő proxyszerveren, amelyet a Moonlight Maze támadás során alkalmaztak a 90-es évek végén. A Kaspersky elemzései azt mutatták, hogy a felfedezett nyílt forráskódú backdoorprogramot 2011-ben és feltételezhetően 2017-ben is használták különböző támadásokhoz. (Guerrero-Saade et al. 2017)

A Moonlight Maze-t követően a legnagyobb vihart kavart APT támadásra 2003-ban derült fény. Ez a támadás a *Titan Rain,* azaz a *Titáneső* nevet kapta.

A feltételezhetően 2000-ben kezdődött támadást csak 2003-ban fedezték fel szintén egy véletlennek köszönhetően. A támadás célpontjai között a NASA mellett egyértelműen olyan hadiipari nagyvállalatok voltak, mint például az amerikai légierő számára harci repülőgépeket fejlesztő Lockheed Martin vagy a Redstone Arsenal, amely vállalat az egyik legfontosabb amerikai rakétavédelmi rendszert gyártja.

A támadók kiléte ebben az esetben is csak feltételezhető. Nagyon sok elemző annak a véleményének adott hangot, hogy a támadások mögött közvetett módon vagy akár közvetlenül is Kína állhatott. E vélemények alapvetően azon alapultak, hogy abban az időben (is) Kína volt az egyike azoknak a hatalmaknak, amelyek a legnagyobb érdeklődést mutatták az USA haditechnikája iránt.

Természetesen hazánk sem mentes az APT támadásoktól. Bár túl sok nyilvános adatot nem találunk, néhány publikált tény azt mutatja, hogy rendszeresek az ilyen támadások a hazai szervezetekkel szemben.



48. ábra
A magyarországi állami és nem állami szervezeteket ért támadások 2015 harmadik negyedévében

Forrás: Bencsik 2015

Az APT-n túl: kiberkémkedés nagyüzemben

Bár a korábban bemutatott APT támadások jelentős része alapvetően az adatszerzést szolgálja, azaz nyugodtan leszögezhetjük, hogy nagy általánosságban az esetek túlnyomó többségében ezeknek a támadásoknak a fő célja nem az áldozat rendszereinek megbénítása, hanem onnan a támadó (vagy a megbízója) számára fontos és használható információk eltulajdonítása, ellopása. Ugyanakkor mégis fontos külön is foglalkozni néhány gondolat erejéig a kiberkémkedéssel.

Az angol terminológiában *cyber espionage*-nak nevezett tevékenység az APT-k egyik fő célja, de természetesen más eszközökkel és módszerekkel is végezhető a kémkedés a kibertérben, mint a korábban bemutatott célzott támadások. Az azonban elvitathatatlan tény, hogy amennyiben az APT támadások mögött álló – alapvetően államilag támogatott – elkövetőkkel kombináljuk a kémkedést, és ezt tekintjük a támadások fő motivációjának, akkor eljuthatunk addig

a megközelítésig, hogy államilag támogatott kiberkémkedéssel állunk szemben nagyon sok APT támadás esetében is.

Ugyanakkor a kiberkémkedés megítélése rendkívül vegyes. A megítélés sok esetben attól függ, hogy mi a célja vagy a feltételezhető célja a kémkedésnek. Sok ország – mint például az USA – egyértelműen elítéli a kiberkémkedést, míg Kína és Oroszország, bár nyilvánosan tagadja és szintén elítéli az ilyenfajta tevékenységet, mégis naponta vannak hírek, hogy ezen országok állami támogatása fedezhető fel egy-egy kipattant kémkedési botrány mögött. Ahogy Martin Libicki fogalmaz egyik, a kiberkémkedés nemzetközi jogi hátterét elemző cikkében: „a kibertér normái érdekében való küzdelem nemcsak a közeg újdonságát tükrözi, hanem a geostratégiai realitásokat is, amelyekben az Egyesült Államok és a hasonló gondolkodású szövetségesei küzdenek egy olyan egyre növekvő nagyhatalommal (Kínával), amely a nemzeti előnyeit nemzetközi környezetben igyekszik maximalizálni, egy hanyatló nagyhatalommal (Oroszország), amelynek vezetői egyre inkább a nyugatellenességükkel igyekszenek meghatározni legitimációjukat, és számos külön utas országgal (Irán és Észak-Korea).” (Libicki 2017)

Kínával kapcsolatos elhíresült kémkedési ügyről (Titan Rain) már tettünk említést. Ugyanakkor 2013-ban a *Mandiant*[16] nevű kiberbiztonsági cég[17] egy több mint 75 oldalas jelentésben foglalta össze a Kínával és a kiberkémkedéssel kapcsolatos tapasztalatait, illetve vizsgálati eredményeit.

---

16 A Mandiant (Mandiant Consulting) jelenleg a FireEye (USA) információbiztonsági céghez tartozó, alapvetően kiberbiztonsági elemzésekkel foglalkozó, több mint 10 éves működésre visszatekintő vállalat. (FireEye 2017)

17 A cég a biztonság másik oldalával kapcsolatosan is bekerült a hírekbe, amikor egyik munkatársuk 2017 nyarán kiberáldozattá vált. Számítógépét ugyanis feltörték, majd a támadók több 100 Mbyte szakmai és személyes adatát hozták nyilvánosságra, mindamellett, hogy LinkedIn-profilját is kompromittálták. Persze a FireEye cáfolta, hogy a céges rendszereket érintette volna az eset. (Reuters 2017; idézi: Nemzeti Kibervédelmi Intézet 2017)

Már a jelentés címe is magáért beszél: *APT1, Exposing One of China's Cyber Espionage Units,* azaz magyarul *APT1, Kína egyik kibertérben működő kémszervezetének bemutatása*. A jelentés címében szereplő *APT* nem véletlen, hiszen ez a kínaiak által mesteri szintre fejlesztett célzott támadásokra utal. A Mandiant több száz céget, valamint az ezek ellen elkövetett APT támadásokat vizsgálta meg és elemezte.

A jelentés kiemeli, hogy 2006 és 2013 között közel 200 APT támadásra szakosodott csoportot azonosítottak, amelyek közül 20 Kínához köthető. Ezek közül az egyiket jelölték APT1-gyel, amelyre a jelentés címében is utaltak. A jelentés kitér arra is, hogy bár az APT1 tevékenységének csak egy kis hányadát voltak képesek feltérképezni, mégis sikerült a csoport közel 150 áldozatát felderíteni. Ez az elemző munka a jelentésben foglaltak szerint közel 7 évig tartott.

Az elemzés során az APT1-et négy sanghaji nagy hálózathoz vezették vissza, amelyek közül kettőt közvetlenül a *Pudong Új Területnek*[18] hívott helyhez tartozónak azonosítottak. Más elemzések is rámutattak, hogy az APT támadásokhoz használt infrastruktúrák, a támadások parancsainak és vezérlésének, illetve a támadások általános eljárási módjának azonosításával jól elkülöníthetők a támadások, valamint a mögöttük álló támadók.

A Mandiant az elvégzett elemzésekből azt a következtetést vonta le, hogy az APT1 valószínűleg a hivatalos kínai kormány által szponzorált csoport. Ezt támasztja alá az is, hogy ez a csoport hosszú távú és igen kiterjedt kiberkémkedést volt képes folytatni. Mindezeken túl a vizsgálatok és az elemzések során a cég azt is kijelentette, hogy az APT1 mögött a Kínai Népi Felszabadító Hadsereg (PLA – People's Liberation Army) Vezérkarának 2. Csoportfőnöksége alatt működő *61398* nevet viselő egysége áll.

---

[18] Pudong New Territory (Pudong Új Terület): Sanghaj 19 km²-es kerülete, amely főleg export- és kereskedelmi tevékenységekre szakosodott cégeknek ad otthont. (GE 1999)

Ez nagyon súlyos és komoly állítás. Ugyanakkor a megállapítást két további tényező is alátámasztja: közvetett bizonyíték lehet, hogy a két szervezet, azaz az APT1 és a 61398-egység Sanghaj ugyanazon negyedében, ugyanabban az utcában, sőt ugyanabban az épületben található. Mindezek mellett közvetett bizonyíték lehet, hogy a két szervezet nagyon hasonló feladatokat lát el, illetve a csapatok képességei és erőforrásai pedig szintén kísértetiesen hasonlítanak egymásra. (Mandiant é. n.)

A vizsgálat az APT1-hez köthető támadásokkal kapcsolatban számos egyéb fontos megállapítást is tett. Az APT1 szisztematikusan több száz terabájt adatot lopott el legalább 141 szervezettől, amelyek 20 különböző iparág képviselői voltak. Az APT1-csoport demonstrálta azt a képességét is, hogy egyidejűleg több tucat szervezettől is képes adatokat lopni. Az APT1-csoport áldozatainak közel 90%-a angolszász nyelvterületen működő cég volt. Megállapították, hogy az APT1 egy nagyon jól definiált támadási módszertannal rendelkezett, amely más APT-csoportokra nem, vagy csak részben volt jellemző. Ezzel a módszertannal évek alatt nagy mennyiségű értékes adatot, szellemi terméket, folyamatleírásokat, teszteredményeket, üzleti terveket, e-mail-címlistákat, valamint névjegyzékeket loptak el. A támadás módszertanához hozzátartozott, hogy miután az APT1 hozzáférést biztosított a megtámadott és kompromittált rendszerhez, ezt a hozzáférést több hónapon át, egyes esetekben több évig is fenntartották. A támadások elemzése során fény derül arra is, hogy ezeket a hozzáféréseket az APT1 átlagosan 356 napig tartotta fenn, de volt olyan áldozat, akinek a rendszere esetén több mint 4 évig megvolt a támadók hálózati hozzáférése. Olyan esetet is bemutat a jelentés, amikor egyetlen áldozattól 6,5 terabájtnyi szellemi tulajdont loptak el.

A jelentés összességében azt a konzekvenciát vonta le, hogy az APT1 fő célja, bár – ahogy láthattuk – a csoport alapvetően a hadsereghez köthető, a szellemi tulajdon ellopása volt különböző cégektől és szervezetektől. (Mandiant é. n.)

Teljesen más motivációval rendelkezik viszont az APT28 néven elhíresült másik, de szintén célzott támadásokra szakosodott csoport. Az APT28, vagy még ismertebb nevén Fancy Bear, alapvetően Oroszországhoz köthető. Legalábbis ezt állítják különböző jelentések. Az első olyan jelentés, amely az APT28 tevékenységét, akcióit és céljait behatóan vizsgálta, 2014-ben látott napvilágot. (Fireeye 2014)

A jelentést kiadó FireEye információbiztonsági vállalat, amely a Mandianon keresztül közvetve a kínai APT1-ről szóló vizsgálatot is jegyezte, már ekkor megnevezte a szervezet mögött álló Oroszországot. Sőt a jelentés kiadásának célját is pont ezzel indokolták: „Akárcsak az APT1-ről szóló jelentésében, itt is fel kellett ismernünk, hogy egyetlen entitás sem érti meg teljesen a kiberkémkedés teljes és összetett képét sok év alatt sem. Ezért célunk ezen jelentés közreadásával, hogy értékelést nyújtsunk, tájékoztassuk és felhívjuk a közösség figyelmét az Oroszországból származó támadásokra." (Fireeye 2014)

Oroszországot mint az APT28 mögötti állami támogatót az Egyesült Államok hivatalosan is nevesítette a 2016-os amerikai elnökválasztással kapcsolatos kibertámadások nyomozása után.[19] (US DHS–FBI 2016)

A FireEye 2014-es jelentésének címe önmagában is nagyon beszédes: *APT28: A Window into Russia's Cyber Espionage Operations?,* azaz *APT28: egy ablak Oroszország kiberkémkedési műveleteire?,* amely arra is utalás, hogy a csoport tevékenysége révén betekintést kaphatunk abba a valóságba, amely az orosz politikát a kibertérben valójában jellemzi, motiválja és mozgatja. (Fireeye 2014)

A cég által végzett vizsgálatok összegzett megállapításait, azaz azokat a tényezőket, amelyek az orosz hivatalos kormány támogatására utalnak, külön is kiemelték a jelentésben.

[19] Erre tettünk utalást a kibertér és a politika összefüggéseit bemutató fejezetünkben.

8. táblázat
Az APT28 által megtévesztésre használt imitált domének

APT 28 domén	Valódi domén
standartnevvs[.]com	A bolgár Standard News weblapja (standard-news.com)
novinitie[.]com, n0vinite[.]com	A bolgár Sofia News Agency weblapja (novinite.com)
qov[.]hu[.]com	A magyar kormányzati domén (gov.hu)
q0v[.]pl, mail[.]q0v[.]pl	A lengyel kormányzati domén (gov.pl) és a mailszerver-domain (mail.gov.hu)
poczta.mon[.]q0v[.]pl	Lengyel Védelmi Minisztérium mailszerver-domén (poczta.mon.gov.pl)

Forrás: FireEye 2014, a szerző szerkesztése

Az APT28 céljai és még inkább célterületei geopolitikai alapon nagyon jól behatárolhatók voltak. Ezek három nagy csoportra oszthatók fel: a Kaukázus, ezen belül is kiemelten Grúzia; Kelet-Európa, ezen belül is a kelet-európai kormányzatok, kormányzati szervezetek és hadseregek, valamint az olyan biztonsági vagy katonai szervezetek, mint a NATO vagy az EBESZ. Ez nem jelenti azt, hogy a csoport más területeken ne fejtett volna ki aktivitást, hiszen – ahogy láttuk – 2016-ban a csoporttól nem volt idegen az Egyesült Államokban való tevékenység, de a FireEye jelentése is megjegyzi, hogy olyan helyeken is találtak a csoport támadásaira jellemző mintákat, mint például Norvégia, Irak vagy éppen Jordánia.

Az APT28 tevékenységét a FireEye 2007 és 2013 között vizsgálta, és többek között sikerült a csoport által alkalmazott módszereket is felderíteni.

Az APT28 egyik fő és bevált támadási módszere a célzott phishinggel kezdődött, amelyek során az áldozatoknak olyan e-mail-üzeneteket továbbítottak, amelyek a címzettek számára releváns témákról szóltak. Ezzel növelték annak az esélyét, hogy a célpontok az ezekben az elektronikus levelekben lévő linkekre rákattintsanak, illetve a levelek csatolmányait megnyissák. Ezt ötvözték azzal a módszer-

rel, amelynek során hamis, de az eredetihez nagyon hasonló doménnevet regisztráltak. Ezeket a doménneveket használták az említett e-mailekben, ami tovább növelte az esélyét annak, hogy az áldozat ne fogjon gyanút, és közvetlenül az e-mailből megnyissa a linken található weboldalt. Ilyen domén volt többek között a magyar kormányzati doménra – a gov.hu-ra – hasonlító quv.hu.info domén is. (FireEye 2014)

A támadások kiindulópontjaként használt célzott phishingtámadásokkal olyan exploitokat futtattak az áldozatgépen, amelyek droppereket, majd ezek segítségével különböző malware-eket – mint például a Sourface, amely egy downloader (azaz letöltő program); vagy az Eviltoss, amely egy backdoor – juttattak a rendszerbe. Ezt követte a második fázis, amikor már a C2 szerverrel biztosított volt a kapcsolat, és amely során szintén dropperek segítségével moduláris felépítésű beépülő malware-eket (például a Chopstickot) helyeztek el az áldozatnál.

A malware-eket megvizsgálva, a jelentés kiemeli, hogy azok nagyon sok jellemzője egyértelműen az APT28-ra utal. A csoport a használt rosszindulatú programokat folyamatosan fejlesztette és javította azokat. Az is nyilvánvalóan látszott, hogy ezeket az eszközöket hosszú távú alkalmazásra szánták, mindamellett hogy a fejlesztések és folyamatos javítások komoly anyagi támogatásról is tanúskodnak. Ezek szintén kormányszintű támogatást sejtetnek a háttérben. (FireEye 2014)

Összességében megállapítható, hogy az APT28 tevékenysége alapvetően politikai motivációjú, és nagy valószínűséggel az orosz kormány által támogatott és/vagy megrendelt akciókat hajtott végre. A támadások célja – eltérően a kínai APT1-től – nem a szellemi tulajdon ellopása, hanem politikai döntéstámogató információk megszerzése, illetve sok esetben politikai befolyásolás volt.

Túl az APT-n: lehet-e fegyverként használni egy malware-t?

A kibertér veszélyeinek bemutatásából természetesen nem maradhat ki a Stuxnet sem. Ha nem is ez volt az első olyan rosszindulatú program,

amely ipari létesítményeket támadott, de minden bizonnyal ez váltotta ki a legnagyobb nemzetközi visszhangot.

2010 őszén a nemzetközi média egy olyan rosszindulatú program gyors terjedéséről számolt be, amely – mint később kiderült – felépítésében és működésében nagyon újszerű megoldásokat alkalmazott, nem is beszélve az általa megtámadott ipari létesítményekről, amelyek nem voltak mások, mint az iráni atomprogram legfontosabb elemei: az urándúsító centrifugák. A malware, amely egy féreg és egy vírus közös jellemzőit is tartalmazta, a *Stuxnet* nevet kapta.

Ahogy korábban utaltunk rá, a rosszindulatú programok több évtizedes múltra tekintenek vissza, de a Stuxnet volt az első olyan szoftver, amelynek alapvető célja már annak készítésekor is az volt, hogy ipari létesítmények vezérlőszoftverei működését támadja.

A Stuxnet számos országban fertőzött meg számítógépeket, de a legtöbb megfertőzött gép Iránban volt. Ebből a szakértők azt a nyilvánvaló következtetést vonták le, hogy a malware célpontja az iráni atomlétesítmények lehettek. A Stuxnet későbbi elemzése közvetett bizonyítékokat szolgáltatott mindehhez, mert számos biztonsági cég arra a következtetésre jutott, hogy a Stuxnet valóban olyan ipari vezérlőszoftverek ellen készülhetett, amelyeket Irán is alkalmazott többek között a busehri atomerőműben vagy a natanzi centrifugáinál. Ezek az ipari vezérlőeszközök nem voltak mások, mint a Siemens által gyártott PLC-k (Programmable Logic Controller). (Kovács–Sipos 2010)

Az információbiztonsággal kapcsolatos elemzések mellett azonban nagyon gyorsan megjelentek a biztonságpolitikai vélemények is. Ráadásul ezek közül nagyon sok pont az informatikai elemzések eredményét használta fel a különböző teóriáinak alátámasztására, hiszen például Bruce Schneier, az információbiztonság egyik legnagyobb szakértője is annak a véleményének adott hangot, miszerint a Stuxnet létrehozása óriási mennyiségű pénzbe és időbe került, nem is beszélve arról, hogy a malware tesztelése csak egy olyan nagyon jól felépített laborban történhetett, amely a célpont (például iráni urándúsító üzemek) infrastruktúráját hatékonyan volt képes szimulálni.

Mindezeken túl a Stuxnet legalább négy zero-day exploitot alkalmazott, ami szintén felveti a pénz és a magas szintű szakértelem kérdését. (Schneier 2010)

Ezek a tények pedig arra utalnak, hogy a Stuxnet-támadás mögött feltételezhetően olyan állam vagy államok állhatnak, amelyeknek politikai célja volt a támadásokkal, illetve annak következményeivel. Ezeknek az államoknak a program létrehozására és a támadás kivitelezésére az említett anyagi és humán háttér biztosítása nem jelentett különösebb gondot.

Ugyanakkor az, hogy ki állt a Stuxnet és a vele elkövetett támadások mögött, csak közvetett bizonyítékok sokaságából következtethető ki. 2011 januárjában a New York Times-ban megjelent egyik cikk utal rá, hogy a Stuxnet mögött Izrael állhatott. A cikk kitér arra – ahogy azt Schneier is felvetette –, hogy a malware-t olyan ipari létesítményben kellett tesztelni, mint a későbbi célpontok. Ilyen létesítménnyel pedig csak az izraeli nukleáris kutatás rendelkezik a régióban, a Negev-sivatagban található Dimona komplexummal. Ez a komplexum jó tesztinfrastruktúra lehetett a Stuxnet hatásainak kipróbálásához. A cikk megemlíti azt is, hogy Hillary Clinton és a Moszad exvezetője, Meir Dagan egymástól függetlenül, de közel azonos időben adtak azon véleményüknek hangot, miszerint remélik, hogy a Stuxnet által okozott károk az iráni atomprogramot akár több évvel is visszavetik. Ebből persze azt a következtetést is levonhatjuk, hogy az USA szintén támogathatta a Stuxnet megalkotását és felhasználását. (Broad–Markoff–Sanger 2011)

A Stuxnet rávilágít arra a tényre, hogy ma egy-egy malware vagy akár a korábban bemutatott APT támadások esetében már jóval többről beszélhetünk, mint „egyszerű" kibertámadás, amelynek esetlegesen semmilyen más célja nincs, csak az anyagi haszonszerzés. A Stuxnet-esetből is levonhatjuk azt a következtetést, hogy az államilag támogatott kibertámadásokkal egy új, sokkal veszélyesebb és sokkal beláthatatlanabb korszak köszöntött be a kibertérben, mint azt korábban feltételeztük.

A Stuxnet ipari létesítményeket támadott, míg az APT támadások esetében láthattuk, hogy azok elsődleges célja az állami szervezetek, illetve azok adatainak megszerzése.

Mindkét esetben állami támogatású elkövetőkről, illetve támadókról beszélhetünk. Ezeknek a tényezőknek az összekapcsolása egy nagyon sötét jövőt vázol fel elénk. Amennyiben egy ország rendelkezik a szigorúan őrzött ipari létesítményekbe való behatolás képességével, valamint képes a jóval kevésbé védett és így jóval sebezhetőbb közigazgatás-rendszerekből úgy adatokat is ellopni, hogy azt akár évekig nem veszik észre, akkor ezek a képességek mint fegyver – sőt mi több új fogalomként *kiberfegyverként* – lesznek alkalmazhatóak egy jövőbeni konfliktusban. (Kovács 2014)

Az emberi tényező: Social Engineering

A technikai és technológiai támadások mellett mindenképpen szólni kell a social engineeringről mint támadási formáról.

Magyarul nagyon nehéz egy szóval visszaadni ennek a támadási formának a megnevezését. Sokan szociohekkerkedésnek vagy humán hekkelésnek, mások pszichológiai befolyásolásnak vagy emberi manipulációnak hívják. Egyik sem a legjobb, sem a legkifejezőbb meghatározás a tevékenység pontos leírására.

A social engineering ember-ember közötti interakciót jelent. Ez a támadás[20] az emberi természetet használja ki, hiszen e tevékenység mesteri módon épít a hiszékenységre, a konfliktuskerülésre vagy éppen az emberek ösztönös segítőkészségére. A probléma csak az, hogy mindezt ártó szándékkal teszi. A támadó a social engineering-

[20] Nem teljesen helyes a social engineeringgel kapcsolatban csak a *támadás* kifejezést használni, mert léteznek olyan auditok, amelyek során – a jogszabályi, etikai, szerződésben stb. rögzített elveket és tevékenységeket betartva – a social engineering az egyik leghatásosabb módszer arra, hogy a munkatársak (információ)biztonsági tudatosságát felmérjük.

gel olyan információkat keres a hálózatról vagy a rendszerről, amelyek nem, vagy csak nagy energiabefektetéssel lennének megszerezhetőek más eszközökkel.

Minden social engineering támadás információgyűjtéssel[21] kezdődik, majd ezt követik a támadás kivitelezésének különböző formái. Számos és változatos social engineering technika létezik: félrevezetés, csalás, zsarolás, fenyegetés, amelyek akár mindegyike is alkalmazható egy megszemélyesítéses támadás során. Ekkor a támadó magát egy belső, azaz a szervezethez tartozó munkatársnak, a célszemély ismerősének vagy akár egy külső ismert szerződő cég dolgozójának kiadva próbál adatokat szerezni. Nyilvánvalóan ezek mindegyikének különböző kombinációja is elképzelhető, vagy akár a korábban említett célzott phishing (spearphishing) is működik a social engineering során.

Egy másik technika a *baitingnek* (magyarul szintén nagyon nehezen és csak felületesen lehetne a fogalom mögötti tartalmat egyetlen szóval visszaadni, de talán az eredeti angol szó magyar jelentése, a *csali* állhat a legközelebb a fogalomhoz) nevezett tevékenység, amely napjaink egyik slágerének tekinthető a social engineering technikákközül. A Norton antivíruscég nagyon találóan fogalmazta meg a baiting mögötti tartalmat: „Az emberek kíváncsi lények. Ez a lényeges ebben a forgatókönyvben. Az elkövető egy olyan eszközt hagy nyilvános helyen, mint például egy USB-háttértár, amely rosszindulatú programokkal fertőzött. Valaki felveszi ezt az eszközt, és bedugja a számítógépébe, hogy lássa, mi van rajta, majd a rosszindulatú szoftver minden gond nélkül telepíti magát a számítógépre.” (Norton 2017)

---

[21] Természetesen egy-egy social engineering nem feltétlenül jelent igazi, rosszindulatú támadást a szervezettel szemben. Ahogy korábban utaltunk rá, az adott szervezet biztonságának vagy az ott dolgozók biztonságtudatosságának vizsgálata gyakran social engineeringet is magában foglaló átvilágítással történik. Ez lehet etikus hekkelés *(ecthical hacking),* amikor a vizsgálatot folytató cég szerződést köt a vizsgálandó szervezettel, amelyben pontosan rögzítik, milyen kiinduló adatokkal, milyen feltételekkel, milyen mélységig lehet és kell az adott szervezetet vizsgálni. Abban az esetben, ha a vizsgálatot végző cég semmilyen kiinduló adatot nem kap, beszélhetünk *black box,* részleges információk esetén *grey box* vagy teljes információ birtokában *white box* típusú vizsgálatról.

Ugyanakkor ez nem feltétlenül csak egy utcán, hanem például nem megfelelően ellenőrzött körülmények miatt egy konferencián is megtörténhet, ahol az elhangzott előadásokat USB-eszközön (memóriakulcs, egér stb.) kapják meg a résztvevők. Ugyanaz a technika és módszer, csak egy kicsit még szofisztikáltabb a megoldás.

A social engineering jelentette kiberbiztonsági kihívást nehéz lenne túlbecsülni. Ennek okai komplexek, de elsősorban abból a tényezőből fakadnak, hogy bármilyen erős is egy rendszer vagy szervezet technikai értelemben megvalósított informatikai védelme, az emberi tényező sok esetben a leggyengébb láncszemnek bizonyul. Nincs ez másként akkor sem, ha látszólag oktatással, képzéssel és tréninggel igyekszik az adott szervezet ezt kiküszöbölni. A probléma megoldásában nyilvánvalóan ezek nem elhanyagolható tényezők, de mint az információbiztonság megannyi területén, itt is elmondható: megbízható megoldást és megnyugtató védelmet csak komplex módon lehet elérni. Amennyiben csak az emberi tényezőre fokuszálunk, és más területeket nem a megfelelő módon és hangsúllyal kezelünk, akkor pont ez a komplexitás fog sérülni. Felborul az az egyensúly, amelynek egyébként is egy dinamikusan változó környezethez kell vagy kellene minden időpillanatban alkalmazkodnia. Ugyanakkor a problémát másik szemszögből megvizsgálva azt láthatjuk, hogy az emberi tényező figyelmen kívül hagyása például a fizikai biztonság megteremtése során szintén oda vezet, hogy azokat a rendszabályokat még elemi szinten sem fogják betartani vagy végrehajtani a munkatársak, amelyek a számukra kényelmetlenek vagy az elviselhetőnél több energiát, illetve időt jelentenek.

A social engineering egyik leghíresebb, illetve sokáig leghírhedtebb alakja Kevin Mitnick volt. Az 1963-ban Los Angelesben született hacker már fiatalkorában nagy tehetséget mutatott a telefontársaságok becsapásában – például a telefontársaságok szervizvonalainak segítségével ingyen körbetelefonálta a világot – és számítógépes rendszerekbe való betörésben, hiszen több mint 40 nagy hálózatba – köztük az IBM és a NASA rendszeribe – tört be, csak a szórakozás kedvéért, vagy

hogy ezen rendszerek sérülékenységeit bizonyítsa. Könyvei, amelyek közül több magyarul is megjelent, szakmai körökben igazi bestsellerekké váltak. Ezekből kiderül, hogy az egyik leghatékonyabb technika, amivel Mitnick fiatalkori hackertevékenysége során élt, az emberek becsapása, azaz a social engineering volt. Sokszor éppen ezért Minicket nevezik a fogalom megalkotójának is. Később Mitnicket saját információbiztonsági céget alapított *Mitnick Security Consulting* néven. (Mitnick 2012)

Mindegyik social engineering támadási mód és támadási forma rendkívül lenyűgöző annak tudatában, hogy ezek sikeressége nagyon magas, és főleg akkor, ha azt olyan professzionalista módon végzik, mint ahogy tette azt Mitnick a 90-es években.

2.2. Támadók, avagy a kibertér (egyéni és csoportos) szereplői

A kiberbiztonság veszélyei nemcsak technikai, hanem – ahogy korábban láthattuk – humán oldalról is jelentkeznek. Ezt a humán oldalt mint a támadások elkövetőit és ötletgazdáit szintén érdemes részletesen megvizsgálnunk.

A következőkben ezeket az elkövetőket, vagy a sokszor használatos kifejezéssel élve a kiberfenyegetések forrásait csoportokba igyekszünk rendezni, és tevékenységüket, valamint a támadások mögött lévő motivációikat nagyon röviden bemutatni. Nyilvánvalóan ez a bemutatás sem lehet teljes. Ennek oka az, hogy már a legismertebb fogalom is, amit ezen a területen használni szoktunk, azaz a hacker is önmagában számos ellentmondást hordoz. A korábban említett Kevin Mitnick talán az egyik legjobb példa arra, hogy a *hacker* kifejezés azért is ellentmondásos, mert önmagában ez az egy szó nem mutatja be és nem jellemzi teljesen jól az elkövetőt. A hacker, bár minden bizonnyal magas szintű informatikai ismeretekkel rendelkezik, és képes hálózatokba, rendszerekbe, számítógépekbe behatolni, akár kettős motivációval is

rendelkezhet: kárt akar okozni, de akár a jó ügy érdekében is elkövet kibertámadásokat.

Az első említett motiváció, azaz a károkozás nyilvánvalóan nem igényel különösebb magyarázatot, hiszen ebben az esetben a hacker általában közvetlen anyagi megfontolásból tör fel rendszereket. A másodikként említett motivációs tényező esetében, azaz a jó ügy érdekében történő támadás azonban már kisebb magyarázatot igényel, hiszen hogyan lehet úgy támadni, hogy annak pozitív eredménye lesz minden fél számára? A magyarázat abban rejlik, hogy az ezzel a szándékkal történő támadások mögött általában a rendszerek sérülékenységeire való figyelemfelhívás, illetve azok bizonyítása áll. Természetesen ez azzal is együtt jár, hogy ilyen esetekben a támadó a tapasztalatait, azaz a rendszer sérülékenységeit, illetve az azokat kihasználni képes technikai vagy humán támadási módszereket átadja a rendszert üzemeltetőnek. A cél itt egyértelműen jó és pozitív, hiszen a támadó nem okoz kárt, sőt a rendszer védelmét szolgálja, ha a feltárt hiányosságokat az üzemeltető megszünteti. Persze sokszor itt kezdődik az igazi probléma, hiszen számos esetben tapasztalható, hogy az üzemeltető nem akarja, vagy nem tudja ezeket megszüntetni, vagy csak egyszerűen nem foglalkozik az egyébként nem ismert, de akár valós sérülékenységeket feltáró támadó bejelentéseivel. Sok esetben ilyenkor a támadó többször is igyekszik a rendszer üzemeltetőjének figyelmét felhívni a problémára. Abban az esetben, ha ezeket – az egyébként jó szándékú – bejelentéseket az üzemeltető nem veszi figyelembe, akkor a támadó sokszor valódi kárt fog okozni. És itt vissza is jutottunk a hacker fogalomban lévő komplexitáshoz: jó és rossz egyszerre, vagy csak a szándék és a motiváció az, amely a kettő között valamilyen különbséget tesz.

49. ábra
A leggyakoribb támadások kiindulópontjai a támadók csoportosítása alapján

Forrás: a szerző szerkesztése

Korábban éppen ezért a hackerek esetében külön fogalmat alkottak azok, akik azért törtek fel rendszereket[22] vagy weboldalakat, hogy bizonyítsák azok sérülékenységeit. A pozitív hozzáállásuk és motivációjuk miatt őket *fehérkalaposoknak* vagy *white hateknek* hívták. A negatív motivációval, azaz alapvetően ártó szándékkal bíró hackereket viszont *fekete kalaposoknak* vagy *black hateknek* nevezték. Ők már a kezdetek kezdetén[23] kriminalizálták magukat azzal, hogy alapvetően anyagi haszonszerzés reményében vagy csak egyszerűen rosszindulatból (például bosszúból) hatoltak be egy-egy rendszerbe. Napjainkra – főleg a média hatására, amely naponta jelenít meg híreket

[22] Ebbe beletartozott a különböző programok feltörése és az azokhoz történő nyilvános hozzáférés biztosítása is, ami azonban már nem volt teljesen pozitív motiváció és eredmény.

[23] A hackerek megjelenése előtt (illetve egy ideig azzal párhuzamosan) nagyon sokszor a *phreak* kifejezés volt használatos azokra, akik telefonvonalat illegálisan használva jutottak anyagi előnyökhöz. A phreakek az akkori telekommunikáció (értsd: vonalas telefon) szakértői voltak az 1980-as években egészen az 1990-es évek elejéig. Nagy tudással rendelkeztek a telefonközpontok vezérlőeszközeivel és a távközlési vonalak ingyen történő használatával kapcsolatban. (Kovács 2006; Haig–Kovács 2012)

a hackerek tevékenységéről – a két, gyökeresen eltérő motivációval rendelkező csoport megnevezése összemosódik, és a *hacker* kifejezés az általánosan használatos. (Kovács 2006; Haig–Kovács 2012)

Mindezeknek megfelelően sok esetben nagyon kevés választja csak el a hackert a számítógépes bűnözőtől. A kiberbűncselekményekről külön is lesz szó, de talán célszerű a kibertámadók esetében is néhány gondolatot szentelni ennek a csoportnak is. A kibertérben elkövetett különböző bűncselekmények – ahogy azt minden támadási formánál láthattuk – egy bizonyos szintű fejlődést, azaz jól lekövethető és feltárható evolúciós lépcsőket jártak be. A hackereknél említett korai szakaszban a black hat típusú elkövetők alapvetően saját maguk számára kerestek pénzt azzal a tudással, amivel rendelkeztek. Ugyanakkor ahogy nőtt ezen bűncselekményekkel megszerezhető pénz nagysága és volumene, úgy jelentek meg a fizikai térben, azaz a valós életben már jól megismert bűnözői, elkövetői körök a kibertérben is. Elsősorban arról beszélhetünk, hogy a korábbi bűncselekmények bevételeiből olyan számítógépes tudással rendelkező szakértőket tudtak és tudnak megvásárolni, akik ebben az új térben tudnak elkövetni különböző bűncselekményeket. Leegyszerűsítve arról van szó, hogy a hagyományos bűnözői körök felismerve az új dimenzióban rejlő potenciális – pénzszerzési – lehetőséget, egyszerűen megvásárolják a hackerek tudását. Ahogy a későbbiekben a kiberbűnözés és kiberbűncselekmények bemutatása során utalni fogunk rá, itt alapvetően arra a tudásra van szüksége a bűnelkövetői körnek, amely a rendszerek manipulálásához, feltöréséhez, onnan adatok kinyeréséhez szükséges. A pénz transzferálása, illetve annak felvétele már a hagyományos bűnözői kör feladata. Ennek megfelelően a kiberbűnözés a gazdaság minden szegmenséből igyekszik hasznot húzni, legyen az DDoS-támadással való zsarolás, vagy egy-egy bank ügyfeleitől phishingtámadással a lehető legtöbb felhasználói adat, majd ennek segítségével a lehető legnagyobb pénz megszerzése. Mindezek természetszerűleg hozták magukkal az említett fejlődési folyamatban azt is, hogy amíg korábban egy-egy sikeres hackerakció után az elkövetők nyilvánosságra hozták és köz-

zétették a kompromittált rendszer sérülékenységeit, illetve az azokat kihasználni képes támadási technikákat és megoldásokat, ez ma már nem jellemző. Ehelyett ezeket vagy eladják, vagy ezeket használják a későbbiekben egy-egy megbízásos támadás során.

Mindenképpen szükséges említést tenni a kibertér szereplői esetében a belső szakértők vagy akár a külső szerződők jelentette veszélyről is. Ebben az esetben is arról a nagyon fontos szakértelemről van szó, amellyel mind a szervezet belső munkatársai (és itt nem feltétlenül csak és kizárólag az informatikai területen dolgozó munkatársakra kell gondolnunk), mint a külső szerződő partnerek munkatársai rendelkeznek. Általában ezek a szakértők olyan szintű hálózati hozzáféréssel rendelkeznek a szervezeten belül, akár a szervezeten kívülről egyaránt, amely lehetővé teszi számukra, hogy – jól szabályozott esetben a csak a jogosultságuknak megfelelő szintig, rosszabb esetben a hálózat egész vertikumában – adatokhoz, információkhoz férjenek hozzá. Ez nyilvánvalóan azzal is járhat, hogy bármilyen konfliktus vagy akár egy – a fentiekben említett – bűnözői kör megkeresése esetében értékes adatokat tudnak eltulajdonítani vagy akár rosszindulatú programokat tudnak a rendszerben elhelyezni. Az ilyen tevékenység elleni védelem rendkívül nehéz, nem beszélve arról, hogy ez energia- és pénzigényes.

Az APT támadások, illetve az azok mögött azonosított támadói csoportok esetében már láthattuk, hogy sok ilyen támadás a szellemi tulajdon ellopására vagy az ipari adatok megszerzésére irányul. Ebben az esetben ipari kémkedésről beszélhetünk. Ráadásul az ipari kémkedés esetében rögtön felmerül még egy nagyon komoly probléma is, ez pedig a hadiipar. Az olyan ágazatokban, mint például a gyógyszergyártás vagy az autóipar, hatalmas anyagi károkat okoz az ipari kémkedés. Azoknál a gyártóknál, illetve vállalatoknál pedig, amelyek katonai vagy nemzetbiztonsági célra szánt eszközöket és rendszereket isgyártanak, már megjelenik a valódi nemzetbiztonsági kockázat kérdése is.

Nemcsak egy országra, hanem globálisan is kockázatot jelent a terrorizmus. A terrorista csoportok, legyenek globális terrorszervezetek, vagy kisebb csoportok szintén a kibertér szereplői. Ezek a szervezetek

ugyanúgy használják az internetet és a különböző információs rendszereket, mint bárki más. Bár a terrorizmus jelentette veszélyről szintén külön is szólunk, az már itt is kijelenthető, hogy attól függően, hogy milyen célból használják az információtechnológiát, két csoportra oszthatók ezen szervezetek. Az első csoportba sorolhatók azok, amelyek propaganda, toborzás, adatszerzés vagy donáció, azaz pénzügyi támogatás megszerzésére használják az internetet, és bár erre egyelőre szerencsére nem látunk gyakran példát, a második csoportba azok a terrorszervezetek tartozhatnak, akik pont az internetet, illetve az információs infrastruktúrát kívánják támadni, pusztítani, és ezzel céljaikat elérni. (Kovács 2006; Haig–Kovács 2012)

2.2.1. Hacktivisták, avagy az internet szabadságharcosai

A kibertér szereplőinek bemutatása nem lehet teljes azoknak a csoportoknak a leírása nélkül, amelyek tagjai hackerszintű tudással rendelkeznek, és olyan politikai (vagy vallási, kulturális stb.) ügy mellé állnak, amely mellett szimpátiájukat ki kívánják nyilvánítani. Ezeket a csoportokat hacktivistacsoportoknak (a hacker és az aktivista szavak összevonásából eredeztethetően) hívjuk.

A hacktivistacsoportoknak meglehetősen hosszú időre visszanyúló múltjuk van. Ugyanakkor nagyon nehéz szétválasztani a korábban is említett állami támogatású akciókat a valódi hacktivistamegmozdulásoktól, hiszen nagyon sok olyan nemzetközi konfliktus van, amelyben egy-egy adott állam a diplomáciai megoldások mellett valami egyéb eszközt is be kíván vetni. Ilyenkor nyilvánvalóan az adott ország, illetve annak kormánya nem vállalja fel a támadás közvetlen támogatását. Ilyen nagyon kétséges támadássorozat történt 1999-ben, amikor az Egyesült Államok vezette szövetséges NATO-csapatok Szerbiát bombázták, amely során találat érte a belgrádi kínai nagykövetséget, ami után kínai hackerek intéztek kibertámadásokat amerikai szerverek ellen. (Haig–Kovács 2012)

Tíz évvel ezelőtt az *Anonymous* nevű csoport még teljesen ismeretlen volt. Mára azonban látványos akcióikkal és még inkább az azokat kísérő médiavisszhangnak köszönhetően hatalmas ismertségre tettek szert,[24] és ma ez a csoport az, amelyet rendszerint a hacktivizmussal azonosítunk.

Az Anonymous nagyon nehezen beazonosítható szervezet, önnön hitvallásuk szerint is hacktivistacsoportok lazán kapcsolódó nemzetközi szervezete. A csoportok nem hierarchikus felépítésűek, nincsenek igazi vezetők, nincs taglista, és nincsenek irodák. Csak elvek és ötletek vannak. Az Anonymousnak mindenki tagja lehet, aki követi azokat az irányelveket, amelyeket a szervezet magáénak vall. A szervezet nagyon jól használja az internetes médiumokat a saját akcióik beharangozására vagy az akciók következményeinek a tálalására.

Az Anonymous csoportot, illetve magának az eszmének a létrejöttét nem sokkal 2003 utánra teszik, amikor a *4chan* nevű internetes fórum megalakult. A 4chan eredetileg egy egyszerű, képalapú internetes fórum volt, ahol bárki képeket oszthatott meg, hozzászólásokat tehetett gyakorlatilag bármilyen témában. A 4chan fórumot saját magukról adott meghatározásuk alapján Japán egyik legnépszerűbb fóruma, a Futaba Channel inspirálta. Ez alapján különféle – alapvetően a japán anime, manga, videojátékok, zene és fotó – témákban lehetséges regisztráció nélküli hozzászólásokat posztolni. A névtelen felhasználókat 2004-ben már anonymousként jelölték, sőt a *4chan's /b/ board* fórum egyik adminisztrátora egy *Forced_Anon* protokollt aktivált, amely minden bejegyzést névtelen aláírással látott el. Ez indíthatta el az Anonymous szervezetet a működés útján, mivel a 4chan felhasználók kisebb csoportokba tömörülve már hacktivistaeseményeket, sőt támadásokat kezdtek szervezni 2006-ban. Az első ilyen téma-

[24] Az Anonymous csoporthoz köthető „hivatalos" weboldal egyik írása is pont így fogalmaz: „10 évvel ezelőtt, ha megemlítettem volna az »Anonymous« nevet, akkor valószínűleg nem tudnád, kire is utaltam. Ma már viszont a szervezet ott van a hírekben, milliók figyelnek rá, és arra, milyen nagy szerepet is játszik világunk igazságának felfedésében." (Anonymous 2017)

dásokat egy finn közösségi oldal – a Habbo Hotel – ellen követték el. (Olson 2012; Kovács 2011; 4chan 2017)

Az Anonymous tagjai magukat *anonoknak* nevezik. Nyilvános helyeken, például tüntetéseken,[25] illetve az interneten megjelenő videóikban előszeretettel viselnek Guy Fawkes maszkot,[26] amely a csoport védjegyévé is vált az elmúlt években.

Az elmúlt 10 évben az Anonymous több nagy támadást is végrehajtott különböző szervezetek ellen, amelyekben mindig valamilyen ügy mellett fejezték ki szimpátiájukat.

2008. év elején a Szcientológia Egyházat támadták meg a *Project Chanology* néven elhíresült akcióban, majd ezt követően egészen az év végéig számos támadást hajtottak végre az egyház és azok tagjai ellen. Az ügy egy videó miatt robbant ki, amelyet egy videoblog tett közzé az egyház egyik rendezvényéről, és amely után az egyház jogi lépésekkel fenyegette meg a közzétevőt. A támadás során az Anonymous DDoS-támadásokkal, tömeges hamis telefonhívásokkal és teljesen fekete oldalak faxolásával támadta az egyházat.[27] A DDoS-támadásban ekkor mutatkozott be az úgynevezett *Low Orbit Ion Cannon (LOIC)*[28] program, amelyet a csoport tagjai számos helyről le tudtak tölteni, és használni tudták a célpont ellen. A LOIC az UDP vagy TCP-csomagokkal floodtámadások kivitelezésére készült szoftver.

---

25 A csoport tevékenységével szimpatizálók nagyon sokszor különböző utcai tüntetéseken is megjelennek.

26 Guy Fawkes volt az egyik nevezetes alakja az 1605-ös angliai úgynevezett *lőpor összeesküvésnek,* amelynek fő célja a Parlament és I. Jakab király felrobbantása, majd egy katolikus király trónra ültetése volt. (Tarján é. n.) Bár Fawkes-t 1606-ban felségárulás miatt kivégezték, nevét mégis a 19. század óta megjelent regények, képregények és filmek hatására alapvetően egy olyan képzeletbeli figurával azonosítják, aki a hatalom ellen a jó érdekében harcolt.

27 A teljesen fekete oldalak tömeges faxolásának célja a festékpatronok kifogyasztása, és így a faxkészülékek működésképtelenségének előidézése volt.

28 A LOIC-t a Praetox Technologies 2008 év végén a Project Chanology akció után nyilvánosan elérhetővé tette. Így az szabadon hozzáférhetővé és bárki által használhatóvá vált. (Kovács 2011)

50. ábra
Az elhíresült Guy Fawkes maszk, amely az Anonymous jelképévé vált

Forrás: History 2017

A támadás során azonban számos kevésbé elővigyázatos Anonymous-tag nem jól védett számítógépről vagy a saját IP-címéről használta az eszközt, ami természetesen letartóztatásokhoz vezetett. Az ilyen esetek elkerülése érdekében a szervezet egy kézikönyvet készített, amelyben nagyon részletesen bemutatják, hogy milyen alapvető technikai és eljárásbeli megoldásokat kell betartania annak az Anonymous-tagnak, aki valóban névtelenül akar aktivista lenni. A kézikönyvben, amely később a Google Docsba is felkerült, ráadásul szabadon letölthető dokumentumként, valóban olyan megoldásokat javasolt a szervezet a tagoknak, amelyek a névtelenséget biztosíthatják. A dokumentum számos olyan proxyszerver IP-címét ajánlja az Anonymous-tagoknak, amelyek nem adják ki a felhasználók IP-címeit, valamint a szervezet ebben a kézikönyvben megjelöli azokat az anonim proxyszolgáltatásokat ígérő társaságokat, amelyek a rendőrségek vagy a nemzetbiztonsági szolgálatok látókörében vannak, és amelyek, bár ígérik, nem biztosítanak névtelenséget azoknak, akik a szolgáltatásaikat használják. A kézikönyv olyan eljárásokat is bemutat, amelyek a komoly informatikai vagy hackertudás nélküli felhasználók

(Anonymous-tagok) számára újdonságot jelenthetnek a saját biztonságuk, azaz felfedezhetetlenségük – anonimitásuk – érdekében.

Az Anonymous következő nagyobb támadássorozata 2010-hez köthető. 2010 novemberében a WikiLeaks Julian Assange vezetésével ezrével kezdte nyilvánosságra hozni azokat a dokumentumokat, közleményeket és táviratokat, amelyeket a szervezet az Egyesült Államok diplomáciai testületétől, nemzetbiztonsági szolgálatoktól és számos más szervezettől szerzett meg, alapvetően illegális eszközökkel. Mivel az Amazon internetszolgáltató a nála hosztolt WikiLeaks hivatalos oldalát szinte a kiszivárogtatások megkezdése után azonnal lekapcsolta, valamint az olyan pénzügyi szolgáltatók, mint a Visa vagy a Mastercard is bejelentették, hogy blokkolják a WikiLeaks rajtuk keresztül menő pénzügyi tranzakcióit, rögtön a hacktivistamozgalmak – így az Anonymous – kereszttüzébe kerültek.

Az Anonymous akciója az Operation Payback, illetve az *Operation Avenge Assange* nevet kapta. Az alapvetően a LOIC-ra épülő DDoS-támadások kisebb-nagyobb kieséseket okoztak az Amazonnak, amelyek a Visa és a Mastercard esetében is jelentkeztek. A támadások megindulása után a Visa és a Mastercard is azonnal közölte, hogy bár valóban támadták a rendszereiket, ezek a támadások nem okoztak jelentős fennakadásokat a szolgáltatásaikban. Információbiztonsági elemzések azonban arra jutottak, hogy a Visa rendszereit kétezer, a Mastercardot pedig közel négyszáz hacker támadta. Ezek a támadások főleg a cégek webes felületeit támadták, így az alapvető pénzügyi szolgáltatásaikban valóban nem volt észrevehető fennakadás, de az internetes oldalaik több órán keresztül elérhetetlenek voltak. (Kovács 2011)

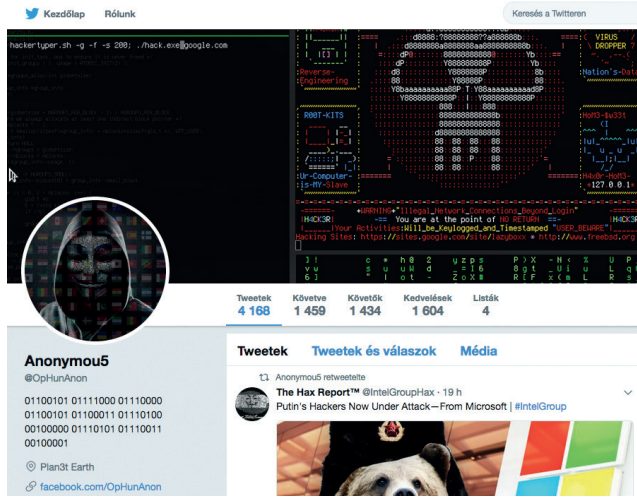
Később az Anonymous támadásai kiterjedtek a Paypalra, sőt Joe Lieberman szenátor weblapja ellen is, aki a WikiLeaks szolgáltatásainak beszüntetését szorgalmazta. Ugyanakkor kiderült, hogy a LOIC már nem hatásos fegyver többé, hiszen annak működése ismertté, és így az ellene való védekezés megoldhatóvá vált. Az Anonymous ezt felismerve más megoldást igyekezett keresni, amely nem volt más, mint olyan zombihálózatok igénybevétele, amelyek masszív DDoS-

támadásokat tudtak végrehajtani. A támadások azonban ezt követően már csak kevéssé voltak sikeresek, a PayPal szolgáltatását is csak egy órára tudták akadályozni. (Olson 2012)

Természetesen Magyarországon is megjelent az Anonymous-jelenség. Számos alkalommal adott hírt a hazai média is sikeres és kevésbé sikeres magyar Anonymous-csoport támadásáról.

Az egyik legelső, nagyobb támadás 2012 márciusában történt, amikor négy magyar fiatalember feltörte az Alkotmánybíróság honlapját, és átírta az Alaptörvény szövegét. A négy fiatalembert egy későbbi DDoS-támadás utáni nyomozásban derítették fel és fogták el, amely során más támadásokat, köztük az alkotmánybírósági támadást is elismerték. (MTI 2012)

Ezt követően számos, alapvetően politikai motivációt sejtető támadás ért sok hazai politikai szervezetet és médiafelületet. A támadások az egyszerű deface-támadástól kezdve a sokkal komolyabb rendszerbehatolásig széles skálán mozogtak. Az egyik legnagyobb visszhangot kiváltó Anonymous-támadás az Origo hírportált érte. 2017. április 12-én a hírportál összes cikke alatt kommentek egész sora jelent meg, amelyek mindegyike azonos (politikai ellenszenvet kifejező) szövegű volt, és azokat egyetlen felhasználó – AnonymusHUN – jegyezte.



51. ábra

Az Anonymous Operation Hungary „hivatalos” Twitter-oldala[29]

Forrás: Twitter 2017

A WikiLeaksről és annak alapítójáról, Julian Assange-ról már többször tettünk említést. Bár sem ez a szervezet, sem a hasonló kiszivárogtatást végző Edward Snowden nem tekinthető teljes egészében hacktivistának, mégis az a jelenség, amelyet a nevük „fémjelez”, több ok miatt is szükségesség teszi e helyen való tárgyalásukat.

A WikiLeaks 1999 óta folyamatosan tett közzé olyan dokumentumokat, amelyek az aktuális hatalom – legyen az kormány, multinacionális nagyvállalat vagy éppen civil szervezet – számára igencsak kínosak, sőt egyes esetekben nagyon is botrányosak voltak.

Ugyanakkor, amennyiben a kiberbiztonság oldaláról tekintünk mind az Assagne-, mind a Snowden-jelenségre, számos következtetést tudunk levonni, amely több mint elgondolkodtató. A politikai felhan-

[29] Az Anonymous Operation Hungary Twitter-oldalán lévő bináris számok az „expect us” szöveget rejtik, amely egy részlet az Anonymous jelmondatává vált idézetből: “We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.” (Anonymous 2017)

gokat félretéve az minden kiszivárogtatás esetében nyilvánvaló kérdésként merül fel, hogy mi a célja a dokumentumokat nyilvánosságra hozónak. Egyszerű hacktivistaideától vezérelt; az igazság, az igaz ügy kérlelhetetlen védelmezője; vagy egészen más indítékot kell sejtenünk a háttérben? A következő kérdés: honnan és hogyan szerzik a kiszivárogtatók ezeket a dokumentumokat? Belső ember, mint például Snowden, aki „csak" háttérmunkát végez egy olyan kiemelten fontos nemzetbiztonsági szervezetnél, mint az NSA, vagy ami még elgondolkodtatóbb, maga a szervezet – például belső személyi feszültségek vagy csatározások okán – juttatja el a hol kevésbe, hol nagyon kínos, de sok esetben mindenképpen kompromittáló dokumentumokat ezekhez szervezetekhez? Azaz összefoglalva ezt a kérdést: milyen szintű biztonság jellemzi ezeket a szervezeteket, mint például a legutóbbi kiszivárogtatásokban érintett CIA-t vagy NSA-t?

Egy másik következtetés már a nyilvánosságra hozott dokumentumok tartalmi elemzéséből vonható le. A WikiLeaks 2017. március elején nyilvánosságra hozott közel kilencezer olyan dokumentumot, amelyek a CIA különböző (kiber)kémkedési és műveleti eljárását mutatják be. Ezek a dokumentumok nagyon sok olyan érdekes technikai megoldást részleteznek, amellyel a nemzetbiztonsági szolgálatok lehallgatásokat és megfigyeléseket végeznek. (Newman 2016)

Julian Assange és a WikiLeaks

A WikiLeaks – a szervezet saját meghatározása szerint – egy multinacionális médiaszervezet és az ahhoz kapcsolódó *könyvtár,* amelyet Julian Assange, az ausztrál származású hacker és hacktivista 2006-ban alapított.

A WikiLeaks legfontosabb tevékenysége az olyan cenzúrázott vagy egyéb nem nyilvános hivatalos dokumentumoknak a közzététele és nyilvánosságra hozatala, amelyek a különböző háborús tevékenységekkel, a kémkedéssel és az állami korrupcióval kapcsolatosak. A szervezet eddig több mint 10 millió dokumentumot és az azokhoz kapcsolódó elemzést publikált. (WikiLeaks 2015)

A WikiLeaks egyik legnagyobb visszhangot kiváltott kiszivárogtatásai 2010-ben voltak, amikor nyilvánosságra hoztak több mint 90 ezer

dokumentumot az afganisztáni és iraki háborúról, köztük egy olyan videofelvételt, amelyen amerikai légitámadásban civilek, köztük iraki újságírók is meghaltak. Szintén 2010-ben hoztak nyilvánosságra közel 250 ezer titkos amerikai diplomáciai táviratot, ami hatalmas diplomáciai botrányt keltett világszerte.

2010-ben Svédország kezdeményezte az akkor Angliában lévő Assagne letartóztatását és kiadatását szexuális bűncselekmények miatt. Assagne azonban Ecuadortól menedékjogot kapott, és 2012 óta Ecuador londoni nagykövetségén él.

Kétségkívül ez az egyik legnagyobb dobás a WikiLeaks-saga történetében, legalábbis abban az értelemben, amely a kiberbiztonságot jelenti. Ezek a dokumentumok nemcsak a diplomácia szövevényes kulisszatitkaiba engednek betekintést, mint az a korábbi WikiLeaks által nyilvánosságra hozott táviratok tették, hanem olyan eszközöket és megoldásokat lepleznek le, amelyek az információtechnológia fejlődésével váltak lehetővé és így természetesen a nemzetbiztonsági szolgálatok által is kihasználhatóvá. A dokumentumok jó része persze nem leplez le nagy titkokat, de olyan megoldásokat mutat meg, mint például az okostelevízióval történő kémkedés, megfigyelés vagy információszerzés. (WikiLeaks 2014)

Ugyanakkor ez a fajta tevékenység már elérte azt a szintet, amikor az olyan információtechnológiai nagyvállalatok is kénytelenek voltak megszólalni, mint például az Apple. A WikiLeaks-eset hatására az Apple úgy döntött, hogy eltávolítja az Apple Store-ból a WikiLeaks-alkalmazást. (Poulsen 2010)

Az Edward Snowden-ügy

Edward Snowden, az 1983-ban született informatikai szakértő dolgozott a CIA-nál és a Dellnél is, mégis az NSA-nél eltöltött néhány hónapos munkája – amelyet egyébként mint szerződéses munkatárs végzett – alapján híresült el. Snowden 2013-ban az NSA Hawaiin lévő állomásán több ezer titkos NSA- és CIA-dokumentum birtokába került, amelyeket át-

adva újságíróknak nyilvánosságra hozott. A Snowden birtokába került titkos dokumentumok pontos száma azonban nem ismert. A dokumentumok az USA olyan globális elektronikus lehallgatási és kibermegfigyelési szervezeteiről, technológiájáról és akcióiról, valamint az ezek mögött lévő – nem mindig tisztázott eredetű – anyagi erőforrásokról rántják le a leplet, amelyeket a közvélemény korábban még sosem láthatott és hallhatott. A világ ezekből a dokumentumokból ismerhette meg például azt a globális rendszert, amely a PRISM nevet viselte, és amelyet az NSA a legnagyobb internetes szolgáltatók bevonásával arra használt, hogy az interneten folyó teljes kommunikációt lehallgassa és elemezze. Edward Snowden jelenleg Moszkvában ismeretlen helyen él, miután az USA elfogatóparancsot adott ki ellene kémkedés vádjával, de Snowden Oroszországtól menedékjogot kapott.

2.2.2. Kiberbűnözők és kiberbűnözés

A kiberbűnözés és a jelenség mögött lévő mindinkább szervezett elkövetői körök egyre nagyobb fejtörést okoznak nemcsak a bűnüldöző szerveknek, hanem ezzel párhuzamosan az információbiztonsági vállalatoknak és szervezeteknek egyaránt. Az évről évre nagyobb anyagi károkat okozó kiberbűnözés változatos formái markánsan jelen vannak mindennapjainkban. A régi szép időkben még csak olyan gazdasági bűncselekmények történtek a kibertérben, amelyek maximum a számlázási rendszerek manipulációiban jelentkeztek. Ahogy nőtt azonban az információtechnológia szerepe a gazdaság minden szegmensében, úgy nőtt azoknak az elkövetői köröknek is a tevékenységi skálája, akik nem törvényes eszközökkel és módszerekkel kívántak és kívánnak anyagi előnyökhöz jutni.

Nagyon érdekes és tanulságos a kiberbűnözés megfogalmazása az Európai Unió Kiberbiztonsági Stratégiájában: „A számítástechnikai bűnözés számos különböző bűncselekményt jelenthet, amelyek során a számítógépek és az információs rendszerek az elsődleges eszközök, illetve ezek az elsődleges célok. A számítástechnikai bűnözés hagyományos szabálysértéseket (például csalás, hamisítás és személy-

azonosság-lopás), tartalmakhoz kapcsolódó szabálysértéseket (például gyermekpornográfia internetes terjesztése vagy fajgyűlöletre uszítás), illetve csak számítógépekre és információs rendszerekre korlátozódó szabálysértéseket (például információs rendszerek elleni támadások, hozzáférés megtagadása vagy rosszindulatú szoftverek) is magában foglal." (Cybersecurity Strategy of the European Union 2013)

A kiberbűncselekmények módszerei egyre inkább egymásra épülnek, hiszen a kiberbűnözés egyre komplexebb elkövetési módszerekkel él. A személyiséglopástól kezdve a célzott phishingtámadásokon át a sokkal szofisztikáltabb technikai és hálózati eszközökkel megvalósított elkövetésekig terjednek ezek a módszerek. A kiberbűnözésre talán az egyik legjellemzőbb tény, hogy ma már egyre ritkább a magányos elkövető, hiszen az összetett védelmi megoldásoknak köszönhetően komplex tudásra és ennek megfelelően összetett támadási módszerekre van szüksége a támadóknak is, esetünkben a bűnözőknek. Ennek megfelelően ma egyre inkább szervezett csoportok az elkövetők, amelyek nagyon sok esetben látszólag semmilyen illegális tevékenységet nem végeznek, csak például adatokat gyűjtenek. Ugyanakkor az adatgyűjtés eredményeként megjelenő adatbázisok (ahogy később utalni fogunk még erre, az e-mail-címek és jelszavak párosítása esetén) nagyon sokat érhetnek.

Korábban már említést tettünk arról a trendről is, hogy a kiberbűnözés is nyilvánvalóan sokszor igényel valamilyen szintű anyagi befektetést. Ehhez sokszor a hagyományos bűnelkövetői körök kapcsolhatók, akik gyakorlatilag megveszik vagy esetenként bérlik azt a tudást vagy technikai hátteret, amely a bűncselekmények (például egy pénzintézet vagy annak ügyfélszámlái megcsapolásának) elkövetéséhez szükséges.

A közelmúlt egyik legnagyobb kiberbűncselekmény-sorozatára, amelyre a különböző módszerek már-már zseniális egymással párhuzamos, egymás hatásait kihasználó alkalmazása volt a jellemző, 2016. év végén került pont több bűnüldöző szervezet – például az Europol,

a European Cybercrime Center (EC3), az Eurojust[30] és az amerikai FBI – összehangolt akciója révén.

Az *Operation Avalanche,* azaz Lavinaművelet során egy akkor már négy éve tartó kitartó nyomozás után egy olyan nemzetközi kiberbűnözői csoportot sikerült felszámolni, amely valóban mesteri módon alkalmazta a legkorszerűbb és a legváltozatosabb internetes és hálózatos technológiákat. Az Europol jelentése szerint a kiberbűnözők az Avalanche nevet kapott hálózatot tömeges, az egész világra kiterjedő olyan platformként használták, amelyen keresztül többek között malware-ekkel elkövetett kibertámadásokat és a pénzügyi rendszerek támadása során elengedhetetlen olyan emberek toborzását is végezték, akik némi anyagi ellenszolgáltatás fejében a zsákmányolt pénzt készpénzben felvették (vagy azzal vásároltak) a bankokban vagy pénzintézetekben.[31]

A becslések szerint a kiberbűnözők az internetes banki rendszerek szisztematikus támadásával közvetlen módon 6 millió eurós kárt okoztak csak Németországban. Mindezeken túl az Avalanche-hálózat keresztül végrehajtott rosszindulatú támadásokkal okozott pénzügyi veszteségek világszerte több százmillió euróra becsülhetők, bár ahogy az Europol is megjegyzi, az okozott kár pontos értékének meghatározása rendkívül nehéz, mivel a hálózaton olyan mennyiségű és olyan változatos malware-eket használtak, ami eleve kizárja azt, hogy azok tényleges céljait és az így elkövetett támadások hatásait teljesen pontosan és nagy bizonyossággal (bizonyítható módon) felderítsék. Ugyanakkor pont az a tény, nevezetesen, hogy számos országra kiterjedt a hálózat működése és a bűncselekmények sorozata, indokolta az Eurojust részvételét, hiszen – ahogy később is utalni fogunk rá – nincs egységes jogrendszer az országok között a kiberbűnözéssel kapcsolatosan.

---

30 Eurojust: The European Union's Judicial Cooperation Unit, azaz az Európai Unió Igazságügyi Együttműködési Egysége.

31 Az ezt a tevékenységet, illetve az azt végzőket *money muleingnak,* illetve *money mule*-nak nevezik.

Az Avalanche-hálózatot működtető kiberbűnözői csoportot egy olyan nemzetközi bűnüldözői és nyomozási együttműködésnek köszönhetően sikerült elfogni, amelyben közel 30 ország ügyészei és nyomozói vettek részt. Az Operation Avalanche eredményeként 5 személyt letartóztattak, közel negyven helyen tartottak házkutatást, és 39 szervert foglaltak le. A malware-ekkel elkövetett támadások áldozatait több mint 180 országban sikerült azonosítani. Mindezek mellett a nyomozásban részt vevő szervezetek 221 egyéb szervert, valamint 800 ezer domént kapcsoltattak le vagy blokkoltattak. (Europol 2016a)

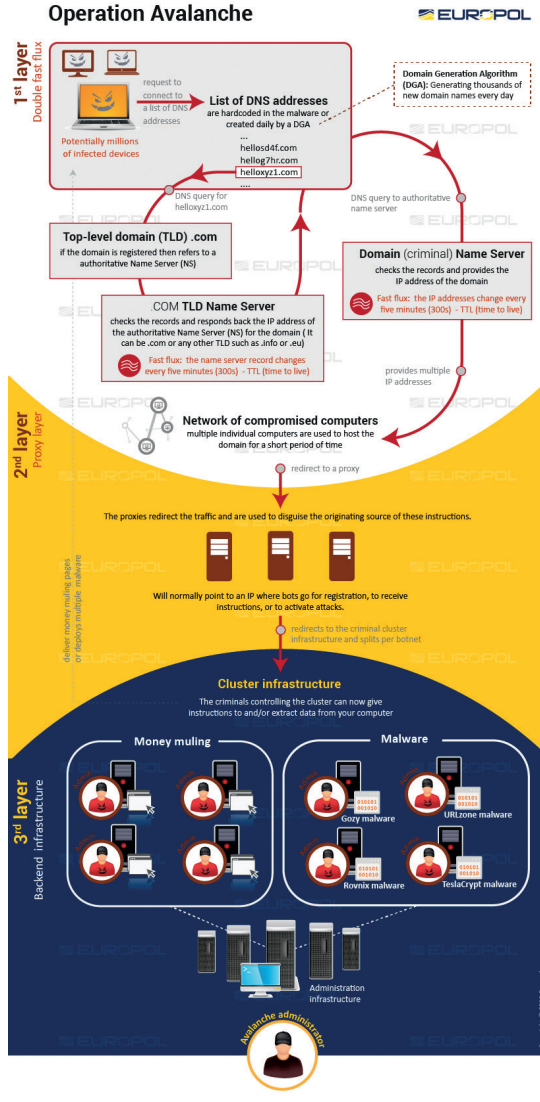
A kiberbűnözők által fenntartott Avalanche-hálózat 2009-ben kezdte meg működését. A pénzügyi bűncselekményeken kívül más célú phishingtámadásokra és spam küldésére is használták a rendszert, amely segítségével hetente legalább 1 millió spamet küldtek szét. A hálózat rendkívül jól felépített volt és kifinomult infrastruktúrával rendelkezett. A robosztus és a különböző helyzetekhez dinamikusan alkalmazkodni képes hálózati kiépítés segítségével az egyes rendszerelemek elkerülhetetlen kiesését, illetve az abból adódó veszteséget kompenzálták, mivel a megszakadt hálózati elemek feladatait tovább osztották a még aktív kiszolgálókra. Az Avalanche-hálózat becslések szerint naponta 500 ezer fertőzött számítógépet foglalt magában. A masszív és robosztus infrastruktúrát többek között a fast flux és a dupla (double) fast flux technológia segítségével tudták fenntartani. Ez a technológia egy viszonylag elterjedt megoldás egyrészt a malware-ek alkalmazása, másrészt a botnethálózatok kiépítése és fenntartása során. A technika lényege: egy *fully qualified domain name,* azaz egy abszolút doménnév[32] mögé nagyon sok IP-címet generálnak, majd ezeket nagyon nagy sebességgel változtatják a DNS-rekordban. Ennek következménye-

[32] Az abszolút doménnév teljesen pontosan meghatározott helyet jelöl a DNS-hierarchiában.

ként egyszerű megoldással nem lehet kitiltani a hálózati forgalomból az adott domén mögött lévő IP-címet, mert az folyamatosan változik.[33]

Az Avalanche működése során több mint 20 különböző malware-családot azonosítottak (például Goznym, Marcher, Matsnu, URLzone, Pandabanker). (Europol 2016a)

[33] A mesterséges intelligencia megoldást jelenthet ebben az esetben, hiszen a segítségével előre lehet jelezni a bűnözők által generált IP-címeket, illetve tartományokat. Ugyanakkor erre a megoldásra a bűnözők „válasza" olyan IP-címek alkalmazása, amelyek valósak (például már nem használt, de valós IP-címek, címtartományok).



52. ábra
Az Avalanche működése

Forrás: Europol 2017a

A kiberbűnözés egyik legnagyobb online terepe a *deep web* (más néven *dark web*), avagy a *láthatatlan web.* Bár megoszlanak a vélemények, hogy ezek a fogalmak teljesen ugyanazokat a tartalmakat jelentik-e, most mégis fogadjuk el, hogy a deep web, azaz a láthatatlan web az internet azon része, amely a keresőmotorok számára valamilyen ok miatt (például algoritmushiba, akarathiány, jogi kérdések stb.) nem, vagy csak részben látható, így az átlagfelhasználó rendszerint és jó esetben nem is találkozik az ott lévő tartalommal.[34]

A deep web egyik elérési lehetősége a TOR. A *TOR* eredeti jelentésben egy ingyenes szoftver és egy nyílt hálózat, amely lényege, hogy „megóvja a felhasználót a forgalomelemzés, a hálózatfigyelés olyan formáitól, amelyek veszélyeztetik a személyes szabadságot és a magánéletet, a bizalmas üzleti tevékenységeket és kapcsolatokat, valamint az állami biztonságot". (TOR 2017)

Ennek megfelelően a TOR egy nagyon jól, ráadásul több szinten titkosított kapcsolatot nyújt szoftveres hálózati elérést lehetővé téve. A TOR-hálózatban a résztvevők (alapvetően ők a node-ok) csak titkosított adatokat küldenek, így a lehallgatásokkal szemben biztonságosnak tekinthető. Megoszlanak a vélemények, hogy a TOR titkosítása az adattartalom vagy az anonimitás biztosítása érdekében működik-e jobban, de egy biztos, még a hatóságok is csak az együttműködő tagok (és azok közül is csak a TOR exiteknek nevezett tagok, akik feladata a hagyományos internet felé a TOR-ban lévő node-ok adatainak továbbítása) együttműködése esetén tudnak arra választ kapni, hogy mi volt az adattartalom a hálózat egy-egy útvonalában. Azt viszont

[34] A *nem látható web* kifejezés már a 2000-es évek elején megjelent. Akkor azonban még alapvetően azok a tartalmak voltak túlsúlyban, amelyek olyan adatállományokat jelentettek, amelyeket a keresőgépek az akkori keresőalgoritmusaikkal nem indexáltak, vagy az adatállományok kezelői nem optimalizálták azokat a keresőgépekre. A másik ok, ami miatt ezek az adatok nem voltak láthatóak, az az volt, hogy akkori technológiai viszonyok miatt nem volt lehetséges ezeket a nagy nyilvánosság számára hozzáférhetővé tenni. (Ellentétben egyes véleményekkel, amelyek az illegális tartalomban keresték ennek okát). Ebben a témában az egyik legtöbbet idézett forrásmunka abból az időszakból M. K. Bergmann tanulmánya, amely még az akkori – weben található – adattartalom nagyságát is megbecsülte. (Bergman 2001)

jelenleg nem lehet visszafejteni, hogy a vizsgált adatcsomagnak ki volt az eredeti feladója. Ez persze a másik oldalról, a védelem oldaláról számos kockázatot rejt magában, ami miatt főleg a bűnüldözésben, valamint a nemzetbiztonsági szolgálatok körében – ezen érthető okok miatt – nem népszerű ez a megoldás.

A deep web viszont napjainkban a kiberbűnözés igazi melegágya, hiszen itt számos olyan alkalmazás, eszköz, rosszindulatú program megvásárolható vagy akár szolgáltatásként bérelhető, amellyel pénzügyi, illetve egyéb visszaéléseket lehet elkövetni.

Egy másik kihívás a kiberbűnözés területén a bitcoin, illetve a kriptovaluták. A bitcoin – hasonlóan a többi a virtuális fizetőeszközhöz – egyáltalán nem illegális. Ami miatt mégis nagy kihívást jelent, az az anonimitásában keresendő, mivel ezzel az eszközzel úgy lehet kereskedni (pénzügyi tranzakciókat végrehajtani, azaz transzferálni, eladni, venni), hogy ahhoz nem kell valós személyazonosság. Ahogy korábban láthattuk, éppen ezért nagyon népszerű a bitcoin például a zsarolóvírusokkal és egyéb hasonló rosszindulatú eszközökkel operáló támadók körében.

A bitcoin

A bitcoin egy nyílt forráskódú internetes – virtuális – fizetőeszköz. Pénzügyi fogalmak szerint nehéz besorolni a hagyományos pénzforgalom eszközei közé. Az EU-szabályozás szerint a bitcoin nem tartozik az elektronikus pénz körébe,[35] ezért esetében a *virtuális fizetőeszköz* megnevezés a célszerűbb. A bitcoin megalkotójáról csak feltételezések vannak, de

[35] Az Európai Unió szabályozása ezen a területen 2009-ben született, amikor elfogadásra került az Európai Parlament és Tanács irányelve az elektronikuspénz-kibocsátó intézmények tevékenységéről. Ez az irányelv tartalmazza az elektronikus pénz fogalmi meghatározását is. Eszerint az elektronikus pénz: „a kibocsátóval szembeni követelés által megtestesített, elektronikusan tárolt – ideértve a mágneses tárolást is – monetáris érték, amelyet pénzeszköz átvételével bocsátanak ki a 2007/64/EK irányelv 4. cikkének 5. pontjában meghatározott fizetési műveletek teljesítése céljából, és amelyet az elektronikuspénz-kibocsátón kívül más természetes vagy jogi személy is elfogad.” (2009/110/EK irányelv) Ennek a meghatározásnak a bitcoin nyilvánvalóan nem felel meg, mert nincs kibocsátója, és így vele szemben a követelést nem lehet érvényesíteni.

nagy valószínűséggel 2009-ben, a világméretű gazdasági válság után alkotta meg Satoshi Nakamoto, akinek csak a nevét ismerjük (ráadásul ez a név is egy internetes fórumban használt felhasználói név, mögötte lehet egy személy, de akár egy csoport is).

A technológia alapját a blokkláncok jelentik. A blokkláncok (blockchains) „olyan nyitott vagy privát megosztott főkönyveket jelentenek, melyek blokkokból (azaz adathalmazokból) épülnek fel, és ezek időrendben egymásra fűződnek – csakúgy, mint egy lánc. Minden blokklánc egyedileg készül, és a blokklánc előállításában és fenntartásában szerepet vállaló résztvevőjének (más néven adatbányásznak) felelőssége van, mivel az (adat)blokkok szét vannak osztva közöttük (innen a megosztottság). Ennek megfelelően olyan főkönyvről beszélhetünk, ahol minden blokk egy lapnak felel meg, és amely lapok meghatározott sorrendben követik egymást. Ez a sorrend nem módosítható. A felelősség (azaz, hogy a főkönyv minden bányásznál megtalálható) szétosztásával értékekkel (zsetonpénz, adat stb.) kereskedhetünk." (Ambrus 2017)

Az adatbányászok, akik a rendszerbe beadott számítási kapacitásaikért cserébe bitcoint kaphatnak, csoportokban (pool) működnek, mert az összeadott számítási kapacitásaiknak meg kell haladnia a rendszer teljes számítási kapacitásának legalább a felét ahhoz, hogy kontrollálni tudják a tranzakciókat. A legtöbb adatbányászcsoport Kínához köthető. (European Commission 2017e)

Mindezek egy elosztott adatbázist jelentenek, amely tartalmazza a fizetések adatait (a fentiek alapján mindezt nem módosítható és nem manipulálható módon), és így garantálja az elektronikus fizetőeszközökkel szembeni legalapvetőbb elvárásokat.

A bitcoinnal lehet kereskedni, azt az erre szakosodott tőzsdéken hagyományos fizetőeszközökre át is lehet váltani, illetve számos hagyományos kereskedelmi és egyéb szolgáltatás ma már elfogadja fizetőeszközként. Sőt speciális ATM-eket is telepítenek ma már világszerte, amelyek készpénzre „váltják" a bitcoinokat. A bitcoin anonimitást biztosít, hiszen az adatbázisban csak a tranzakció adatai jelennek meg, azaz csak annyit tudni, hogy két cím között egy adott bitcoinmennyiség mozgott, a tulajdonosok adatai nem látszanak, azok nem visszafejthetőek.

Ugyanakkor pont ez az anonimitás az, amely miatt nagyon sok kritika éri a bitcoint. Önmagában a bitcoin egyáltalán nem illegális, sőt egy nagyon előremutató technológiára épül, de mivel ezt előszeretettel használják bűnözői körök az illegális tevékenységeik finanszírozásában, meg-

nehezítve ezzel a bűnüldöző szervek munkáját, meglehetősen negatív megítélés társul hozzá.

Mindezek mellett a bitcoin alapját is jelentő blokkláncokat számos olyan helyen alkalmazhatják majd a jövőben, ahol a decentralizáltság – és az a tény, hogy az adattartalom nem (vagy csak nem arányos befektetéssel) módosítható – követelmény.

Ugyanakkor a bitcoin kapcsán érdemes megjegyezni, hogy ennek előállítása, azaz a bitcoinbányászat, illetve az azt lehetővé tevő számítógépek jelenleg óriási villamosenergia-mennyiséget fogyasztanak. Egyes források szerint ez az energiamennyiség összemérhető Dánia vagy Szerbia éves villamosenergia-igényével. (Digiconomist 2017)

Hiba a kiberbűnözés rendszerében

A kiberbűnözés is követ el hibákat. Egy ilyen – bár kétségtelen, hogy véletlen – hiba volt, amikor az egyik legismertebb spamküldő csoport, a River City Media 1,37 milliárd e-mail-címét tartalmazó adatbázisa – állítólag egy rosszul címzett biztonsági másolat miatt – nyilvánosságra került. Az esetről hírt adó *The Guardiannak* nyilatkozó Chris Vickery biztonsági szakértő nagyon találóan fogalmazta meg az eset mögött lévő tényeket: „Nagy eséllyel ön vagy legalább egyvalaki az ismerősei közül érintett az esetben". (Hern 2017a)

Azaz az internetet használó közel 3 milliárd ember felének az e-mail-címét tartalmazta ez az adatbázis. A MacKeeper biztonsági cég egyenesen *Spammergate: avagy egy birodalom bukása* címmel jellemezte az esetet. (MacKeeper 2017)

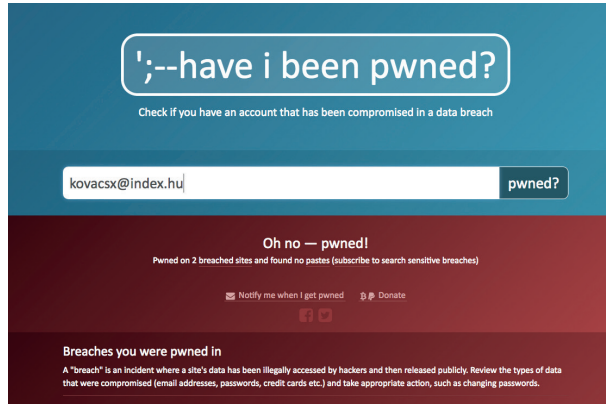
Egy másik hasonló esetben két forrásból összesen közel 850 millió e-mail-cím került nyilvánosságra. A probléma ebben az esetben is az volt, hogy nemcsak az e-mail-címek, hanem az azokhoz tartozó jelszavak is nyilvánosságra kerültek. Természetesen már az is rendkívül elgondolkodtató, hogy ezek az adatbázisok egyáltalán tartalmazták az e-mailekhez tartozó jelszavakat.

Egy információbiztonsági szakértő, nevezetesen Troy Hunt igyekezett ezeknek a kérdéseknek utánajárni. Hunt a már korábban létrehozott *Have I been pwned?* (azaz szabad fordításban: Engem is átvertek?) oldallal, illetve az az mögött működő adatbázisokkal nyújt segítséget az egyszerű internetfelhasználóknak. Ezen az oldalon bárki le tudja ellenőrizni, hogy az ő e-mail-címe szerepel-e a közel 3 milliárd e-mail-cím között, amelyeket az előbb ismertetett esetekben (vagy korábban) valamilyen alkalmazás, illetve rendszer sérülékenységét kihasználva kiberbűnözők elloptak. (Hunt 2017a)

A jelenség mögött lévő igazi problémát az jelenti, hogy számtalan felhasználó az egy helyen megadott belépési nevét (sok esetben ez az e-mail-címe) és a hozzá tartozó jelszót számos másik rendszerben, illetve alkalmazás esetében is gyakorlatilag változtatás nélkül használja. Az ugyanannak a belépési név-jelszó párosnak a használata már a biztonsági terminológiában külön nevet is kapott: ez a jelszó-újrafelhasználási probléma. Mivel az autentikáció számtalan helyen majdnem kizárólag felhasználási név-jelszó párosra épül (talán ez alól kivételek csak a bankok és az online pénzintézetek), az ilyen adatok birtokába jutó támadóval szemben nagyon nehéz megvédeni a szervezetet. Ezen adatok birtokában a belépés a támadó számára nem kérdés, hiszen a szervezet a valódi felhasználó személyének fogja hitelesíteni a támadót is. Másik probléma, hogy ezeket az adatbázisokat használva egy – könnyen elérhető – alkalmazás segítségével a megtámadni kívánt szervezet bejelentkezési rendszere automatizálható módon válik támadhatóvá, hiszen csak futtatni kell az adatbázisban a keresőt, és nagy valószínűséggel a belépési adatok ott is lesznek. (Hunt 2017a)

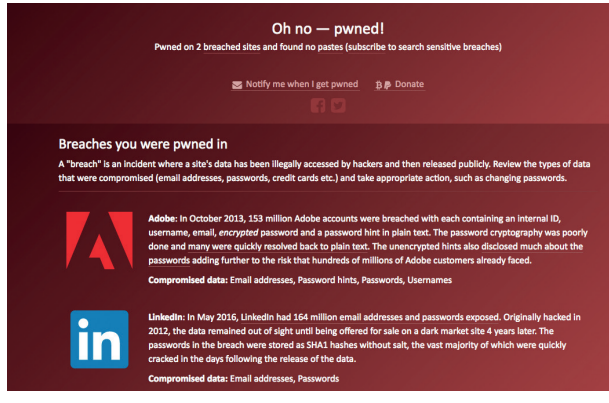
A *Have I been pwned?* oldalon jelen írás szerzője is leellenőrizte az egyik gyakran használt e-mail-címét, vajon az szerepel-e az említett nyilvánosságra került e-mail-adatbázisokban? Az eredmény elszomorító, mert sajnos az pozitív lett.

Ugyanakkor az említett oldal abban is segítséget ad, hogy honnan kerülhetett ki a kompromittált e-mail-cím, illetve az ahhoz tartozó jelszó. (Mint ahogy azt a következő kép is szemlélteti).



53. ábra
A Have I been pwned? oldalon a szerző egyik e-mail-címének ellenőrzése és annak eredménye

Forrás: HUNT 2017b



54. ábra
A Have I been pwned? oldalon a szerző egyik e-mail-címének ellenőrzése és a feltételezhető források

Forrás: HUNT 2017b

A kiberbűnözés és a jogrendszer válasza

Alapvetésként rögtön ki kell jelentenünk, hogy sajnálatos módon a kiberbűncselekmények vonatkozásában a jogalkotás és ennek megfelelően sokszor maga a jogalkalmazás jelenleg a legjobb esetben is csak követi az eseményeket. Ennek okait értelemszerűen több helyen és több tényezőben kell keresnünk. Az egyik ilyen összetett ok a nemzetállamok eltérő jogalkotási és jogalkalmazási gyakorlatában keresendő. Ez még az olyan – elvileg egységes jogi háttérrel rendelkező – nemzetközi szervezeten belül is igaz, mint az Európai Unió. A kiberbűncselekmények elleni jogi fellépés EU-s szabályozásáról később részletesen is szólunk, de röviden ezen a helyen is említést kell tennünk erről a kérdésről, hiszen az előbbi, kissé negatív kritika ellenére természetesen a kiberbűncselekmények területének átfogó jogi szabályozására történtek már kezdeményezések korábban is.

Az egyik legfontosabb – és tegyük hozzá rögtön, a legkorábbi – ilyen kezdeményezés Európában a *Budapest Convention,* azaz *Budapest Konvenció* néven született 2001-ben. (Council of Europe 2001)

A Budapest Convention megállapodást Magyarország 2004-ben iktatta törvénybe. Ez a 2004. évi LXXIX. törvény, amelynek hivatalos címe a következő: *az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről*. (2004. évi LXXIX. törvény)

A megállapodás fő célja a kiberbűnözés és a kiberbűncselekmények elleni tevékenység nemzeti jogszabályokban rögzített harmonizációja. A megállapodást napjainkig közel 60 ország ratifikálta.[36] Ugyanakkor néhány olyan – ezen a területen nagyon fontos – állam, mint Oroszország vagy India különböző okokra hivatkozva ezt nem tette meg. (Council of Europe 2017)

[36] Ugyanakkor számos ország kisebb-nagyobb eltéréseket alkalmaz, illetve megjegyzésekkel ratifikálta az eredeti egyezményt.

Később az Európai Unió a kibertér egységes védelmét az EU Kiberbiztonsági Stratégiájába mint egy keretrendszerbe kívánta beilleszteni. Ez a stratégia külön kitér a kiberbűncselekmények jelentette egyre nagyobb problémára és veszélyre, valamint ezzel összefügésben a kiberbűncselekmények elleni tevékenységekre is. (Cybersecurity Strategy of the European Union 2013)

A stratégiában megfogalmazottakkal összhangban az EU hivatalos bűnüldöző szerve, az Europol kiemelt szerepet játszik a kiberbűnözés visszaszorításában. Az Europol kilenc kiemelt bűncselekmény-területet nevez meg, amelyek mindegyike esetében többéves stratégiai tervet dolgoztak ki. Az EMPACT (European Multidisciplinary Platform Against Criminal Threats, azaz az Európai Multidiszciplináris Platform a a Bűnügyi Fenyegetettség Ellen) nemcsak cselekvési tervet, hanem operatív intézkedéseket is tartalmaz. Az EMPACT kilenc prioritása – például az illegális migráció elleni fellépés, kábítószer-kereskedelem elleni tevékenység, vagyon elleni bűncselekmények felderítése – között megtalálható a kiberbűncselekmények elleni fellépés is. A kiberbűncselekmények körében az Europol többek között az online banki és bankkártyacsalások, valamint az olyan szervezett bűnözői körök által elkövetett bűncselekmények ellen lép fel, mint amelyek például a gyermekek szexuális kizsákmányolása, vagy az olyan számítógépes támadások ellen, amelyek az EU kritikus infrastruktúráját és kritikus információs infrastruktúráit veszélyeztetik. (Europol 2017b)

Az Európai Unió kiberbűnözés elleni irányelvei

2001: Az Európai Tanács kerethatározata a nem készpénzes fizetőeszközökkel kapcsolatos csalás és hamisítás elleni küzdelemről. E határozat legfontosabb célja, hogy meghatározza azokat a csaló magatartásokat, amelyeket az EU-tagállamoknak büntetendő bűncselekménynek kell tekinteniük. (2017 szeptemberében az Európai Bizottság az Európai Parlamenttel közösen egy új javaslatot dolgozott ki a nem készpénzes fizetésekkel kapcsolatosan). (2001/413/IB) [2017/0226(COD)]

2002: Az Európai Parlament és az Európai Tanács közös irányelve az elektronikus hírközlésről és adatvédelemről. Ezen irányelv értelmében az elektronikus hírközlési szolgáltatók felelősek szolgáltatásaik biztonságáért és az ügyfélinformációk titkosságáért. (2009/136/EC)

2011: Az Európai Parlament és az Európai Tanács közös irányelve a gyermekek szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről. Ez az irányelv már elsősorban az online környezetben megjelenő – gyermekek sérelmére elkövetett bűncselekmények – környezetével és az itt megjelenő újfajta veszélyekkel foglalkozik. (2011/92/EU)

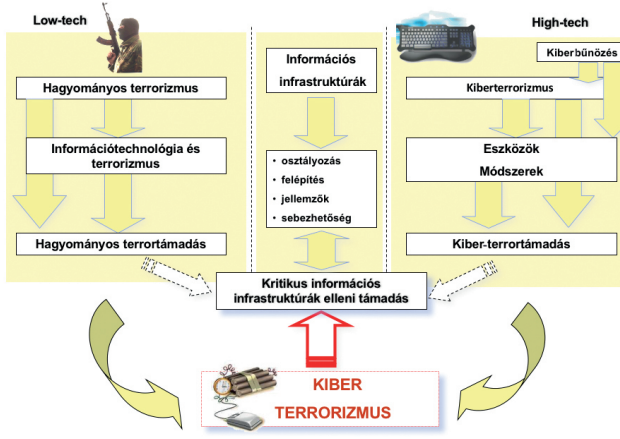
2013: Az Európai Parlament és az Európai Tanács közös irányelve az információs rendszerek elleni támadásokról. Ennek célja a nagy méretű számítógépes támadások elleni küzdelem, felhíva a figyelmet a tagországok nemzeti számítógépes bűnözés elleni törvényeinek büntetőjogi szankcióinak szigorítására, illetve azoknak olyan átalakítására, amelyek hatásosabbá és hatékonyabbá teszik a kiberbűnözés elleni fellépést. (Ez az irányelv váltotta le a 2005-ben kiadott 2005/222/JHA irányelvet). (2013/40/EU)

2017: Az Európai Parlament és a Tanács irányelvjavaslata a készpénz-helyettesítő fizetési eszközökkel összefüggő csalás és hamisítás elleni küzdelemről és a 2001/413/IB tanácsi kerethatározat felváltásáról. [2017/0226(COD)]

2.2.3. Terroristák a kibertérben

A kibertér szereplőinek bemutatásakor meglehetősen furcsának tűnhet a terrorizmus, illetve a terroristák említése. Korábban nagyon sokat kutattuk a kiberterrorizmust, és ezek eredményeit rendszeresen publikáltuk. Ezekben a kutatásokban és vizsgálatokban azokat a vélt vagy valós tevékenységeket kívántuk feltárni és elemezni, amelyeket a terrorista szervezetek az interneten vagy az információtechnológia alkalmazásával végeznek vagy végezhetnek. Ezeknek a vizsgálatoknak és kutatásoknak az egyik eredménye, hogy a terrorizmus és a terrorista szervezetek a kibertér szereplőinek bemutatásakor is helyet kell, hogy kapjanak.

A 2001. szeptember 11-e utáni világméretű sokkot követően a terrorizmus újra a mindennapjaink részévé vált, és ekkor joggal merült fel annak a kérdésnek a kutatása, amely a hagyományos terrorizmus esetleges kibertérre történő kivetülését volt hivatott feltárni. Azt is vizsgáltuk, hogy egy-egy potenciális, a kibertérben elkövetett terrortámadás következményeiben és hatásaiban mit is jelentene a korábban már sokszor említett információtechnológia által okozott társadalmi függőségünkben vagy akár a kritikus infrastruktúráink, illetve a kritikus információs infrastruktúráink[37] vonatkozásában.



55. ábra
A kiberterrorizmus kutatásának felépítése 2006-ban

Forrás: Kovács 2006

Korábbi kutatásainkban annak is utánajártunk, hogy meghatározható-e definíciószerűen maga a kiberterrorizmus. A fellelt és később magunk által is alkotott meghatározások alapvetően – az egyébként nem teljesen egységes és nem is teljesen jól megfogható – hagyomá-

[37] Különbséget kell tennünk a kritikus infrastruktúrák és a kritikus információs infrastruktúrák között. A későbbiekben ezeket a biztonság szempontjából külön is bemutatjuk és elemezzük.

nyos terrorizmusfogalmakból indultak ki. Ilyen volt többek között az FBI kibervédelmi részlege korábbi vezetőjének, Keith Lourdeau-nak a meghatározása, amely szerint „a kiberterrorizmus olyan bűncselekmény, amelyeket számítógépekkel és telekommunikációs lehetőségekkel úgy hajtanak végre, hogy azok rombolják és/vagy megzavarják a szolgáltatások működését, zavart és bizonytalanságot keltve ezzel a lakosságban. Ezen akciók célja a kormányzat vagy a lakosság erőszakos befolyásolása a szervezet egyéni politikai, társadalmi vagy ideológiai céljai érdekében." (FBI 2004)

Hasonló megfogalmazással élt Dorothy Denning professzor asszony, aki rögtön 2001. szeptember 11-e után írta: „a kiberterrorizmus számítógép alapú támadást vagy fenyegetést jelent, amelynek célja, hogy megfélemlítsék, vagy kikényszerítsék a kormányok vagy a társadalmak részéről az adott terrorszervezet politikai, vallási, vagy ideológiai céljainak elérését." (Denning 2001)

Ezekből a definíciókból, valamint az elvégzett vizsgálatainkból számos nyilvánvaló következtetés adódott. Az egyik ilyen következtetés a terrorszervezetek információtechnológia-használatára vonatkozott. Ez azt jelenti, hogy nagyon jól elkülöníthetőek azok a tevékenységek, amelyek a (hagyományos)[38] terrorszervezetek információs eszközök használatában és alkalmazásában jelentkeznek. Ezeket a tevékenységeket két csoportra osztottuk. Az első csoportba azok a terrorista szervezetek tartoznak, amelyek propagandára, toborzásra, adatszerzésre vagy rejtett, tehát titkosított kommunikációra használják az internetet és a különböző infokommunikációs rendszereket. Ezért az ebbe a csoportba tartozó szervezeteket, illetve az ő általuk végzett tevékenységeket úgynevezett *soft,* azaz *puha* típusú kiberterrorizmusnak neveztük el. Vizsgálataink során azonban jól el tudtunk különíteni egy második csoportot is. Ebbe a csoportba azok a terrorista szervezetek és tevékenységeik tartoznak, amelyek elsősorban az internetet, a kritikus információs infrastruktúrát, illetve azok egyes elemeit tekintik

[38] A hagyományos jelző itt azért lehet indokolt, mert korábban nem láttunk (és azóta sem jellemző) a teljesen és kizárólag a kibertérben működő terrorszervezet.

pusztítandó célpontnak. Ennek megfelelően ezt a csoportot *hard,* azaz *kemény* jelzővel illettük. (Haig–Kovács–Ványa 2011)

Kutatásaink során azt is körvonalaztuk, hogy a már említett terrorszervezetek által végzett tevékenységek mit is takarnak, azaz milyen kézzelfogható bizonyítékai lehetnek a terrorszervezetek információtechnológia-használatának. Ezek alapján felvázoltuk azokat a tevékenységi formákat, amelyeket a terrorszervezetek az interneten végeznek, és amelyek közül több is az elmúlt években – köszönhetően a terrorizmus ismételt előtérbe kerülésének – sokkal nagyobb intenzitású tevékenységgé vált, mint korábban.

Ilyen internetes, illetve információtechnológiai alkalmazási példa a különböző akciók megtervezése vagy a már említett titkosított kommunikáció a terrorszervezet tagjainak vagy szimpatizánsainak kapcsolattartása vagy akár az akciók összehangolásának és koordinációjának érdekében. Mindezek mellett a toborzás, valamint a pénzügyi támogatás[39] elnyerése során azonosítottunk olyan tevékenységeket, amelyeket a terrorszervezetek az internet segítségével (is) végeznek. Számos olyan weboldalt találtunk, amelyeken nyíltan is történt az új tagok toborzása, verbuválása.

Külön ki kell emelnünk azokat a tapasztalatokat és eredményeket, amelyek a terrorszervezetek nyílt források felhasználásával végzett adat- és információszerzési tevékenységére hívták fel a figyelmet. Ezek a források, bár nem tartalmaznak minősített adatokat, olyan információk birtokába juttatják az adott terrorszervezetet, amelyek alapján a célpontjaikról gyakorlatilag mindent megtudhatnak. Hozzá kell tennünk, hogy sok esetben eredménytelen figyelmeztetéseket tet-

[39] A terrorizmus interneten keresztül történő finanszírozása nem új keletű dolog, hiszen a terrorszervezetek weblapjai gyakran adtak meg ehhez olyan egyszerű megoldásokat (például bankszámlaszám), amelyek nem voltak közvetlenül a szervezethez köthetők. Ugyanakkor az olyan virtuális fizetőeszközök terjedésével, mint a már említett bitcoin a helyzet is megváltozik, hiszen ezzel gyakorlatilag anonim módon tud az adott szervezet pénzügyi tranzakciókat végrehajtani világszerte. Az EU számára készült egyik szakértői jelentés ugyanakkor kiemeli, hogy a veszély valós, de mivel nagyon új technológiáról van szó, ezért a terrorszervezetek esetében még hiányzik ennek használatához a megfelelő szakértelem. (European Commission 2017e)

tünk ez ügyben az adott szervezet felé. Ezen a területen meg kellett állapítanunk, hogy az információ szabad áramlása miatt a terrorszervezetek számára is adott a lehetőség, hogy sok olyan információhoz is hozzájussanak, amelyek egy-egy adott vagy potenciális célponttal kapcsolatosak, illetve az azokban okozható legnagyobb kárhoz szükséges módszerekre és eszközökre (például azok előállítására, azokhoz való hozzájutáshoz) adnak tanácsokat. (Haig–Kovács–Ványa 2011)

Ilyen a támadások módszereire ötleteket és részletes kivitelezési tanácsokat adó médium például az al-Káida által 2010-ben indított *Inspire* (Inspiráció) című magazin, amely nyíltan elérhető az interneten, sőt saját Wikipédia-oldala is van. Ebből a magazinból bárki ötleteket tud venni többek között házi készítésű robbanóeszközök előállításához, ráadásul úgy, hogy ehhez semmilyen illegális eszközt vagy anyagot nem is kell beszereznie.[40]

56. ábra

Az Inspire magazin egyik számának borítója és annak „bombaiskolája”

Forrás: Inspire 2014

40 Ugyanakkor már az *Inspire* magazin birtoklása is illegális tevékenységet és bűncselekményt jelent néhány országban – például az Egyesült Királyságban – az adott ország terrorizmus elleni törvényei szerint. Ezért is lehet érdekes és furcsa, hogy az interneten ma is szabadon hozzáférhető az az oldal, ahonnan a magazin számai szabadon letölthetők.

Annak a véleményünknek is hangot adtunk – hiszen erre kutatásaink tudományos bizonyítékokkal szolgáltak –, hogy bár eddig nem következett be egyetlen egy olyan átfogó és kiemelkedő kibertámadás sem, amely megrengette volna a világot, de abból kiindulva, hogy akár a kiberbűnözés által elkövetett támadások és a velük együtt járó károk sajnálatos részei mindennapjainknak, úgy a kiberterrorizmus is hasonló veszélyeket rejt magában, hiszen a terrorista célú kibertámadások során alkalmazható eszközök és módszerek hasonlóak lehetnek, mint a kiberbűnözés eszközei. Persze a célok – részben – mások lesznek, hiszen amíg a kiberbűnözés alapvetően pénzszerzési céllal követi el akcióit, addig a hard típusú kiber-terrortámadások célpontjai egészen mások lesznek. A kiberterrorizmus feltételezhető célpontjaivá válhatnak „az energiaellátó rendszerek rendszerirányító számítógép-hálózatai, a kommunikációs hálózatok, a pénzügyi-gazdasági rendszer számítógép-hálózatai, a védelmi szféra riasztási, távközlési, számítógép-hálózatai, a közigazgatás információs rendszerei.” (Haig–Kovács–Ványa 2008)

Amellett sem mehetünk el szó nélkül, hogy a kiberterrorizmus akár az olyan eszközöket is felhasználhatja, mint amilyeneket a Stuxnet esetében korábban ismertettünk. Ez úgy lehetséges, ha az olyan rosszindulatú programok, vagy azok egyes elemei, mint a Stuxnet, amelyeket egyébként – ahogy láthattunk – állami támogatással fejlesztettek, kikerülnek az állami ellenőrzés alól és például a deep weben áruként megjelennek. Amennyiben ezt egy terrorszervezet a megfelelő anyagi források megléte esetén meg tudja vásárolni, akkor a fentiekben említett igen érzékeny célpontok támadására fel tudja használni. (Haig–Kovács–Ványa 2011)

A kibertérben megjelenő terrorizmust azonban a legmarkánsabban napjainkban a különböző terrorszervezetek által kifejtett online propaganda révén tudjuk nyomon követni. A különböző közösségi oldalakon és videomegosztó site-okon naponta jelennek meg a szélsőséges szervezetek különböző bejegyzései, üzenetei és videói. Ezek a ma főleg az ISIS-hez kapcsolható propagandatevékenységek a világon

mindenhol láthatóak, hiszen a Facebookon, a Twitteren vagy a Youtube-on az ISIS nagyon sok esetben professzionálisan kezelve ezeket a médiumokat úgy teszi közzé üzeneteit, hogy azok a lehető legtöbb emberhez eljussanak. Az üzenetek egy része a fiatalokat mint potenciális tagokat veszi célba. Ugyanakkor az ISIS nemcsak ezeken a médiumokon keresztül fejt ki nagyon agresszív propagandát, hanem saját internetes oldalain és blogjain keresztül is. Ezeken az oldalakon és blogokon már sokkal mélyebb és radikálisabb üzeneteket juttatnak el a közönség – elsősorban a már valamennyire radikalizált szimpatizánsok – felé. A terrorszervezet akcióit, „hőseit" és céljait bemutató videók, képek és publikációk mellett, azokat jól alátámasztva számos Korán-idézettel igyekszenek az említett radikalizmust tovább építeni. (Shamieh–Szenes 2015)

A fentiek figyelembevételével összességében kijelenthetjük, hogy „a kiberterrorizmus jelentette fenyegetés valós (természetesen a realitásokat figyelembe véve kell felmérni ezt a veszélyt), hiszen egy-egy ilyen támadás következménye nem csak technikai és anyagi értelemben lenne hatalmas, hanem bizony akár emberéletekben is beláthatatlan károkat okozna". (Kovács 2014)

Vákát oldal

3. A kiberbiztonság megvalósítása

A korábbi fejezetekben többször utaltunk rá, hogy a kiberbiztonság valamint annak elérése, megvalósítása és folyamatos fenntartása összetett, komplex tevékenységek egész sorát igényli. Arra, hogy a kiberbiztonságra miért is van szükség, az előző fejezetek reményeink szerint választ adtak.

Ugyanakkor, mint nagyon sok fiatal területen, így a kiberbiztonság területén is ki kell jelentenünk, hogy nagyon sokszor a fogalmi meghatározások sem egységesek még. Ezért könyvünk legelején megadtuk azokat a legfontosabb fogalmakat és a mögöttük lévő tartalmi elemeket, amelyek a fent említett komplex tevékenység során relevánsak lehetnek, és amelyeket használunk könyvünk egyes részeinek magyarázatakor, valamint az ezeket alátámasztó elemzéseink során. Ezek a meghatározások azonban, ahogy arra korábban szintén utaltunk, nem örök érvényűek, nagyon sok definíció nem feltétlenül jogszabályban (azaz törvényben, nemzetközi szabványban, ajánlásban stb.) rögzített, és nagyon sok nem is „hivatalos" meghatározás. Mindezek ellenére (vagy talán éppen ezért) a különböző területek problémáit és kihívásait, illetve az azokra adandó válaszok megértését elősegíthetik. Továbbá hangsúlyozzuk, hogy a terminológiai vitában nem kívánunk állást foglalni, hiszen úgy gondoljuk, hogy a terület fejlődése magával hozza azt az evolúciós folyamatot is, amely során azok a fogalmak és meghatározások, amelyek fontosak a védelmi tevékenységek során, egyre inkább általánossá és szakmailag elfogadhatóvá válnak.

A kiberbiztonság azonban számos kisebb területre osztható, amelyek mellett a különböző kapcsolódó – a kiberbiztonsággal valamilyen szinten átfedést biztosító – egyéb részterületek találhatóak.

3.1. A kiberbiztonság tulajdonságai és kapcsolatai

Nagyon sok esetben a kiberbiztonság említett részterületeinek megnevezései egymás szinonimájaként is használatosak, hiszen például az információbiztonság már több évtizede jelen van a szakmai terminológiában, és amikor a *kiberbiztonságról* beszélünk, sokszor azt az *információbiztonság* kifejezéssel azonosítjuk. Pedig a *kiberbiztonság* talán egy kicsit tágabb és bővebb fogalmi meghatározás, mint az információbiztonság. Persze, ha az *információbiztonságot* komplex módon értelmezzük, akkor nagyon kis különbséget tudunk felfedezni a két fogalom által lefedett terület között.

Könyvünk legelején nagyon röviden meghatároztuk a kiberbiztonság fogalmát. Ennek a definíciónak azonban nyilvánvalóan számos olyan kiegészítést is kell tartalmaznia, amely hozzájárul a megértéshez.

A már többször ismertetett ITU meghatározása alapján a kiberbiztonság: „az eszközök, politikák, biztonsági koncepciók, biztonsági garanciák, biztonsági technológiák, irányelvek, kockázatkezelési módszerek, tevékenységek, képzések, valamint a legjobb gyakorlatok összessége, amelyek arra irányulnak, hogy megvédjék a számítógépes környezetet, az ezt használó szervezetek és felhasználók eszközeit, rendszereit”. (ITU 2017b)

Ezt a meghatározást kicsit leegyszerűsítve kijelenthetjük, hogy a kiberbiztonság a meglévő biztonsági kihívásokra választ adva vagy azokkal szemben biztosítja azt az állapotot (nyilvánvalóan védelmi intézkedések egész sorával, és itt kapunk rögtön választ a komplexitásra), amely a szervezet, valamint a felhasználó eszközeinek (ideértve az adatot és az információt is), vagy a szervezet különböző folyamatainak, az azokban lévő biztonsági tényezőknek az elérését és fenntartását teszi lehetővé. (ITU 2017b)

Mindezeket alátámasztja a hazai kiberbiztonság, illetve információbiztonság területén kiemelkedő szerepet játszó információbizton-

sági törvény[1] által adott meghatározás, amely szerint „[a] kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez". (Ibtv. 1. § 26. pont)

Természetszerűleg merül fel a kérdés, hogy melyek lehetnek ezek az előbb említett biztonsági tényezők? Ennek megválaszolásához azonban egy kis magyarázatra, illetve bevezetőre van szükség.

Az információbiztonságban korábbról léteznek már jól bevált olyan tényezők, amelyek viszonylag jól mérhetőek, és amelyekkel felmérhető egy adott szervezet információbiztonságának adott szintje vagy milyensége. Nyilvánvalóan ezek a tényezők a védelem megvalósításának oldaláról pont azokat a összetevőket jelentik, amelyekkel a védelemnek meg kell valósulnia, és amelyekre a védelemnek hatással kell lennie. Ezek a nemzetközileg is elfogadottá vált tényezők a *bizalmasság, sértetlenség* és *rendelkezésre állás*. Az angol terminológiában ezt a hármast *confidentiality* (bizalmasság), *integrity* (sértetlenség) és *availability* (elérhetőség) kifejezésekkel jelölik, innen ered a három angol szó kezdőbetűjéből a *CIA-elv.* Ez a hármas az információbiztonság három legfontosabb tényezője, vagy másként megfogalmazva biztonsági tulajdonságai.

A bizalmasság olyan biztonsági tulajdonságot jelent, amely lehetővé teszi, hogy az információhoz az arra nem jogosult személyek vagy folyamatok ne férhessenek hozzá. Amennyiben a bizalmasság sérül vagy elveszik, az azt jelenti, hogy az adat vagy az információ olyan személyek birtokába jutott, azaz olyan személyek ismerték ezeket meg vagy rendelkeztek ezekről, akiknek nem volt ehhez jogosultságuk.

---

[1] A röviden csak információbiztonsági törvénynek, vagy Ibtv.-nek nevezett jogszabály a *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról* hivatalos címet viseli.

A sértetlenség a következő biztonsági tulajdonság. Ez azt jelenti, hogy a védeni kívánt adat nem változik meg külső – akár szándékos akár nem szándékos – behatás következtében, valamint azt csak az arra jogosultak tervezett módon változtathatják meg. E tulajdonság egyik jellemzője az is, hogy az említett védendő adat az elvárt forrásból származik. Ez a hitelesség kritériuma. Nyilvánvalóan az adat akkor lesz hiteles, ha annak tartalma és annak létrehozója esetében is fennáll a sértetlenség. A sértetlenséghez egy másik tulajdonság is kapcsolható, ez pedig a letagadhatatlanság. A letagadhatatlanság az adott rendszerben végbemenő folyamatok ellenőrizhetőségét, valamint az azt kiváltó személyek esetén bizonyítékokat nyújt annak érdekében, hogy a folyamatok és/vagy személyek jogosultak voltak a rendszerben tevékenységet végezni. Összességében a sértetlenség mint tulajdonság sérül, ha az adatokat jogosulatlanul módosítják, vagy – akár részben, akár egészben – azokat megsemmisítik, vagy külső hatásra azok megsemmisülnek, illetve sérülnek.

A rendelkezésre állás a harmadik fő biztonsági tulajdonság. Ez a tulajdonság annak a leírására (bemutatására vagy jellemzésére) szolgál, ami alapján eldönthető, hogy a rendszer adott erőforrása a szükséges folyamatok, illetve a felhasználó számára elérhető-e, illetve az elvártaknak megfelelően használható-e. Amennyiben a rendelkezésre állás megszűnik, abban az esetben a felhasználó vagy egyes rendszerelemek a kívánt erőforrásokat – részlegesen vagy teljes egészében – nem tudják használni.

Ugyanakkor számos olyan értelmezési területet látunk a mindennapokban, amelyek bár szorosan összefüggenek és esetenként akár egymást átfedő területeket is jelentenek, mégis sokszor pont az eltérő definíciós készlet az, amely a tisztánlátást és az értelmezést megzavarja.

Mindezeken belül a biztonság megvalósítása – ahogy korábban említettük – komplex módon érhető csak el. A komplex információbiztonság számos területet fed le, amelyeken a védelmi intézkedésekkel és védelmi folyamatokkal megvalósítható és fenntartható a biztonság.

Ennek értelmében beszéltünk korábban a védelemről mint tevékenységek sorozatáról, amely a biztonságot mint állapotot hivatott létrehozni vagy fenntartani.

A komplex információbiztonság elmélete abból az összetett veszélyeztetettségből indul ki, amely számos dimenzióban és számos területen érheti az adott rendszert. Sok meghatározás egészen messziről, például a biztonságpolitika területéről indítja az érvrendszerének alátámasztását, azaz azokat a dimenziókat, amelyekben a veszélyeztetés fennáll, a biztonságpolitika területeiből vezeti le. Ilyen területek, illetve dimenziók a Buzan-i[2] elvek mentén a katonai, politikai, gazdasági, társadalmi és környezeti biztonság dimenziója. Ez egészül ki a 20. század vége óta a kibertérrel mint biztonsági dimenzióval. Bár rögtön hozzá kell tennünk, hogy ezt az eredeti felosztás nyilván még nem tartalmazta.

A komplex információbiztonság által védendő rendszer lehet az adott felhasználó vagy az adott szervezet rendszere, de lehet olyan kritikus információs infrastruktúra is, amelynek védelme akár nemzeti szinten lehet fontos és kiemelt. Haig megfogalmazásában: „Az információs társadalom információbiztonsága szempontjából tehát a fő cél a kritikus információk megóvása." (Haig 2015) Mivel ezt a célt csak az előbb említett több dimenzióban és több területen együttesen lehet elérni, illetve érvényesíteni, a komplex információbiztonságnak is ezek lesznek a főbb területei. Ennek megfelelően ezek a területek a következők: személyi biztonság, fizikai biztonság, adminisztratív biztonság[3]

---

[2] Barry Buzan, Ole Wæver és Jaap de Wilde 1998-ban megjelent könyvükben, amely a *Security: A New Framework for Analysis,* azaz *Biztonság: egy új keretrendszer az elemzéshez* címet viselte, a szerzők szakítottak az addigi biztonságpolitikai iskolával, amely alapvetően a politikai és katonai viszonyok elemzéséből vezette le a biztonságot, és felvázolták a biztonság kiterjesztésének szükségességét a gazdaság, a társadalom és a környezet mint dimenziók bevezetésével. (Buzan–Wæver–de Wilde 1998)

[3] Korábban az adminisztratív biztonságot *dokumentumbiztonságnak* nevezték.

és elektronikus információbiztonság.[4] (Haig 2015) Ugyanakkor ezek mindegyike további területekre osztható. Témánk relevanciája miatt itt most csak az elektronikus információbiztonság – egyébként önmagában is komplex – területeire térünk ki felsorolásjelleggel. Az elektronikus információbiztonság részterületei, mint az átviteli biztonság, a kompromittáló kisugárzás elleni védelem, a számítógép-biztonság,[5] a hálózati biztonság és a rejtjelzés azok, amelyek a későbbiekben meghatározóak a számunkra.

Mindezidáig számos területről tettünk említést, sőt egyes esetekben az említett részterületeket egymással nemcsak átfedő módon, hanem egymás szinonimájaként is használtuk.

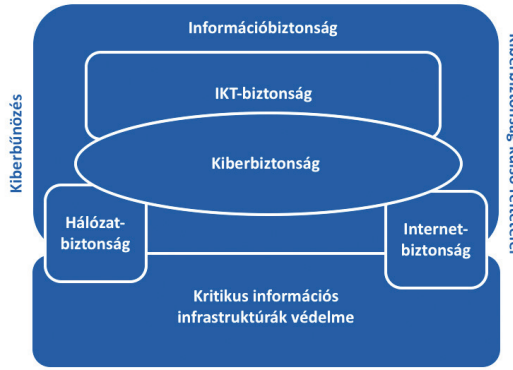
Ennek megfelelően szükséges a kiberbiztonság kapcsán a kapcsolódó területekre is némi pillantást vetni, és azokat is vizsgálat alá vonni. Ez nyilvánvalóan magával hozza azt is, hogy az említett területeket, valamint azok egymáshoz való viszonyát, az egymásra gyakorolt hatásaikat, valamint egymással való kapcsolataikat felvázoljuk.

Ezt talán a legkönnyebben egy olyan ábrával célszerű szemléltetni, amely tartalmazza azokat a területeket, valamint azok kapcsolatait, amelyek a kiberbiztonsággal, illetve a kibertérrel szoros relevanciát mutatnak. Ezek a területek nem fontossági sorrendben és nem is a teljesség igényével a következők lehetnek: kiberbiztonság, információbiztonság, kritikus információs infrastruktúra-védelem, kiberbűnözés.

---

4 Természetesen azoknál a szervezeteknél – legyenek azok a védelmi szférában működő vagy akár gazdasági szervezetek – esetenként megjelenik a komplex információbiztonság egy ötödik, speciális területe – az elhárítás – is.

5 Sok forrás a számítógép-biztonságot a hálózati biztonsággal egy kategóriának és egy területnek veszi. Például az említett Haig-műben is így szerepel a komplex információbiztonság szegmenseinek bemutatása. (Haig 2015)



57. ábra
A kiberbiztonság és a hozzá kapcsolódó területek

Forrás: KLIMBURG 2012, a szerző szerkesztése

Ezek közül elsőként a kiberbiztonság kritikus infrastruktúrák, valamint a kritikus információs infrastruktúrák területén játszott szerepét kívánjuk bemutatni. Az, hogy ezzel a területtel kezdjük a kibervédelem és kapcsolódó részeinek bemutatását, abban az egyszerű tényben keresendő, hogy ezek nélkül az infrastruktúrák nélkül nincs kibertér, valamint abban nyilvánvalóan nem működhetnek azok a rendszerek és szolgáltatások sem, amelyeket korábban bemutattunk. Ha pedig ezek nem működnek, akkor nagyon nehezen értelmezhető a 21. század társadalma. Mindezen infrastruktúrák hiányában sem a gazdaság, sem a politika, sem a kultúra, de még a védelmi rendszerek sem működnek, nem is beszélve azokról a funkciókról, amelyek ezen ágazatokon belül kapnak helyet, és játszanak fontos szerepet életünkben.

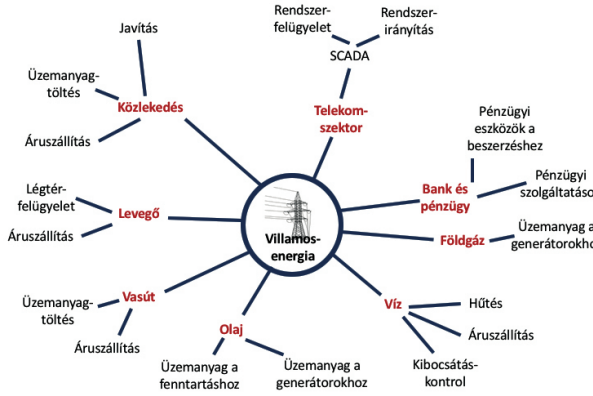
Az egyetemi előadások során, amikor a kritikus infrastruktúrák fontosságáról értekezünk, gyakran elhangzik az a kissé provokatívnak tűnő kérdés: tényleg nem tudunk ezek nélkül az infrastruktúrák nélkül élni a 21. században? Sokszor maga a kérdés is megdöbbenést kelt, majd jó esetben elgondolkodtat, hiszen a kérdés mögött az is megbújik, hogy ezekre az infrastruktúráinkra ma már olyan természetességgel tekintünk, hogy nagyon gyakran észre sem vesszük azok működését.

Esetleg akkor gondolkodunk el ezek szerepéről, amikor azok nem működnek, azaz nincs víz, nincs áram, nem lehet telefonálni, és hírekhez sem jutunk, mert sem az internet, sem a „hagyományos" médiumok (televízió, rádió) nem működnek.

3.2. Kiberbiztonság a kritikus infrastruktúrákban

Az előző fejezetek választ adtak arra, hogy az információtechnológia és az internet, valamint azok a szolgáltatások egész sora, amelyek ezekre a technológiákra épülnek, elengedhetetlenek a modern 21. századi társadalmi, gazdasági, politikai és kulturális életünk zavartalan biztosításához.

Ugyanez igaz azokra az infrastruktúrákra, azaz azokra a rendszerekre és az azok által nyújtott szolgáltatásokra, amelyek meghatározzák, és így szintén alapjait jelentik az előzőekben említett infokommunikációs rendszereknek és szolgáltatásoknak. Ezek közül az infrastruktúrák közül nagyon sok ma olyannyira nélkülözhetetlen, hogy a működésük kritikus a társadalom különböző folyamatainak ellátásához vagy biztosításához. Amennyiben ezek közül a rendszerek közül néhány kiesik, vagy működésében sérül akár időlegesen is, az beláthatatlan következményekkel jár a társadalom említett funkcióinak ellátásában. Ráadásul ma már ezek az infrastruktúrák egymással olyan kapcsolatban állnak, hogy egy-egy rendszer vagy rendszerelem kiesésének másik rendszerre gyakorolt valamennyi hatása csak nagyon nehezen jelezhető előre teljes bizonyossággal.



58. ábra
A kritikus infrastruktúrákon belüli interdependencia egy példája: a villamos-energia-szolgáltatás kapcsolatai és hatásai

Forrás: Rinaldi–Peerenboom–Kelly 2001, a szerző szerkesztése

Mindezeknek megfelelően szükséges megvizsgálni, hogy melyek ezek az infrastruktúrák, ezeket milyen veszélyek és kihívások fenyegetik, valamint hogy az egyes országok, vagy az olyan szövetség, mint az Európai Unió, hogyan szabályozzák és valósítják meg ezen rendszerek védelmét.

Ha a kiberbiztonság esetében azt a megállapítást tettük, hogy fiatal területről van szó, akkor ez igaz a kritikus infrastruktúra és a kritikus információs infrastruktúrák területeire is, hiszen ezek a fogalmak is csak néhány évtizede vannak jelen mindennapjainkban.

3.2.1. Kritikus infrastruktúrák és kritikus információs infrastruktúrák meghatározása

A jelenleg érvényben lévő – a kritikus infrastruktúrák védelmének szabályozását hivatott – jogszabályok meglehetősen jó meghatározást

adnak a *kritikus infrastruktúra* fogalmára. Bár a hazai szabályozás valamilyen rejtélyes oknál fogva a *kritikus* szót kerüli, és a *létfontosságú* kifejezést használja, úgy gondoljuk, hogy a két kifejezés szinonimaként használható. Ennek alapján a hazánkban ezen a területen áttörést jelentő 2012-ben megjelent törvény a kritikus infrastruktúra[6] esetében így fogalmaz: „meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna". (2012. évi CLXVI. tv. 1. § f. pont) Mindezeken túl a törvény meghatározza az európai értelemben vett kritikus infrastruktúra[7] fogalmát is: „a törvény alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős hatással lenne – az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve – legalább két EGT-államra". (2012. évi CLXVI. tv. 1. § c. pont)

A kritikusinfrastruktúra-védelmi törvény végrehajtási rendeleteként kiadott kormányrendelet meghatározza *a kritikus információs rendszer* és *létesítmény*[8] fogalmát is: „a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek". [65/2013. (III. 8.) Korm. rendelet 1. § 3. pont]

---

6 A törvény a *létfontosságú rendszerelem* megnevezést használja. (2012. évi CLXVI. tv. 1.§ f. pont)

7 Az európai értelemben vett kritikus infrastruktúra vonatkozásában a korábban említettekhez hasonló módon a törvény az *európai létfontosságú rendszerelem* kifejezést használja. (2012. évi CLXVI. tv. 1. § c. pont)

8 A kormányrendelet *létfontosságú információs rendszer és létesítmény* megnevezést használ. [65/2013. (III. 8.) Korm. rendelet 1. § 3. pont]

9. táblázat
A magyarországi kritikus infrastruktúra ágazatai és alágazatai

	Ágazat	**Alágazat**
1	Energia	villamosenergia-rendszer létesítményei (kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek)
2		kőolajipar
3		földgázipar
4	Közlekedés	közúti közlekedés
5		vasúti közlekedés
6		légi közlekedés
7		vízi közlekedés
8		logisztikai központok
9	Agrárgazdaság	mezőgazdaság
10		élelmiszeripar
11		elosztó hálózatok
12	Egészségügy	aktív fekvőbeteg-ellátás
13		mentésirányítás
14		egészségügyi tartalékok és vérkészletek
15		magas biztonsági szintű biológiai laboratóriumok
16		egészségbiztosítás informatikai rendszere
16a		gyógyszer-nagykereskedelem
17	Pénzügy	pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei
18		bank- és hitelintézeti biztonság
19		készpénzellátás

	Ágazat	Alágazat
26	Infokommunikációs technológiák	internet-infrastruktúra és internethozzáférés-szolgáltatás
27		vezetékes és vezeték nélküli elektronikus hírközlési szolgáltatások, vezetékes és vezeték nélküli hírközlő hálózatok
28		rádiós távközlés
29		űrtávközlés
30		műsorszórás
31		postai szolgáltatások
32		kormányzati informatikai, elektronikus hálózatok
33	Víz	ivóvíz-szolgáltatás
34		felszíni és felszín alatti vizek minőségének ellenőrzése
35		szennyvízelvezetés és -tisztítás
36		vízbázisok védelme
37		árvízi védművek, gátak
38	Jogrend – Kormányzat	kormányzati rendszerek, létesítmények, eszközök
39		közigazgatási szolgáltatások
40		igazságszolgáltatás
41	Közbiztonság – Védelem	rendvédelmi szervek infrastruktúrái
42	Honvédelem	honvédelmi rendszerek és létesítmények

Forrás: 2012. évi CLXVI. tv. 1., 2., 3. mellékletek, a szerző szerkesztése

A kritikusinfrastruktúra-védelem hazai története

A kritikusinfrastruktúra-védelem jogszabályi kereteinek kidolgozása során az első jelentős mérföldkövet a 2008-as év jelentette. Ekkor jelent meg a *Kritikus Infrastruktúra Védelem Nemzeti Programról* szóló (2080/2008. számú) kormányhatározat. Maga a jogszabály, mindamellett, hogy nagyon sok általánosságot tartalmazott – ez a tény is utal arra a kompromisszumos munkára, amely az jogszabály elfogadásával együtt járt –, nagyon előremutató volt, hiszen ez a dokumentum tartalmazta elsőként hazánkban a kritikus infrastruktúra ágazatainak és alágazatainak felosztását. A védelem kialakítása során a következő nagy állomás a katasztrófavédelmi törvény *(A katasztrófavédelemről és a hozzá kap-*

csolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény) megjelenése volt 2011-ben, amely többek között megteremtette a jelenleg is működő szervezeti hátteret a kritikusinfrastruktúra-védelemhez azzal, hogy egyrészt létrehozta az Országos Katasztrófavédelmi Főigazgatóságot, másrészt ezen belül a három pillérre épülő katasztrófavédelemben – a tűzoltóság, a polgári védelem mellett – kialakította az iparbiztonság szervezetrendszerét, amely felügyeli a kritikus infrastruktúrákat. Ezt követően 2012-ben jelent meg a *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről* (röviden kritikusinfrastruktúra-védelmi törvény), amely valóban teljes spektrumban teremtette meg a kritikus infrastruktúra hazai védelmének törvényi hátterét úgy, hogy a szabályozás kiterjed a szervezeti háttérre, valamint a felelősségi körökre egyaránt. Természetesen e törvény vonatkozásában is szükség volt egy olyan pontosító, a részletes szabályokat lefektető – alacsonyabb szintű – jogszabályra, amely a mindennapi munkát és feladatokat is képes szabályozni. Ez a kritikusinfrastruktúra-védelmi törvény 2013-ban megjelent végrehajtási rendelete, azaz a *65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról*. Mindezek alapján világosan látszik az a komoly és meglehetősen gyors fejlődés, amely hazánkban az Európai Unió jogszabályi környezetével párhuzamosan, nyilván annak hatására, a kritikus infrastruktúra védelmének területén nyomon követhető.

A hazai kritikusinfrastruktúra-védelem jogszabályi kereteinek kidolgozása kronologikus sorrendben:

2008: 2080/2008. (VI. 30.) Korm. határozat A Kritikus Infrastruktúra Védelem Nemzeti Programról

2010: 1249/2010. (XI. 19.) Korm. határozat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról

2012: 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2013: 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.

A fentiekben láthattuk, hogy a kritikus infrastruktúra ágazatokra és alágazatokra történő felosztása viszonylag korán megtörtént hazánkban is. Azonban ezen a területen az egyik legnagyobb problémát és kihívást az jelenti, hogy milyen módon, és nem utolsósorban milyen kritériumok mentén, illetve milyen módszerekkel történik egy-egy infrastruktúra azonosítása. (Haig et al. 2009)

Ez leegyszerűsítve nem jelent mást, mint azoknak a kritériumoknak a meghatározását, amelyek alapján eldönthető, hogy egy infrastruktúra, illetve annak egyik eleme kritikus-e vagy sem. Persze még ekkor is komoly kérdésként merülhet fel a besorolást vagy az azonosítást végző szubjektív nézőpontja, hiszen nem minden infrastruktúra tekinthető ugyanolyan fontosnak, azaz kritikusnak az összes – helyi, regionális, állami stb. – szinten.

Mindezeket a kritikus infrastruktúrák azonosítása és besorolása érdekében nélkülözhetetlen elveket és az azok alkalmazásához szükséges kritériumokat határozza meg és fekteti le a már említett 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.

E kormányrendelet alapján az azonosítás „az a folyamat, amely során a lehetséges létfontosságú rendszerelemeket kockázatelemzés, valamint az ágazati és horizontális kritériumok alapján meghatározzák". [65/2013. (III. 8.) Korm. rendelet 1. § 1. pont]

Nyilvánvalóan az azonosításhoz, illetve a besoroláshoz fel kell mérni az adott rendszerrel vagy rendszerelemmel szemben megjelenő kockázatokat. Ez tehát kockázatelemzést igényel, amely szintén az említett kormányrendelet megfogalmazásában nem jelent mást, mint „fenyegetettségi és kockázati tényezők vizsgálata a rendszerelemek sebezhetőségének, valamint a megzavarásuk vagy megsemmisítésük által okozott következmények értékelése céljából." [65/2013. (III. 8.) Korm. rendelet 1. § 2. pont]

A kormányrendelet nagyon világosan és egyértelműen meghatározza az említett – az azonosítás folyamatában szükséges – kritériu-

mokat is, amelyek egy vagy egymással közvetlenül összefüggő eseményekkel kapcsolatban Magyarország területére vonatkoztatva öt fő kritériumcsoportot fogalmaznak meg: a veszteségek kritériumát, a gazdasági hatás kritériumát, a társadalmi hatás kritériumát, a politikai hatás kritériumát, valamint a környezeti hatás kritériumát. Ezek – idézve a jogszabályt – a következőket tartalmazzák részleteikben:

A veszteségek kritériuma:

- 24 óra leforgása alatt az áldozatok száma a 20 főt meghaladja, vagy a súlyos sérültek száma legalább 75 fő, vagy
- 72 óra leforgása alatt az áldozatok száma a 40 főt meghaladja, vagy a súlyos sérültek száma legalább 150 fő.

A gazdasági hatás kritériuma: a gazdasági veszteség mértéke vagy termékek és szolgáltatások romlásának mértéke, a rendszer és létesítmény fizikai sérüléséből, elvesztéséből fakadó közvetlen vagy közvetett károk, amelyek ötvenezer fő vonatkozásában meghaladják az egy főre eső bruttó nemzeti jövedelem (GNI) bármely 30 napos időszakra vetített mértékének 25%-át.

A társadalmi hatás kritériuma: 300 fő/km^2-nél sűrűbben lakott területen a köznyugalom súlyos megzavarása, beleértve a lakosságot érő káros pszichológiai és közegészségügyi hatásokat is.

A politikai hatás kritériuma: az állam és intézményei iránti közbizalom megszűnése, valamely állami szerv működésképtelenné válása miatt a lakosság biztonságérzete kritikus szint alá csökken.

A környezeti hatás kritériuma: az az esemény vagy folyamat, amely miatt a természeti vagy épített környezetben különösen:

- az infrastruktúrában bekövetkező sérülés vagy zavar, az épített vagy természetes környezet oly mértékű rongálódását idézi elő, amelynek következtében
  - 10 ezer fő kimenekítése vagy kitelepítése válik szükségessé, vagy
  - legalább 100 km^2 nagyságú terület tartósan szennyeződik, vagy

  - a felszín alatti vizek vagy azok természetes víztartó képződményei, a folyóvizek és természetes tavak, valamint ezek medre vagy élővilága szenved tartós károsodást;
- az ország tájegységeiben, kiemelkedő földrajzi területeiben visszafordíthatatlan negatív változás következik be. [65/2013. (III. 8.) Korm. rendelet 1. melléklet]

A hazai kritikusinfrastruktúra-védelem szorosan illeszkedik az Európai Unió ezen a területen kialakított irányelveihez. Az EU kritikusinfrastruktúra-védelmi tevékenységét, amelyről mindenképpen érdemes megjegyezni, hogy a 2000-es évek elején kezdődött, külön kiemelve is bemutatjuk. Ebben a tevékenységben az egyik legjelentősebb lépés 2006-ban következett be, amikor megjelent az EU úgynevezett EPCIP-programja, azaz az European Programme for Critical Infrastructure Protection (EPCIP), magyarul a Kritikusinfrastruktúra-védelem Európai Programja. Nagyon fontos annak hangsúlyozása, hogy hasonlóan sok más területhez a kritikus infrastruktúrák védelmét az Európai Unió tagállami hatáskörben tartja, azaz minden tagállamnak magának kell gondoskodnia a saját infrastruktúráinak védelméről. Az Európai Unió ebben koordináló, felügyelő és tanácsadó szerepet tölt be.

Ugyanakkor az Európai Unió jogalkotói tevékenysége ezen a területen is nagyon konzekvens, amit egy egységes rendszerben kell elképzelni. Ebbe illik bele a kritikus infrastruktúrákkal kapcsolatos szabályozás is, amely összhangban van a 2015-ben megjelent *Európai Biztonsági Menetrenddel*[9] (European Commission 2015c), az *Egységes Digitális Piaci Stratégiával* (European Commission 2015b), valamint a *Kiberbiztonsági Stratégiával* (Cybersecurity Strategy of the Euro-

[9] Az Európai Biztonsági Menetrend 2015−2020 az Európai Bizottság politikai irányelveit fordítja le végrehajtható ackiótervekké az európai biztonság megteremtése érdekében. (European Commission 2015c)

pean Union 2013) Mindezeken túl a *NIS*[10] (NIS Directive 2016) irányelve is tartalmaz olyan utalásokat, amelyek a kritikus infrastruktúrákra vonatkoznak. Ez utóbbi direktíva 2018 májusában életbe lépve, bár közvetlenül nem a kritikus infrastruktúrákra vagy a kritikus információs infrastruktúrákra vonatkozik elsősorban, a kiberbiztonság megteremtésével, illetve annak növelésével közvetett módon hozzájárulhat a kritikus információs infrastruktúrák védelméhez is. (Deighton 2017)

A NIS alapvető szolgáltatásokat nyújtó szereplőket határoz meg, amelyek a következő kritériumoknak megfelelő közjogi vagy magánjogi szervezetek: „a szervezet a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt; az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ; és az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában". (NIS Directive 2016 5. cikk 2. pont) Az irányelv ezeket a szolgáltatásokat – hasonlóan a kritikus infrastruktúrákhoz – ágazatokra és alágazatokra osztja. Ezek a következő táblázatban láthatóak.

10. táblázat

A NIS-direktíva által meghatározott alapvető szolgáltatásokat nyújtó szereplők

Ágazat	**Alágazatok**
Energia	a) Villamos energia b) Kőolaj c) Földgáz
Közlekedés	a) Légi közlekedés b) Vasúti közlekedés c) Vízi közlekedés d) Közúti közlekedés

[10] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről. (NIS Directive 2016)

Ágazat	Alágazatok
Banki szolgáltatások	
Pénzügyi és piaci infrastruktúrák	
Egészségügy	Egészségügyi ellátó létesítmények (beleértve a kórházakat és a magánklinikákat is)
Ivóvízellátás és -elosztás	
Digitális infrastruktúra	IXP-k DNS-szolgáltatók TLD-névnyilvántartók

Forrás: NIS Directive 2016 II. melléklet, szerkesztette: szerző

Azt is látnunk kell, hogy a kritikus infrastruktúrákon belül már a szabályozásról való első egyeztetések során megjelenik az infokommunikációs szektor mint kritikus ágazat, azonban a kritikus információs infrastruktúrákról külön nem született direktíva, bár azt el kell ismerni, hogy az EU létrehozta és folyamatosan működteti az ENISA-t (European Union Agency for Network and Information Security, azaz az Európai Uniós Hálózat- és Információbiztonsági Ügynökséget), amelynek egyik fő feladata a kiberbiztonság különböző kérdéseinek, így a kritikus infrastruktúrák és kritikus információs infrastruktúrák területeinek koordinációja. Az ENISA-ról mint az EU egyik legfontosabb kiberbiztonsági szervezetéről külön is szólunk a későbbiekben.

A kritikusinfrastruktúra-védelem európai uniós története

A 2000-es évek elején az Európai Unióban többször napirendre került a kritikus infrastruktúrák kérdése, de az első kézzelfogható lépés csak 2004-ben történt, amikor az Európai Bizottság (2004. október 20-án) közleményt fogadott el *A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben* címmel. (European Commission 2004)

Ebben a közleményben található meg első ízben a bizottság által tett kritikusinfrastruktúra-meghatározás, amely szerint: „A kritikus infrastruktúrák magukban foglalják mindazon fizikai és információs tech-

nológiai létesítményeket, hálózatokat, szolgáltatásokat és eszközöket, amelyek megzavarása vagy pusztítása komoly hatással lenne az állampolgárok egészségére, biztonságára, gazdasági jólétére, vagy közvetlen hatással lenne a tagállamok kormányzati működésére." (European Commission 2004)

Ugyanakkor ez a dokumentum a 2004-ben és 2005-ben bekövetkezett terrortámadásokban fogalmazta meg a fő veszélyforrásokat.

A következő nagy lépés 2005-ben történt, amikor az Európai Bizottság közzétette az úgynevezett *Zöld Könyvét.* (European Commission 2005) A dokumentum már megnevezi azt a 11 szektort és 37 terméket (szolgáltatást), amely az európai kritikus infrastruktúrák felosztását jelenti.

Ugyanakkor a területen az igazi áttörés 2006-ban következett be, amikor is az Európai Bizottság elfogadta és kiadta az *European Programme for Critical Infrastructure Protection (EPCIP),* azaz *a Kritikus-infrastruktúra-védelem Európai Programját.* (European Commission 2006)

Az EPCIP lefektette a kritikus infrastruktúrák védelmének növelését célzó minden olyan tevékenységnek az általános kereteit, amelyek az EU minden tagországára, valamint minden ágazatra érvényesek. A korábbi irányelvektől eltérően az EPCIP már nemcsak a terrorizmust tekintette fő fenyegetésnek, hanem az egyéb bűncselekményeket, illetve a természeti és ipari katasztrófákat is idesorolta. Mindezeken túl a program úgynevezett CIP kapcsolattartó pontokat is meghatározott, amelyek alapján rendszeres információcsere vált lehetővé az EU-tagállamok között. (European Commission 2017g)

Az EPCIP-t 2008-ban egy olyan direktíva követte, amely valójában a program végrehajtási utasításaként fogható fel. (2008/114/EC)

A *Directive on European Critical Infrastructures (ECI),* azaz *az Európai Kritikusinfrastruktúra-direktíva* alapvető célja azoknak az eljárásoknak a létrehozása és kialakítása volt, amelyek alapján az európai kritikus infrastruktúrák azonosítása és kijelölése, valamint a védelem értékelése elvégezhető. Az irányelv azonban csak az energia- és közlekedési ágazatra vonatkozik, bár ebben az ágazatban kijelölt kritikus infrastruktúra tulajdonosai és üzemeltetői számára biztonsági tervek előkészítését írja elő, valamint meghatározza úgynevezett biztonsági összekötők kijelölését, akik a tulajdonos vagy üzemeltető kapcsolatát biztosítják a kritikus infrastruktúrák védelméért felelős nemzeti hatósággal. (European Commission 2017g)

Mindezeken túl az Európai Bizottság javaslatot fogadott el egy olyan információs hálózat létrehozásáról, amely a tagországok kritikus infrastruktúrákat érintő kommunikációját hivatott segíteni. Ez a hálózat a *Critical Infrastructure Warning Information Network (CIWIN),* azaz a *Kritikus infrastruktúrák figyelmeztető információs hálózata* nevet kapta. A CIWIN az EPCIP részévé vált annak elfogadásakor. (European Commission 2008)

Az Európai Unió kritikusinfrastruktúra-védelem jogszabályi kereteinek kidolgozása kronologikus sorrendben:

2004: Critical Infrastructure Protection in the Fight against Terrorism. (European Commission 2004)

2005: Zöld könyv egy kritikusinfrastruktúra-védelmi európai programról. (European Commission 2005)

2006: European Programme for Critical Infrastructure Protection – EPCIP. (European Commission 2006)

2008: Directive on European Critical Infrastructures – ECI. (European Commission 2008)

3.2.2. Kritikus infrastruktúrák és kritikus információs infrastruktúrák támadhatósága

Korábban már számos példát említettünk a kibertér olyan veszélyforrásairól, amelyeken keresztül közvetlenül, vagy ahogy a Stuxnet példája is bizonyítja, közvetett módon lehetséges a kritikus infrastruktúrák, ezeken belül is nyilvánvalóan a kritikus információs infrastruktúrák támadása.

Bár feltételezhetően nem a Stuxnettel elkövetett támadás volt az egyetlen kibertérből érkező ipari rendszereket ért támadás az el-

múlt évtizedekben,[11] mégis ez volt az első olyan nagy művelet, amely a kiberbiztonsági szakmán kívül a nemzetközi politikai életben is komoly visszhangot váltott ki.

Ahogy a Stuxnet esetében is utaltunk rá, alapvetően az olyan politikai, gazdasági vagy katonai konfliktusokkal párhuzamosan, mint a Stuxnet esetében az iráni atomprogram volt, jelennek meg ezek a nagy anyagi befektetéssel és nagy előkészületekkel járó, a kibertérből indított kritikus infrastruktúrákat célzó támadások. Ennek oka természetesen nagyon is egyszerű: a kritikus infrastruktúrákon keresztül, függően a támadások kiterjedtségétől, illetve azok volumenétől (azaz melyik kritikus rendszert és milyen módon támadnak), egy adott ország gazdasága és társadalma nagymértékben befolyásolható.

Nyilvánvaló, hogy a kiberbűnözés csakúgy, mint a korábban szintén említett állami támogatású kibertámadók, kitűnő terepet lát a kritikus infrastruktúrákban, illetve a kritikus információs infrastruktúrákban, hiszen még ha komoly károkat nem is okoz ezen rendszereknek, illetve azok egyes elemeinek támadásával, a destabilizáció, azaz az állam vagy a társadalom normál működésének a megbontása mindig azzal jár, hogy ott a bűnözés teret nyer és erőre kap, hiszen nincs, vagy nem működik megfelelő hivatalos kontroll. Ugyanez igaz abban az esetben, ha államilag támogatott támadásokról beszélünk, hiszen egy másik ország destabilizálása így sokkal kisebb energiabefektetéssel jár, amely során akár a lakosság, akár az adott ország egyes politikai erői könnyen befolyásolhatóak.

---

[11] Korábban sokáig tartotta magát az a vélemény, hogy az 1982 júniusában bekövetkezett transzszibériai gáz- és olajvezeték-robbanást egy, a létesítmény SCADA-rendszereibe történő CIA-beavatkozás okozta. Ennek megfelelően ezt tekintették sokáig az első olyan „kibertámadásnak", amely ipari létesítményt célzott. Ezt a teóriát azonban Jeffrey Carr blogjában erősen megkérdőjelezi. (Carr 2012) A szerzőről tudni kell, hogy számos műve jelent meg a kiberbiztonság és kiberhadviselés témában, köztük az eredetileg 2009-ben kiadott, majd 2011-ben már második kiadást megért *Inside Cyber Warfare: Mapping the Cyber Underworld* (amely magyar címe talán a következő lehetne: *A kiberhadviselés belülről: a kiber alvilág feltérképezése*) világszerte ismert könyve. (Carr 2011)

A kritikus infrastruktúrákban rejlő egyik legnagyobb kihívás az, hogy azokban a régi és az új rendszerek egyszerre vannak jelen. Különösen igaz ez a későbbiekben részletesen bemutatni és elemezni kívánt SCADA (Supervisory Control and Data Acquisition, azaz felügyeleti, irányító és adatgyűjtő) rendszerek esetében. Ráadásul a kritikus infrastruktúrákon belül a régi és az új rendszerelemek használata az energiaszektorban a leglátványosabb, hiszen az új technológia alkalmazása a költséghatékonyabb energiaelőállítás, -tárolás és -szállítás esetében egyre inkább a fontos szempontok és a prioritások elején található. Ezt támasztja alá az EU egyik szakértői csoportjának – a kiberbiztonság az energiaszektorban platform (Energy Expert Cyber Security Platform [EECSP] – Expert Group) – 2017. év elején született jelentése is, amelyben megállapítják, hogy az említett új technológiák olyan intelligens komponenseket (például mérőberendezések, digitális szelepek, szivattyúk) jelentenek, amelyek már kommunikációs megoldásaikban is különböznek a korábbi technológiától, hiszen már nemcsak egyirányú vezetékes kommunikációt, hanem kétirányú, illetve vezeték nélküli adatkapcsolatokat is használnak. Ennek megfelelően az analóg rendszereket, illetve rendszerelemeket egyre inkább digitális rendszerek váltják fel. (ECCS 2017)

Az említett szakértői csoport tíz olyan területet azonosított, amelyek kiberbiztonsági vetületű kihívások lehetnek az energiaszektoron belül. Ezek a kihívások a határokon átnyúló villamosenergia-átviteli hálózatok stabilitási problémái; a releváns fenyegetéseket és veszélyeket tartalmazó védelmi koncepciók; a kibertámadások kezelése az EU-ban; a villamosenergia-rendszer és a nukleáris létesítmények elleni kibertámadások kezelésének nem teljesen kidolgozott szabályai; új technológiák és szolgáltatások megjelenése, illetve bevezetése; az infrastruktúrák és a szolgáltatások kiszervezése; az energiarendszerekben használt elemek integritása; a piaci szereplők közötti kölcsönös és egyre növekvő függőség; valamint a kiberbiztonsági intézkedések és a valós idejű szolgáltatás és rendelkezésre állás közötti ellentmondás. (ECCS 2017)

Az azonosított kihívások és veszélyek mindegyike erős kapcsolatot mutat a kibertérrel, ami tovább erősíti azt, hogy a kritikus infrastruktúrákon belüli kiberbiztonság megvalósítása elemi érdeke kell hogy legyen minden infrastruktúra-tulajdonosnak és üzemeltetőnek.

A kritikus infrastruktúrák elleni támadások lehetséges forgatókönyvei

2009-ben készítettük el, majd 2010-ben jelent meg a *Digitális Mohács* című forgatókönyvünk. A forgatókönyv elkészítése mögött lévő okok nagyon egyszerűek, de nagyon markánsak voltak, ugyanis, ahogy korábban itt is utaltunk rá, a kritikusinfrastruktúra-védelem területén hazánkban nem, vagy csak nagyon visszafogott lépések születtek 2009-ig. Pedig már akkor is nyilvánvaló volt, hogy olyan mértékben függünk az infrastruktúráinktól, hogy azok biztonsága érdekében egy kormányzatilag felügyelt koordinált védekezés elengedhetetlen. (Kovács–Krasznay 2010)

A Digitális Mohács szcenárió egy gondolatkísérlet volt, azaz elképzelt eseményeket és azok egymásra és az országra (lakosság, gazdaság, politika) gyakorolt hatásait vázoltuk fel. Ezeket az elképzelt eseményeket Magyarország kritikus infrastruktúrái, valamint kritikus információs infrastruktúrái ellen elkövetett különböző támadási módszerekkel írtuk le. Megvizsgáltuk, hogy a hazai kritikus információs infrastruktúrákat ért esetleges támadásoknak milyen következményei lehetnek.

A forgatókönyv célja – az annak elkészítése mögött rejlő okokhoz hasonlóan – rendkívül egyszerű volt. Arra a tényre kívántuk felhívni a figyelmet, hogy Magyarország esetében is igaz az, hogy nem túlságosan bonyolult eszközökkel gyakorlatilag bárki végre tud hajtani olyan támadásokat, amelyek célpontjai az általunk is kiválasztott legfontosabb infrastruktúrák közül kerülnek ki, és amelyek kiesése beláthatatlan következményekkel jár az ország egészére nézve. A forgatókönyv meg-

írásakor alapvető tényként kezeltük, hogy a célpontként kiválasztott infrastruktúrák vagy azok egyes elemeinek üzemeltetői mindent megtesznek a védelem érdekében. A problémát abban azonosítottuk, hogy ha párhuzamos, azaz több infrastruktúrát egyszerre érő támadások következnek be, akkor koordinált – és itt a koordináció alatt elsősorban az állami szerepvállalást kell érteni – védekezés hiányában az üzemeltetők pont az intra- és interdependenciákból következően nem, vagy csak részben ismerik fel a támadások mibenlétét, volumenét és azok okait. Ebben az esetben nagy valószínűséggel a védelmi akcióik és tevékenységeik hatástalanok lesznek, mert az okokat, azaz a támadások kiindulópontjait nem, csak az okozatokat lesznek képesek kezelni.

A szcenárióhoz csak nyílt forrásokból, alapvetően az internetről gyűjtöttünk információkat. Ugyanakkor az ilyenfajta információgyűjtésből eredő veszélyekre korábban már többször is felhívtuk a figyelmet, hiszen a nyíltan rendelkezésre álló és szabadon elérhető információk segítségével bárki olyan releváns és valóban jól használható tudás birtokába kerülhet, amely alapján egy-egy infrastruktúra a legaprólékosabban feltérképezhető, beleértve annak sérülékeny és támadható pontjait is.

A forgatókönyv felépítése során egymást követő, illetve egymással időben kisebb átfedésben lévő támadásokat írtunk le. Ez a támadássorozat egy pszichológiai műveleti kampánnyal indul, amelyet különböző kritikus infrastruktúraelemek ellen elkövetett informatikai, valamint kisebb mértékű fizikai támadások követnek. A pszichológiai műveletek során a lakosság befolyásolása volt a cél. Ennek során az elektronikus médiumok informatikai támadásával, azokban valótlan híreket elhelyezve az álhírekkel a lakosságot kívántuk befolyásolni. Ezt követte a földfelszíni műsorszórás korlátozása vagy megszüntetése, majd az álhírekkel elárasztott internetes hírportálokkal a befolyásolás fokozása. Az álhírek a bankrendszer összeomlását vetítették előre, amely hírek nem csak hazánkban alkalmasak arra, hogy pánikot keltsenek nagy tömegekben. Ezt az előkészítő szakaszt a konkrét támadási fázis felvázolása követte, amely során elsőként az internet támadhatóságát,

valamint annak sikere esetén a következményeket vizsgáltuk. Ezekkel a támadásokkal párhuzamosan a közlekedés különböző elemeinek támadhatóságát vázoltuk fel. Megvizsgáltuk a budapesti tömegközlekedés, majd a légi közlekedés támadásának egyes megoldásait. Mindezeken túl a villamosenergia-rendszer támadását irányoztuk elő, hiszen ez az egyik legfontosabb kritikusinfrastruktúra-ágazat. Enélkül nagyon nehéz elképzelni a többi ágazat működését. A forgatókönyv elkészítésekor végzett vizsgálataink alapján arra a következtetésre jutottunk, hogy tisztán informatikai támadásokkal csak részlegesen lehet kárt okozni a villamosenergia-szolgáltatásban. Az igazi károkozáshoz – akár az internetről szerzett információk segítségével – viszont fizikai támadások is szükségesek. Ezekkel a hazai villamosenergia-rendszer működése is korlátozható. A villamosenergia-rendszer ilyen módszerekkel történő támadásaiból, illetve azok elképzelt következményeiből azt a nem túl eredeti következtetést is levontuk, hogy ezek a támadások okozhatják a legnagyobb rendszerkieséseket, amelyek ráadásul a szolgáltatások összekapcsolása miatt nemcsak hazánkban, hanem akár az egész régióban olyan áramkimaradásokat eredményezhetnek, amelyek következményei jóval túlmutatnak az elképzelt forgatókönyvünkön. (Kovács–Krasznay 2010)

Az első Digitális Mohács forgatókönyvet, illetve az abból levonható tanulságokat azóta folyamatosan megjelenítjük az egyetemi szintű oktatásban is, hiszen a bemutatott példákon keresztül a kritikus infrastruktúrák és a kritikus információs infrastruktúrák védelmének szükségessége nyilvánvalóvá vált.

Az első forgatókönyvet 2016-ban egy második elképzelt szcenárió, illetve az arra épülő vizsgálatok követték. A *Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint* című forgatókönyvben négy támadási fázist képzeltünk el, amelyek egymást követve szintén a hazai – információs rendszerekre épülő – kritikus információs infrastruktúrákat célozzák meg. A támadási fázisok sorát itt is a pszichológiai műveletek nyitják, benne internetes hamis hírekkel, azok széles körű terjesztésével. A második fázisban látványos

informatikai támadásokat, benne DDoS-támadásokat vázoltunk fel, majd a harmadik fázisban a politika befolyásolására mutattunk be módszereket. Az utolsó, azaz a negyedik támadási fázist a konkrét infrastruktúrák elleni támadásokban határoztuk meg, amely az első forgatókönyv tapasztalataira is építve a villamosenergia-rendszer elleni tevékenységet emelte ki. (Kovács–Krasznay 2017)

Ellentétben az első forgatókönyvvel, itt nem a támadások következményeinek bemutatása volt a fő célunk, hanem annak felmérése, hogy a szakma képviselői, azaz az információbiztonsági szakemberek hogyan reagálnának egy-egy támadásra, és milyen válaszokat adnának azokra. A válaszadás megkönnyítésére minden támadási fázis esetében megjelöltünk négy lehetséges tevékenységet mint választ.

Összességében a szakértőktől kapott vélemények alapján megállapítottuk, hogy a Digitális Mohács 2.0 forgatókönyvben szereplő támadások reálisak, és azok meg is valósíthatók. Ez alátámasztja azt a korábban már többször hangsúlyozott tényt is, hogy a kritikus infrastruktúráinkkal, ezen belül is a kritikus információs infrastruktúráinkkal szemben fennálló függőségünk továbbra is megköveteli azok koordinált és centralizált védelmét. Összességében megállapíthattuk, hogy a Digitális Mohács 2.0 esetén felvázolt forgatókönyvünkben a támadások intenzitását növelve a szakemberek is egyre inkább az államilag szervezett és felügyelt (koordinált) védekezést jelenítették meg, kiemelve ebben a hazai Nemzeti Kibervédelmi Intézet szerepét. (Kovács–Krasznay 2017)

A kritikus infrastruktúra elleni támadás megvalósult forgatókönyve: Ukrajna esete a BlackEnergyvel

2015. december 23-án egy az ukrán regionális villamosenergia-elosztó és villamosenergia-átviteli vállalat, a PJSC Kyivoblenergo (KOE) rendszereiben komoly üzemzavar keletkezett. A szolgáltatásokban jelentkező kiesések oka már az első néhány órában világossá vált: a cég szá-

mítógépeibe és SCADA-rendszereibe valaki behatolt. A rendszerekbe behatolók helyi idő szerint délután 3 óra 35 perckor hét 110 kV-os, valamint huszonhárom 35 kV-os alállomást kapcsoltak le. Ezek miatt a szolgáltatásokban keletkezett zavar több mint három órán keresztül tartott. (SANS 2016)

A későbbi elemzések után kiderült, hogy az elosztó hálózat más számítógépeibe, sőt más villamosenergia-vállalatok rendszereibe is bejutottak a támadók. Összesen hat ilyen céget azonosítottak a későbbi vizsgálatok. A villamosenergia-átviteli rendszerben bekövetkezett kiesés miatt közel 225 ezer fogyasztó nem jutott áramhoz többek között Ivano-Frankivszk, Gorodenkovszkij, Kalush, Dolinszk, Tysmenytsia, Nadvirna és Jaremcse területeken. A szolgáltatók a helyzet normalizálása érdekében kénytelenek voltak kézi vezérlésre váltani. (SANS 2016)

Az ukrán média rögtön az események után arról adott hírt, hogy a támadók nagy valószínűséggel Oroszországból követték el a támadásokat. Az ukrán hivatalos hírügynökség meg is nevezte a támadókat, amikor *Orosz hackerek az energiarendszer felforgatását tervezik Ukrajnában* szalagcímmel adott ki közleményt nem sokkal a támadások után. A közlemény az Ukrán Biztonsági Szolgálat[12] (SBU) rövid sajtóközleményére épült, amelyben az SBU olyan rosszindulatú szoftverek felfedezéséről adott hírt, amelyeket az ukrán villamosenergia-szolgáltatók számítógépein találtak. (Ukrinform 2015)

A SANS későbbi elemzése megállapította, hogy a támadók egész sor szofisztikált eszközt és eljárást alkalmaztak a támadás során. Többek között használták a célzott phishingtámadásokat, a BlackEnergy három malware-ét és azok különböző változatait, valamint kompromittált Microsoft Office dokumentumokat alkalmaztak, amelyek tartalmazták a kártevőket. A támadások módjai és eszközei arra engedtek következtetni, hogy az elkövetők nagyon jól ismerték az ipari vezérlőrendszer (Industrial Command System, ICS) hálózatainak technikai

[12] Az ukrán biztonsági szolgálat hivatalos megnevezése: Служба Безпеки України (СБУ).

felépítését, de emellett olyan területeken is nagy szakértelemmel rendelkeztek, mint az ICS-ek humán felügyeleti rendszere. A SANS elemzése arra is utal, hogy a támadók számos egyéb képességükről is tanúbizonyságot adtak, hiszen olyan e-maileket írtak, amelyek nemcsak hogy egészen hihetőek voltak, de a célzott adathalász-támadások során az energiaipari cégek alkalmazottai meg is nyitották ezeket. A támadók még a telefonrendszerekbe is behatoltak, hiszen olyan megoldásokat is használtak, amelyek telefonhívásokkal – phone-flooding – árasztották el a szolgáltatók technikai helpdeskjeit, így a valódi hibabejelentések nem jutottak el hozzájuk. Mindezeken túl a támadók VPN-eket használtak az ICS-rendszerek elérésére, valamint korábban számos felhasználó adatát ellopták a hálózatokba való behatolás érdekében. A támadások során az elkövetők behatoltak a távoli elérést biztosító eszközökbe, amelyekkel a távvezérelhető ipari hálózati eszközöket – például a terhelosztó alállomásokat – kompromittálták, és így kapcsolták le azokat. A helyi hálózat adatátviteli eszközeiben egészen firmware-szintig jutottak el. Használták a Disakil nevű trójai módosított változatát (Symantec 2016), amelynek fő célja a célpont rendszerében a master boot record módosítása, valamint számos Windows log fájl manipulálása vagy törlése volt. (SANS 2016)

BlackEnergy

A Kaspersky meghatározása szerint a BleckEnergy egy olyan trójai program, amelyet DDoS-támadásokra, kiberkémkedésre és olyan más kibertámadásokra használnak, ahol a cél az információ megsemmisítése.

A trójait eredetileg egy Cr4sh nevű programozó készítette, aki miután 2007-ben befejezte annak fejlesztését, eladta a szoftver forráskódját. Elemzések szerint a programot 2008-ban a Grúzia elleni DDoS-támadások során már használták. (Kaspersky 2016)

A BlackEnergy SCADA specifikus változataival (pluginjeivel) feltételezhetően 2014-ben kezdték az ipari vezérlőrendszereket támadni. Ez is bizonyítja azt, hogy a BlackEnergy, illetve az ezt használó támadók jóval tapasztaltabbak egy átlagos támadást (például DDoS-t használó) elkövetőknél. A Kaspersky azonosított egy BlackEnergy APT-csoportot, amely 2015 közepe óta aktívan használja a spearphishing támadásokat. Ennek

során makróvírusos Excel-dokumentumokat használtak arra, hogy megfertőzzék a számítógépeket egy célzott hálózatban. Azonban 2016 januárjában a Kaspersky Lab kutatói egy új, rosszindulatú dokumentumot fedeztek fel, amely a rendszert BlackEnergy trójai programokkal fertőzi meg. A korábbi támadásokban használt Excellel ellentétben ez egy Microsoft Word dokumentum. A fájl megnyitásakor a felhasználó egy párbeszédpanelt kap, amely a dokumentum megtekintéséhez makrók engedélyezését kéri. A makrók engedélyezése aktiválja a BlackEnergy fertőzést a felhasználó számítógépén. (Kaspersky 2017)

Mindezek arra engednek következtetni, hogy az elkövetők a támadásokat megelőzően – megfelelő anyagi, technikai és nem utolsósorban politikai támogatással a háttérben – komoly felderítő munkát végezhettek. Ennek során nemcsak az ukrán energiaszektor egyes technikai elemeit térképezték fel, hanem olyan információgyűjtést is végeztek, amelyek során az energiaellátó vállalatok vezetőiről, vezető mérnökeiről és kulcsfontosságú munkatársairól gyűjtöttek adatokat.

Ezt támasztja alá a SANS elemzése is, amelyben hivatkozva az USA Belbiztonsági Minisztériuma ICS-CERT-jének elemzésére, megállapítja, hogy a támadók számos nyílt forrás felhasználásával (is) végezhették a felderítő tevékenységüket. Olyan, interneten nyíltan elérhető források álltak rendelkezésükre, amelyekben többek között az ICS-rendszereket gyártó cégek tették közzé azoknak a távoli elérést biztosító terminálóknak (Remote Terminal Unit, RTU) a típusát és verziószámát ismertetve, amelyeket az ukrán villamosenergia-elosztó cégeknek szállítottak. (SANS 2016; ICS-CERT 2016)

Itt mindenképpen utalnunk kell arra a figyelmeztetésünkre, amelyet a Digitális Mohács szcenáriók esetén tettünk. Ez pedig a helytelenül értelmezett információszabadság. Számos olyan információ vagy információrészlet van, amelyek a kritikus infrastruktúrák esetében az átláthatósággal szemben inkább annak veszélyeztetését jelenthetik. Ezek az információk – mint ahogy az ukrán példánál is látjuk – inkább jelentenek fenyegetést és veszélyt, semmint valami pozitív dolgot.

Ezeknek a kritikus információknak a védelme ugyanolyan fontos szerepet játszik a kritikus infrastruktúrák védelmében, mint például a fizikai védelem.

A 2015-ös ukrajnai eset kapcsán szintén meg kell jegyeznünk, hogy bár nincsenek megcáfolhatatlan bizonyítékok arra, hogy valóban Oroszország áll az ország energiaszektorát ért támadások mögött, mégis nagy a valószínűsége, hogy egy olyan állami támogatású kibertámadás tanúi lehettünk, amely politikai indíttatású volt, ráadásul a 2015-ös decemberi támadásokat 2016 decemberében újabbak követték. Ez utóbbi támadások már Ukrajna fővárosát, Kijevet is érintették. (Polityuk–Vukmanovic–Jewkes 2017)

A korábban már említett biztonságpolitikai kihívásokkal, illetve a politikai-katonai krízisekkel párhuzamosan megjelennek a kibertérben történő különböző tevékenységek. Ezek a tevékenységek az állami szereplők megjelenésével egyre inkább a kiberhadviselés kategóriájába lépnek.

Mindezekkel összefüggésben napjainkban egyre több szó esik arról, hogy az ukrajnai eset csak egy főpróba volt egy komolyabb – például az USA energiaszektorát célzó – támadás előtt. 2017 nyarán a meglehetősen óvatos kommunikáció arról adott hírt, hogy külföldi országok hackerei behatoltak számos amerikai erőmű számítógépes rendszerébe, köztük a kansasi Wolf Creek atomerőművébe. A híradások alapján azt is feltételezni lehet, hogy nemcsak közvetlenül az amerikai villamosenergia-rendszerbe hatoltak be a támadók, hanem az azokhoz nélkülözhetetlen rendszereket gyártó cégbe vagy cégekbe már ezt megelőzően jóval korábban beépülhettek.[13] (Riley–Dlouhy–Gruley 2017)

Az első számú gyanúsított természetesen Oroszország mint a támadók mögött álló hatalom. Bár ez egyelőre nyilvánvalóan csak gyanú és feltételezés, hiszen kézzelfogható bizonyítékkal még egyik

[13] Itt ismét utalnunk kell arra a korábbi megállapításunkra, amely a szoftver- vagy hardvergyártó cégek, illetve a termékeik kompromittálódását elemezte. A szállítók megbízhatósága nyilvánvalóan egy olyan kiemelt szektor esetében is, mint a villamos energia elengedhetetlenül fontos.

hivatalos szerv sem állt elő, mindenesetre ez az elmúlt évek eseményeinek fényében különösen aggasztó. Oroszország az említett ukrán energiarendszerbe való behatolással, valamint a már szintén említett 2016-os amerikai elnökválasztási kampányban történt támadásokkal bizonyította képességeit és lehetőségeit. (Riley–Dlouhy–Gruley 2017)

A SCADA és sérülékenységei

A SCADA (Supervisory Control and Data Acquisition, azaz felügyeleti, irányító és adatgyűjtő) rendszerek az iparban több évtizede használatosak, ami eleve magában hordozza azt, hogy ezek a rendszerek olyan sérülékenységeket tartalmaznak, amelyeken keresztül a támadók az ipari folyamatokhoz hozzáférhetnek. A SCADA-rendszerek legfontosabb felhasználási területe az ipar, de más olyan folyamatokban is használatosak, ahol a különböző adatok gyűjtése, összehasonlítása, és ezek alapján valamilyen beavatkozás, szabályozás szükséges. (Ilyen folyamat lehet egy katonai – automatizált – felderítő rendszer működtetése is). A SCADA egy olyan egységes vezérlőrendszer-architektúrának tekinthető, amely magában foglalja a számítógépeket, a hálózati adatkommunikációt és a grafikus felhasználói felületeket (ezt gyakran *Human-Machine Interface*-nek nevezik). Célja az adott szervezet folyamatainak automatikus felügyelete és irányítása. Ennek érdekében perifériás eszközöket, például PLC-ket (Programmable Logical Controller, azaz programozható logikai vezérlők) is használhat. A SCADA-rendszer valós idejű vezérlést és szabályozást tesz lehetővé a szenzoroktól és aktuátoroktól érkező (vagy az azokhoz továbbított) adatok és információk alapján. A SCADA-rendszerek a korai 70-es évektől kezdve jelen vannak az ipari folyamatok irányításában. Ennek megfelelően a fejlődésüket általában négy szakaszra osztják: monolitikus rendszerek szakasza, elosztott rendszerek szakasza, a hálózati szakasz és az IoT-eszközök szakasza. A SCADA-rendszerek biztonságának megvalósítása azok decentralizáltsága, számtalan hálózati kapcsolata, valamint hosszú életciklusuk okán sokszor megkérdőjeleződik. Sok régebbi SCADA-rendszer még mindig soros portokat használ az RTU-kommunikációhoz (Remote Terminal Unit vagy Remote Telemetry Unit). Ugyanakkor a modernebb SCADA-rendszerek is hordoznak magukban sérülékenységeket. Az egyik ilyen sérülékenység a vezérlőszoftver kompromittálhatósága vagy az ahhoz való jogosulatlan hozzá-

férés, hiszen ezt akár rosszindulatú szoftverrel is el lehet érni, ráadásul ezek sokszor semmilyen titkosítást nem alkalmaznak. A hálózati elemekhez való fizikai hozzáférés lehetősége az említett számtalan hálózati elem és eltérő helyszíneken való kiépítettség miatt szintén komoly sérülékenységet jelent, hiszen a fizikai hálózati hozzáféréssel akár a PLC-be is be lehet avatkozni, vagy akár a szenzorok értékeit lehet módosítani, illetve hamis parancsot lehet adni az aktuátoroknak.

3.3. Kiberbiztonság Magyarországon

Az információtechnológia és ennek a társadalomra, valamint a gazdaságra gyakorolt hatását Magyarországon viszonylag korán felismerte a kormányzat. Ennek megfelelően már az 1990-es évek végén és 2000-es évek legelején megjelent az a stratégiai gondolkodás, amely az információs társadalom kiépítését, majd annak fejlesztését tekintette egyrészt a kibertérben,[14] másrészt az ország jövőjét tekintve a legfontosabb irányoknak. Néhány szakértői anyag és tanulmány[15] közreadása után 2001-ben jelent meg a Nemzeti Információs Társadalom Stratégia, amely fő célkitűzéseit tekintve a gazdaság információtechnológiára alapozott fejlesztését, az oktatás és kultúra, a társadalompolitika, valamint az elektronikus kormányzati és önkormányzati fejlesztéseket tartalmazta. Mindezek mellett az ezekhez a célokhoz szükséges infrastrukturális rendszerek további kialakítását és fejlesztését irányozta elő. (NITS 2001) Meg kell jegyeznünk, hogy ez a stratégia nemcsak azért volt előremutató, mert az európai trendekkel nagyjából egy időben született, hanem azért is, mert átfogó módon kívánt stratégiaalapot nyújtani a kibertérre épülő technológiai háttér kormányzati biztosításával a társadalom és a gazdaság különböző dimenzióinak fejlesztéséhez.

---

14 Nyilvánvalóan ekkor még az internet és az infokommunikációs szektor volt az, amelyre ezek a stratégiai elképzelések megszülettek. A kibertér mint fogalom csak ezt követően jelent meg és terjedt el.

15 Ilyen szakértői anyag volt többek között a *Magyar válasz az Információs Társadalom kihívásaira* (Havass–Lengyel 1999) vagy a *Tézisek az információs társadalomról* című tanulmánykötet. (Talyigás 2000)

Ugyanakkor 2003-ban egy új stratégia megalkotása történt ezen a területen, hiszen 2002-ben új kormányzati ciklus következett, és benne egy új kormány kezdte meg működését. E stratégiának, amely a *Magyar Információs Társadalom Stratégia* címet viselte, legfontosabb céljai nem sokban különböztek az előző kormány hasonló elképzeléseitől. A fő cél: „Magyarországon tudásalapú gazdaságot létrehozva, az információs társadalom fejlesztésével az egyén és a közösség életminőségének és életkörülményének javítását lehessen elérni." (MITS 2003)

A 2010-es években már egyre nyilvánvalóbbá vált a kibertér társadalomra és gazdaságra gyakorolt megkerülhetetlen hatása, amely magával hozta a terület stratégiai elképzeléseinek generális felülvizsgálatát is.[16] Így 2010-ben (ne felejtsük el, hogy ekkor ismét új kormányzati ciklus kezdődött) megjelent a *Digitális megújulás cselekvési terv 2010–2014: Az infokommunikációs ágazat cselekvési terve a társadalom és a gazdaság megújulásáért* címmel. Ez az EU 2020 Digitális Menetrendbe illeszkedő stratégia egy helyzetelemzésre építve vetíti fel az oktatástól kezdődően a gazdaság különböző szektorai versenyképességének fejlesztési szükségességét. Ez az első olyan stratégiai dokumentum, amely külön figyelmet szentel a kibertérben megjelenő biztonságnak, valamint az IT-biztonsági jogszabályok átdolgozásának. A cselekvési terv nemcsak feladatokat írt elő, hanem egy indikátorrendszert is felállított, amelyen keresztül a stratégiában megfogalmazottak hatásai mérhetővé váltak. (DMCST 2010)

A digitális megújulási cselekvési tervet 2014-ben az infokommunikációs szektor vonatkozásában egy olyan új stratégia követte, amely

[16] Ugyanez igaz a kritikus infrastruktúrák vonatkozásában is. Ahogy korábban utaltunk rá 2008-ban született meg a 2080/2008. (VI. 30.) Korm. határozat a *Kritikus Infrastruktúra Védelem Nemzeti Programról,* majd közel négy évig kellett várni arra a törvényre, amely végre szabályozta a kritikus infrastruktúrák azonosítását és védelmét. Ez a korábban már szintén bemutatott *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*. Ugyanakkor ez a törvény sem adott végleges választ a kritikus információs infrastruktúrák védelmének átfogó megoldására. [2080/2008. (VI. 30.) Korm. határozat]

az ágazat és benne nyilvánvalóan a kibertér különböző összetevőinek további fejlesztését célozta. *A Nemzeti Infokommunikációs Stratégia 2014–2020* című dokumentum áttekintette az addig született stratégiai kezdeményezéseket, majd az általunk is említett digitális ökoszisztéma[17] alapján meghatározta azokat a pilléreket – digitális infrastruktúra, digitális kompetenciák, digitális gazdaság, digitális állam –, amelyek a legfontosabb fejlesztendő területeket jelentették. Mindezek mellett három olyan horizontális tényezőt is leír a stratégia, amelyek az említett pillérek mindegyikénél megjelennek. Ezek az *e-befogadás,*[18] a *K+F+I,* valamint a *biztonság.* A biztonság ilyen megjelenítése szintén előremutató. A stratégia így fogalmaz ennek kapcsán a biztonság vonatkozásában: „a kritikus információs infrastruktúrák, a közigazgatási belső rendszerek és külső alkalmazások, valamint az ezekben megjelenő felhasználói adatok maximális védelme, illetve a felhasználók folyamatos tájékoztatása a tényleges biztonsági kockázatokról és ezek kezelésének lehetőségeiről." (Nemzeti Infokommunikációs Stratégia 2014)

Az információs társadalom, illetve az infokommunikáció fejlesztésére irányuló stratégiák közül ez volt az első, amelyben explicit módon megjelenik a (kiber)biztonságról való gondolkodás. Az ezt megelőző elképzelések csak érintőlegesen tárgyalták a biztonságot,[19] hiszen azok mindegyike a társadalom, a gazdaság, illetve az ezek fejlesztéséhez szükséges infrastruktúra megteremtését tekintették fő célnak, és ezek mellett nem vagy csak közvetett módon tettek említést a terület biztonságáról.

A kiberbiztonság területén az egyik legfontosabb mérföldkő Magyarországon 2012-höz köthető. Ebben az évben jelent meg Magyar-

17 Meg kell jegyezni, hogy ez az első olyan stratégiai dokumentum hazánkban, amelyben megjelenik a *digitális ökoszisztéma* kifejezés.

18 Az e-befogadás a digitális ökoszisztémából eddig kimaradó emberek bevonását jelenti úgy, hogy az infokommunikációs fejlesztések különböző területei számukra is elérhetővé válnak.

19 Ezt felismerve született meg 2002-ben egy kutatócsoportunk révén az a tanulmány, amely azonosította és felmérte az információs társadalom akkor meglévő veszélyforrásait, majd javaslatokat tett a kormányzat részére azok műszaki és szervezeti megoldásaira. (Makkay et al. 2002)

ország új Nemzeti Biztonsági Stratégiája, amelybe kiemelt helyen került be a kibertérben megjelenő veszélyek csoportja. Az új Nemzeti Biztonsági Stratégiába a területtel kapcsolatban olyan megállapítások is helyet kaptak, mint például a következő: „Az állam és a társadalom működése – a gazdaság, a közigazgatás vagy a védelmi szféra mellett számos más területen is – mind meghatározóbb módon a számítástechnikára épül." [1035/2012. (II. 21.) Korm. határozat], de mindezek mellett a legfontosabb következtetést abból kell levonnunk a stratégiával kapcsolatban, hogy az „mégis előremutató, hiszen államilag elfogadott, a nemzet biztonságát meghatározó stratégiai elvek először tartalmazzák e terület fontosságát és védelmének szükségességét". (Kovács 2014)

A stratégia meghatározza a biztonsági fenyegetéseket, kockázatokat és azok kezelését is. Itt jelenik meg önálló kihívásként és kezelendő területként a kiberbiztonság is, amely azonban csak általános jellemzést ad e terület veszélyeiről: „Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem-állami – akár terrorista – csoportok arra használhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését." [1035/2012. (II. 21.) Korm. határozat]

Értelemszerűen a veszélyek – még ha azok csak általános értelemben vett meghatározása történik is meg – bemutatása után azok kezelésére is iránymutatást ad a stratégia. A dokumentum meghatározza, hogy a kibervédelem feladatainak ellátására – ebbe beleértve a nemzeti kritikus infrastruktúra működésének biztosítását is – koordinált védelmet kell kialakítani és meg kell kezdeni a védelmi célú felkészülést. Ezek alapján a stratégia feladatként jelöli meg a kibertérben jelentkező meglévő vagy jövőbeni potenciális kihívások, fenyegetések és kockázatok rendszeres felmérését, azok priorálását, a kormányzati koordináció erősítését, a társadalmi tudatosság fokozását, valamint a nemzetközi együttműködési lehetőségek kiaknázását. [1035/2012. (II. 21.) Korm. határozat]

Ezekből a feladatokból nagyon jól levezethetők a később megfogalmazásra kerülő ágazati stratégiák – köztük a Nemzeti Kiberbiztonsági Stratégia –, illetve az azokban meghatározott részletes feladatok, valamint az azokhoz szükséges szervezetrendszer.

A Nemzeti Kiberbiztonsági Stratégiát 2013. év elején fogadta el a kormány. [1139/2013. (III. 21.) Korm. határozat] Ez a stratégia szintén olyan mérföldkő a hazai kiberbiztonság területén, amely meghatározó jelentőséggel bír. A dokumentum felvázolja hazánk kiberbiztonsági környezetét, megadja Magyarország kiberbiztonsági értékrendjét, jövőképét és céljait. Ahogy korábban utaltunk rá, a stratégia kissé szokatlan fogalomhasználattal ugyan, de bevezette a *magyar kiberteret,* valamint meghatározta mindazokat a feladatokat, amelyeket végre kell hajtani – akár a magyar kibertérben – ahhoz, hogy a kiberbiztonság megteremthető legyen. Mindehhez kormányzati koordinációt, együttműködést és szakosodott intézmények létrehozását határozza meg feladatként a stratégia. [1139/2013. (III. 21.) Korm. határozat]

Ezek a kissé triviálisnak tűnő feladatok – ne felejtsük el, hogy már 2013-at írunk – azonban nagyon komoly szándékot takarnak, hiszen ekkor még nincs, vagy nem teljes a terület egységes kormányzati koordinációja, nincsenek meg az együttműködés kialakult folyamatai, és még nincs meg az igazi olyan szervezeti keretrendszer, amely a legmagasabb szinttől a legalacsonyabb szintig képes lenne a kibertérben a biztonsággal kapcsolatos feladatok ellátására.

A szervezeti keretrendszer annak ellenére hiányzott, hogy már ekkor is működtek CERT-k hazánkban, hiszen közel egy évtizede – 2002-ben – alapították meg a CERT-Hungaryt[20] a Puskás

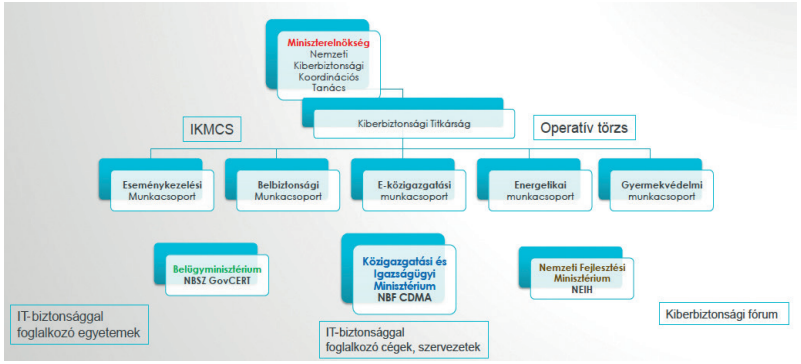
[20] A CERT-Hungary 2002 és 2010. január 1. között működött ezen a néven, amikor is *Az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendelet* alapján a *Nemzeti Hálózatbiztonsági Központ* nevet kapta kiterjesztett feladatokkal. (Kormányzati Eseménykezelő Központ 2009) Ezt követően a 2013. évi L. törvény alapján (2013. július 1-jén) létrejött a Kormányzati Eseménykezelő Központ (GovCERT-Hungary), így a CERT-Hungary, illetve a Nemzeti Hálózatbiztonsági Központ megszűnt.

Tivadar Közalapítvány keretében, és szintén működött a SZTAKI CERT-je is. Ugyanakkor ezek a CERT-k nyilvánvalóan nem kaphatták az egész hazai kiberbiztonság megvalósítását feladatul.

A stratégia által felvázolt koordinációs és együttműködési feladatok ellátására létrejött a Nemzeti Kiberbiztonsági Koordinációs Tanács, amely a Miniszterelnökség alatt kezdte meg működését. A tanács a legfontosabb és a legmagasabb szintű politikai koordinációs testület lett a kiberbiztonság területén, hiszen olyan tagokból állt, mint például a különböző miniszterek, illetve azok képviselői – például a belügyminiszter, a honvédelmi miniszter, a külügyminiszter, a fejlesztési miniszter – vagy az olyan hivatalok képviselői, mint például a Nemzeti Média és Hírközlési Hatóság. A tanács napi munkáját Magyarország kiberkoordinátora irányította. A tanács több munkacsoportot is létrehozott, például az eseménykezelési munkacsoportot, belbiztonsági munkacsoportot, e-közigazgatási munkacsoportot, energetikai munkacsoportot, illetve a gyermekvédelmi munkacsoportot. (Kovács–Szentgáli 2015)

A Nemzeti Kiberbiztonsági Stratégia abban a tekintetben is előremutató volt, hogy erre építve megvalósulhatott a *2013. évi L. törvény az állami és önkormányzati szervek elektronikus iinformációbiztonságáról,* amelyet a Parlament 2013. április 15-én fogadott el. Ez az úgynevezett *információbiztonsági törvény (Ibtv.),* amely „szintén egy nagyon nagy űrt pótol hazánk kibervédelmében, mert végre törvényi alapokon szabályozott a kibervédelem területén szerepet kapó szervezetek mintegy 75–80%-ának feladata, jog- és hatásköre". (Kovács 2014)

Ugyanakkor az említett jogszabályok hatására is létrejövő hazai kiberbiztonsági szervezeti rendszer meglehetősen heterogén volt, sok szervezeti elemmel és gyakran egymás feladataiban jelentős átfedésekkel.



59. ábra
A hazai kibervédelmi szervezetek 2015 előtt

Forrás: Bencsik 2015

A 2014-ben indult újabb kormányzati ciklusban azonban elkezdődött a szervezeti keretrendszer és a kiberbiztonsági feladatok racionalizálása és harmonizációja is. Az előző négy évben a Közigazgatási és Igazságügyi Minisztérium alatt működő Nemzeti Biztonsági Felügyelet (NBF) a Belügyminisztérium (BM) fennhatósága alá került, csakúgy mint a korábban a Nemzeti Fejlesztési Minisztérium égisze alatt feladatait ellátó Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH). Szintén a Belügyminisztérium lett a felelős a Nemzeti Kiberbiztonsági Koordinációs Tanács működtetéséért.

A parlament azonban 2015 júliusában módosította[21] az Ibtv.-t. Ezzel a módosítással egy átláthatóbb szervezeti elemekből álló, letisz-

[21] A 2013. évi L. törvény vonatkozásában nagyon sok alapvető szervezeti és hatásköri változást is hozott ez a törvénymódosítás. Magának a törvénymódosításnak már a címe is nagyon érdekes: *2015. évi CXXX. törvény az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról.*

tultabb feladatstruktúrával rendelkező hazai kiberbiztonsági szervezetrendszer állt fel.[22]

A törvény módosításával 2015. október 1-jével létrejött a Nemzeti Kibervédelmi Intézet (NKI). Az NKI működtetését a BM felügyelete alatt lévő Nemzetbiztonsági Szakszolgálat (NBSZ) kapta feladatul, ami nem véletlen, hiszen az NKI egyik legfontosabb pillére a GovCERT-Hungary, amelyet már korábban is az NBSZ üzemeltetett. Mindezeken túl az NBF-nél működő Cyber Defence Management Authority (CDMA), amely alapvetően sérülékenységvizsgálati szakhatósági jogkörrel rendelkezett, megszűnt, és ezeket a feladatokat szintén az NKI kapta meg. A NEIH, amely 2015. január 1-jétől a Belügyminisztérium főosztályaként tevékenykedett, szintén az NKI-hoz került.

Az Ibtv. módosítása számos fontos jogszabályi változást is indukált, ami a következő táblázat foglal össze.

[22] Bár jelen könyvnek sem a véleményformálás, sem a minősítés nem célja, mégis a hazai kiberbiztonsági szervezetek esetében meg kell ezt tennünk. Ezért itt azt a – bár meglehetősen szubjektív és nyilvánvalóan kissé felületes – megállapítást tesszük, amikor azzal a kijelentéssel élünk, hogy 2015-től egy átláthatóbb hazai kiberbiztonsági szervezeti rendszer jött létre. Természetesen vállalva az ellenvéleményekben rejlő reális megállapításokat, azt is tényszerűen kell látnunk, hogy az átláthatóbb struktúra még nem feltétlenül jár együtt a tökéletes működéssel vagy a kiberbiztonság 100%-os megvalósulásával. Ugyanakkor egy adott ország kiberbiztonságának meghatározására objektív méréssel többek között az ITU vállalkozik. Ez a mérés nemzetközi összehasonlítást is lehetővé tesz a kiberbiztonság területén. A szervezet minden évben kiad egy globális kiberbiztonsági indexet (Global Cybersecurity Index – GCI). Ennek 2017-es kiadásában Magyarország a világ országai közül az 51. helyet érte el. (Az előző évi rangsorban elfoglalt helyünkkel, amely a globális rangsorban a hatodik, míg regionálisan a harmadik helyet jelentette, nem lehet összehasonlítani ezt az évet és ezt a helyezést, mert 2017-ben új indexrendszert vezetett be az ITU). Természetesen az 51. pozíció nem mondható előkelő helyezésnek. Ugyanakkor az említett jelentés Magyarországot példaértékűnek tartja a kiberbiztonsági ajánlások szervezetek számára történő implementálása területén. A GCI külön kiemeli és más országok figyelmébe ajánlja hazánkat, mert az állami és önkormányzati dolgozók számára kiberbiztonsági képzéseket ír elő, külön nevesítve a Nemzeti Közszolgálati Egyetemet mint ezen képzések szervezőjét és lebonyolítóját. (ITU 2017c)

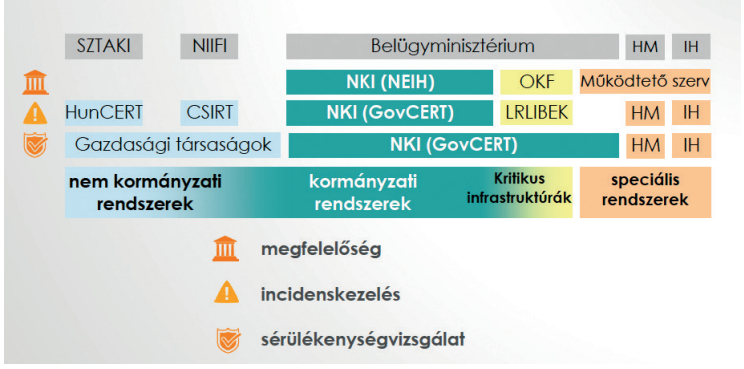
11. táblázat
A 2013. évi L. törvény 2015-ben történt módosítását követően megjelent új jogszabályok

Jogszabály száma/fajtája	Jogszabály címe
187/2015. (VII. 13.) Korm. rendelet	Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
185/2015. (VII. 13.) Korm. rendelet	A kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól
41/2015. (VII. 15.) BM rendelet	Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
42/2015. (VII. 15.) BM rendelet	Az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről

Forrás: a szerző szerkesztése

Az Ibtv. módosítása, illetve a bekövetkezett szervezeti változások alapvetően alakították át a hazai kibervédelmi szervezeteket és azok kapcsolatait. Ennek megfelelően hazánkban az állami szintű kibervédelem három nagy szervezeti egységét és ezzel együtt természetesen a felelősségi köröket tudjuk elkülöníteni. Az első a már említett NKI, a második a kritikus infrastruktúrák védelméért is felelős Országos Katasztrófavédelmi Főigazgatóság (OKF), illetve az alatta működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő

Központja (LRLIBEK), valamint a Honvédelmi Minisztérium (HM) irányítása mellett feladatát végző Katonai Nemzetbiztonsági Szolgálatnál (KNBSZ) felállt katonai CERT (HÁEIEK, azaz Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ).



60. ábra
A 2015 óta működő hazai állami kibervédelmi szervezetek

Forrás: Bencsik 2015

A Nemzeti Kibervédelmi Intézet három pillérre épül. Az első a Kormányzati Eseménykezelő Központ, amely saját megfogalmazása szerint olyan koordinációs szervezet, amely egyrészt a hazai és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra-védelmi szervezetekkel tartja a kapcsolatot, másrészt végzi a közigazgatásban (kormányzati és önkormányzati szervezeteknél) megjelenő informatikai incidensek kezelését és azok elhárításának koordinálását, valamint közzéteszi a felismert és publikált szoftversérülékenységeket. (Kormányzati Eseménykezelő Központ 2017) Az NKI második pillére a NEIH, amely az Ibtv.-ből, illetve a kapcsolódó jogszabályokból adódóan végzi az Ibtv. alá tartozó elektronikus információs rendszerek[23]

[23] Néhány kivétellel, amelyet az Ibtv. 2.§-a szabályoz. Ilyen kivételek a nemzetbiztonsági szolgálatok rendszerei, egyes zárt célú elektronikus információs rendszerek, vagy például a honvédelmi célú rendszerek. [Ibtv. 2.§ (3)–(6)]

biztonságának felügyeletét. A 187/2015. (VII. 13.) Korm. rendelet nemzeti információbiztonsági hatóságként a Nemzetbiztonsági Szakszolgálatot jelöli ki. [187/2015. (VII. 13.) Korm. rendelet 1. § (3) bekezdés]

A harmadik pillér pedig az információbiztonság és hálózatbiztonság tudatosításában jelentkezik, hiszen az NKI egyik nagyon komoly feladata „az állami és önkormányzati szervek munkatársainak felkészítése az internet minél tudatosabb és biztonságosabb használatára, szemléletformáló kampányok, tudatosító előadások formájában." (Kormányzati Eseménykezelő Központ 2017)

3.4. Kiberbiztonság az Európai Unióban

Korábban már utaltunk rá, hogy a 2008-as gazdasági világválság után az európai gazdaság kitettségének és sérülékenységének csökkentése, valamint az EU versenyképességének növelése érdekében az Európai Bizottság 2010-ben *Európa 2020* címmel egy olyan stratégiát hirdetett meg, amely öt fő célkitűzést tartalmazott. Ezek a célok pillérekre és alpillérekre támaszkodnak. Az első pillér a kiemelt növekedést célozta meg, amely magában foglalja az *Európai Digitális Menetrendet*. (European Commission 2017h)

Az Európai Digitális Menetrend legfontosabb célja, hogy az unió tagországai számára egy egységes digitális piacot hozzon létre, amelyre támaszkodva a fenntartható gazdasági és szociális előnyök minden európai polgár számára elérhetővé válnak. A menetrend az Európai Unió meglévő gazdasági, társadalmi kihívásainak és hiányosságainak (például a digitális piac szegmentáltsága, interoperabilitási kihívások, kiberbűnözés terjedése, hálózati beruházások hiánya, alacsony szintű K+F-tevékenység, a digitális írástudás alacsony szintje) feltárása és elemzése után, ezeknek a területeknek a fejlesztésére tesz javaslatokat és határoz meg különböző akciókat. (European Commission 2017h)

Az Európai Digitális Menetrend fent említett megállapításai alapján 2013-ban készült el az *EU kiberbiztonsági stratégiája,* utalva arra

az információs technológiával és információs rendszerekkel szembeni függőségre, amely a társadalom és a gazdaság minden szegmense esetében jelen van. Ebből következően szükségszerűen meg kell jelennie a kibertér biztonságára vonatkozó szabályozásnak is, hiszen ha nem működnek az említett információs rendszerek, az nemcsak a gazdasági, hanem a társadalmi funkciókban is komoly zavarokat – egyes esetekben működésképtelenséget – okoz. (Cybersecurity Strategy of the European Union 2013) Az azonban kijelenthető, hogy ez az a stratégia, amely az első komoly lépés az egységes európai kiberbiztonság alapjainak lefektetése útján.

Ahogy korábban már utaltunk rá, a stratégia az EU-nak az európai telekommunikációs rendszerek meghibásodásának és az azok ellen indított támadások megelőzésére, illetve az ilyen esetekre kidolgozott válaszlépésekre vonatkozó egységes uniós stratégiai elképzeléseit tartalmazza. A meglehetősen hosszú és vitáktól sem mentes egyeztetéseket és koordinációt követően a stratégiára vonatkozó javaslatot 2013 februárjában két részben tették közzé, amelyből az első rész az Európai Bizottság és a külügyi és biztonságpolitikai főképviselő közleménye az EU kiberbiztonsági stratégiájáról, amely maga a stratégia, a második rész pedig az Európai Bizottság irányelvjavaslata a hálózat- és az információbiztonsággal kapcsolatban, amely a NIS-irányelvcsomagként vált ismertté.

A stratégia öt olyan alapelvre épül, amelyek prioritásként is megjelennek az Európai Unió jövőjét tekintve, hiszen nagyon fontos kiemelni azt a felismerést – amely az EU hivatalos kommunikációiban is nagy hangsúlyt kap – miszerint a fizikai térben megvalósuló biztonsághoz hasonló módon a kibertér biztonsága ugyanolyan fontossággal bír.[24]

[24] Ez a felismerés, illetve annak hivatalos kommunikációja analóg módon megjelenik a NATO hasonló gondolkodásában is. 2016 júliusában a NATO varsói csúcsértekezlete kinyilatkoztatta, hogy a hagyományos hadviselési dimenziók mellett a kibertér is megjelenik hadszíntérként. (NATO 2016)

A stratégia öt alapelve (prioritása): a kibertámadásokkal szembeni ellenálló képesség megteremtését, a kiberbűnözés[25] drasztikus visszaszorítását, a kibervédelmi politika kidolgozását és a közös biztonság- és védelempolitikába való beágyazását, illetve annak a tagállamok képességek terén jelentkező fejlesztését, a kiberbiztonsághoz szükséges ipari és technológiai erőforrások előteremtését, valamint az EU által képviselt, a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozását és az alapvető uniós értékek terjesztését célozza meg. (Cybersecurity Strategy of the European Union 2013)

A kibertámadásokkal szembeni ellenálló képesség megteremtése érdekében a stratégia hangsúlyozza az állami hatóságok és a magánszektor összefogását, a kapacitások, erőforrások és a hatékonyság fejlesztését. E cél elérése azonban nem képzelhető el a kiberbiztonsági események megelőzésének, feltárásának és kezelésének javítása, valamint ezek EU-s szinten történő koordinálása nélkül. Ebben a stratégia kiemelt szerepet szán az ENISA-nak. A stratégia megállapítja, hogy bár vannak ezen a területen – értsd a prioritásként megjelölt koordinált ellenállóképesség megteremtésében – bizonyos előrelépések, még mindig vannak hiányosságok számos tagországban, amelyek elsősorban a nemzeti képességekben, a határokon átnyúló események bekövetkezése esetén a koordinációban vagy a magánszektor felkészültségének elősegítése területeken jelentkeznek. Ezért a stratégiát követnie kell egy jogalkotási folyamatnak. Ez a jogalkotás ki kell, hogy térjen olyan minimumkövetelmények megfogalmazására, amelyek alapján nemzeti hatóságokat lehet kijelölni, létrehozhatók jól működő, hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT-k), valamint a területre vonatkozó nemzeti stratégia és nemzeti együttműködési terv elfogadása is lehetővé válik. (Cybersecurity Strategy of the European Union 2013)

A tudatosság területén a stratégia a felhasználók internetes tevékenységeinek minél nagyobb biztonságát célozza meg azzal a kijelen-

[25] A stratégia hivatalos magyar fordítása a *kiberbűnözés* helyett a *számítástechnikai bűnözés* kifejezést használja.

tésével, miszerint „fel kell világosítani őket a rájuk leselkedő internetes veszélyekről, és egyszerű védelmi lépésekre kell őket megtanítani." (Cybersecurity Strategy of the European Union 2013)

A cél megvalósítása érdekében a stratégia nagyban számít az ENISA-ra, valamint az olyan szervezetekre, mint az Europol és az Eurojust. A dokumentum külön kiemeli az ENISA által kezdeményezett *Európai kiberbiztonsági hónap*[26] rendezvénysorozatot. Ezt a programot a 2013-as indulása óta rendszeresen megrendezik hazánkban is. A stratégiában az Európai Bizottság külön kéréssel fordul a tagállamok felé. A kérésben szerepel, hogy a tudatosság növelése érdekében a tagországok a *Biztonságosabb Internet*[27] programban vegyenek részt, 2014-től vezessék be a biztonsággal kapcsolatos képzéseket az iskolákban, a számítástechnika szakos diákok a biztonságos szoftverfejlesztéssel, valamint személyes adatok védelmével kapcsolatos képzésben is részesüljenek, továbbá legyen a területet bemutató alapképzés a közigazgatásban dolgozó személyzet számára.[28] (Cybersecurity Strategy of the European Union 2013)

---

26 A rendezvénysorozat 2017-ben már ötödik évfordulóját ünnepelte. 2017-ben közel 300 partner bevonásával több ezer rendezvény megtartására került sor. Ebben az évben Magyarországon közel húsz partner több tucat rendezvényen, hetente más tematikával – például kiberbiztonság a munkahelyen, kiberbiztonság otthon, kiberbiztonsági készségek vagy EU-s szabályozások implementációjára (információbiztonság és adatvédelem) – hívta fel a figyelmet a kiberbiztonságra. A rendezvénysorozat egyik csúcspontja volt az első alkalommal megrendezett Nemzeti Kiberbiztonsági Konferencia. (NEIH 2017)

27 A *Biztonságosabb Internet* programban nem kormányzati szervezetek és bűnüldöző hatóságok hálózatos formában információkat és bevált gyakorlatokat osztanak meg egymással az interneten terjedő jogsértő, illetve a gyermekek szexuális kizsákmányolásával kapcsolatos anyagok terjesztése ellen. A program magában foglalja azoknak a kutatóknak a hálózatát is, akik a gyermekekkel kapcsolatos internetes kockázatokat és azok következményeit kutatják vagy azokról gyűjtenek információkat. A program külön EU-s finanszírozással bír. (Cybersecurity Strategy of the European Union 2013)

28 A stratégia ezen célja egybevág a hazai 2013. évi L. törvényben foglalt egyes rendelkezésekkel, amelyek alapján a közigazgatásban dolgozók különböző információbiztonsági képzéseken kell, hogy részt vegyenek. Erre utaltunk korábban az ITU 2017-es Global Cybersecurity Indexben foglaltak ismertetésekor, hiszen a közigazgatási szereplők ilyen képzéseinek megvalósítását az ITU is példaértékűnek látja. (ITU 2017c)

A kiberbűnözés drasztikus csökkentése érdekében megfogalmazott cél esetében, mint a stratégia kiemelt prioritása, természetszerűleg maga a kiberbűnözés, illetve ahogy a dokumentum hivatalos magyar fordítása fogalmaz, a *számítástechnikai bűnözés* mint veszélyforrás elemzése és az az elleni legfontosabb nemzetközi tevékenység szorgalmazása történik meg. A cél elérése érdekében a stratégia egységes, lényegesen erélyesebb és így szigorúbb, de hatékonyan működő jogszabályi környezetet szorgalmaz a kiberbűncselekmények visszaszorítása érdekében. Bár korábban a területen már születtek nemzetközi egyezmények, mint például a már említett *Európa Tanács számítástechnikai bűnözésről szóló egyezménye* – más néven a Budapest Konvenció – amely egyébként kötelező erejű nemzetközi szerződés az azt aláíró országok számára, és amely hatékony jogszabályi alapot biztosítana a nemzeti kiberbűnözést szabályozó jogszabályok elfogadásához vagy a már korábban szintén említett gyermekek online szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló irányelv,[29] de igazi áttörés a területen még nem született. A stratégia alapján az Európai Bizottság a kiberbűnözés visszaszorításában nagymértékben számít az Europolon belül megalakult Számítástechnikai Bűnözés Elleni Európai Központ (European Cybercrime Centre, EC3) munkájára és hatékony akcióira. Az EC3 mellett az Európai Bizottság a CEPOL-t,[30] azaz az Európai Rendőrakadémiát is nevesíti és ösztönzi, hogy olyan képzéseket indítson a szervezet, amelyek a bűnüldöző hatóságok munkatársai számára nyújtanak megfelelő ismereteket. (Cybersecurity Strategy of the European Union 2013)

[29] A stratégia itt a 2004/68/IB tanácsi kerethatározat felváltásáról szóló 2011/93/EU irányelvet említi. (Cybersecurity Strategy of the European Union 2013)

[30] A CEPOL, hivatalos angol megnevezése *European Union Agency for Law Enforcement Training* központja Budapesten van. A CEPOL számos képzést, tanfolyamot és konferenciát szervez a kiberbiztonság területén is.

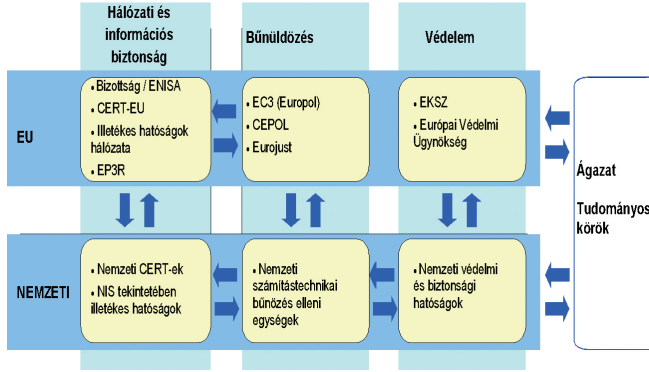
A stratégia következő kiemelt célja a közös európai biztonság- és védelempolitika (Common Security and Defence Policy, CSDP) mentén történő kibervédelmi politika és képességek fejlesztése. Ez a NATO-val közösen, a civil és a katonai infokommunikációs rendszerek szorosabb együttműködésben megvalósított védelmét jelentené. E cél elérése érdekében az Európai Bizottság az Európai Védelmi Ügynökség (European Defence Agency, EDA) segítségét kéri. A munka ki kell, hogy terjedjen „Az uniós civil és katonai szereplők közötti párbeszéd és együttműködés ösztönzésére – különös hangsúlyt fektetve a bevált gyakorlatok és az információk cseréjére –, valamint a korai előrejelzésre, az eseményekre való reagálásra, a kockázatértékelésre, a tudatosság növelésére és a kibervédelem prioritásként való kezelésére." (Cybersecurity Strategy of the European Union 2013)

A stratégia egyik talán legfontosabb célkitűzése (már amennyiben a kiemelt célokat egyáltalán lehetséges fontossági sorrendbe állítani) a kiberbiztonsági ipari és technológiai erőforrások kifejlesztése. Ezen belül a dokumentum kitér a kibervédelem területén meglévő és a jövőben megjelenő termékek számára biztosítandó egységes piac megteremtésére, amely alapvetően a NIS-direktívában megfogalmazottak alkalmazását is magával kell, hogy hozza az ilyen termékeket gyártók részéről. Mint ahogy a többi célkitűzés esetében itt is megjelenik a célok elérése érdekében definiált finanszírozási és támogatási háttér. Így a stratégia a K+F-célú beruházásokat és az innovációt ösztönzi, amely többek között a *Horizont 2020* program segítségével jöhet létre. Erről a programról külön, részletesen is szólunk könyvünk későbbi alfejezeteiben.

Mindezeken túl a stratégia egy olyan nemzetközi szakpolitika létrehozását is indítványozza, amely a már meglévő nemzetközi szabályozásokat elfogadva – az internet nyitottságát és szabadságát megőrizve – a digitális szakadékok leküzdéséhez járulhat hozzá. Mindezeknek nyilvánvalóan az EU alapértékei – azaz az emberi méltóság, a szabadság, a demokrácia, az egyenlőség, a jogszerűség és az alapvető

jogok tiszteletben tartása – mellett kell megvalósulniuk.[31] (Cybersecurity Strategy of the European Union 2013)

Ez a célkitűzés magában foglalja azt is, hogy – amint említettük – az EU-nak a közös kül- és biztonságpolitikája részévé kell tennie a kibertér kérdéseit, valamint azt is, hogy a nem EU-s, de az unióval interakcióba kerülő harmadik országokban is erősíteni kell a kibertér védelmét, amely munkában az EU-nak is jelentős szerepet kell vállalnia.



61. ábra

A kiberbiztonság átfogó kezelésének három pillére az Európai Unióban

Forrás: Cybersecurity Strategy of the European Union 2013

2017. szeptember 13-án Jean-Claude Juncker, az Európai Bizottság elnöke az unió helyzetéről szóló szokásos éves beszámolójában kijelentette: „Az elmúlt három évben előrelépéseket tettünk az európaiak online biztonságának garantálása terén. Ám Európa még mindig nem rendelkezik elég eszközzel a kibertámadások elhárítására. A bizottság

[31] Ezek az alapértékek meglehetősen patetikusan hangzanak. Ugyanakkor, ha belegondolunk, hogy néhány ország (és itt gondolhatunk Kínára, Oroszországra vagy éppen Törökországra) nem feltétlenül ezen értékek mentén valósítja meg a kibertérben érvényesülő folyamatokat, akkor rögtön értelmet nyer az említett értékek mentén folytatott munka fontossága.

ezért ma új eszközöket javasol az ilyen támadásokkal szembeni védelem megerősítésére, többek között egy európai kiberbiztonsági ügynökség létrehozását." (European Commission 2017d)

Ennek megfelelően 2017 szeptemberében az Európai Bizottság egy javaslatcsomaggal állt elő, amely az európai kiberbiztonsági helyzet teljes reformját irányozta elő. Mindez annak a felismerésnek a tanúbizonysága, amely során megállapítást nyert, hogy többek között a 2016-os zsarolóvírus-támadások, a 2017-es francia, majd a német választások körül tapasztalható – alapvetően a kibertérben jelentkező –, a demokratikus választási rendszerekbe való beavatkozásokat célzó események és kiberincidensek kezelésére az Európai Unió nincs teljesen felkészülve. E felismerés vezetett oda, hogy az Európai Bizottság és a külügyi és biztonságpolitikai főképviselő az említett kiberbiztonság megerősítésére irányuló javaslatcsomagot dolgozott ki. A javaslatok többek között tartalmaztak egy olyan új *Európai Uniós Kiberbiztonsági Ügynökség* felállítására irányuló elképzelést, amely a tagállamokat segítené a kiberincidensek kezelésében, valamint a digitális termékek és szolgáltatások biztonságos használatát lehetővé tevő, illetve azokat garantáló új európai tanúsítási rendszer kidolgozását. (European Commission 2017d)

Az Európai Uniós Kiberbiztonsági Ügynökség az ENISA-ra épülve, annak egy állandó EU-s intézménnyé válásával, a tagállamok számára nyújt segítséget a kibertámadások megelőzésében, illetve az azokra való reagálásban. Az ügynökség feladata lesz megszervezni és levezetni az európai kiberbiztonsági gyakorlatokat. Ezekkel, valamint új információmegosztási és elemző központok létrehozásával a fenyegetettséggel összefüggő információ- és tudásmegosztás magasabb szintre léphet az unióban. A sorok között olvasva az új ügynökség kvázi hatósági feladatokat is kap, amely kiterjed a NIS-direktíva tagállamokban történő végrehajtásának ellenőrzésére, valamint ezen belül a súlyos incidensek nemzeti hatóságok felé történő bejelentésének ellenőrzésére is.

Mindezeken túl a Kiberbiztonsági Ügynökség feladata lenne az Európai Bizottság által kidolgozandó új, a digitális termékek és szolgáltatások számítástechnikai szempontból való biztonságosságának garantálása érdekében előterjesztett uniós tanúsítási keretrendszer[32] kialakításában és végrehajtásában való közreműködés is. (European Commission 2017i)

Nyilvánvalóan a stratégiai környezetet számos jogszabállyal kiegészítve kell kezelnünk ahhoz, hogy a kiberbiztonság teljes spektrumában vizsgálható legyen.

Ilyen jogszabály, illetve ajánlás (ha tetszik: direktíva) többek között a korábban már említett NIS, valamint az adatvédelem területén áttörést jelentő GDPR-irányelv, amely célja ugyan nem a szorosan vett kiberbiztonság megteremtése, de közvetett módon – a benne foglalt intézkedésekkel – nagy hatással lesz a kiberbiztonságra is.

Ezeket, illetve a kutatás-fejlesztés területén – többek között az ICT-szektorra, továbbá a kiberbiztonságra is komoly anyagi támogatást biztosító – *Horizont 2020* programra is érdemes néhány pillantást vetnünk.

3.4.1. A NIS-direktíva

Az EU kiberbiztonsági stratégiájának fontos része a hálózat- és információbiztonságra vonatkozó irányelv (NIS Directive – Network and Information Systems Directive, azaz „hálózat és információs rendszerek”-irányelv), amelynek meglehetősen hosszú, így ebből következően kissé nehezen is érthető hivatalos címe van: *az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati*

[32] Az új európai kiberbiztonsági tanúsítványok kialakításának célja, hogy azok garantálják a digitális eszközök (beleértve az IoT-eszközöket is) és szolgáltatások megbízhatóságát. Hasonló tanúsítványok kialakítása a cél, mint amelyek például az élelmiszeriparban és kereskedelemben már évtizedek óta megvannak. (European Commission 2017i)

és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.[33] (NIS Directive 2016)

Ahogy korábban már utaltunk rá, az irányelv első tervezetét már 2013-ban, azaz az EU kiberbiztonsági stratégiájának elfogadását követően napirendre tűzte mind az Európai Parlament, mind az Európai Bizottság. Az eredeti elképzelés szerint az Európai Unió előírta volna a tagállamok számára egy saját NIS-stratégia kialakítását, valamint egy olyan nemzeti NIS-hatóság kijelölését is felvetette, amelynek megfelelő erőforrásokkal kell vagy kellene rendelkeznie a kockázatok és incidensek megelőzéséhez, valamint az ezekre a kockázatokra adandó válaszlépések megtételéhez. Mindezeken túl a NIS-irányelvjavaslat a tagállamok és a bizottság közötti együttműködési mechanizmus kidolgozását is tartalmazta, amely alapján lehetőség lenne az incidensekre vonatkozó adatok gyors és megbízható megosztására a tagállamok között. Ez a hálózatokkal, illetve informatikai rendszerekkel szembeni fenyegetésekkel és eseményekkel szembeni közös fellépést elősegítő korai riasztást tenné lehetővé. Az eredeti irányelvjavaslatnak fontos eleme volt, hogy egyes informatikai vállalatok és szolgáltatók számára előírják speciális kockázatkezelési eljárás kidolgozását, valamint a jelentősebb informatikai biztonsági események bejelentését az illetékes nemzeti hatóságnak. Ugyanakkor közel hároméves tárgyalássorozat eredménye az, hogy magát az irányelvet 2016 nyarán mind az Európai Parlament, mind az Európai Bizottság közösen – különböző kompromisszumokkal ugyan, de végül – elfogadta. (European Commission 2017e)

Az elfogadott irányelv valamennyi tagállam számára kötelező érvényű előírásokat fogalmaz meg. Ezek közül talán a legfontosabb, hogy minden tagállamnak a hálózati és információs rendszerek biztonságának megteremtésére irányuló nemzeti stratégiát kell kidolgoznia. (NIS Directive 2016)

---

[33] A NIS-irányelv hivatalos angol címe sem sokkal egyszerűbb és könnyebben érthető: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Bár hazánk rendelkezik kiberbiztonsági stratégiával,[34] kérdés, hogy ez egy az egyben megfeleltethető-e a NIS-ben elvárt hálózati és információs rendszerek biztonságának megteremtésére irányuló stratégiának, hiszen a nemzeti kiberbiztonsági stratégiánk lényegesen generálisabb elvek mentén fogalmazódik meg.[35] Ugyanakkor kétségtelen, hogy a hazai stratégia mind időben, mind filozófiájában messze megelőzte a NIS-ben megfogalmazott elvárásokat, és számos olyan utalást tartalmaz, amelyek a NIS nemzeti kiberbiztonsági stratégiát meghatározó részében vannak. Ilyenek például a nemzeti kiberbiztonság területén lévő stratégiai célok eléréséhez szükséges keretrendszer meghatározása a kormányzati szereplők és egyéb más szervezetek feladatainak és jogköreinek meghatározásával együtt, vagy akár a felkészülésre, az incidenskezelésre, az oktatásra, a területen szükséges kutatás-fejlesztésre, illetve a köz- és a magánszféra közötti együttműködés meghatározására szolgáló feladatokat is.

A NIS meghatározza, hogy dedikált és egyedüli nemzeti kapcsolattartó pontot, illetve CSIRT-ket[36] kell felállítani a tagállamokban, amelyek működési feltételeit is biztosítani kell. A CSIRT-k esetében külön is rendelkezik az irányelv, amely szerint kritikus ágazatonként, illetve alágazatonként kell ezeket a szervezeteket létrehozni és működtetni, valamint biztosítani kell, hogy ezek a CSIRT-k hálózatot tudjanak alkotni az unióban, elősegítve ezzel a bizalmat, valamint a hatékony és operatív együttműködést. Mindezek azzal a nyilvánvaló ténnyel is kiegészülnek, hogy az „alapvető szolgáltatásokat nyújtó szereplők megfelelő, illetve arányos műszaki és szervezési intézkedéseket tesznek a működésük során általuk használt hálózati és információs

34 Jelen sorok írásakor a 2013. évi stratégia van érvényben, bár annak felülvizsgálata zajlik, és feltételezhetően a NIS-irányelvekben megfogalmazottakat is tartalmazni fogja a várhatóan 2018. év elején megjelenő új stratégia.

35 Ennek megfelelően hazánk Nemzeti Kiberbiztonsági Stratégiájának felülvizsgálata, és erre a stratégiára építve új kiberbiztonsági stratégia kialakítása kezdődött meg 2017-ben. Ez az új stratégia (illetve könyvünk írásakor annak még csak tervezete) már tartalmazza a NIS-irányelv követelményeit.

36 Computer Security Incident Response Team

rendszerek biztonságát fenyegető kockázatok kezelése érdekében." (NIS Directive 2016)

Az irányelv és annak 2018 májusában történő életbelépése hatalmas előrelépés – ahogy maga a direktíva is fogalmaz – az egységes digitális gazdasági és társadalmi tevékenységek, illetve különösen a belső piac működése szempontjából, hiszen a hálózatos információs rendszerek biztonságáról végre egy közös forgatókönyvből, ha tetszik szabálykönyvből tudják kiolvasni a tennivalókat a tagországok.

3.4.2. A GDPR-irányelv

Az Európai Parlament és az Európai Tanács 2016 áprilisában elfogadta az úgynevezett GDPR-szabályozást (General Data Protection Regulation, azaz az EU általános adatvédelmi rendelete). (2016/679 EK európai parlamenti és a tanácsi rendelet)

A GDPR felváltja a korábbi és a már meglehetősen idejét múlt 95/46/EK adatvédelmi irányelvet,[37] és egy olyan összehangolt adatvédelmi jogszabályt jelent az uniós tagországoknak, amelynek alapvető célja az uniós polgárok személyes és magánadatainak védelme. A korábbi – 1995-ben megjelent – egységes adatvédelmi irányelv óta eltelt időszakban alapjaiban alakult át az állampolgárok személyes adatai kezelése köszönhetően az információtechnológiának. Többek között ez tette szükségessé egy új, alapjaiban más filozófiát követő szabályozás kidolgozását. (2016/679 EK európai parlamenti és a tanácsi rendelet)

A 2018. május 25-én életbe lépő egységes európai adatvédelmi szabályozás hatalmas változást hoz ezen területen minden uniós országban. A GDPR vonatkozásában az egyik legtöbbet idézett szabályozás

[37] Ez az 1995-ben megjelent adatvédelmi szabályozás *az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról* volt. (95/46 EK európai parlamenti és a tanácsi rendelet)

nem más, mint egy nagyon kemény büntetés, illetve szankcionálás kilátásba helyezése. Ez a büntetési tétel nem kevesebb, mint a szabályokat megsértő szervezet éves forgalmának 4%-áig terjedhet, vagy akár húsz millió euró (amelyik nagyobb összeg) is lehet. Ez a súlyos büntetés a maximálisan kiszabható bírság az olyan legsúlyosabb jogsértések esetén, mint például a személyes adatok engedély nélküli feldolgozása és kezelése. Ugyanakkor a direktíva az olyan szabályszegések esetén is, mint például a nem megfelelő adatnyilvántartás vagy jogsértés esetén a felügyeleti hatóság értesítésének elmulasztása 2%-os éves forgalommal egyenértékű büntetési tételt helyez kilátásba. Ezek a büntetési tételek vonatkoznak az adatkezelőkre és az adatfeldolgozókra is, azaz a felhőszolgáltatást nyújtók is a szabályozás alá tartoznak. (2016/679 EK európai parlamenti és a tanácsi rendelet)

A GDPR számos új, nagyon szigorú rendelkezést tartalmaz az adatvédelem területén. Ilyen szabályozás például a szabálysértési értesítés. Ez arra vonatkozik, hogy amennyiben az állampolgárok jogait és szabadságát veszélyeztető adatvédelmi szabályszegés következik be, a felügyelőhatóságot 72 órán belül értesíteni kell erről. Ugyanígy értesítési kötelezettsége van az adatfeldolgozónak is az ügyfelek felé, ha adatszegést észlel. (2016/679 EK európai parlamenti és a tanácsi rendelet)

A GDPR az ügyfelek személyes adatainak kezelése terén hatalmas áttörést jelent. A *jogszerűség, tisztességes eljárás és átláthatóság* [2016/679 EK európai parlamenti és a tanácsi rendelet 5. cikk (1) a. pont] szellemében született direktíva ugyanis előírja, hogy az adatalanyoknak (azaz kicsit leegyszerűsítve az ügyfeleknek) joga van ahhoz, hogy az adatkezelőtől megerősítést kapjanak arról, hogy az őket érintő személyes adatokat mikor, hol és hogyan dolgozzák fel, azokat hol és hogyan tárolják, vagy azokat kinek adták esetlegesen tovább (ha erre törvényes lehetőség van egyáltalán). Ez növelheti az adatkezelés átláthatóságát. Mindezeken túl az adatkezelőnek elektronikus formában, ráadásul ingyenesen meg kell adnia az ügyfeleknek a róluk kezelt személyes adatok másolatát is.

A GDPR meghatározza *a törléshez való jog* („az elfeledtetéshez való jog") fogalmát is. Ez azt jelenti, hogy az ügyfél (vagy ahogy a direktíva fogalmaz: érintett) jogosult arra, „hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje" [NIS Directive 2016 17. cikk (1) pont], ha a meghatározott feltételek fennállnak. Ez például a korábban említett Facebook adatkezelésében óriási változásokat fog hozni, hiszen ez a platform az egyike azoknak, amelyeknél tudott, hogy semmilyen adatot nem törölnek felhasználóikról, még akkor sem, ha látszólag a felhasználó a saját felületén azt megtette.

Ezek persze csak kiragadott szabályok a komplex GDPR-direktívából. Ugyanakkor az adatvédelem területén valóban áttörést jelentő szabályozásra komoly felkészülés szükséges. Ehhez – többek között – az Egyesült Királyság független, információs jogokkal foglalkozó szervezete (Information Commissioner's Office – ICO) egy útmutatót is készített, amely összefoglalja a GDPR-ra történő felkészülés legfontosabb lépéseit. A 12 pontos javaslatcsomag kitér a tudatosságra (amelyben a vezetői felelősség az egyik legfontosabb tényező), az adattárolásra (a tárolt személyes adatokról szóló nyilvántartás hangsúlyozásával), az adatvédelmi információk kommunikációjára (az adatvédelmi közlemények áttekintésére és GDPR szerinti esetleges átalakítására tett javaslattal), az ügyfelek jogaira (például az ügyfél joga a személyes adatainak törlését kérni), kiskorúakra (például a kiskorúak esetében a szülő, illetve a gondviselő hozzájárulásának kérése a gyermek személyes adatainak kezeléséhez), adatkezelési szabálysértés kezelésére (felkészült eljárások a szabálysértések megelőzésére, bekövetkezésük esetén a felügyelőhatóság és az ügyfél felé történő jelentések megtételére), adatvédelmi hatásvizsgálatokra (meglévő vagy új adatkezelési megoldások megfelelőségi vizsgálatának elvégzésére), adatvédelmi felelősre (meghatározott személy kinevezése az adatvédelmi feladatok ellátására az adott szervezetnél), illetve a nemzetközi tevékenységet végző szervezetekre (azaz milyen szabályokat kell betartani,

ha nem csak egy EU-s országban végez az adott szervezet tevékenységet). (ICO 2017)

Mindezek alapján komoly veszélyforrást jelenthetnek a szabályozás alapján azok a támadások, amelyek pont a szabályozással kapcsolatos retorziókat mint hatást kívánják elérni. Azaz – persze csak teoretikusan végiggondolva a lehetőségeket – a támadások pont azért jönnek majd létre, hogy a támadó a megtámadott szervezetet közvetett módon kellemetlen helyzetbe hozza, hiszen a támadások során megszerzett személyes, illetve egyéb – a GDPR hatálya alá tartozó – adat eltulajdonításával a konkurencia adatvédelmi vizsgálatot, sőt esetlegesen egy nagyon komoly büntetést is kikényszerít az adott szervezettel (például gazdasági versenytárssal) szemben.

3.4.3. A HORIZONT 2020

A korábban bemutatott jogi szabályozások nyilvánvalóan nagyon fontosak az EU kiberbiztonsági stratégiai céljainak eléréséhez, de önmagukban nem biztos, hogy elegendőek. Ezért azokat a végrehajtásukban kiegészítő, azokat segítő olyan intézkedéscsomaggal is támogatni kell, mint például a korszerű technikai és technológiai környezetet, illetve eljárásokat lehetővé tevő kutatás-fejlesztési programok, illetve lehetőségek.

Az egyik ilyen – és talán a legnagyobb – kutatás-fejlesztési innovációs keretprogram az Európai Unió *Horizont 2020* programja. A 2014-ben útjára indított program 2020-ig, azaz hét év alatt közel 80 milliárd euró értékben támogatja az európai uniós tagállamok innovatív ötleteit és azok megvalósulását. A program fő célja az unió globális versenyképességének javítása, illetve annak növelése. A keretprogram a már említett Európa 2020 stratégia *Innovatív Unió* elnevezésű kiemelt kezdeményezésének egyik alappillére. (H2020 2017a)

A *Horizont 2020* program egyszerűsített adminisztrációt lehetővé tevő online felületen pályázható, közvetlenül Brüsszelből. Így minden

tagország annyi pályázatot tud benyújtani, amennyit az adott ország kutatás-fejlesztési innovációs potenciálja lehetővé tesz, és így annyi pályázati forráshoz tud hozzájutni, amennyit az adott ország innovációs potenciálja elbír. A pályázatok elbírálása több körös, amelyekben az egyik legfontosabb szempont a kiválóság, valamint a több tagállamra kiterjedő, konzorciumi formában történő megvalósítás. A bírálatok során a szakmai megvalósíthatóság mellett az egyik lényeges szempont a konzorcium vezetésének és menedzselésének kérdése.

A *Horizont 2020* alapvetően három – egymástól viszonylag jól elkülöníthető – témacsoportra épül. Az első a *Kiváló tudomány,* amely az Európai Unió tudományos kiválóságát hivatott növelni. Ez a témacsoport a *H2020* teljes költségvetésének közel a 32%-át tartalmazza. A második témacsoport a *Vezető ipari szerep.* A *H2020* teljes költségvetésének 22%-ával rendelkező csoportban olyan pályázatokat vár az EU, amelyek segítenek – elsősorban a kis- és közepes vállalkozásokon keresztül – az ipari fejlődés és a csúcstechnológia területén az uniót világszinten is vezető szerephez juttatni. Mindezt a projekt is innovatív módon teszi meg, hiszen az ebben a csoportban pályázó kis- és közepes vállalkozásokat az ötletektől kezdve a megvalósításon át azok piaci bevezetéséig támogatja. A harmadik kutatási témacsoport a *Társadalmi kihívások* címet kapta. Itt olyan társadalmi kihívások és kérdések megoldásához vár innovatív elképzeléseket az unió, amelyek az egészségügy, az élelmezésbiztonság és a fenntartható mezőgazdaság, az energia, a közlekedés, az éghajlatváltozás és környezetvédelem, a biztonságos társadalmak területén jelentkeznek. Ez a kutatási témacsoport a *H2020* teljes költségvetésének a 38%-ával rendelkezik. (H2020 2017a)

A biztonságos társadalmak kutatási témacsoportot külön is érdemes kiemelni, hiszen ebben számos olyan pályázati kiírás (a *H2020* eredeti angol terminológiájával élve *call*) található, amelyek a kiberbiztonsághoz, a digitális szolgáltatásokhoz, illetve a kritikus infrastruktúrákhoz vagy kritikus információs infrastruktúrákhoz, illetve azok védelméhez kapcsolódnak.

Ennek megfelelően a „biztonságos társadalmak” szekció pályázati kiírásainak elsődleges célja a társadalom természeti vagy egyéb eredetű katasztrófákkal szembeni túlélőképességének növelése. Ez magában kell, hogy foglalja a kritikus infrastruktúrák védelmén túl az olyan új szerevezési és menedzsmenteszközök kialakítását, amelyek például egy katasztrófahelyzetben a kommunikáció interoperabilitását hivatottak biztosítani. Ez a témacsoport tartalmazza azokat a pályázati kiírásokat is, amelyek a bűnözés és a terrorizmus elleni küzdelemben használhatóak, beleértve a kiberterrorizmust is. Ezeknek többek között a nyomozati cselekmények új megoldásait vagy a robbanóeszközök és robbanószerek elleni bűnüldözői munkát kell segíteniük.

A pályázati kiírásokban találhatóak még a határőrizetre (akár szárazföldi, akár tengeri határokra) vagy az ellátási lánc biztonságára vonatkozó témák is. Jelen vizsgálódásaink szempontjából nyugodtan kijelenthetjük, hogy talán a legérdekesebb pályázati kiírások a kiberbiztonság növelése kapcsán jelennek meg.

A nagy kutatási témacsoportokon belül úgynevezett fókuszterületeket *(focus areas)* találunk. Ez igaz a digitális biztonságra, illetve a kiberbiztonságra is. A kiberbiztonság területére meghirdetett pályázatok elsősorban a jelenlegi alkalmazások, szolgáltatások és infrastruktúrák biztonságának növelésére összpontosítanak, amelyek során a cél, hogy azokba a legkorszerűbb biztonsági megoldásokat és folyamatokat integrálják. A projektek támogatásának további célja nem titkoltan az, hogy így a vezető piacokat és a piaci ösztönzőket is kialakítsák. Ennek megfelelően a projektek által létrejövő termékek vagy szolgáltatások célközönsége a bűnüldöző szervek, a kritikus infrastruktúrák üzemeltetői, az IKT-szolgáltatók, az IKT-gyártók vagy akár a polgárok lesznek. Ugyanis ők azok a piaci szereplők, akik a projektek révén létrejövő megoldásokat használni, illetve alkalmazni fogják. A kutatási projektek támogatójának egyik legfontosabb célja, hogy a pályázók a kutatás-fejlesztésbe vonjanak be minden olyan felet, akik a biztonság területén érdekeltek lehetnek. Így a projektek megvalósításában lehetőség szerint vegyenek részt az iparági szereplők kis- és közepes vál-

lalatai, a kutatóintézetek, az egyetemek, valamint e területen releváns hatóságok, nem kormányzati szervezetek, illetve lehetőség szerint minél szélesebb körű állami és magán-biztonságiszervezetek. Természetesen a végfelhasználók nem egyszerű passzív jelenléte az elvárt, hanem azok minél aktívabb tevékenységének az ösztönzése a cél a projektek során. (H2020 2017b)

A kiberbiztonság, illetve ahogy a *H2020*-ban ezt a fókuszterületet hivatalos névvel illetik, digitális biztonság területen 2016-ban számos pályázati kiírás jelent meg. Ezek nyolc jól elkülöníthető területet fedtek le: 1. IKT-rendszerek megbízhatóságának növelése a biztonságos tanúsítási szolgáltatásokkal és megoldásokkal; 2. kiberbiztonság a kis- és közepes vállalatok, a helyi közigazgatási szervezetek, valamint az állampolgárok számára; 3. egészségügyi adatok biztonságának rendszerszintű növelése; 4. a kiberbiztonság gazdaságtana; 5. EU-együttműködés és nemzetközi párbeszéd a kiberbiztonság és az adatvédelem területén; 6. kriptográfia; 7. a kiberbiztonság területén megjelenő új fenyegetések és azok kezelése; 8. személyes adatok kezelése, adatvédelem, digitális identitás. (H2020 2017b)

Minden fókuszterület, illetve az itt megjelenő pályázati kiírások meghatározott eredményt várnak el. Így például az említett új fenyegetésekről és azok kezeléséről szóló kiírás egyaránt elvár kutatást (elméleti megalapozást), valamint gyakorlatban megvalósított innovációt is, azaz közel kész terméket vagy szolgáltatást kell eredménytermékként elkészítenie a pályázatban résztvevőknek. (H2020 2017c)

Magyarország 2017 év közepéig közel 540 sikeres *H2020* pályázatot adott be, ami elnyert támogatásban közel 153 millió euró összeget jelent. Természetesen a *H2020* pályázatokban a legaktívabb hazai szereplők a Magyar Tudományos Akadémia különböző kutatóintézetei, valamint a nagy kutatóegyetemeink. Ugyanakkor több mint 140 kis- és közepes vállalkozás is sikeresen pályázott a kutatási alaphoz, amelyből 42 millió euró támogatást kaptak. Magyarország *H2020* pályázati aktivitása mind a megkötött támogatási szerződések számát, mind az elnyert támogatási összeget tekintve a 28 európai uniós országból

a 17. helyre elegendő, amely bár nem rossz, nagyon messze van az élmezőnytől. (H2020 2017d)

A *Horizont 2020* egy olyan egyedülálló lehetőség, amely a kutatás-fejlesztés-innováció bűvös háromszögén túl valós és kiemelkedő pénzügyi támogatást ad azoknak az ötleteknek, amelyek az EU célkitűzéseivel összhangban a gazdasági versenyképességen túl a biztonság megvalósítását és növelését célozzák meg. A támogatásra érdemes projektek és a mögöttük lévő ötletek kiválasztása egy nagyon jól átgondolt és szakmailag megalapozott szűrőrendszeren keresztül történik.[38] Az a közel 80 milliárd euró, amely a *H2020* hétéves futamideje alatt ezekre a célokra rendelkezésre áll, valóban nagy lökést adhat Európa és ezen belül térségünk fejlődéséhez is.

3.4.4. A kiberbiztonság európai uniós szervezetei

Az előzőekben nagyon röviden bemutattuk az Európai Unió stratégiai szintű tevékenységét a kiberbiztonság területén. Nyilvánvalóan a tagállamok nagy fokú önállósága ezen a területen is megvan, de pont a kibertér sajátosságai miatt elengedhetetlen, hogy legyen vagy legyenek uniós szinten is olyan szervezetek, amelyek a stratégiai irányelveknek megfelelő akciókat a gyakorlatban is meg tudják valósítani. Ez nagyon komoly koordinációs tevékenységet is jelent, hiszen például az EU kiberbiztonsági stratégiája esetében is láthattuk, hogy évek kellettek az egyszerű javaslatból végül minden tagország számára elfogadható döntés megszületéséhez.

---

[38] 2016-ban az Európai Bizottság felkérésére szakértőként részt vettem *H2020* pályázatok bírálatában a *Biztonságos társadalom* kutatási témacsoport *Digitális biztonság* fókuszterületen. A munka során tapasztalt kiválasztási és támogatást megelőző komplex eljárásrendszerbe bepillantást nyerve vált világossá számomra, hogy egy valóban jól működő pályázati rendszerről beszélhetünk a pályázatok benyújtásától azok elbírálásán át a későbbi megvalósítással és monitoringeljárásokkal bezárólag.

Ennek megfelelően a következőkben két európai uniós szervezetet – az EU Hálózat- és Információbiztonsági Ügynökséget (ENISA), valamint az EU Kiberbűnözés Elleni Központját (EC3) – mutatjuk be.

ENISA – Európai Uniós Hálózat- és Információbiztonsági Ügynökség

Az Európai Unió egyik legfontosabb kiberbiztonsági szervezete az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (European Network and Information Security Agency, ENISA).

Az ENISA központja Kréta szigetén Iraklióban (Görögország) található, de az ügynökség egy athéni operatív irodával is rendelkezik. (ENISA 2017a)

A 2004-ben alapított szervezet aktív közreműködője az uniós hálózati és információbiztonság megteremtésének és fejlesztésének. Az ENISA szoros kapcsolatban áll a tagállamokkal és a magánszektorral is. Mind az állami, mind a magánszféra számára képes tanácsokat adni és megoldásokat nyújtani a kiberbiztonság különböző területein. Az ügynökség egyik nagyon fontos tevékenysége a páneurópai kiberbiztonsági gyakorlatok megszervezése és megrendezése.[39] Mindezeken túl az ENISA fontos szerepet tölt be a tagállamok nemzeti kiberbiztonsági stratégiáinak kialakítása során is, hiszen konzultációs szervezetként a nemzetközi jó gyakorlatokkal ezekhez a dokumentumokhoz is elengedhetetlenül fontos tanácsokat ad.

[39] Ilyen nemzetközi kiberbiztonsági gyakorlat, illetve gyakorlatsorozat a 2010 óta kétévente megrendezett Kibereurópa (Cyber Europe). Ezeken a gyakorlatokon olyan – több országot érintő – kiberbiztonsági események szimulációi zajlanak, amelyek kezelése uniós szinten koordinált védekezést igényel. A kibergyakorlatok az incidenskezelés begyakorlása mellett lehetőséget adnak a kiberbiztonsági események technikai elemzésére, valamint az összetett üzletmenet-folytonosság és válságkezelési helyzetek gyakorlására. (ENISA 2017b)

Az ENISA részt vesz a nemzeti CSIRT-k együttműködésének szervezésében, és azok képességeinek fejlesztéséhez szintén hatékonyan hozzájárul.

Az ügynökség rendszeresen készít és tesz közzé tanulmányokat például az olyan kiberbiztonsági kihívásokról, mint a felhőalapú alkalmazások biztonságos használata, de emellett az adatvédelmet vagy a magánélet védelmét erősítő eljárások és technológiák is gyakran terítékre kerülnek.

Ugyanakkor az ENISA legfontosabb szakmai tevékenysége az Európai Unió, a kiberbiztonság területén megjelenő politikájának és jogi kérdéseinek kidolgozásában, valamint azok végrehajtásának támogatásában keresendő.

Az ENISA mindezen célok és feladatok elérése érdekében saját stratégiával rendelkezik. Ebben a ügynökség öt stratégiai célkitűzés mentén határozza meg saját feladatait a 2016–2020 közötti időszakra vonatkozóan. Első stratégiai célként a szakvélemény nyújtása jelenik meg a tagországok és azok kiberbiztonsági szervezetei számára. E tevékenység során a szervezet az új kihívások feltárásával, az azokról minél több és relevánsabb információ összegyűjtésével, elemzésével és a felhasználók rendelkezésre bocsátásával támogatja az európai digitális fejlődést. A második cél az EU kiberbiztonsági politikájának támogatása, amely magában foglalja a már említett uniós politika és jogrendszer kidolgozását, végrehajtásuk támogatását mind uniós, mind tagállami szinten. A következő célkitűzés a kapacitásbővítés és -fenntartás támogatása. Mind az uniós szervezetek, mind a tagállamok jelentős kiberbiztonsági kapacitásbővítést igényelnek az igen gyorsan változó technikai és technológiai kihívásoknak való megfelelés érdekében, így szükséges az ENISA részéről annak minél szélesebb körű támogatása. A negyedik cél a kommunikáció és a párbeszéd erősítése. Ez az európai hálózat- és információbiztonsági közösség együttműködésének erősítését jelenti, amely során az uniós és tagállami szintű párbeszéd katalizátora az ENISA. E párbeszéd erősítése nemcsak az uniós szervezetekre és az állami szereplőkre koncentrál,

hanem markáns figyelmet kap a magánszektor is. Az ötödik kiemelt cél az ENISA hatásának megerősítése. Ezt a szervezet erőforrásainak hatékonyabb kezelésével és a tagállamok, valamint az uniós intézmények intenzívebb bevonásával kívánják elérni. (Enisa 2017c)

EC3 – European Cybercrime Center

Az Európai Unióban csakúgy, mint a világ számos más táján, a kiberbűnözés egyre nagyobb károkat okoz. Bár korábban már említettük néhány kiberbűncselekmény által okozott kár mértékét, mégis nyugodtan kijelenthetjük, hogy a kiberbűnözés által okozott teljes kár nagyságrendjére is csak hozzávetőleges becslések[40] léteznek.

Magára a kiberbűnözésre sem találunk egységesen elfogadott meghatározást vagy definíciót. Az Interpol meghatározása alapján a kiberbűncselekmények két fő típusát lehet megkülönböztetni, amelyek egyben meg is határozzák a terület fogalmát: fejlett számítógépes bűnözés (vagy high-tech bűnözés), amely nagyon kifinomult támadásokat jelent a számítógépes környezet (hardverek és szoftverek) ellen, valamint a kibertér jelentette előnyök[41] kihasználására épülő bűnözés, amely a hagyományos bűncselekmények új dimenzióban történő folytatását jelenti, úgymint gyermekekkel szembeni bűncselekmények, a pénzügyi visszaélések és bűncselekmények, akár a terrorizmust is ideértve. (Interpol 2017)

Ahogy korábban utaltunk rá, az EU Kiberbiztonsági Stratégiája is tartalmaz egyfajta meghatározást a kiberbűnözésre, amely nagyban hasonlít a fenti Interpol által leírt definícióhoz, hiszen ebben is hangsúlyosan jelenik meg a hagyományos bűncselekmények online térben való folytatása, valamint „az információs rendszerek elleni támadások,

40 Az Interpol évente több milliárd dollárra teszi a globális kiberbűncselekmények által okozott károk nagyságrendjét. (Interpol 2017)

41 Az Interpol ebben az esetben a *cyber-enabled* angol terminust használja.

hozzáférés megtagadása vagy rosszindulatú szoftverek" alkalmazása. (Cybersecurity Strategy of the European Union 2013)

Ennek megfelelően az Europol is három nagy területre osztja a kiberbűnözést. Az első a szervezett bűnözői csoportok által elkövetett bűncselekmények, ezeken belül is különösen azok, amelyek nagy profitot jelentenek az elkövetőknek (például online csalások). A második csoportba azok a bűncselekmények tartoznak, amelyek súlyos kárt okoznak az áldozatoknak (például a gyermekek online szexuális zaklatása, kihasználása). A harmadik csoportba pedig azok a bűncselekmények sorolandók, amelyek az EU kritikus infrastruktúráit és információs rendszereit – beleértve a számítógépes támadásokat is – érintik. (Europol 2016b)

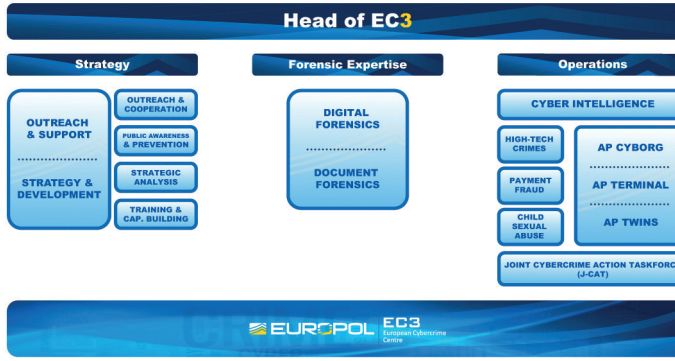
Mindezek miatt szükségessé vált az Európai Unióban is egy olyan központi szervezet felállítása, amely országhatárokon átívelő képességekkel, lehetőségekkel és kapacitásokkal képes felvenni a küzdelmet az online bűnözéssel szemben.

Az Európai Unió közös rendőri szervezete – az Europol – European Cybercrime Center (EC3), azaz Európai Kiberbűnözés elleni Központ néven egy olyan szervezetet hozott létre, amelynek fő feladata a kiberbűnözés visszaszorítása. (Europol 2017c)

Az EC3 2013 januárjában kezdte meg működését. Három nagy területre fókuszál: a kriminalisztikai vizsgálatokra (IT forensics), a kiberbűnözés elleni stratégiaalkotásra, valamint a kiberbűncselekmények felderítése érdekében végzett nyomozati cselekményekre.

Az EC3 a kiberbűnözés korábban említett mindhárom területén rendelkezik képességekkel, hiszen bűnügyi információs és hírszerzési központként is szolgál mindamellett, hogy operatív elemzésekkel, koordinációval és szakértőkkel támogatja a tagállamok kiberbűnözés elleni műveleteit és vizsgálatait. Az EC3 különböző stratégiai elemző

termékeket nyújt,[42] amelyek hozzájárulnak a kiberbűnözés elleni tevékenység során a reális döntések meghozatalához. A szervezet átfogó tájékoztatási funkcióval is bír, amely összeköti a tagországok bűnüldöző hatóságait, a magánszektor érintett szereplőit, az egyetemeket, kutatóintézeteket, valamint nemzetközi bűnüldöző szerveket. Az EC3 képzésekkel és kapacitásépítéssel támogatja a tagállamok kiberbűnözéssel foglalkozó hatóságait, de technikai és digitális igazságügyi szakértői támogatást is nyújt a kiberbűncselekmények felderítése és nyomozása során szükségessé vált vizsgálatokhoz. (Europol 2017c)



62. ábra

Az Európai Kiberbűnözés elleni Központ felépítése

Forrás: Europol 2017c

[42] Ilyen elemzés például a SOCTA (Serious and Organised Crime Threat Assessment, azaz a súlyos és szervezett bűnözéssel kapcsolatos fenyegetésértékelés), az IOCTA (Internet Organised Crime Threat Assessment, azaz az internetes szervezett bűnözéssel kapcsolatos fenyegetésértékelés), a TE-SAT (Terrorism Situation and Trend Report, azaz az EU terrorizmus helyzetéről és trendjeiről szóló jelentése), vagy a SCAN (Scanning, Analysis and Notification, azaz felderítés, elemzés és értesítés). (Europol 2017d)

Az EC3 két kriminalisztikai csoportot működtet, amelyek közül az egyikben a digitális igazságügyi szakértők, a másikban a dokumentumok bűnügyi szakértői kapnak helyet. A konkrét kriminalisztikai munkája mellett mindkét csoport az EC3 működésének támogatását, valamint kutatás-fejlesztést is végez. (Europol 2017c)

A stratégiaalkotás és azok fejlesztése szintén két csoportban történik: az első csoport feladata a tájékoztatás és támogatás, így koordinálva a már említett partnerek (EU-tagországok, más bűnüldöző hatóságok, nemzetközi szervezetek, akadémiai és gazdasági együttműködők) között a megelőzési és tudatosítási intézkedéseket. A másik csoport felelős a kiberbűnözés elleni stratégiai elképzelések kidolgozásáért és azok fejlesztéséért, amelyen belül stratégiai elemzéseket, politikai és jogalkotási intézkedések megfogalmazását, valamint szabványosított képzések fejlesztését végzik.

A kiberbűncselekmények elleni közvetlen tevékenység során annak a három csoportnak megfelelően történt a szervezet kialakítása, amelyek a kiberbűncselekményekben elkülöníthetőek. Ennek megfelelően az EC3 műveleti részlege tartalmaz egy high-tech kiberbűncselekmények elleni csoportot, egy online pénzügyi visszaélések elleni csoportot, illetve egy gyerekek online szexuális kihasználása elleni csoportot.

Mindezeket a csoportokat, illetve azok tevékenységeit egy úgynevezett Kiber Felderítési Csoport (Cyber Intelligence Team, CIT) is támogatja. A CIT gyűjti és dolgozza fel mindazokat a kiberbűnözéssel kapcsolatos információkat, amelyek állami, illetve magánforrásból vagy éppen egyéb nyílt forrásokból származnak, és amelyek alapján azonosíthatóak a kiberbűnözésre legjellemzőbb fenyegetések (továbbá az azokra utaló jelek és minták).

Az EC3 munkájának további támogatására egy Közös Kiberbűnözési Akciócsoport elnevezésű egységet (Joint Cybercrime Action Taskforce, J-CAT) is létrehoztak. E csoport legfontosabb feladata a kiemelt nemzetközi kiberbűncselekmények esetében a tagállamok bűnüldöző hatóságainak és szervezeteinek közvetlen támogatása. (Europol 2017c)

Az EC3 céljai elérése érdekében szorosan együttműködik a korábban már említett ENISA-val, valamint tagja a több mint 54 országot tömörítő *Globális szövetség a gyermekek ellen elkövetett online szexuális visszaélések (Global Alliance against Child Sexual Abuse Online)* megnevezést viselő kezdeményezésnek. Ezt az együttműködést az EU és az USA közösen indította el 2012. december 5-én. E kezdeményezésnek, illetve szövetségnek a legfontosabb céljai közé tartozik, hogy radikálisan csökkenjen a gyermekek kárára interneten elkövetett szexuális visszaélések száma. Ennek érdekében nemcsak az ilyen bűncselekményekkel kapcsolatos közös adatbázis felállítását, hanem többek között felvilágosító kampányok lebonyolítását is célul tűzték ki az együttműködő országok és szervezetek. (European Commission 2012)

3.5. Kiberbiztonság a NATO-ban

A NATO-ban komoly politikai és emellett stratégiai dilemmát is okozott a 2007-es észt incidens.[43] Ennek oka elsősorban az, hogy a szövetség fennállása alatt ez volt az első olyan – nem a fizikai dimenzióban bekövetkező – incidens (értsd kibertámadás), amely a kibertér veszélyeire, egyszersmind egy új korszakra hívta fel a figyelmet, és amely ráadásul a szövetség egyik tagországát érte. Ebben az új korszakban az egyik leglényegesebb elem maga a kibertér, illetve annak a realitása, hogy egy ország már nemcsak a korábban jól körülírt és viszonylag jól jellemezhető hagyományos dimenziókban (szárazföld, levegő, tenger, űr), hanem bizony az új dimenzión keresztül, azaz a kibertéren át is támadható.

Ez a felismerés a szövetségben oda vezetett, hogy a 2010-es lisszaboni NATO-csúcstalálkozó után a szervezet stratégiai koncepciójába is

[43] Az incidensre a DoS, illetve DDoS-támadások tárgyalásakor már utaltunk.

bekerült a katonai híradó és informatikai rendszerek védelmének feladata.[44] (NATO 2010)

A kiberfenyegetettség jelentette stratégiai szintű gondolkodás szerencsére azonban itt nem állt meg a NATO döntéshozói körében, hiszen 2011. június 8-án a NATO-tagországok védelmi miniszterei aláírták a szövetség új kibervédelmi politikáját. Ez a dokumentum nemcsak a kibervédelemre vonatkozó stratégiai elképzeléseket tartalmazta, hanem egy cselekvési tervet is magában foglalt. Ennek a cselekvési tervnek a részletes programját 2011 októberében fogadták el. (Kovács 2014)

2012 februárjában aztán elindult a NATO kiberincidens-kezelési képességének (NATO Cyber Incident Response Capability, NCIRC) teljes kiépítése, amellyel egyidőben egy úgynevezett kiberfenyegetés előrejelző központ (Cyber Threat Awareness Cell) kialakítása is megkezdődött. (NATO 2017; Kovács 2014)

Ugyanakkor a NATO életében a kiberteret érintő legnagyobb áttörésnek mégis a 2016-os varsói csúcstalálkozó nevezhető, hiszen ahogy korábban utaltunk rá, ekkor deklarálta a szövetség hivatalosan is, hogy a kibertér műveleti dimenziónak tekinthető. A kibertér tehát – legalábbis katonai értelemben – hadviselési dimenzióvá is vált. Mivel ez meghatározó jelentőségű a szövetség kiberteret érintő gondolkodásában, érdemes szövegszerűen is idéznünk a NATO hivatalos közleményéből a vonatkozó részt: „A számítógépes támadások egyértelműen kihívást jelentenek a szövetség biztonsága szempontjából, és ugyanolyan károsak lehetnek a modern társadalmak számára, mint a hagyományos támadások. Walesben megállapodtunk abban, hogy a számí-

[44] Ezt megelőzően a 2002-es prágai NATO-csúcsértekezletet követő zárónyilatkozatba már bekerült a szövetséget, illetve a tagországokat fenyegető veszélyek meghatározásánál a kibertámadások növekvő száma, illetve az ezekkel szembeni fellépés fontossága. Bár a zárónyilatkozatban összesen csak egy alkalommal szerepel a *kiber* mint kifejezés („Növelni kell védelmi képességeinket a kibertámadásokkal szemben” eredeti angol szöveg szerint “Strengthen our capabilities to defend against cyber attacks”), előremutató ez a tény, hiszen mindezen veszélyeket sajnálatos módon igazolták a 2007-es észtországi események. (NATO 2002)

tógépes védelem része a NATO kollektív védelmi feladatainak. Most Varsóban megerősítjük a NATO védelmi mandátumát, és elismerjük a kiberteret olyan műveleti területnek, amelyben a NATO-nak olyan hatékonyan kell megvédenie magát, mint a levegőben, a szárazföldön és a tengeren."[45] (NATO 2016)

Nemzetközi jog vs. kiberhadviselés, avagy a tallinni kézikönyvek

A kiberbiztonság egyik legszélsőségesebb, illetve legradikálisabb területe a kiberhadviselés. Amennyiben egy-egy kibertámadás vagy támadássorozat mögött egy ország áll, a támadás céljától és motivációjától függetlenül kiberhadviselésről beszélhetünk. Ugyanakkor addig, amíg a hagyományos fegyveres konfliktusokra már nagyon régóta szigorú és az egész világra kiterjedő nemzetközi hadijogi (vagy más néven humanitárius jogi) szabályozás létezik (például hágai egyezmények,[46] genfi konvenció[47]) a kiberhadviselésre jelenleg nem találunk egy az egyben alkalmazható nemzetközi jogi szabályokat. A *Tallinn Manual,* azaz a tallinni kézikönyv első kiadása 2013-ban jelent meg. Fő célja a kiberhadviselés területén alkalmazható nemzetközi jogi és nemzetközi hadijogi kérdések vizsgálata volt. A NATO tallinni kiberbiztonsági kiválósági központ koordinációjában számos egyetem és kutatóintézet közreműködésével elkészült munka – két nagy részre osztva: nemzetközi kiberbiztonsági jog (International Cyber Security Law), illetve a kiberhadijog (The Law of Cyber Armed Conflict) – hét fejezetben 95 úgynevezett szabályt azonosított és vizsgált meg a nemzetközi jog területén, amely

45 Az eredeti angol nyelvű szöveg: "Cyber attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea." (NATO 2016)

46 1899-ben, valamint 1907-ben Hágában nemzetközi konferenciák keretében olyan megállapodások születtek, amelyek komoly hatással voltak a hadviselésre (szárazföldi, tengeri, és már a légi hadviselésre is), és amelyek a modern hadi, illetve humanitárius jog alapjai. Az itt született megállapodások nyújtottak alapot a későbbi genfi konvenció megalkotásához. (Gazdag 2011)

47 1949 augusztusában Genfben elfogadott négy egyezmény, amelyek a hágai egyezményekre építve megállapítják a legfontosabb nemzetközi jogi szabályokat a fegyveres konfliktusokra.

vizsgálatok esetében alapvetően ezeknek a szabályoknak a kiberhadviselésben való alkalmazhatósága volt a fókuszban. (Schmitt 2013)

2016-ban jelent meg a *Tallinn Manual 2.0,* amely az első rész aktualizált és jelentősen kibővített változata. A könyv címe részben módosult, hiszen a kiberhadviselés explicit módon való megjelenítése helyett *A nemzetközi jog kiberműveletekben való alkalmazhatósága* címet kapta. A közel 600 oldalas tanulmány négy részre osztva már 154 olyan szabályt elemez, amelyek a nemzetközi jogból a kiberműveletekre lennének alkalmazhatóak. (Schmitt 2016)

3.6. Nemzetközi kiberbiztonsági szabványok és ajánlások

Ahogy láthatjuk, a kibertér védelme egy rendkívül dinamikusan változó és fejlődő terület. A technikai kihívásokra adott válaszoknak nemcsak technikai oldalról, hanem szabályozási oldalról is meg kell jelenniük. Ezért fontos azoknak a nemzetközi – esetenként hazai – szabványoknak és ajánlásoknak a megléte – valamint nem utolsósorban azoknak a mindennapi működés vagy üzemeltetés során történő alkalmazása –, amelyek egységes elvek mentén adnak választ arra a sokszor nem is egyszerű kérdésre, hogy milyen védelmi megoldásokat is alkalmazzunk, legyen szó technikai eszközökről, szoftverekről vagy akár szabályok bevezetéséről.

A következőkben bemutatni kívánt szabványokat és ajánlásokat javarészt az adott területen megfelelő tapasztalatokkal és nem utolsósorban nagy megbízhatósággal rendelkező szervezetek alkotják meg. Sokszor elhangzik az a megállapítás, miszerint a legjobb gyakorlatok összegyűjtésének és szabályzókba való átültetésének fontosságát nehéz lenne túlbecsülni. A többször és több helyen, ráadásul nemzetközi környezetben kipróbált megoldások, illetve az azokból levont, az ajánlásokban megjelenő következtetések jelenthetik a megoldást a terület biztonságának növelése érdekében.

A szabványok alkalmazása több évtizedes múltra tekinthet vissza, hiszen ezek bevezetése az adott szervezetben számos olyan előnnyel jár, amelyek hatékonyságnövekedést, magasabb fokú integrációt vagy akár az interoperabilitás növekedését jelenthetik. Így a szabványok alkalmazása nemcsak a biztonságban, hanem akár gazdasági előnyben is tetten érhető. Ez a kiberbiztonságra talán még hatványozottabban is igaz, hiszen a kibertér rendkívül összetett és komplex rendszerek egymásra épülése révén jön létre, amelyben a környezet standardizálása megfelelő út lehet a biztonság megteremtése felé (hiszen így átláthatóbb és egységesebb lesz a biztonság rendszere is), és akár az új technológiák bevezetése is egyszerűbbé és biztonságosabbá válik. Ebben az esetben is igaz, hogy a biztonság növelése egyenes arányban van az esetleges veszteségek csökkenésével. (Purser 2014)

Mindezeknek megfelelően nagyon röviden – a teljesség igénye nélkül – vizsgáljunk meg néhány olyan információbiztonsági szabványt, illetve ajánlást, amelyek a kiberbiztonság területén alkalmazhatóak!

3.6.1. Common Criteria (ISO 15408)

A *Common Criteria,* avagy teljes nevén *Common Criteria for Information Technology Security Evaluation,* azaz *Közös Követelményrendszer az Információtechnológia Biztonsági Értékeléséhez* egy olyan keretrendszer, amelynek segítségével meghatározhatóak a biztonság funkcionális és megbízhatósági követelményei. Ezek alapján az IKT-rendszerek és/vagy termékek függetlenül azok gyártóitól, illetve azok fajtáitól biztonsági osztályokba sorolhatók. Így meghatározható azok biztonsága. A röviden csak CC-nek hívott követelményrendszer nemzetközi szabvánnyá vált, hiszen az ISO az IEC-vel közösen ISO/IEC 15408 néven elfogadta (először 1999-ben még csak az ISO, majd

2005-ben az IEC-vel[48] közösen) azt. A CC jelenleg a 3.1[49] verziónál tart. A közös követelményeket 17 ország közösen fogadta el, és ezt az eredeti egyezményt közel egy tucat ország – köztük Magyarország is – társult tagként jegyzi.

Az eredeti egyezményt aláíró felek (és természetesen később a társult országok) négy nagy célt tűztek ki maguk elé a CC bevezetésével és alkalmazásával kapcsolatosan: annak biztosítását, hogy az IKT-termékek és védelmi profilok értékelése magas és következetes normákon alapuljon, és azok jelentősen járuljanak hozzá ezeknek a termékeknek és rendszereknek a biztonságához, valamint ezeken keresztül az ezek alkalmazása iránti bizalomhoz; növekedjen a biztonságos IKT-termékek száma; egységes legyen a termékek biztonságára irányuló vizsgálati módszertan; valamint hogy növeljék az értékelés hatékonyságát, és csökkentsék azok költségeit.

Az egyezményt aláíró országok képviselőket delegáltak egy úgynevezett irányító bizottságba, amely iránymutatásokat dolgoz ki az értékelési és érvényesítési tevékenységekre és megoldásokra vonatkozó nemzeti rendszerekhez. (Common Criteria 2017b)

A különböző IKT-termékeket kompetens és független, engedéllyel rendelkező laboratóriumok értékelik. Ezek a laborok a biztosítékok arra, hogy a vizsgált és minősített termékek megfelelnek a biztonsági követelményeknek. A bevizsgált és értékelt termékek biztonsági tulajdonságairól tanúsítványt állítanak ki. Ezeket a tanúsítványokat a CC-t aláíró országok elismerik. (Common Criteria 2017a)

A CC termékfüggetlenül hét védelmi szintre – *EAL1–EAL7* (azaz *Evaluation Assurance Level,* magyarul értékelési megbízhatósági szint) – sorolja be a vizsgált eszközöket és rendszereket. Egy-egy védelmi szint természetesen különböző olyan biztonsági követelmé-

---

48 *IEC: International Electrotechnical Commission,* azaz a *Nemzetközi Elektrotechnikai Bizottság (IEC)* a világ egyik olyan vezető szervezete, amely előkészíti és közzéteszi az elektromos, elektronikus és kapcsolódó technológiák nemzetközi szabványait. (IEC 2017)

49 A jelenleg érvényben lévő CC-változat pontos megnevezése: *CC version: 3.1 revision 5.* Ezt a verziót 2017 áprilisában adták ki. (Common Criteria 2017a)

nyeket tartalmaz, amelyek jól definiálhatók és így egymástól elválaszthatók, de azok garanciát nyújthatnak az azonos besorolást kapó termékek összehasonlítására. Ugyanakkor meg kell jegyezni, hogy ezek semmiképpen nem jelentik automatikusan a biztonság garantálását, hiszen az sok egyéb tényezőtől – például a felhasználás és alkalmazás különböző módjaitól, környezetétől és egyéb más összetevőktől – is függ.

A CC hazai adaptálása a MEH Informatikai Tárcaközi Bizottság 16. számú ajánlásaként 1998-ban történt meg (nyilvánvalóan az akkor érvényben lévő CC 1.0 verzióra érvényes módon). (Muha 2002)

3.6.2. ISO/IEC 27001

Az ISO/IEC 27000-es szabványcsalád az elektronikus információbiztonság – és így talán a kiberbiztonság – egyik legfiatalabb, ugyanakkor legmeghatározóbb tényezője. A szabványcsalád tagjai mára már az egyik legfontosabb nemzetközi szabvánnyá váltak a területen.

Az ISO/IEC 27000-es szabványcsalád ma több mint 20 különálló részből áll. Ezek a különálló szabványok mégis egy területhez – az *Információbiztonsági Irányítási Rendszerhez (IBIR)* vagy az angol megnevezéssel *Information Security Management System (ISMS)* –, illetve annak bevezetéséhez, fenntartásához és fejlesztéséhez adnak nemzetközileg elfogadott és a gyakorlatban is sok alkalommal kipróbált, bizonyított támpontokat.

A szabványcsalád története 1995-re nyúlik vissza. Ekkor jelent meg a brit BS7799, majd ezt követően 1999-ben a BS7799-2 szabvány. E két szabvány képezi a 2000-ben kiadott ISO/IEC 17799 szabvány alapjait. Ebből vált 2005-ben igazi információbiztonsági szabvánnyá az ISO/IEC 27000.

A szabványcsalád egyik legmarkánsabb tagja az ISO/IEC 27001-es szabvány. A szabvány hivatalos angol címe: ISO/IEC 27001:2013 *Information technology. Security techniques. Information security*

management systems. Requirements. Az ISO/IEC 27001:2013 hazai adaptációja az MSZ/T ISO/IEC 27001:2014, amely *Informatika. Biztonságtechnika. Információbiztonsági irányítási rendszerek. Követelmények* címet viseli. Ez váltotta fel a szabvány nyolc évvel korábban kiadott (hazai) változatát, az MSZ ISO/IEC 27001:2006-ot.

A 27001-es szabvány a tanúsítás alapja, azaz ez a szabvány az útmutató ahhoz a felkészüléshez – és természetesen magához az auditáláshoz is –, amely alapján felmérhető, hogy az adott szervezet az információbiztonsági irányítási rendszer területén milyen lépéseket tett, megfelel-e a szabványban leírtaknak. Önmagában természetesen ez is fontos, de talán a minősítésnél, illetve auditálásnál sokkal lényegesebb, hogy a szabványt alkalmazva valóban lehetőség van egy jól működő – fenntartható és folyamatosan fejleszthető – információbiztonsági irányítási rendszer kialakítására. Ez a tény önmagában is nagy előrelépést jelenthet az adott szervezetnél az információbiztonság fokozására. A 27001 szerkezeti felépítése tudatosan követi az ISO/IEC szabványok felépítését, azaz a más területek irányítási rendszereinek szabványai felépítésével harmonizál (ilyen szabványok például az ISO 9001, 14001, 18001).

Az ISO/IEC 27001 az úgynevezett *Plan-Do-Check-Act (PDCA)* modellre épül, ami a folyamatszervezés tudományában a különböző termékek és folyamatok menedzselésére az egyik legelterjedtebb módszer.

A 27001-es szabvány törzsszövegének terjedelme mindösszesen néhány oldal (egészen pontosan 12 oldal), amit egy nagyon fontos melléklet követ. Ez az „A" melléklet,[50] amely a *Szabályozási célok és szabályozások*[51] címet viseli. Ebben a mellékletben kaptak helyet azoknak a területeknek a szabályzói, amelyek lefedik a komplex információ-

[50] Az eredeti *ISO/IEC 27001:2005* szabványban az „A" melléklet után még két melléklet kapott helyet: a „B" melléklet, amely az OECD alapelveit és a szabvány kapcsolatát, amíg a „C" melléklet más szabványokkal – például ISO 9001 – való kapcsolódást mutatta be. (ISO/IEC 27001:2005)

[51] Az „A" melléklet angol címe: *Reference control objectives and controls.*

biztonság minden területét, kezdve az adminisztratív biztonságtól az elektronikus információbiztonságon keresztül a fizikai biztonságig. Ezek a kontrollok fontos szerepet játszanak a szervezet információbiztonságának megvalósításában, hiszen az adott szervezet egy úgynevezett *Alkalmazhatósági nyilatkozatban (Statement of Applicability, SoA)* rögzíti, hogy az adott kontrollok közül melyiket alkalmazza és melyiket nem. A szabvány ezeknek a kontrolloknak az alkalmazását nemcsak ebben a nyilatkozatban kéri, hanem a különböző területekre – például az incidenskezelés – külön szabályzót és külön dokumentációt is előír.

Természetesen a szabványcsalád többi tagja is fontos, hiszen például az MSZ ISO/IEC 27002:2011, amelynek hivatalos magyar címe *Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve,* aprólékosan elmagyarázza mindazokat a kontrollokat, azaz szabályozási javaslatokat, amelyeket a 27001 meghatároz.

Az auditálást, azaz egy adott szervezet szabványnak való megfelelőség vizsgálatát az MSZ ISO/IEC 27006:2013 – hivatalos magyar címén *Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszereinek auditját és tanúsítását végző testületekre vonatkozó követelmények* – szabvány írja le. (Magyar Szabványügyi Testület 2017)

3.6.3. A NIST kiberbiztonsági kiadványai

Az Amerikai Egyesült Államok korábban is élen járt az információbiztonságot meghatározó szabályzók kialakításában. Gondoljunk csak például az úgynevezett *TCSEC* (*Trusted Computer System Evaluation Criteria,* azaz a magyarul használatos címével élve *Biztonságos Számítógépes Rendszerek Értékelési Kritériumai*) kiadványra, amelynek első kiadása 1983-ban jelent meg az USA Védelmi Minisztériumának megrendelésére, és amely az informatikai biztonsági követelményeket gyűjtötte össze olyan előremutató módon, hogy annak egyes elemei

még napjainkban is használatosak mint meghatározó követelmények a katonai eszközök beszállítóinak vonatkozásában. (Department of Defense 1983)

A NIST (National Institute of Standards and Technology, azaz Nemzeti Szabványügyi és Technológiai Intézet) az Amerikai Egyesült Államok Kereskedelmi Minisztériumának szabványügyekkel és tanúsításokkal foglalkozó intézménye. (NIST 2017)

A NIST számos kiadvánnyal segíti az információbiztonságot és a kiberbiztonságot. Ezek közül talán az egyik legfontosabb a *NIST Special Publication 800,* ezen belül is a *NIST SP 800-53,* amely a szövetségi információs rendszerek és szervezetek számára ír le információbiztonsági és adatvédelmi irányítási elveket. (NIST 800-53 2013)

A NIST ezen kívül a kritikusinfrastruktúra-védelem területére is ad ki ajánlásokat.[52] Ezeknek – mint például a *Keretrendszer a kritikus infrastruktúra kiberbiztonságának fejlesztésére* (amelynek az eredeti angol címe: *Framework for Improving Critical Infrastructure Cybersecurity*) – fő célja a gazdaság gerincét és működőképességét jelentő kritikus infrastruktúrán belüli különböző ágazatokban megjelenő kiberbiztonság növelése. A keretrendszer legfőbb filozófiája a saját megfogalmazása szerint: „A kormányzat és a magánszektor együttműködésével létrehozott keretrendszer közös nyelvet használ a kiberbiztonsági kockázatok kezelésére, valamint azok költséghatékony módon az üzleti igények alapján történő csökkentésére anélkül, hogy további szabályozási követelményeket határozna meg." (NIST 2014)

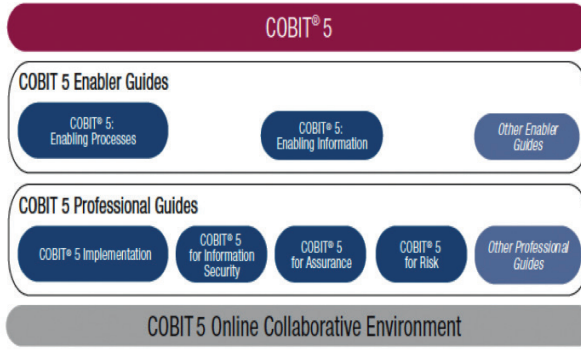
[52] A NIST ilyen irányú tevékenysége törvényi kötelezettség is. Az USA Kongresszusa 2014-ben például a *Törvény a kiberbiztonság növelésére (Cybersecurity Enhancement Act of 2014)* jogszabállyal a NIST-nek is számos feladatot adott a kiberbiztonság növelésének területén. (S.1353 – Cybersecurity Enhancement Act of 2014)

3.6.4. COBIT

A *COBIT* (*Control Objectives for Information and Related Technology,* azaz *Informatikai Irányítási és Ellenőrzési Módszertan*) eredetileg az ISACA[53] és az IT Governance kiadványa, amely elsősorban üzleti környezetben ad eligazítást – és így nyilván nem kis segítséget – az információtechnológia alkalmazásához és annak menedzseléséhez a gazdasági tevékenységet végző szervezetek esetében. Mindezeken belül négy fő üzleti folyamatra, illetve az azokban alkalmazható informatikai megoldásokra – tervezés és szervezés; beszerzés és üzembe állítás; informatikai szolgáltatás és támogatás; felügyelet – helyezi a hangsúlyt. (Muha–Krasznay 2014)

Az ISACA a *COBIT-ot* első változatban 1996-ban jelentette meg. Ma már a *COBIT* ötödik kiadása, illetve ötödik verziószámú változata van érvényben. Maga az ajánlás gyakorlatilag egy egész ajánláscsomag, amely magában foglalja azokat az útmutatókat, amelyek részletesen bemutatják az irányítási képességeket. Ezek két nagy részre oszthatók: *COBIT 5: engedélyezési folyamatok;* valamint *COBIT 5: szakmai útmutatók,* amelyeken belül megtalálhatók az implementációra és a jövőben tervezetten többek között a megbízhatóságra és a kockázatokra vonatkozó ajánlások. (ISACA 2017)

[53] ISACA: Information Systems Audit and Control Association.



63. ábra
A COBIT 5 összetevői

Forrás: ISACA 2017

3.6.5. ITIL

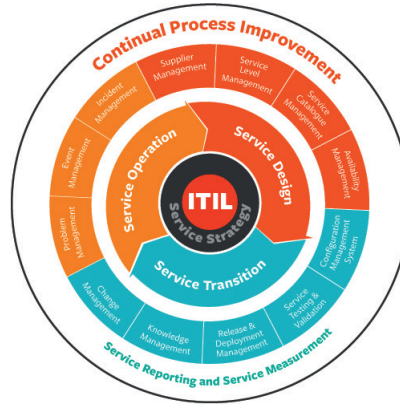
Az *ITIL,* azaz az *Information Technology Infrastructure Library,* azaz a hazai szakmai terminológiában *Az informatikaszolgáltatás módszertana* egy olyan módszertani kézikönyvsorozat, amely eredetileg szintén egy brit ajánlásra épült. Az ITIL ma már nemzetközi szabvánnyá vált, ugyanis ez a BS 15000 ISO/IEC 20000 szabvány. (Muha–Krasznay 2014)

Az ITIL legfontosabb célja, hogy olyan magas szintű, ugyanakkor költséghatékony informatikai szolgáltatásokhoz adjon ajánlásokat, amelyek a termékek és rendszerek teljes életciklusára vonatkoznak a tervezéstől/bevezetéstől a működtetésen át azok kivezetéséig, illetve az újabb rendszerek bevezetéséig. Az ITIL, az ISO/IEC 27001-hez hasonlóan szintén a PDCA-modellt használja.

Az ITIL, illetve az ebből szabvánnyá vált ISO/IEC 20000 egy olyan legjobb módszergyűjtemény és az ezekből kialakított minimumkövetelmények meghatározása, amely az informatikai infrastruktúra üzemeltetésére és az informatikai szolgáltatások menedzselésére

ad támpontokat. Ezt a tevékenységet sok gyártó – például a Microsoft – azzal igyekszik segíteni (és ezzel együtt persze saját piaci előnyeiket is), hogy termékeiket eleve az ITIL-nek megfelelően gyártják.

Az ITIL olyan tevékenységekhez is segítséget nyújt, mint például a felhőszolgáltatások bevezetése során az adatok felhőbe történő migrálása. (Haentjens 2012)



64. ábra
Az ITIL életciklusa

Forrás: BMC 2016

Az ITIL első hazai adaptálása a MEH Informatikai Tárcaközi Bizottság 15. számú ajánlása volt 2002-ben, amelyben az ITIL 3.1-et adták ki. (Muha 2002)

3.6.6. Hazai információbiztonsági ajánlások

Bár meglehetősen régen – 2008-ban – látott napvilágot a korábban már részeiben említett hazai ajánlásokat összefoglaló, illetve azokat leváltó ajánlássorozat, amely a Közigazgatási Informatikai Bizottság 25. számú ajánlása, érdemes néhány pillantást vetnünk ezekre is.

Az 1990-es évek közepétől folyamatosan jelentek meg hazánkban is olyan ajánlások, amelyek jórészt az információbiztonság különböző területeinek nemzetközi ajánlásait, illetve szabványait adaptálták hazai környezetre. Ilyenek voltak például az ITB 8. számú ajánlása, amely *Az informatikai biztonság módszertani kézikönyve* címet viselte, az ITB 12. számú ajánlása, amelynek címe *Az informatikai rendszerek biztonsági követelményeiről* volt, illetve a már említett ITB 16. számú ajánlás *A Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertanáról*.

Ezeket az ajánlásokat váltotta fel, illetve egészítette ki a 2008-ban kiadott ITB 25. számú ajánlásgyűjteménye, amely a *Magyar Informatikai Biztonsági Ajánlások (MIBA)* címet kapta. (Muha–Krasznay 2014)

A *MIBA* magában foglalta a *Magyar Informatikai Biztonsági Keretrendszert (MIBIK),* amely a szervezetek számára ad a biztonságos informatikai rendszerek irányításához, azok menedzseléséhez ajánlásokat; a *Magyar Informatikai Biztonság Értékelési és Tanúsítási Sémát (MIBÉTS),* amely a szervezetek helyett technológiai szempontú megközelítésben kezeli az informatikai biztonságot építve a Common Criteriára; valamint az *Informatikai Biztonsági Iránymutató Kis Szervezetek Számára (IBIX)* című ajánlást. Az *IBIX* olyan kisvállalkozásoknak nyújt eligazodást az informatikai rendszereik biztonságos kialakításához és üzemeltetéséhez, amelyeknek nincs jelentősebb informatikai háttere, illetve nincs különálló informatikai kezelőszemélyzete. (Muha–Krasznay 2014)

3.7. A kiberbiztonság gyakorlati megvalósításáról

A kiberbiztonság, illetve az információbiztonság komplex területeire többször is utaltunk már jelen könyv korábbi fejezeteiben. Az nyilvánvaló, hogy minden egyes terület – legyen szó adminisztratív, fizi-

kai, személyi vagy akár a több elemében már érintett elektronikus információbiztonságról – külön-külön is olyan nagy területek, amelyek terjedelmükben nemcsak, hogy egy könyvben, több kötetben sem lennének teljes egészében bemutathatók.

Ráadásul mind a kiberbiztonság, mind ezen belül az információbiztonság fejlődése és folyamatos változása olyan ütemű, hogy annak követése és bemutatása hagyományos eszközökkel majdhogynem lehetetlen. Igaz ez jelen könyvre is, hiszen annak megírása és megjelenése bár csak néhány hónapot vett igénybe, ezen idő alatt számos dolog alapjaiban változott meg.

Persze számos olyan izgalmas eleme van a kiberbiztonságnak és az információbiztonságnak is, amelyek a számítógépeink mint munkaállomások jelszavas, tűzfalakkal ellátott védelmétől a hálózatbiztonságon át a kibertérben megvalósuló folyamatosan fenntartott, stratégiai szinten meghatározott intézkedések és azok betartásának vagy (akár hatósági úton történő) betartatásának területéig terjed.

Ugyanakkor a fentieknek megfelelően a korábban is említett filozófia szerint a kiberbiztonság olyan elemeire, tényezőire és összefüggéseire fókuszálunk csak, amelyek majdhogynem függetlenek az említett gyors technikai és technológiai változásoktól.

A kiberbiztonságot is meghatározzák az olyan alapvetések, mint a kockázatokkal arányos védelem kialakítása – amely feltételezi a kockázatok felmérését és azok reális kezelését – vagy a fizikai védelmi intézkedések mellett a humánerőforrást – azaz az adatokat, információkat vagy az információs rendszereket kezelőket, üzemeltetőket – érintő felkészítés, oktatás, továbbképzés folyamatos és visszacsatolt megléte, vagy az egyre inkább meghatározó jelentőségű korai előrejelzés – benne a jól működő riasztással és jelzéssel –, amelyek egyre inkább elengedhetetlenül fontossá válnak.

Mindezeknek megfelelően a kiberbiztonság teljes volumenére kiterjedő védelem egészének alapos bemutatása helyett egy-egy fontosabb részterület bemutatására vállalkozunk csak a továbbiakban.

Mielőtt azonban ezt megtennénk, ki kell térnünk az információbiztonság komplex értelmezésére és annak komplex megvalósítására egy szervezetnél, ami paradox módon nem a védelem kialakításával kezdődik, hanem egy dokumentummal. Ez a dokumentum pedig nem mást tartalmaz, mint az adott szervezet informatikai biztonságpolitikáját. Ez a gyakorlatban egy nagyon rövid, de világosan és érthetően megfogalmazott kinyilatkoztatása annak, hogy az adott szervezet vezetése elkötelezett a biztonság iránt. Ebben a politikában kap helyet annak a kifejezése is, hogy az adott társaság mely összetevőket (például az ügyfelek adatai) tekinti a legfontosabb védendő tényezőnek, és mit tesz meg annak érdekében, hogy ez megvalósuljon. Ez egy olyan nyilvános dokumentum, amely az adott szervezet biztonság iránti elkötelezettségét hivatott bemutatni, és amely dokumentum alapját képezi az adott szervezet információbiztonsági stratégiájának. Így ez közvetve hatással van a szervezet információbiztonsági szabályzatára, hiszen a politikában megfogalmazott elvek és célkitűzések megvalósítását írja majd le a szabályzat.

Mindezen dokumentumok az információbiztonsági alapelvek – bizalmasság, sértetlenség, rendelkezésre állás – figyelembe vételével készülnek úgy, hogy a fizikai, az adminisztratív és logikai védelmi intézkedések meghatározásán túl, azokban megjelenik a szükséges anyagi és humánerőforrások biztosítása is.

3.7.1. Kockázatok felmérése és kezelése

Az ma már alapvető, hogy a kibertér biztonságának megteremtése azoknak a kockázatoknak a felmérésével kezdődik, amelyek a legnagyobb kihívásokat jelentik az információs rendszereinkre. A kockázatok felmérése azonban egy rendkívül összetett folyamat. Bár számos nemzetközi szabvány és ajánlás is foglalkozik a kérdéssel – például

az ISO/IEC 27005[54] –, meglehetősen nagy misztikum övezi a kérdést. Sok esetben az adott szervezet hozzáértés és tapasztalat hiányában vagy csak a kezelhetőség és a gyorsaság miatt kiszervezi ezt a feladatot, azaz egy erre szakosodott céget bíz meg a kockázatelemzés elkészítésével.

A kockázatelemzés és a kockázatok kezelése együtt jelenti a kockázatmenedzselést, amely során a releváns – a rendszereinkben és a szervezetünkben meglévő sebezhetőségeket és sérülékenységeket esetlegesen kihasználó – veszélyforrások feltérképezése és a kockázatokkal arányos védelem kialakítása is megtörténik.

A kockázatmenedzsment első fázisa a kockázatelemzés, amely általában egy adott szervezet esetében inkább kockázatbecslést jelent. Erre számos módszer terjedt el az elmúlt években és évtizedekben, sőt némelyik, mint például a CRAMM[55], szoftveres támogatással is rendelkezik. A kockázatok felmérésénél első feladat annak meghatározása, hogy milyen eszközökkel is rendelkezik az adott szervezet. Ez hivatalos megfogalmazás szerint a vagyonleltár elkészítését jelenti, amelyet az ISO/IEC 27001-es szabvány konkrétan meg is követel. A probléma azonban az, hogy nagyon sok szervezet, bár rendelkezik eszköznyilvántartással, nem tudja megmondani 100%-os biztonság-

---

54 Az ISO/IEC 27005 szabvány azokat az információbiztonsági kockázatkezelésre vonatkozó irányelveket írja le, illetve mutatja be, amelyek egy szervezetre vonatkozóan alkalmazandóak az ISO/IEC 27001 szabványban megfogalmazott követelmények szerint. Ugyanakkor ez a szabvány – hasonlóan a 27001-hez – nem határoz meg konkrét módszereket az információbiztonsági kockázatkezelésre. A kockázatok kezelésére alkalmazandó módszerek kiválasztása az adott szervezet feladata. Ebből következően maga a kockázatfelmérés és kockázatkezelés megközelítése, azaz annak filozófiája is nyitott lehet. Így az adott szervezetre van bízva, hogy a létező számos kockázatkezelési módszertan közül melyiket alkalmazza. (ISO/IEC 27005:2011)

55 A CRAMM a brit Központi Kommunikációs és Telekommunikációs Ügynökség (Central Communication and Telecommunication Agency, CCTA, jelenleg új nevén Office of Government Commerce, OGC) által kidolgozott kockázatelemzési és -kezelési módszer (Risk Analysis and Management Method). A módszer alapvetően az ipar és a kormányzati szervezetek számára készült, hiszen az ott használt legjobb gyakorlatokra épülő megoldásokat tartalmazza alapként. Természetesen más szervezetek számára is alkalmas lehet a kockázat felmérésére e módszer. (ENISA 2017d)

gal, hogy milyen eszközei – beleértve a hardver és szoftver összetevőket is – vannak. Ebben az esetben a kockázatelemzés valóban csak kockázatbecslés lesz, hiszen ha nem tudni a pontos eszközöket, azok technikai részleteit vagy pontos specifikációit, akkor azt sem nagyon tudja az adott szervezet eldönteni, milyen sérülékenységeket tartalmazhatnak az ezeken a hardvereken futó szoftverek vagy akár maguk a hardverek.

A kockázatelemzés következő lépése pedig pont annak a meghatározása, hogy a sérülékenységeket számba véve milyen támadásokkal vagy konkrét veszélyekkel kell számolnia az adott szervezetnek. Az is nyilvánvaló, hogy a veszélyek feltárásának a humánerőforrás, azaz a dolgozók vonatkozásában is meg kell történnie, sőt az adott szervezet munkafolyamatait is fel kell térképezni a vagyonleltár készítése során, hiszen ebben is jelenhetnek meg olyan sérülékenységek, amelyeket egy-egy támadás kihasználhat, és így kiesik az adott munkavállaló, aki pont kulcsfontosságú az adott folyamatban. A korábban már említett három alapvetés, azaz a bizalmasság, sértetlenség és rendelkezésre állás az a hármas tétel, amely alapján a kockázatokat minden egyes vagyonelemnél értékelni kell. Ezt követően lehet ezeket a kockázatokat összegezni és meghatározni, hogy ezek közül melyek azok, amelyek kezeléséhez szükséges valamilyen intézkedés meghozatala és végrehajtása.

Nyilvánvalóan a kockázatok felmérésére és kezelésére egy olyan stratégia kialakítása célszerű, amely az adott szervezet irányítási rendszerével (céljaival, folyamataival és nem utolsósorban szervezeti kultúrájával) harmonikus viszonyban van. Nagyon gyakran tapasztalni, hogy a kockázatok kezelése érdekében meghozott intézkedések az adott szervezet működésébe olyan drasztikus beavatkozásokat jelentenek, amelyek pont az ellenkező hatást váltják ki, mint amelyet az intézkedések meghozatalával remélnek.

Ugyanakkor természetesen lesznek olyan kockázatok, amelyek kezelése csak irreális befektetéssel vagy energiával lenne csak végre-

hajtható. Ilyenkor nem marad más választása az adott szervezetnek, mint felvállalni ezeket a kockázatokat.

A megfelelő kockázatmenedzsment és annak szabályzói (kontrolljai) szerves részei lesznek a jól működő információbiztonsági irányítási rendszernek. Fontos azt hangsúlyozni, hogy minél nagyobb, minél összetettebb az adott szervezet, annál inkább biztos, hogy az információbiztonság jól körülhatárolható területein túl is figyelembe kell venni számos tényezőt. Ebben az esetben már sokkal inkább kiberbiztonságról beszélhetünk, hiszen ebben az esetben már a más szervezetekhez, esetleg az államhoz vagy a közigazgatás más szereplőihez, akár az országhatárokon átnyúlva is meg kell határozni az adott szervezet biztonságának számos elemét, ami a logisztikától – és az abban foglalt kiberbiztonságtól – kezdődően, a képzésen és humánerőforrás utánpótlásának biztosításán át, akár a beszállítók és az ott megvalósuló kiberbiztonság kialakításáig, megteremtéséig, illetve annak folyamatos ellenőrzéséig tart.

3.7.2. Korai előrejelzés a kibertérben

Az első hallásra kissé meglepő kifejezés – korai előrejelzés a kibertérben – mögött nagyon reális igény van. Mivel a kibertámadások, amennyiben azok bekövetkeznek, néhány ezred másodperc alatt le is zajlanak – kivétel ez alól persze a túlterheléses támadások, amelyek akár hosszú időn keresztül is fennállhatnak, illetve az APT támadások, amelyek pont amiatt veszélyesek, mert sok kisebb, főleg információszerzési célú támadást foglalnak magukba és sokáig észrevétlenek –, ezért azok ellen a bekövetkezésük után már nagyon nehéz bármit is tenni, és ebben az esetben a védekezés már csak a támadások következményeinek felszámolására vagy az okozott károk csökkentésére koncentrálhat. Ebbe bele lehet, sőt bele is kell érteni a bekövetkezett támadások elemzéséből levont következtetések felhasználását a védelem fokozása, javítása érdekében. Ebben az esetben az idő az egyik legfontosabb

tényező, hiszen minél gyorsabban az incidenskezelő tudomására jut egy-egy támadás (incidens), és minél gyorsabban sikerül annak működési mechanizmusát,[56] (arról a sérülékenységről szóló információval együtt, amelyet a támadás kihasznált) megérteni, annál valószínűbb, hogy hatékonyan lehet fellépni a jövőben bekövetkező hasonló támadásokkal szemben, illetve annál hatékonyabb lehet a támadás által okozott károk felszámolása. Ehhez a munkához számos ajánlás áll az incidenskezelők rendelkezésére, amelyeket többek között az ENISA adott ki az elmúlt években. (ENISA 2017e)

Ugyanakkor a támadások megelőzésére reális igény mutatkozik, amely a potenciálisan bekövetkező támadások felderítésén és azok előrejelzésén alapulhat. Ennek érdekében korai figyelmeztető és előrejelző rendszerek kialakítására van szükség.

Ezek az előrejelző rendszerek összetett rendszerek, amelyek különböző forrásokból származó adatok és információk összegyűjtésével, feldolgozásával és elemzésével a potenciális támadókat, illetve azok támadási módszereit kutatják.

Az adatok és információk különböző automatizált, a hálózatban, illetve a védendő infrastruktúrában különböző helyeken elosztva telepített szenzoroktól (ezek lehetnek hardverek és szoftverek is) származhatnak, amelyek a közigazgatás vagy az ipar információs rendszereiben, illetve hálózataiban vannak elhelyezve. Ugyanakkor ezen adatgyűjtés során az ipari folyamatokban lévő SCADA- és PLC-rendszerek esetében kiemelt fontosságú, hogy az azokon keresztül megvalósuló folyamat ne sérüljön, így a szenzorok adatait alapvetően nem helyben, hanem emulálva dolgozzák fel.

---

[56] Ezzel kapcsolatban nagyon érdekes és előremutató tanulmányt jelentetett meg a Lockheed Martin cég három munkatára 2011-ben, amelyben a katonai terminológiából kölcsönzött *kill-chain* kifejezésnek, azaz szabad fordításban a *támadás folyamatának* nevezték és írták le a támadás működési mechanizmusát. A tanulmány arra a tényre hívta fel a figyelmet, hogy a megelőző felderítés és információszerzés, valamint az így megszerzett használható információk segítségével kialakított védelemmenedzsment mennyiben lehet hatékonyabb az eseménykövető, azaz a támadások bekövetkezése utáni információszerzésen alapuló védekezésnél. (Hutchins–Cloppert–Amin 2011)

Az előrejelző rendszerek olyan mintákat keresnek, amelyek korábbi támadások módszereit elemezve már rendelkezésre állnak, illetve esetenként olyan honeypotokat[57] tartalmaznak, amelyek adatai szintén felhasználhatóak a támadások előrejelzésénél. A szenzoroktól származó adatok párhuzamos feldolgozása, azok összevetése a hálózati forgalom – például az abban megjelenő, a megszokottól eltérő jelek – elemzése eredményeként megjelenő információkkal a biztonsági központokban (Security Operation Center, SOC), illetve a központok munkatársainak elemzéseivel kiegészítve, grafikus megjelenítéssel társítva hozzájárulhatnak a potenciális támadások időbeni (előre) jelzéséhez.

A kibertéri korai előrejelző rendszerre egy megvalósult példa a lengyelországi Arakis-Gov rendszer, amelyet a Cert.Gov.pl működtet. (Kovács 2012)

Az Arakis-Gov egy olyan internetes korai figyelmeztető rendszer, amelyet a lengyel Belső Biztonsági Ügynökség és a NASK[58] intézeten belül működő CERT Polska közösen fejlesztett. Az Arakis-Gov rendszer célja, hogy támogassa a lengyel közigazgatás információs rendszereinek védelmét. Hangsúlyozni kell az Arakis-Gov esetében is, hogy ez nem egy hagyományos biztonsági rendszer, és nem helyettesíti a már megszokott hálózati védelmi rendszereket – mint például a tűzfalakat, IDS- és IPS-rendszereket – hanem azokat kiegészítve járul hozzá a biztonság növeléséhez. (CERT.GOV.PL 2017)

---

57 A honeypotok azok a csapdák, amelyek az éles rendszerek felépítéséhez, illetve az abban lévő folyamatokhoz megszólalásig hasonló módon, de az éles rendszerektől elválasztva, a behatolókat (támadókat) megtévesztve működnek. Így ezek a csapdák a támadók tevékenységének, képességeinek, kapacitásainak és lehetőségeinek a megfigyelésére alkalmazható védelmi megoldások.

58 A NASK kutatóintézet a lengyel Digitális Ügyek Minisztériumának alárendelt szervezeteként a kiberbiztonság különböző területein végez kutatás-fejlesztési munkát. Ilyen K+F-tevékenység például a biometrikus azonosítási módszerek a szolgáltatások biztonságának növelése, de ezen kívül a szervezet a NASK Akadémián keresztül oktatásokat és tudatosító kampányokat is szervez és vezet. Mindezeken kívül a NASK a doméntartomány lengyel nemzeti nyilvántartója. A NASK-on belül működik egy Nemzeti Kiberbiztonsági Központ, amelynek feladata a kiberbiztonsági fenyegetések kezelése. (NASK 2017)

3.7.3. Biztonság a fizikai térben

Bár a kibertér és annak határai nehezen megfoghatók, a fizikai eszközök – számítógépek, hálózati, adatátviteli, kommunikációs és tucatnyi más eszköz – azok, amelyeken keresztül a kibertér felépül és megvalósul úgy, hogy annak mi is részesei vagyunk.

Ebből következően ezeknek az eszközöknek a fizikai védelme hasonlóan fontos terület, mint a kiberteret felépítő szoftverek vagy az abban lévő információk és folyamatok védelme. A fizikai biztonság megvalósítása azonban összetett intézkedéseket igényel. E terület szakirodalma is meglehetősen gazdag, amelyben általában a területet a mechanikai védelemre, az elektronikai védelemre és az élőerős védelemre osztják. (Muha–Krasznay 2014)

Ezen a ponton szintén utalnunk kell arra, hogy a terület átfogó és teljes körű elemzése helyett csak annak fontosságát kívánjuk hangsúlyozni. A szervezet információbiztonsága a fizikai környezetben megvalósuló fizikai védelmi megoldások, intézkedések és eszközök rendszerbe foglalt együtteséből kell, hogy álljon. Gyakran elhangzó bírálat és anekdotaszerű idézet, hogy az információbiztonság egyik leggyengébb láncszeme maga az ember, vagyis a felhasználó. Sokszor azzal a vicces mondással is jellemzik ezt a tényt, hogy az információbiztonság egyik leggyengébb pontja a billentyűzet és a szék között foglal helyet. Ezt bár gyakran az élet írta, jellemzően igaz tapasztalat, mégis sokszor jellemző a fizikai biztonságra is.

Már az eszközök fizikai elhelyezésének megtervezése során számos olyan kritériumot vagy rendezőelvet kell, pontosabban kellene figyelembe venni, amelyek megvalósítása szervezettől függően nem mindig lehetséges (például anyagi, elhelyezései stb. okok miatt). Ilyen elv többek között, hogy a biztonsági rendszerek és folyamatok ne jelentsenek kockázatot magukra a védendő eszközökre, illetve folyamatokra. Hasonlóan fontos elv, hogy a természeti vagy ipari katasztrófák által jelentett esetleges kockázatok minimálisak legyenek, illetve a funkcionálisan elkülönülő rendszerek fizikailag is legyenek elvá-

lasztva, amely során még azt is meg kellene valósítani, hogy a fizikai hozzáférés csak az arra jogosultak számára legyen lehetséges. (Muha–Krasznay 2014)

Ugyanakkor a fizikai biztonság területe az egyik leginkább érintett terület akkor, amikor a szervezet fejlesztése és fejlődése bekövetkezik. Az információbiztonságban az már korábban is sokszor hangsúlyozott alapvetés volt, hogy a szervezet kialakításával párhuzamosan, annak megindításakor célszerű a szervezet várható teljes életciklusára egy olyan biztonsági tervet készíteni, amelyben a szervezet várható fejlődése (például méretnövekedése, munkatársak számának, fizikai helyének változása vagy a mobilitásuk biztosítása) lehetőség szerint előre megtervezett, és a fizikai védelmi megoldások is ehhez igazodnak. Ez azonban nehezen kiszámítható és nehezen prognosztizálható. Ennek megfelelően a tervezés nagyon gyakran a jelen információit felhasználva történik, és abban az esetben, amikor a szervezet növekedését a fizikai védelemnek követnie kell, az nagy befektetést követelne meg. Ebből következően nagyon sokszor szükségmegoldások lesznek azok, amelyeket a szervezet meglép, és amelyek nagy valószínűséggel nem elégítik ki a megfelelő védelmet. Ez még abban az estben is igaz, ha jogszabályi követelménynek kell megfelelnie az adott szervezet fizikai biztonságának, hiszen attól még, hogy azt jogszabály írja elő, nem biztos, hogy ehhez finanszírozási keret is társul.

3.8. A kiberbiztonság humán oldala

A kiberbiztonság egyik meghatározó tényezője a felkészült felhasználó, aki a rá vonatkozó mértékben tisztában van azokkal az eszközökkel és rendszerekkel, amelyeket használ, ráadásul képes mindazokat a kockázatokat is kezelni, amelyek az adott szervezet esetén megjelennek.

Ugyanakkor a felhasználó felkészítése komoly kihívás, hiszen ez is egy folyamat, amelynek el kell(ene) kezdődnie már gyerekkorban,

az általános iskolában, sőt egyes vélemények szerint már azt megelőzően szükség lenne rá, hiszen ma már az óvodáskorú gyermek is találkozik napi rendszerességgel az infokommunikációs eszközökkel, az internettel, valamint ezeken keresztül számos veszélyforrással.

Olyan vélemények is megjelennek, amelyek az iskolarendszerű oktatáson kívüli felkészítést is hangsúlyosabbá tennék, hiszen egyrészt nem mindenki jár iskolába – gondoljunk csak az idősebb generációra –, és a technikai fejlődés üteme is azt igényli, hogy az iskolában megtanult ismereteket időszakonként felfrissítsük vagy kiegészítsük. Ez a megállapítás azokra vonatkozik, akik korábban bár tanultak ilyeneket és találkoztak az iskolai éveik alatt ezekkel a kérdésekkel, az elmúlt időszakban bekövetkezett technikai változások, a megjelent új veszélyek számukra is szükségessé tennék az ezekről szóló ismeretek átadását.

Mindezeknek megfelelően a kiberbiztonsági oktatásnak be kellene kerülnie a Nemzeti alaptantervbe, azaz a felhasználói szintű informatikai ismeretek mellett a kiberbiztonság (információbiztonság és informatikai biztonság) egyes kérdéseit is oktatni kell, valamint azok elméleti kérdéseinek gyakorlatban történő alkalmazását is el kell kezdeni a közoktatásban is.

3.8.1. Oktatás, képzés, kutatás

A kibertérben megjelenő, jól felkészült, az ott lévő eszközöket, rendszereket és szolgáltatásokat biztonságtudatosan használni tudó felhasználók számára lehetőséget biztosító szakirányú oktatáson kívül meg kell teremteni annak a felkészítésnek és oktatásnak a rendszerszintű alapjait is, amelyek során a felhasználók valóban tisztában lesznek azokkal a legalapvetőbb ismeretekkel, amelyek segítenek számukra eligazodni a kibertérben megjelenő veszélyforrások között. A támadások jelentős része ugyanis pont a felhasználókat célozza meg, és pont a felhasználók felkészületlenségét próbálja kihasználni.

Az ilyen típusú felkészítés és oktatás területén előremutató kezdeményezés a Nemzeti Közszolgálati Egyetemen megalapított Kiberbiztonsági Akadémia (KBA).

A KBA fő célja a kiberbiztonsági területen folyó oktatási és részben kutatási tevékenységek koordinációja. A KBA-t egy programigazgató koordinálja, aki nemcsak az egyetemen belül, hanem a szakmai szervezetekkel, a közigazgatás érintett szereplőivel – minisztériumokkal, nemzetbiztonsági szolgálatokkal, kibervédelmi szervezetekkel (például Nemzeti Kibervédelmi Intézet) –, valamint egyéb szervezetekkel tartja a kapcsolatot. A programigazgató nyomon követi és egyezteti a fenntartói és egyéb kormányzati szakmai igényeket az egyetem kiberbiztonsági képzési[59] és kutatás-fejlesztési feladataival kapcsolatban. A programigazgató munkáját együttműködőként egy szakmai irányító testület segíti. A KBA munkája kiterjed az egyetem karai, intézetei és különböző kutatóműhelyei tevékenységének figyelemmel kísérésére, valamint ezen szervezetek erőforrásainak, különböző programjainak és kezdeményezéseinek az összehangolására.

A KBA egy olyan kapcsolati pontot is jelent, amelyen keresztül a nemzetközi és hazai intézményi kapcsolatok is becsatornázhatók. Így akár hazai vagy nemzetközi képzési programok kezdeményezése, akár szakmai rendezvények szervezése is megvalósulhat. Mindezeken túl a Kiberbiztonsági Akadémia felügyeli és koordinálja az egyetem különböző kiberbiztonsági gyakorlatainak megszervezését, valamint akár ezekhez, akár az oktatáshoz és kutatáshoz szükséges informatikai infrastruktúra kialakítását és fejlesztését is.

A kezdeményezés egyik nagyon fontos célja, hogy elősegítse a kutatások eredményeinek hazai és nemzetközi publikációkban való megjelenését, hiszen a nemzetközi térben ezek lehetnek alapjai annak, hogy a kutatásokhoz együttműködő partnereket találjunk.

---

[59] Ilyen képzési igény például a már említett 2013. évi L. törvény alapján az NKE-re dedikált elektronikus információbiztonsági vezetőképzések és továbbképzések.

A KBA egyik nem titkolt célja egy olyan nemzetközi – alapvetően angol nyelvű – posztgraduális képzés megalapítása és elindítása, amely vonzó lehet a régió kiberbiztonsági szakemberei számára.

Rögtön felmerül a kérdés, hogy mit is oktassunk az ilyen, akár nemzetközi képzéseken, akár a kiberbiztonság más szintű oktatásain. Ehhez adhat eligazodást az olyan oktatási és képzési referenciaajánlás, mint amelyet például egy NATO-munkacsoport hozott létre 2016-ban.

A *Cybersecurity. A Generic Reference Curriculum,* azaz *Kiberbiztonság. Egy általános referencia-tanterv* című dokumentum elkészítésében 17 országból vettek részt kiberbiztonsággal foglalkozó szakértők és kutatók.[60] A munka fő célja az volt, hogy a kiberbiztonság területére egy olyan átfogó, mégis rugalmasan alakítható tantervet dolgozzon ki, amely alapján elegendő szintű ismeretek adhatók át a kiberbiztonság technikai területeiről a nem technikai szakértők részére is, de amely alkalmas arra is, hogy a technikai szakértők is megértsék a kiberbiztonság stratégiai, illetve biztonság- és védelempolitikai összefüggéseit. A négy fő részből álló tanterv – *A kibertér és a kiberbiztonság alapjai; Kockázati vektorok; Nemzetközi kiberbiztonsági szervezetek, politikák és ajánlások; A kiberbiztonság menedzselése nemzeti környezetben* – komoly hozzáadott értéke, hogy minden fő részhez meghatározza a tanulás során elsajátítandó követelményeket. A tanterv nemcsak a követelményekhez, de a tananyaghoz is ad referenciákat, illetve megadja azokat a javasolt releváns forrásokat, amelyek segítségével a követelmények mögött lévő ismeretek elsajátíthatók. (NATO ATC 2016)

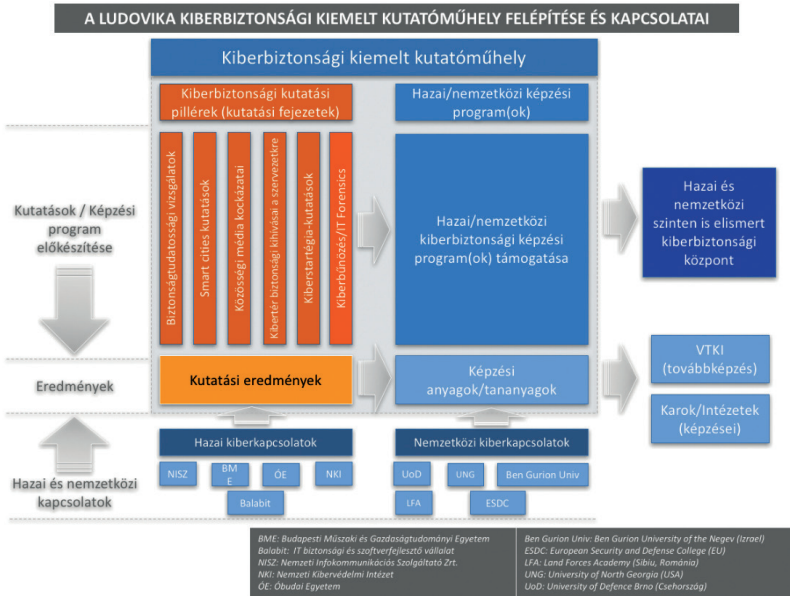
[60] Ehhez a kezdeményezéshez hasonló kiberbiztonsági referencia-tanterv született 2017-ben öt ország öt katonai felsőoktatási intézménye által, az úgynevezett *Stratégiai Partnerség Projekt* keretében kidogozott *Cybersecurity (Kiberbiztonság)* közös modullal. A projekt célja egy olyan nemzetközi egyetemi félév, illetve az abban oktatandó tantárgyak meghatározása és kialakítása volt, amely alapján az európai katonai felsőoktatásban egységes tantervi elemek és egységes oktatási anyagok – e-book, e-learning, hagyományos tankönyvek és oktatási anyagok – alapján végezhető a képzés. E munka során a projektben részt vevő intézmények kilenc közös modulra tettek javaslatot, amelybe beletartozott az említett Cybersecurity is. (Emilyo 2017)

Tudományos kutatás, valamint kutatás-fejlesztés nélkül azonban nem nagyon képzelhető el oktatás sem. 2017-ben ezen alapvetés mentén indult el szintén a Nemzeti Közszolgálati Egyetemen egy karközi, az egyetem által biztosított pályázati forrásból megvalósuló kiberbiztonsági kutatás egy kutatóműhely formájában.[61]

A kutatóműhely célja, hogy kiberbiztonsági kutatásokkal és azok kutatási eredményeivel a jelenleg az egyetem karain és intézeteiben meglévő széttagolt munkához koordinációs segítséget nyújtson. Az elképzelés ezzel kívánja katalizálni az egyetem kiberterületen meglévő kutatási tevékenységeinek, illetve kutatói potenciáljának mind hatékonyabb kihasználását és fejlesztését. A kutatás két fő részre tagolódik. Az első részben a kiberbiztonsági kutatások, a második részben pedig a nemzetközi, illetve hazai kiberbiztonsági képzési program(ok) alapjainak kidolgozása áll a fókuszban. A kiberbiztonsági kutatásokon belül hat kutatási fejezetet határoztak meg. A fejezetek – a kibertér szereplőinek biztonságtudatossági vizsgálatai; a korszerű technológia hatása az urbanizált terek társadalmi folyamataira; a közösségi média lehetőségei és kockázatai; a kibertér biztonsági kihívásai a szervezetre; kiberstratégiai kutatások; kiberbűnözés/IT forensics – bár nem homogén, egy síkon folyó kutatásokat takarnak, egy irányba mutatnak. A kutatás végső célja, hogy azok eredményeivel hozzájáruljon Magyarország kiberbiztonságának növeléséhez.

---

[61] Ez a kutatás, illetve maga a kutatóműhely a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, *A jó kormányzást megalapozó közszolgálat-fejlesztés* elnevezésű kiemelt projekt keretében jött létre, és a Ludovika Kiemelt Kiberbiztonsági Kutatóműhely nevet viseli.



65. ábra
A kiberbiztonsági kiemelt kutatóműhely felépítése a Nemzeti Közszolgálati Egyetemen

Forrás: a szerző szerkesztése

Semmilyen kutatás esetén sem hanyagolható el azok financiális támogatása. Az említett kiberbiztonsági kiemelt kutatóműhely a közigazgatást és a közszolgálat fejlesztését előirányzó – alapvetően európai uniós – program támogatásával jött létre. Ennek megfelelően a közvetlen kutatási célokon túl a kutatások közvetett hatásait is célszerű röviden felvázolni. A hazai Közigazgatási és Közszolgáltatás-fejlesztési Stratégia több helyen is megfogalmazza, hogy a hálózatbiztonság, az információbiztonság, valamint a tágabb értelemben vett kiberbiztonság nemzetbiztonsági szempontból is kritikus jelentőségű, de minden egyes szolgáltató és felhasználó szintjén értelmezhető elvárás. Az e-kormányzati szolgáltatások esetében fontos, hogy a közigazgatás oldalán maximálisan garantálható legyen a hálózatok, rendsze-

rek, folyamatok és felhasználói adatok biztonsága. Mindezek mellett a stratégia kitér arra is, hogy „[a]z infokommunikációs szolgáltatások egyaránt kulcsfontosságú tényezője a hálózatok, az informatikai infrastruktúra, a hozzáférés, az alkalmazások és a felhasználói végpontok szintjén egyaránt értelmezhető bizalom és biztonság." Kutatásainkkal ezekhez a stratégiai célokhoz kívánunk hozzájárulni nemcsak a szűken vett egyetemi szinten, hanem a megvalósuló szerteágazó együttműködéseken keresztül a hazai közigazgatás szintjén is. (KÖFOP 2015)

A kutatás számszerűsíthető eredményeként megjelenik számos tudományos monográfia, tankönyv, valamint több tucat tudományos nemzetközi és hazai folyóiratcikk. A kutatás eredményeit hazai és nemzetközi tudományos-szakmai konferenciákon és workshopokon mutatjuk be, amelyek a tudományos eredmények bemutatásán túl hozzájárulnak a tudatosság növeléséhez, hiszen ezeken a rendezvényeken nemcsak a szűkebb értelemben vett kutatók, hanem egyetemi hallgatók, sőt a téma iránt igazán fogékony középiskolás diákok is részt vesznek. A kutatóműhely hazai és nemzetközi tudományos-szakmai konferenciákat is megrendezett, amelyek szintén hozzájárultak a nemzetközi térben a kiberbiztonság megteremtéséhez.

A kutatás nem számszerűsíthető eredményeként megvalósul az NKE kiberkutatásainak koordinációja, bizonyos szintű integrációja, amely a közszolgálati hivatásrendek oktatását és továbbképzését fogja támogatni. A megjelenő tudományos publikációk az egyetemi alap-, mester-, doktori, valamint szakmai képzéseiben tananyagként használhatóak. A kutatómunka során megvalósuló hazai és nemzetközi kutatási együttműködések szintén hozzájárulnak Magyarország kiberbiztonságának növeléséhez.

A kiberbiztonságnak egy olyan gyorsan változó környezetben kell megvalósulnia, amely nagyon rövid időn belül igényli az újabb és újabb ismeretek megszerzését, majd azok átadását. Ennek megfelelően a kutatóműhely olyan eredmények elérésére törekszik, amelyek a tankönyveken és oktatási anyagokon, az azokban leírt tényeken kívül magas szintű tudományosan megalapozott szemléletet sugallnak

és adnak át a hallgatóknak, legyen szó közigazgatási szakemberről, katonáról vagy leendő rendőrről. Reményeink szerint mindezek hozzájárulnak a hallgatók kibertérben való könnyebb tájékozódásához, jövőbeni tevékenységük biztonságtudatos megvalósításához.

Az említett kutatások egyik pillére a már többször említett biztonságtudatosság növelése. E kutatási terület különösen fontos, hiszen ennek első kutatási fázisában azt igyekszik a kutatócsoport felmérni, hogy a magyar közigazgatásban a kiberbiztonsággal kapcsolatban milyen ismeretekkel, illetve milyen percepciókkal rendelkeznek különböző életkorú és a különböző helyeken/szinteken dolgozók (vagy az oda készülők, akik a kutatás idején egyetemi hallgatók még). Ehhez első körben egy olyan kérdőíves felmérést végzett a kutatócsoport, amely során kiindulóadatokat kapott a közigazgatás említett szintjeit reprezentáló válaszadóktól. Ezeknek az adatoknak a feldolgozása után különböző csoportokba szervezve felmérték, hogy egy-egy kiberbiztonsági képzés mennyiben változtatta meg és mennyiben járult hozzá az adott csoport tagjainál a biztonságtudatossághoz, illetve mennyiben látják másként a terület kihívásait, eszközeit és lehetőségeit. Ezeket az adatokat összehasonlítva van lehetőség az adott képzés tematikájába – és ha szükséges, akkor annak didaktikai megoldásaiba – beavatkozni, azaz azokat a kívánt irányba megváltoztatni. Így lehetőség van arra, hogy egy-egy kiberbiztonsági képzés vagy tanfolyam ne csak kötelező legyen, hanem maximális hatékonyságot érjen el az adott idő alatt. (Kovács et al. 2017)

3.8.2. Tudatosítás

Az infokommunikációs eszközök és az internet biztonságos használatát tanulni kell. Ez nem generáció- vagy iskolaivégzettség-függő kérdés. Korábban már többször utaltunk rá, hogy akár naponta is több tucat újabb és újabb veszéllyel, kihívással kell szembenéznie annak, aki a kibertérbe látogat. Ezért a felhasználót fel kell készíteni ezen ki-

hívások kezelésére, természetesen a rájuk vonatkozó szintig. Ez persze több lépcsőben és több fokozatban képzelhető csak el.

Ahogy korábban utaltunk rá, nagyon sokan azon a véleményen vannak, hogy ennek a felkészítésnek már az óvodában el kell kezdődnie, hiszen ma már ez az a legfiatalabb korosztály, amely találkozik az internettel és annak elérését lehetővé tevő eszközökkel. Azonban joggal merül fel a kérdés: hol és mit tanítsunk, ráadásul hogyan? A kérdés jogos, hiszen például, ha már az óvodában el kell kezdenünk ezt a fajta felkészítést (tanítást, tréninget stb.), akkor természetesen az óvodapedagógusok előzetes felkészítését, illetve az ő oktatásukat is meg kell valósítani, ráadásul így máris szembesülünk azzal a problémával, hogy a felnőttek oktatása, az ott alkalmazandó – hatékony – felkészítés mind didaktikájában, mind tartalmi elemeiben eltér attól, mint amelyeket a különböző korosztályú gyermekek oktatásánál, illetve felkészítésénél alkalmaznunk kell.

Az nyilvánvaló, hogy ez a fajta összetett tevékenység nem képzelhető el egyik napról a másikra. Csak fokozatosan, egy előre jól meghatározott és felépített rendszerben képzelhető el a siker.

A tudatosítás egyes elemeire – akár kampányban történik az, akár iskolarendszerű oktatás keretében – nagyon fontos kezdeményezéseket találunk számos szervezet koordinálásában, amelyek elsősorban a megcélzott közönség biztonságtudatosságának emelését célozzák.

Ilyen biztonságtudatosság emelését célzó kampányokat vezet például az Europol, amelyekben a szervezet a kiberbűnözés elleni védekezéshez, illetve például az online kereskedelem – vásárlói oldalról történő – biztonságos használatához adnak tanácsokat. A kiberbűnözés elleni tudatosságnövelés kiemelten fontos terület, hiszen – ahogy korábban láthattuk – ezek mint feladatok megjelennek a különböző stratégiákban is. Ugyanakkor ezen a területen is elmondható, hogy a célközönség meghatározása, majd a számukra célzottan összeállított információk meghatározó jelentőségűek. A gyerekek számára például az egyszerű és világos üzenetek eljuttatása úgy lehet hatásos, ha azt az egyéb területek oktatásával kombináljuk, hiszen ez a korosztály

nagyon fogékony az újdonságok befogadására, ráadásul a játszva tanulás valóban jelentheti azt az esetükben, hogy rögzülnek az elhangzottak, és így egy olyan tudás birtokában lévő nemzedék nő fel, akik nem mellesleg nemcsak elméletben, hanem a gyakorlatban is képesek alkalmazni a kiberbiztonság számos elemét.

A kiberbiztonság tudatosításában természetesen számtalan módszer és megoldás létezik. Ezen a téren a fent említett megoldásokon kívül rendkívül nagy szerepe van a szakmai konferenciáknak is. Hazánkban is rendeznek ilyen konferenciákat, amelyeknek fő célja és célcsoportja sok esetben a szakmai közönség, de olyan széles előadói és tartalmi elemekkel rendelkező konferenciasorozatokról beszélhetünk, amelyek közvetett módon a kiberbiztonsági tudatosság növeléséhez nagyban hozzájárulnak.

Ilyen konferencia – természetesen eltérő célközönséggel és eltérő szakmai tartalommal – például az *ITBN,* azaz az *Informatikai Biztonság Napja* című konferencia, amely 2005-ben indult, és amely elsődleges célja az volt, hogy „egy független, minden piaci szereplő és felhasználó érdekét képviselő fórumot teremtsen”. (ITBN 2017)

A konferencia az indulása óta eltelt több mint tíz év alatt sokat fejlődött, látogatói száma már meghaladja a 2500 főt. Ezen kívül már nemcsak szakmai konferencia, hanem kiállítás és expó is egyben, amely nagymértékben hozzájárul a biztonságtudatosság fejlesztéséhez. (ITBN 2017)

66. ábra
Az Europol online vásárlással kapcsolatos kiberbiztonsági tudatosító plakátja

Forrás: Europol 2017e

Hasonló szakmai rendezvény a *Hacktivity-konferencia,* amely 2003-as indulása óta Kelet-Közép-Európa egyik legrangosabb hackerkonferenciájává nőtte ki magát. A rendezvény évente több mint 1200 látogatót vonz, és igazi nemzetközi hackertalálkozóvá vált, hiszen az USA-tól kezdve Portugálián át Németországig terjed azon országok sora, ahonnan előadók, résztvevők és érdeklődők érkeznek a rendezvényre. A konferencia számos szakmai versenyt is magában foglal, de akár mély hackerismeretek hiányában is megtalálja minden érdeklődő a számára érdekes előadást, bemutatót vagy programot. A konferencia

kiállítás is egyben, és nem mellesleg a különböző médiamegjelenéseknek köszönhetően nagymértékben formálja és irányítja a figyelmet a kiberbiztonság – elsősorban technikai – kérdéseire. (Hacktivity 2017)

A biztonságtudatosság formálásában hasonlóan komoly érdemei vannak az Ethical Hacking konferenciasorozatnak, amely 2008 óta ad teret a „jó oldalon" álló hackereknek, akik olyan informatikai szakemberek, akik tudásukat és nem utolsósorban e tudás biztonságszempontú alkalmazását be is mutatják a nagyközönség előtt. A konferencia szervezői olyan fiatal tehetségeknek is teret adnak, akik a legújabb technológiákban – például a drónok alkalmazásában – lévő biztonsági kihívásokat keresik, és azokra igyekeznek válaszokat adni. (HVG 2016)

Természetesen mindezen konferenciák mellett számos más rendezvényt és szakmai fórumot rendeznek évről évre, amelyek egyik legnagyobb erénye, hogy más-más szempontból mutatják be a szakmai és a nem szakmai közönségnek az informatikai, információ- és kiberbiztonsági kihívásokat, trendeket, eszközöket és megoldásokat.

A biztonságtudatosság tárgyalása során a fenti konferenciákon túl mindenképpen szót érdemel egy olyan kiberbiztonsági kezdeményezés, amely a kiberbiztonsági szakemberek önkéntes összefogásán alapul. A KIBEV, azaz az Önkéntes Kibervédelmi Összefogás célja, hogy a szervezet tagjai az állam számára felajánlják tudásukat és szakértelmüket a kibertér védelme érdekében.

A KIBEV e céllal párhuzamosan közvetlen módon, együttműködve a hazai civil szervezetekkel az állampolgárok biztonságtudatosságának fejlesztését kívánja támogatni. Ehhez a célhoz a szervezet koordinációval és különböző szakmai fórumok megteremtésével járul hozzá. A KIBEV többek között internetes és egyéb médiamegjelenéssel dolgozik, amelyek során többek között az olyan munkákat is propagálják, mint például a Kritikus Biztonsági Kontrollok magyar kiadású posztere, amely az ipari rendszerek (például SCADA-k) biztonságához járulhat hozzá. (KIBEV 2017)

A biztonságtudatosításban az említett tényezőkön – oktatás, konferenciák, médiakampányok stb. – kívül egészen meglepő szereplők is megjelennek. Erre az egyik legjobb példa a Könyvtári Egyesületek és Intézmények Nemzetközi Szövetsége (International Federation of Library Associations and Institutions, IFLA), amely szervezet közel 100 éve a könyvtári és információs szolgáltatások és a felhasználók érdekeit képviselő vezető nemzetközi szervezet. (IFLA 2017a)

67. ábra
Infografika a hamis hírek kiszűrésének lehetséges módszereiről. Jó példa a biztonságtudatosság növelésére egy civil szervezettől

Forrás: IFLA 2017b

Mint ilyen szervezet fontosnak tartja a hiteles információk átadását, illetve azoknak a módszereknek a tudatosítását, amelyek alkalmazásával az egyszerű embereknek is lehetősége van a hamis híreket a valódi

hírektől és információktól megkülönböztetni.[62] Ehhez a honlapján rendszeresen közöl ilyen megoldásokat népszerűsítő leírásokat, sőt az azok könnyebb megértését lehetővé tevő infografikákat is.

[62] A hamis hírek elleni védekezés azonban a fenti tudatosító példák ellenére is sok esetben meghaladja az átlagos felhasználó tudását, tapasztalatait és lehetőségeit. Ezért ezen a területen szükség van olyan nagy információ- és tartalomszolgáltatók segítségére is, mint például a Google. Ennek egyik nemrégen elindult példája az, ahogyan a Google a kereséseket pontozza. A hamis vagy megtévesztő keresési találatokat a felhasználók jelezhetik a keresőóriásnak egy *feedback,* azaz *visszajelzés* menüben. A Google algoritmusai ezt feldolgozzák, az ilyen találatokat negatívan pontozzák, így a hamis híreket tartalmazó találatok a keresési listában hátrébb fognak kerülni. (Hern 2017b)

Rövidítések jegyzéke

Rövidítés	Angol nyelvű magyarázat	Magyar nyelvű magyarázat
APT	Advanced Persistent Threat	Célzott, folyamatosan fennálló, fejlett támadás
ÁROP		Államreform Operatív Program
ASP	Application Service Provider	Alkalmazásszolgáltatási modell
ATM	Automated Teller Machine	Pénzkiadó automata
BCP	Business Continuity Plan	Üzletmenetfolytonossági terv
BM		Belügyminisztérium
BS	British Standard	Brit szabvány
C2	Command & Control	Vezetés és irányítás
CAN	Controller Area Network	Vezérlőhálózat
CC	Common Criteria	Közös kritérium
CCDCoE	Co-opreative Cyber Defence Centre of Excellence	Kiberbiztonsági Kiválósági Központ (NATO)
CERT	Computer Emergency Response Team	Számítógép-vészhelyzeti reagáló csoport
CIA	Central Intelligence Agency	Központi Hírszerző Ügynökség
CIP	Critical Infrastructure Protection	Kritikusinfrastruktúra-védelem
CIT	Cyber Intelligence Team	Kiberfelderítési csoport
CIWIN	Critical Infrastructure Warning Information Network	Kritikus infrastruktúrákra figyelmeztető információ hálózata
COBIT	Control Objectives for Information and Related Technology	Informatikai irányítási és ellenőrzési módszertan
CPS	Cyber-physical Systems	Kiber-fizikai rendszer

CSDP	Common Security and Defence Policy	Közös európai biztonság- és védelempolitika
CSIRT	Computer Security Incident Response Team	Számítógép-biztonsági incidenskezelő csoport
DDoS	Distributed Denial of Service	Elosztott túlterheléses támadás
DESI	Digital Economy and Society Index	Digitális gazdaság- és társadalomindex
DJP		Digitális Jóléti Program
DNS	Domain Name Service	Doménnév-szolgáltatás
DoS	Denial of Service	Túlterheléses támadás
DRP	Disaster Recovery Plan	Katasztrófavédelmi terv
EAL	Evaluation Assurance Level	Értékelési megbízhatósági szint
EBESZ		Európai Biztonsági és Együttműködési Szervezet
EC3	European Cybercrime Centre	Európai kiberbűnözés elleni központ
ECI	European Critical Infrastructures	Európai kritikus infrastruktúrák
EDA	European Defence Agency	Európai Védelmi Ügynökség
EECSP	Energy Expert Cyber Security Platform	Energiaipari kiberszakértői platform
EESZT		Elektronikus Egészségügyi Szolgáltatási Tér
EKOP		Elektronikus Közigazgatás Operatív Program
eMMC	Electronic Multimedia Card	Elektronikus multimédiakártya
EMPACT	European Multidisciplinary Platform Against Criminal Threats	Európai multidiszciplináris platform a bűncselekmények fenyegetettsége ellen
ENISA	European Union Agency for Network and Information Security	Európai Hálózat- és Információbiztonsági Ügynökség
ENSZ		Egyesült Nemzetek Szervezete

EPCIP	European Programme for Critical Infrastructure Protection	Kritikusinfrastruktúra-védelem Európai Programja
EU	European Union	Európai Unió
FBI	Federal Bureau of Investigation	Szövetségi Nyomozó Iroda
GCI	Global Cybersecurity Index	Globális kiberbiztonsági index
GDP	Gross Domestic Product	Nemzeti össztermék
GDPR	General Data Protection Regulation	Általános adatvédelmi rendelet
GDPR	General Data Protection Roles	Általános adatvédelmi szabályok (EU)
GNI	Gross National Income	Bruttó nemzeti jövedelem
GPS	Global Position System	Globális helyzetmeghatározó rendszer
GSM	Global System for Mobile Communications	Mobilkommunikációs globális rendszer
HÁEIEK		Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ
HM		Honvédelmi Minisztérium
HTML	HyperText Markup Language	Hiperszöveges jelölőnyelv
IBIR		Információbiztonsági irányítási rendszer
IBIX		Informatikai Biztonsági Iránymutató Kis Szervezetek Számára
ICO	Information Commissioner's Office	Információs jogokkal foglalkozó iroda
ICS	Industrial Command System	Ipari vezérlőrendszer
IDS	Intrusion Detection System	Behatolásdetektáló rendszer
IEC	International Electrotechnical Commission	Nemzetközi Elektrotechnikai Tanács
IKT		Infokommunikációs technológia
IoT	Internet of Things	A dolgok internete
IoT-GSI	Global Standards Initiative on Internet of Things	A dolgok internetének globális szabványa

IP	Internet Protocol	Internetprotokoll
IPS	Intrusion Prevention System	Behatolást megelőző rendszer
ISACA	Information Systems Audit and Control Association	Információs Rendszerek Audit- és Kontrollszövetsége
ISIS	Islamic State of Iraq and Syria	Irak és Szíria Iszlám Állama
ISMS	Information Security Management System	Információbiztonsági irányítási rendszer
ISO	International Organization for Standardization	Nemzetközi Szabványügyi Szervezet
ITIL	Information Technology Infrastructure Library	Az informatikaszolgáltatás módszertana
ITU	International Telecommunication Union	Nemzetközi Telekommunikációs Szervezet
ITU-D	ITU Development Sector	A Nemzetközi Telekommunikációs Szervezet fejlesztésekért felelős ágazata
ITU-R	ITU Radiocommunication Sector	A Nemzetközi Telekommunikációs Szervezet rádiókommunikációs ágazata
ITU-T	Telecommunication Standardisation Sector	A Nemzetközi Telekommunikációs Szervezet telekommunikáció egységesítésért és szabványosításért felelős ágazata
IVSZ		Informatikai Vállalkozások Szövetsége
J-CAT	Joint Cybercrime Action Taskforce	Egyesített kiberbűnözés elleni akciócsoport
KIBEV		Önkéntes Kibervédelmi Összefogás
KKV		Kis- és közepes vállalkozások
KNBSZ		Katonai Nemzetbiztonsági Szolgálat
KÖFOP		Közigazgatás- és Közszolgáltatás-fejlesztési Program
KSH		Központi Statisztikai Hivatal
LOIC	Low Orbit Ion Cannon	Alacsony Orbitális Ionágyú

LRL IBEK		Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja
LTE	Long Term Evolution	Hosszú távú fejlődés
M2M	machine-to-machine	Gép-gép közötti (kapcsolat)
MEH ITB		Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság
MIBA		Magyar Informatikai Biztonsági Ajánlások
MIBÉTS		Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma
MIBIK		Magyar Informatikai Biztonsági Keretrendszer
MIT	Massachusetts Institute of Technology	Massachusettsi Műszaki Egyetem
MSZ		Magyar szabvány
NATO	North Atlantic Treaty Organisation	Észak-atlanti Szerződés Szervezete
NBF		Nemzeti Biztonsági Felügyelet
NBSZ		Nemzetbiztonsági Szakszolgálat
NCIRC	NATO Cyber Incident Response Capability	NATO kiberincidens-reagáló képesség
NEIH		Nemzeti Elektronikus Információbiztonsági Hatóság
NHS	National Health Service	Nemzeti Egészségügyi Szolgálat (brit)
NHTCU	National High Tech Crime Unit	Számítástechnikai Bűncselekmények Elleni Egység (holland)
NIS	Network and Information Systems	Hálózati és információs rendszer
NIST	National Institute of Standards and Technology	Nemzeti Szabványügyi és Technológiai Intézet
NKI		Nemzeti Kibervédelmi Intézet

NSA	National Security Agency	Nemzetbiztonsági Ügynökség
NTG		Nemzeti Távközlési Gerinchálózat
OBD	On-Board Diagnostic	Fedélzeti diagnosztika
OECD	Organisation for Economic Co-operation and Development	Gazdasági Együttműködési és Fejlesztési Szervezet
OKF		Országos Katasztrófavédelmi Főigazgatóság
OTA	Over the Air	Levegőn keresztüli
OWASP	Open Web Application Security Project	Nyíltwebalkalmazás-biztonsági Projekt
PDA	Personal Digital Assistant	Kézi számítógép
PDCA	Plan-Do-Check-Act	Tervezés-cselekvés-ellenőrzés-beavatkozás
PLA	People's Liberation Army	Kínai Népi Felszabadító Hadsereg
PLC	Programmable Logic Controller	Programozható kontroller
RFID	Radio Frequency Identification	Rádiófrekvenciás azonosítás
RNC	Republican National Committe	Republikánus Nemzeti (Választási) Tanács
RSA	Rivest–Shamir–Adleman	Aszimmetrikus titkosító algoritmus (megalkotók neveinek kezdőbetűiből alkotott rövidítés)
RTU	Remote Terminal Unit	Távoli terminál
SCADA	Supervisory Control and Data Acquisition	Felügyeleti, irányító és adatgyűjtő
SDK	Software Development Kits	Szoftverfejlesztő kit
SMB	Server Message Block	Szerverüzenet-blokk
SOA	Service-Oriented Architecture	Szolgáltatásorientált architektúra
SPI	Serial Peripheral Interface	Soros port
SPU	Strategy and Policy Unit	(Az ITU) Stratégiai és Politikai Egysége

SQL	Structured Query Language	Strukturált lekérdezőnyelv
SSH	Secure SHell	Nyilvános titkosítású protokollcsalád
SSL	Secure Sockets Layer	Biztonságos protokoll (szállítási réteg és alkalmazási réteg között)
STEM	Science, Technology, Engineering and Mathematics	Természet- és mérnöki tudományok
SZTAKI		Számítástechnikai Automatizálási Kutatóintézet
TCP	Transmission Control Protocol	Szállítási réteg
TCSEC	Trusted Computer System Evaluation Criteria	Biztonságos Számítógépes Rendszerek Értékelési Kritériumai
TLS	Transport Layer Security	Szállításiréteg-biztonság
TOR	The Onion Router	A hagymaelosztó
UDP	User Datagram Protocol	Szállítási protokoll (datagram szállítása)
UK NISCC	United Kingdom National Infrastructure Co-ordination Center	Egyesült Királyság Nemzeti Infrastrukturális Biztonsági Koordinációs Központja
UMTS	Universal Mobile Telecommunications System	Univerzális mobil telekommunikációs rendszer (3G)
URL	Uniform Resource Locator	Egységes erőforráshely
USB	Universal Serial Bus	Univerzális soros busz
V4	Visegrad Four	Visegrádi négyek
WAP	Wireless Application Protocol	Vezeték nélküli adatátvitel nyílt nemzetközi szabványa
WAP	Wireless Application Protocol	Vezetéknélkülialkalmazásprotokoll
XSS	Cross site scripting	Weboldalon elhelyezett ártó szándékú kód

Vákát oldal

Illusztrációk jegyzéke

1. ábra. *A digitális ökoszisztéma összetevői*
Forrás: Nemzeti Infokommunikációs Stratégia 2014
2. ábra. *A digitális forradalom társadalomra gyakorolt hatása: a zenehallgatás és a hírek forrása*
Forrás: European Commission 2015a, szerk.: szerző
3. ábra. *A DESI index fő mérőszámcsoportjai*
Forrás: European Commission 2016b, szerk.: szerző
4. ábra. *Az Európai Unió tagországainak DESI index alapján elfoglalt helye 2016-ban*
Forrás: European Commission 2016b
5. ábra. *Az Európai Unió tagországainak DESI index alapján elfoglalt helye 2016-ban*
Forrás: European Commission 2016c
6. ábra. *Az Európai Unió tagországainak DESI index alapján elfoglalt helye 2017-ben*
Forrás: European Commission 2017a
7. ábra. *Néhány fejlett ország (vezetékes) széles sávú internetelérésének és az adott ország GDP-értékének viszonya*
Forrás: OECD 2015/2016, szerk.: szerző
8. ábra. *Az internetet nem használók aránya a világon*
Forrás: ITU 2016, szerk.: szerző
9. ábra. *A V4-ek és Ausztria internet-penetrációja 2010–2016 között*
Forrás: Eurostat 2017a, szerk.: szerző
10. ábra. *Ausztria és a V4-ek internethasználóinak teljes lakossághoz viszonyított százalékos aránya 2016-ban*
Forrás: Eurostat 2016a, szerk.: szerző
11. ábra. *Ausztria és a V4-ek napi internethasználóinak teljes lakossághoz viszonyított százalékos aránya 2016-ban*
Forrás: Eurostat 2016b, szerk.: szerző

12. ábra. *Ausztria és a V4-ek olyan lakosainak teljes lakossághoz viszonyított százalékos aránya, akik sohasem használnak internetet 2016-ban*
Forrás: Eurostat 2016c, szerk. szerző
13. ábra. *Ausztria és a V4-ek olyan lakosainak teljes lakossághoz viszonyított százalékos aránya, akik a magas ár miatt nem használnak internetet 2016-ban*
Forrás: Eurostat 2016d, szerk.: szerző
14. ábra. *Ausztria és a V4-ek szélessávúinternet-előfizetéseinek száma 100 lakosra vetítve 2016-ban*
Forrás: Eurostat 2016e, szerk.: szerző
15. ábra. *Ausztria és a V4-ek szélessávúinternet-előfizetéseinek sávszélességenkénti ára 2015-ben*
Forrás: Eurostat 2016f, szerk.: szerző
16. ábra. *Ausztria és a V4-ek mobiltelefonon keresztüli interneteléréseinek száma 2016-ban a teljes interneteléréseknek százalékos arányában*
Forrás: Eurostat 2016g, szerk.: szerző
17. ábra. *Internet-előfizetések száma Magyarországon 2008 és 2016 között*
Forrás: KSH 2017
18. ábra. *Az internet-előfizetések megoszlása technológia szerint Magyarországon 2016. év végén*
Forrás: KSH 2017
19. ábra. *A magyarországi mobilhálózati adatforgalom megoszlása hálózati technológia szerint 2016. év végén*
Forrás: KSH 2017
20. ábra. *Ausztria és a V4-ek mobiltelefon-előfizetéseinek száma 2015-ben (millió darab)*
Forrás: Eurostat 2016j, szerk.: szerző
21. ábra. *A magyarországi mobiltelefon-előfizetések számának alakulása 2005 és 2016 között*
Forrás: KSH 2017
22. ábra. *Ausztria és a V4-ek lakosainak teljes lakossághoz viszonyított százalékos aránya, akik már rendeltek árut vagy szolgáltatást az interneten 2016-ban*
Forrás: Eurostat 2016k, szerk.: szerző

23. ábra. *Ausztria és a V4-ek lakosainak teljes lakossághoz viszonyított aránya, akik már rendeltek árut vagy szolgáltatást másik EU-s országból az interneten 2016-ban*
Forrás: Eurostat 2016m, szerk.: szerző
24. ábra. *Ausztria és a V4-ek vállalkozásainak aránya, amelyek használták ez e-kereskedelem valamilyen formáját 2016-ban*
Forrás: Eurostat 2016n, szerk.: szerző
25. ábra. *Ausztria és a V4-ek vállalkozásainak e-kereskedelemből származó bevétele a teljes bevétel százalékos arányában 2016-ban*
Forrás: Eurostat 2016o, szerk.: szerző
26. ábra. *Ausztria és a V4-ek internethasználóinak aránya, akik legalább egy alkalommal használtak e-közigazgatási szolgáltatást 2016-ban*
Forrás: Eurostat 2016p, szerk.: szerző
27. ábra. *Ausztria és a V4-ek internethasználóinak aránya, akik legalább egy alkalommal használtak e-közigazgatási szolgáltatást, és ott legalább egy elektronikus ügyiratot ki is töltöttek 2016-ban*
Forrás: Eurostat 2016q, szerk.: szerző
28. ábra. *Ügyfélkapu-belépések száma 2009–2015 között*
Forrás: NISZ, idézi: Kaiser 2016
29. ábra. *Az ASP-rendszer kapcsolatai*
Forrás: Belügyminisztérium 2017b, szerk.: szerző
30. ábra. *Az IoT-technológia fejlődése*
Forrás: Sarwar 2012, szerk.: szerző
31. ábra. *A dolgok internete és kapcsolatai*
Forrás: Sarwar 2012, szerk.: szerző
32. ábra. *A Cisco „dolgok internete"-referenciamodellje*
Forrás: Cisco 2014, szerk.: szerző
33. ábra. *A Mirai által fertőzött IoT-eszközökkel elkövetett támadás vázlata*
Forrás: Trend Micro 2017a, szerk.: szerző
34. ábra. *A dolgok internetének biztonsági modellje*
Forrás: Cisco 2014, szerk.: szerző
35. ábra. *Korszerű személyautó elektronikai rendszerei*
Forrás: Walz 2016, szerk.: szerző

36. ábra. *Az okosváros lehetséges összetevői*
Forrás: Schneider-electric 2015, szerk.: szerző
37. ábra. *A Madridi Műszaki Egyetem okosvárosprojektjének pillanatnyi adatai*
Forrás: Smart CEI Moncloa 2017
38. ábra. *Magyarországi okosvárosok és azok rangsora*
Forrás: Schopp 2014
39. ábra. *Budapest okosváros-kapcsolatai és céljai*
Forrás: Finta–Barta–Balogh 2017
40. ábra. *Az okosotthon összetevői*
Forrás: pixabay.com, szerk.: szerző
41. ábra. *A 20 legjelentősebb rosszindulatú program 2016-ban*
Forrás: Garnaeva et al. 2016, szerk.: szerző
42. ábra. *WannaCry képernyőkép*
Forrás: Hlács 2017
43. ábra. *A WannaCry hatása egy németországi vasúti pályaudvar utastájékoztató terminálján*
Forrás: Graham 2017
44. ábra. *A NoPetya képernyőképe*
Forrás: MTI, Bolcsó 2017
45. ábra: *A kép készítésének pillanatában működő botnetek*
Forrás: MalwareTech 2017
46. ábra. *A botnet általános felépítése (példa)*
Forrás: szerző
47. ábra. *Az APT életciklusa*
Forrás: szerző
48. ábra. *A magyarországi állami és nem állami szervezeteket ért támadások 2015 harmadik negyedévében*
Forrás: Bencsik 2015
49. ábra. *A leggyakoribb támadások kiindulópontjai a támadók csoportosítása alapján*
Forrás: szerző
50. ábra. *Az elhíresült Guy Fawkes maszk, amely az Anonymous jelképévé vált*
Forrás: History 2017

51. ábra. *Az Anonymous Operation Hungary „hivatalos" Twitter-oldala*
Forrás: Twitter 2017
52. ábra. *Az Avalanche működése*
Forrás: Europol 2017a
53. ábra. *A "Have I been powned?" oldalon a szerző egyik e-mail-címének ellenőrzése és annak eredménye*
Forrás: Hunt 2017b
54. ábra. *A "Have I been powned?" oldalon a szerző egyik e-mail-címének ellenőrzése és a feltételezhető források*
Forrás: Hunt 2017b
55. ábra. *A kiberterrorizmus kutatásának felépítése 2006-ban*
Forrás: Kovács 2006
56. ábra. *Az Inspire magazin egyik számának borítója és annak „bombaiskolája"*
Forrás: Inspire 2014
57. ábra. *A kiberbiztonság és a hozzá kapcsolódó területek*
Forrás: Klimburg 2012, szerk.: szerző
58. ábra. *A kritikus infrastruktúrákon belüli interdependencia egy példája: a villamosenergia-szolgáltatás kapcsolatai és hatásai*
Forrás: Rinaldi–Peerenboom–Kelly 2001, szerk.: szerző
59. ábra. *A hazai kibervédelmi szervezetek 2015 előtt*
Forrás: Bencsik 2015
60. ábra. *A 2015 óta működő hazai állami kibervédelmi szervezetek*
Forrás: Bencsik 2015
61. ábra. *A kiberbiztonság átfogó kezelésének három pillére az Európai Unióban*
Forrás: Cybersecurity Strategy of the European Union 2013
62. ábra. *Az Európai Kiberbűnözés elleni Központ felépítése*
Forrás: Europol 2017c
63. ábra. *A COBIT 5 összetevői*
Forrás: ISACA 2017
64. ábra. *Az ITIL életciklusa*
Forrás: BMC 2016

65. ábra. *A kiberbiztonsági kiemelt kutatóműhely felépítése a Nemzeti Közszolgálati Egyetemen*
Forrás: szerző
66. ábra. *Az Europol online vásárlással kapcsolatos kiberbiztonsági tudatosító plakátja*
Forrás: Europol 2017e
67. ábra. *Infografika a hamis hírek kiszűrésének lehetséges módszereiről. Jó példa a biztonságtudatosság növelésére egy civil szervezettől*
Forrás: IFLA 2017b

Táblázatok jegyzéke

1. táblázat. *A világ internet-penetrációja*
Forrás: Internet World Stats 2017, szerk.: szerző
2. táblázat. *A világ internet-penetrációjának előrejelzése 2030-ra*
Forrás: saját szerkesztés)
3. táblázat. *Ausztria és a V4-ek GDP-, internet- és mobiltelefon-felhasználóinak összehasonlítása (GDP 2015-re, többi adat 2016-ra vonatkoztatva) szerk.:* szerző
4. táblázat. *IoT-sérülékenységek az OWASP alapján*
Forrás: OWASP 2017b, szerk.: szerző
5. táblázat. *Programtípusú malware-ek és jellemzőik*
Forrás: Kovács 2006
6. táblázat: *Szövegtípusú malware-ek fajtái (példák)*
Forrás: Kovács 2006
7. táblázat. *Jellemző informatikai támadási módszerek*
Forrás: szerző
8. táblázat. *Az APT28 által megtévesztésre használt imitált domének*
Forrás: FireEye 2014, szerk.: szerző
9. táblázat: *A magyarországi kritikus infrastruktúra ágazatai és alágazatai*
Forrás: 2012. évi CLXVI. tv. 1., 2., 3. mellékletek, *szerk.:* szerző
10. táblázat: *A NIS-direktíva által meghatározott alapvető szolgáltatásokat nyújtó szereplők*
Forrás: NIS Directive 2016 II. melléklet, szerk.: szerző
11. táblázat: *A 2013. évi L. törvény 2015-ben történt módosítását követően megjelent új jogszabályok*
Forrás: szerző

Vákát oldal

Irodalomjegyzék

1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

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

187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

2011. évi CLXXIV. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény és egyes kapcsolódó törvények, valamint a miniszteri hatósági hatáskörök felülvizsgálatával összefüggő egyes törvények módosításáról

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

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

2015. évi CXXX. törvény az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról

2017/0226(COD) az Európai Parlament és a Tanács Irányelve. Javaslat a készpénzhelyettesítő fizetési eszközökkel összefüggő csalás és hamisítás elleni küzdelemről és a 2001/413/IB tanácsi kerethatározat felváltásáról {SWD(2017) 298 final}{SWD(2017) 299 final} Brüsszel, 2017.9.13. COM(2017) 489 final

2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programról

39/2016. (XII. 21.) EMMI rendelet az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról

4chan (2017): What is 4chan? Forrás: www.4chan.org/ (Letöltés ideje: 2017. 08. 25.)

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

Akamai (2016): *DDOS and web application attacks stats & trends July – September 2016.* Forrás: www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report-infographic.pdf (Letöltés ideje: 2017. 08. 25.)

Akamai (2017): *Company History: How Akamai got its start.* Forrás: www.akamai.com/us/en/about/company-history.jsp (Letöltés ideje: 2017. 08. 25.)

Almár Iván (1999): *A SETI szépsége.* Budapest, Vince Kiadó.

Ambrus Éva (2017): Blokkláncok. *Hadmérnök,* 12. évf. 2. sz. 224–234. Forrás: http://hadmernok.hu/172_18_ambrus.pdf (Letöltés ideje: 2017. 08. 25.)

Anonymous (2017): *News.* Forrás: www.anonews.co/anon-10-things (Letöltés ideje: 2017. 08. 25.)

Az Európai Parlament és a Tanács 2009/110/EK Irányelve (2009. szeptember 16.) az elektronikuspénz-kibocsátó intézmények tevékenységének megkezdéséről, folytatásáról és prudenciális felügyeletéről, a 2005/60/EK és a 2006/48/EK irányelv módosításáról, valamint a 2000/46/EK irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács 2011/92/EU Irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról

Az Európai Parlament és a Tanács 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

Az Európai Tanács határozata 2008/114/EC (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint a védelem javításának fokozásáról

Az Európai Tanács kerethatározata 2001/413/IB (2001. május 28.) a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről

Bauer Béla – Pillók Péter – Ruff Tamás – Szabó Andrea – Szanyi F. Eleonóra – Székely Levente (2017): *Magyar Ifjúság Jelentés 2016.* Budapest, Magyar Ifjúság Kutatás.

BBC (2017): *Massive Ransomware Infection Hits Computers in 99 Countries.* Forrás: www.bbc.com/news/technology-39901382 (Letöltés ideje: 2017. 08. 25.)

Belügyminisztérium (2016): *Intézkedések a kormányzati hálózat védelmében*. Forrás: www.kormany.hu/hu/belugyminiszterium/hirek/intezkedesek-a-kormanyzati-halozat-vedelmeben (Letöltés ideje: 2017. 08. 25.)

Belügyminisztérium (2017a): *Az önkormányzati ASP.* Forrás: http://alkalmazaskozpont.asp.lgov.hu/sites/alkalmazaskozpont.asp.lgov.hu/files/prezentacio_szakmapolitika_01_24_bm.pdf (Letöltés ideje: 2017. 08. 25.)

Belügyminisztérium (2017b): *Tájékoztató az önkormányzati ASP országos kiterjesztése kapcsán a csatlakoztatási konstrukcióról*. Forrás: http://alkalmazaskozpont.asp.lgov.hu/sites/alkalmazaskozpont.asp.lgov.hu/files/me_tajekoztato_csat_konstr_asp_2_0_2017_kincstar_plusz_nisz.pdf (Letöltés ideje: 2017. 08. 25.)

Bencsik Balázs (2015): *GovCERT-Hungary bemutatása*. Előadás, Budapest, Nemzeti Kibervédelmi Intézet.

Bergman, Michael K. (2001): White Paper: The Deep Web: Surfacing Hidden Value. *The Journal of Electronic Publishing,* Vol. 7. No. 1.

BMC (2016): *ITIL Processes and Best Practices*. Forrás: www.bmc.com/guides/itil-introduction.html (Letöltés ideje: 2017. 08. 25.)

Bocsok Viktor – Boldizs Péter Ferenc – Loós Csaba – Major Tamás (2015): *A dolgok internete. Technológiai háttér, információbiztonsági és adatvédelmi aspektusok*. Forrás: http://fornax.hu/wp-content/uploads/2016/09/Informa%CC%81cio%CC%81biztonsa%CC%81g-e%CC%81s-adatve%CC%81delem-az-IoT-vila%CC%81ga%CC%81banv02jav.pdf (Letöltés ideje: 2017. 08. 25.)

Bodmer, Sean – Kilger, Max – Carpenter, Gregory – Jones, Jade (2012): *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. New York, McGraw-Hill Osborne Media.

Bolcsó Dániel – Haász János (2017): Zsarolóvírus söpört végig a világon. *Index.hu,* 2017. 05. 12. Forrás: http://index.hu/tech/2017/05/12/kibertamadas_erhetett_angliai_korhazakat (Letöltés ideje: 2017. 08. 25.)

Bolcsó Dániel (2016): Magyar kórházakat támadnak zsarolóvírusokkal. *Index.hu,* 2016. 04. 21. Forrás: http://index.hu/tech/2016/04/21/korhazi_zsarolovirus_kiberbiztonsag_adatvedelem (Letöltés ideje: 2017. 08. 25.)

Bolcsó Dániel (2017): Így védekezzen a zsarolóvírusok ellen! *Index.hu,* 2017. 06. 28. Forrás: https://index.hu/tech/helpdeszka/2017/06/28/petrwrap_petya_wannacry_zsarolovirus_kiberbiztonsag_vedekezes_megelozes (Letöltés ideje: 2017. 08. 25.)

Broad, William J. – Markoff, John – Sanger, David E. (2011): Israeli Test on Worm Called Crucial in Iran Nuclear Delay. *New York Times,* 2011. 01. 16. Forrás: www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&scp=2&sq=stuxnet&st=cse (Letöltés ideje: 2017. 08. 25.)

Buzan, Barry – Wæver, Ole – de Wilde, Jaap (1998): *Security: A New Framework for Analysis.* Boulder, Lynne Rienner Publishers.

Carr, Jeffrey (2012): *The Myth of the CIA and the Trans-Siberian Pipeline Explosion*. Forrás: http://jeffreycarr.blogspot.hu/2012/06/myth-of-cia-and-trans-siberian-pipeline.html (Letöltés ideje: 2017. 08. 25.)

Carr, Jefrrey (2011): *Inside Cyber Warfare: Mapping the Cyber Unerworld.* Sebastopol, O'Reilly Media.

Castells, Manuel (2005): *A hálózati társadalom kialakulása – Az információ kora*. I. kötet. Budapest, Gondolat–Infonia.

Cellan-Jones, Rory (2014): Stephen Hawking warns artificial intelligence could end mankind. *BBC,* 2014. 12. 04. Forrás*:* www.bbc.com/news/technology-30290540 (Letöltés ideje: 2017. 08. 25.)

CERT (2017): *Authorized Users of "CERT".* Forrás: www.cert.org/incident-management/csirt-development/cert-authorized.cfm? (Letöltés ideje: 2017. 08. 25.)

CERT GOV.PL (2017): *System ARAKIS-GOV.* Forrás: www.cert.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html (Letöltés ideje: 2017. 08. 25.)

Checkoway, Stephen – McCoy, Damon – Kantor, Brian – Anderson, Danny – Shacham, Hovav – Savage, Stefan – Koscher, Karl – Czeskis Alexei – Roesner, Franziska – Kohno, Tadayoshi (2011): *Comprehensive Experimental Analyses of Automotive Attack Surfaces.* Forrás: www.autosec.org/pubs/cars-usenixsec2011.pdf (Letöltés ideje: 2017. 08. 25.)

Cisco (2014): *The Internet of Things Reference Model.* Forrás: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf (Letöltés ideje: 2017. 08. 25.)

Cisco (2016): *Cisco IoT System Security: Mitigate Risk, Simplify Compliance, and Build Trust.* Forrás: https://cubecyber.com/wp-content/uploads/2016/01/iot-system-security-wp.pdf (Letöltés ideje: 2017. 08. 25.)

Common Criteria (2017a): *Publications.* Forrás: www.commoncriteriaportal.org/cc (Letöltés ideje: 2017. 08. 25.)

Common Criteria (2017b): *Publications.* Forrás: www.commoncriteriaportal.org/ccra (Letöltés ideje: 2017. 08. 25.)

Conger, Kate (2017): *Facebook Tells Developers to Not Use Data for Surveillance.* Forrás: https://techcrunch.com/2017/03/13/facebook-tells-developers-not-use-data-for-surveillance (Letöltés ideje: 2017. 08. 25.)

Council of Europe (2001): *Concention on Cybercrime.* Forrás: www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (Letöltés ideje: 2017. 08. 25.)

Council of Europe (2017): *Chart of Signatures and Ratifications of Treaty 185.* Forrás: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (Letöltés ideje: 2017. 08. 25.)

Cybersecurity Strategy of the European Union (2013): *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.*

Deighton, Ben (2017): Critical Infrastructure Under Daily Attack – ERNCIP Head Georg Peter. *Horizon,* 2017. 03. 20. Forrás: https://horizon-magazine.eu/article/critical-infrastructures-under-daily-attack-erncip-head-georg-peter_en.html (Letöltés ideje: 2017. 08. 25.)

Denning, Dorothy E. (2001): *Is Cyber Terror Next?* Forrás: http://essays.ssrc.org/sept11/essays/denning.htm (Letöltés ideje: 2017. 08. 25.)

Department of Defense (1983): *Department of Defense Trusted Computer System Evaluation Criteria*. Forrás: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf (Letöltés ideje: 2017. 08. 25.)

Digiconomist (2017): *Bitcoin Energy Consumption Index*. Forrás: https://digiconomist.net/bitcoin-energy-consumption (Letöltés ideje: 2017. 08. 25.)

DigitalHungary (2017): *Digitalizáció: megváltozott a vállalatvezetők hozzáállása*. Forrás: www.digitalhungary.hu/e-volution/Digitalizacio-megvaltozott-a-vallalatvezetok-hozzaallasa/4066 (Letöltés ideje: 2017. 08. 25.)

Digitális Jóléti Program (2017a): *1488/2016. (IX. 2.) Korm. határozat Magyarország digitális gyermekvédelmi stratégiája.*

Digitális Jóléti Program (2017b): *1491/2016. (IX. 15.) Korm. határozat Magyarország digitális exportfejlesztési stratégiája.*

Digitális Jóléti Program (2017c): *1536/2016. (X. 13.) Korm. határozat Magyarország Digitális Oktatási Stratégiája.*

Digitális Jóléti Program (2017d): *1858/2016. (XII. 27.) Korm. határozat Magyarország digitális startup stratégiája.*

Digitális Megújulás Cselekvési Terv 2010–2014. DMCST (2010).

Directive 2013/40/EU European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

Dorrans, Barry (2017): The release of the patch probably isn't going to help that £15m MRI machine that runs XP embedded whose maker went bankrupt 10 years ago. *Twitter.com,* 2017. 05. 13. Forrás: https://twitter.com/blowdart/status/863364192316735488 (Letöltés ideje: 2017. 08. 25.)

EECSP – Energy Expert Cyber Security Platform (2017): *Cyber Security in the Energy Sector. Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector.* Forrás: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf (Letöltés ideje: 2017. 08. 25.)

Emilyo (2017): *Common Modules.* Forrás: www.emilyo.eu/node/988 (Letöltés ideje: 2017. 08. 25.)

ENISA (2017a): *About ENISA.* Forrás: www.enisa.europa.eu/about-enisa (Letöltés ideje: 2017. 08. 25.)

ENISA (2017b): *Cyber Europe.* Forrás: www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme (Letöltés ideje: 2017. 08. 25.)

ENISA (2017c): *ENISA Strategy 2016–2020.* Forrás www.enisa.europa.eu/publications/corporate/enisa-strategy (Letöltés ideje: 2017. 08. 25.)

ENISA (2017d): *Cramm.* Forrás: www.enisa.europa.eu/publications/articles/standards-for-cyber-security (Letöltés ideje: 2017. 08. 25.)

ENISA (2017e): *Actionable Information for Security Incident Response.* Forrás: www.enisa.europa.eu/publications/actionable-information-for-security (Letöltés ideje: 2017. 08. 25.)

EUGO (2017): *eGovernment in Hungary.* Forrás: http://eugo.gov.hu/key-facts-about-hungary/egovernment-hungary (Letöltés ideje: 2017. 08. 25.)

Europe 2020 Strategy (2010): *Europe 2020 – A Strategy for Smart, Sustainable and Inclusive Growth.*

European Commission (2004): *Critical Infrastructure Protection in the Fight Against Terrorism*.

European Commission (2005): *Zöld Könyv egy Kritikus Infrastruktúra Védelmi Európai Programról.*

European Commission (2006): *European Programme for Critical Infrastructure Protection.*

European Commission (2008): *Critical Infrastructure Warning Information Network (CIWIN).*

European Commission (2012): *Declaration on the Launch of the Global Alliance Against Child Sexual Abuse Online.* Forrás: http://europa.eu/rapid/press-release_MEMO-12-944_en.htm (Letöltés ideje: 2017. 08. 25.)

European Commission (2015a): *A Digital Single Market for Europe.* Forrás: https://ec.europa.eu/commission/sites/beta-political/files/2-years-on-dsm_en_0.pdf (Letöltés ideje: 2017. 08. 25.)

European Commission (2015b): *A bizottság közleménye az európai parlamentnek, a tanácsnak, az európai gazdasági és szociális bizottságnak és a régiók bizottságának. Európai digitális egységes piaci stratégia.* Forrás: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:52015DC0192 (Letöltés ideje: 2017. 08. 25.)

European Commission (2015c): *The European Agenda on Security. Forrás:* https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en (Letöltés ideje: 2017. 08. 25.)

European Commission (2016a): *DESI 2016 Country Profiles.* Forrás: https://ec.europa.eu/digital-single-market/en/news/desi-2016-country-profiles (Letöltés ideje: 2017. 08. 25.)

European Commission (2016b): *What is the Digital Economy and Society Index?* Forrás: http://europa.eu/rapid/press-release_MEMO-16-385_en.htm (Letöltés ideje: 2017. 08. 25.)

European Commission (2016c): *Digital Economy and Society Index (DESI) 2017.* Forrás: http://europa.eu/rapid/press-release_MEMO-17-352_en.htm (Letöltés ideje: 2017. 08. 25.)

European Commission (2017a): *The Digital Economy and Society Index (DESI).* Forrás: https://ec.europa.eu/digital-single-market/desi (Letöltés ideje: 2017. 08. 25.)

European Commission (2017b): *The Digital Economy and Society Index (DESI) Country Profiles.* Forrás: https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2017 (Letöltés ideje: 2017. 08. 25.)

European Commission (2017c): *Digital Single Market Bringing Down Barriers to Unlock Online Opportunities.* Forrás: https://ec.europa.eu/commission/priorities/digital-single-market_en (Letöltés ideje: 2017. 08. 25.)

European Commission (2017d): *Az Unió helyzetéről szóló 2017. évi beszéd – Kiberbiztonság: a Bizottság megerősíti a kibertámadásokkal szembeni uniós reagálási képességet.* Forrás: http://europa.eu/rapid/press-release_IP-17-3193_hu.htm (Letöltés ideje: 2017. 08. 25.)

European Commission (2017e): *Kiberbiztonsági reform Európában 2017.* Forrás: www.consilium.europa.eu/hu/policies/cyber-security (Letöltés ideje: 2017. 08. 25.)

European Commission (2017f): *Report from the Commission to the European Parliament and to the Council on the Assessment of the Risks of Money Laundering and Terrorist Financing Affecting the Internal Market and Relating to Cross-border Situations.* Brussels, 26.6.2017 SWD(2017) 241 final PART 2/2. Forrás: http://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a-5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF (Letöltés ideje: 2017. 08. 25.)

European Commission (2017g): *Critical Infrastructure.* Forrás: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en (Letöltés ideje: 2017. 08. 25.)

European Commission (2017h): *Az európai digitális menetrend.* Forrás: https://europa.eu/european-union/file/1515/download_hu?token=BR0rWYPW (Letöltés ideje: 2017. 08. 25.)

European Commission (2017i): *Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification "Cybersecurity Act".* Forrás: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF (Letöltés ideje: 2017. 08. 25.)

Europol (2016a): *'Avalanche' Network Dismantled in International Cyber Operation*. Forrás: www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation (Letöltés ideje: 2017. 08. 25.)

Europol (2016b): *Europol Review 2015.* Forrás: www.europol.europa.eu/sites/default/files/documents/europol_review_2015.pdf (Letöltés ideje: 2017. 08. 25.)

Europol (2017a): *Operation Avalanche – Infographic – Technical.* Forrás: www.europol.europa.eu/publications-documents/operation-avalanche-infographic-technical (Letöltés ideje: 2017. 08. 25.)

Europol (2017b): *EU Policy Cycle – EMPACT.* Forrás: www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact (Letöltés ideje: 2017. 08. 25.)

Europol (2017c): *European Cybercrime Centre – EC3. Combating Crime in a Digital Age.* Forrás: www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Letöltés ideje: 2017. 08. 25.)

Europol (2017d): *Strategic Analysis. Complementing Operational Analysis.* Forrás: www.europol.europa.eu/activities-services/services-support/strategic-analysis (Letöltés ideje: 2017. 08. 25.)

Europol (2017e): *Golden Rules – Safe Online Shopping.* Forrás: www.europol.europa.eu/sites/default/files/documents/goldenrules-hungary.pdf (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016a): *Ausztria és a V4-ek internethasználóinak teljes lakossághoz viszonyított százalékos aránya 2016-ban*. Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”internet-usage”,”indicator”:”i_iu3”,”breakdown-group”:”total”,-”unit-measure”:”pc_ind”,”time-period”:”2016”,”ref-area”:[„AT”,”CZ”,”-HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016b): *Ausztria és a V4-ek napi internethasználóinak teljes lakossághoz viszonyított százalékos aránya 2016-ban.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”internet-usage”,”indicator”:”i_iday”,”breakdown-group”:”total”,”unit-measure”:”pc_ind”,”time-period”:”2016”,”ref-area”:-[„AT”,”CZ”,”HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016c): *Ausztria és a V4-ek olyan lakosainak teljes lakossághoz viszonyított százalékos aránya, akik sohasem használnak internetet 2016-ban.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”internet-usage”,”indicator”:”i_iux”,”breakdown-group”:”total”,”unit-measure”:”pc_ind”,”time-period”:”2016”,”ref-area”:[„AT”,”CZ”,”HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016d): *Ausztria és a V4-ek olyan lakosainak teljes lakossághoz viszonyított százalékos aránya, akik a magas ár miatt nem használnak internetet 2016-ban.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”bbquality”,”indicator”:”h_xcost”,”breakdown-group”:”hhbytype”,”unit-measure”:”pc_hh”,”time-period”:”2016”,”ref-area”:[„A”,”CZ”,”HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016e): *Ausztria és a V4-ek szélessávúinternet-előfizetéseinek száma 100 lakosra vetítve 2016-ban.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”broadband”,”indicator”:”bb_penet”,”breakdown-group”:”total”,”unit-measure”:”subs_per_100_pop”,”time-period”:”2016-06”,”ref-area”:-[„AT”,”CZ”,”HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016f): *Ausztria és a V4-ek szélessávúinternet-előfizetéseinek sávszélességenkénti ára 2015-ben.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”bbquality”,”indicator”:”Price_Internet_Fixed_Tel”,”breakdown-group”:”byDownloadSpeed4”,”unit-measure”:”minimum_euro_PPP”,”time-period”:”2015-10”,”ref-area”:[„AT”,”CZ”,”HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016g): *Ausztria és a V4-ek mobiltelefonon keresztüli internetelérése inek száma 2016-ban.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”mobile”,-”indicator”:”i_iu3g”,”breakdown-group”:”total”,”unit-measure”:”pc_ind”,”-time-period”:”2016”,”ref-area”:[„AT”,”CZ”,”HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016h): *Ausztria és a V4-ek mobiltelefon-előfizetéseinek száma 2010-ben.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”mobile”,”indicator”:”mob_subs”,”breakdown-group”:”total”,”unit-measure”:”nbr_subs”,”time-period”:”2010”,”ref-area”:[„AT”,”CZ”,”HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016j): *Ausztria és a V4-ek mobiltelefon-előfizetéseinek száma 2015-ben.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”mobile”,”indicator”:”mob_subs”,”breakdown-group”:”total”,”unit-measure”:”nbr_subs”,”time-period”:”2015”,”ref-area”:[„AT”,”CZ”,”HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016k): *Ausztria és a V4-ek lakosainak teljes lakossághoz viszonyított aránya, akik már rendeltek árut vagy szolgáltatást az interneten 2016-ban.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”ecommerce”,”indicator”:-”i_blt12”,”breakdown-group”:”total”,”unit-measure”:”pc_ind”,”time-period”:”2016”,”ref-area”:[„AT”,”CZ”,”HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016m): *Ausztria és a V4-ek lakosainak teljes lakossághoz viszonyított aránya, akik már rendeltek árut vagy szolgáltatást másik EU-s országból az interneten 2016-ban.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”ecommerce”,”indicator”:”i_bfeu”,”breakdown-group”:”total”,-”unit-measure”:”pc_ind”,”time-period”:”2016”,”ref-area”:[„AT”,”CZ”,”-HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016n): *Ausztria és a V4-ek vállalkozásainak aránya, amelyek használják az e-kereskedelem valamilyen formáját 2016-ban.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”ecommerce”,”indicator”:”e_esell”,”breakdown-group”:”total”,”unit-measure”:”pc_ent_aesell”,”time-period”:”2016”,”ref-area”:[„AT”,”CZ”,”HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016o): *Ausztria és a V4-ek vállalkozásainak e-kereskedelemből származó bevétele 2016-ban.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”ecommerce”,”indicator”:”e_eturn”,”breakdown-group”:”total”,”unit-measure”:”pc_turn”,”time-period”:”2016”,”ref-area”:[„AT”,”CZ”,”-HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016p): *Ausztria és a V4-ek internethasználóinak aránya, akik legalább egy alkalommal használtak e-közigazgatási szolgáltatást 2016-ban.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”egovernment”,”indicator”:”i_iugov12”,”breakdown-group”:”total”,”unit-measure”:”pc_ind_ilt12”,”time-period”:”2016”,”ref-area”:[„AT”,”CZ”,”HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2016q): *Ausztria és a V4-ek internethasználóinak aránya, akik legalább egy alkalommal használtak e-közigazgatási szolgáltatást, és ott legalább egy elektronikus ügyiratot ki is töltöttek 2016-ban.* Forrás: http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={„indicator-group”:”egovernment”,”indicator”:”i_igov12rt”,”breakdown-group”:”total”,”unit-measure”:”pc_igov12nrt”,”time-period”:”2016”,”ref-area”:[„AT”,”CZ”,”HU”,”PL”,”SK”]} (Letöltés ideje: 2017. 08. 25.)

Eurostat (2017a): *A V4-ek és Ausztria internet-penetrációja 2010–2016 között.* Forrás: http://ec.europa.eu/eurostat/tg m/table.do?tab=table&init=1&language=en&pcode=tin00091 (Letöltés ideje: 2017. 08. 25.)

Facebook (2017): *Adatkezelési szabályzat.* Forrás: https://hu-hu.facebook.com/privacy/explanation (Letöltés ideje: 2017. 08. 25.)

FBI (2004): *Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004.* Forrás: www2.fbi.gov/congress/congress04/lourdeau022404.htm (Letöltés ideje: 2017. 08. 25.)

Finta Sándor – Barta Zsombor – Balogh Samu Márton (2017): *Smart Budapest: Budapest okos város jövőképe.* Budapest, Budapest 2024 Nonprofit Zrt.

FireEye (2014): *APT28: A Window Into Russia's Cyber Espionage Operations?* Forrás: www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf (Letöltés ideje: 2017. 08. 25.)

FireEye (2017): *Mandiant Consulting Services. Responding to the Most Critical Breaches and Empowering Companies to Protect their Key Assets.* Forrás: www.fireeye.com/content/dam/fireeye-www/global/en/services/pdfs/ds-mandiant-consulting-services.pdf (Letöltés ideje: 2017. 08. 25.)

FireEye (é.n.): *APT1 Exposing One of China's Cyber Espionage Units.* Forrás: www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (Letöltés ideje: 2017. 08. 25.)

Galeon, Dom – Reedy, Christianna (2017): Kurzweil Claims That the Singularity Will Happen by 2045. *Futurism.com,* 2017. 10. 05. Forrás: https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045 (Letöltés ideje: 2017. 10. 05.)

Gallagher, Sean (2017): Apple Deleted Server Supplier after Finding Infected Firmware in Servers. *Arstechnica.com,* 2017. 02. 24. Forrás: https://arstechnica.com/information-technology/2017/02/apple-axed-supermicro-servers-from-datacenters-because-of-bad-firmware-update (Letöltés ideje: 2017. 08. 25.)

Garnaeva, Maria – Sinitsyn, Fedor – Namestnikov, Yury – Makrushin, Denis – Liskin Alexander (2016): *Kaspersky Security Bulletin: Overall Statistics for 2016.* Forrás: https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky_Security_Bulletin_2016_Statistics_ENG.pdf (Letöltés ideje: 2017. 08. 25.)

Gartner (2017): *Gartner Forecasts Flat Worldwide Device Shipments Until 2018.* Forrás: www.gartner.com/newsroom/id/3560517 (Letöltés ideje: 2017. 08. 25.)

Gazdag Ferenc szerk. (2011): *Biztonsági tanulmányok – Biztonságpolitika.* Budapest, ZMNE.

Ge, Wei (1999): *Special Economic Zones and the Economic Transition in China.* (Economic Ideas Leading to the 21st Century, 5.) Singapore, World Scientific Publishing.

Gibson, William (1992): *Neurománc.* Ford. Ajkay Örkény. Budapest, Valhalla Páholy.

GKI Digital (2016a): *E-toplista 2016 – A legnagyobb webáruházak listája*. Forrás: www.gkidigital.hu/2016/06/02/etoplista2016 (Letöltés ideje: 2017. 08. 25.)

GKI Digital (2016b): *A hazai vállalatok szerint a digitalizáció a jövőbeni versenyképesség kulcsa.* Forrás: www.gkidigital.hu/2016/05/25/a-hazai-vallalatok-szerint-a-digitalizacio-a-jovobeni-versenykepesseg-kulcsa (Letöltés ideje: 2017. 08. 25.)

Goodin, Dan (2017): NSA-leaking Shadow Brokers Just Dumped its Most Damaging Release Yet. Windows Zero-days, SWIFT Bank Hacks, Slick Exploit Loader among the Contents. *Arstechnica.com,* 2017. 04. 14. Forrás: https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet (Letöltés ideje: 2017. 08. 25.)

Gov-CERT (2017): *Az SMB sérülékenységet kihasználó PetrWrap Ransomware kampány.* Forrás: www.cert-hungary.hu/node/381 (Letöltés ideje: 2017. 08. 25.)

Graham, Chris (2017): Cyber Attack Hits German Train Stations as Hackers Target Deutsche Bahn. *The Telegraph,* 2017. 05. 13. Forrás: www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche (Letöltés ideje: 2017. 08. 25.)

Greenberg, Andy (2016): Hackers Fool Tesla S's Autopilot to Hide and Spoof Obstacles. *Wired.com,* 2016. 04. 08. Forrás: www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles (Letöltés ideje: 2017. 08. 25.)

Gubbi, Jayavardhana – Buyya, Rajkumar – Marusic, Slaven – Palaniswami, Marimuthu (2013): Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems,* Vol. 29, No. 7. 1645–1660. Forrás: https://arxiv.org/ftp/arxiv/papers/1207/1207.0203.pdf (Letöltés ideje: 2017. 08. 25.)

Guerrero-Saade, Juan Andres – Raiu, Costin – Moore, Daniel – Rid, Thomas (2017): *Penquin's Moonlit Maze. The Dawn of Nation-State Digital Espionage.* Forrás: https://securelist.com/files/2017/04/Penquins_Moonlit_Maze_PDF_eng.pdf (Letöltés ideje: 2017. 08. 25.)

Gyányi Sándor (2007): DDoS támadások veszélyei és az ellenük való védekezés. *Hadmérnök,* Robothadviselés 7. tudományos szakmai konferencia különszám. Forrás: http://hadmernok.hu/kulonszamok/robothadviseles7/gyanyi_rw7.html (Letöltés ideje: 2017. 08. 25.)

Gyányi Sándor (2012): *Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem.* Doktori értekezés. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem.

H2020 (2017a): *Horizont 2020.* Forrás: www.h2020.gov.hu/horizont2020-program (Letöltés ideje: 2017. 08. 25.)

H2020 (2017b): *Secure Societies – Protecting Freedom and Security of Europe and its Citizens.* Forrás: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens (Letöltés ideje: 2017. 08. 25.)

H2020 (2017c): *Horizon 2020 Work Programme 2016–2017. 14. Secure societies – Protecting Freedom and Security of Europe and its Citizens.* Forrás: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf (Letöltés ideje: 2017. 08. 25.)

H2020 (2017d): *Hungary.* Forrás: http://ec.europa.eu/research/horizon2020/pdf/country-profiles/hu_country_profile_and_featured_projects.pdf#zoom=125&pagemode=none (Letöltés ideje: 2017. 08. 25.)

Hacktivity (2017): *Contact – About Us.* Forrás: https://hacktivity.com/en/contact/rolunk (Letöltés ideje: 2017. 08. 25.)

Haentjens, Axel (2012): *IT Service Management – ISO/IEC 20000 Eases Transition to Cloud Computing for Orange.* Forrás: www.iso.org/news/2012/05/Ref1577.html (Letöltés ideje: 2017. 08. 25.)

Haig Zsolt – Hajnal Béla – Kovács László – Muha Lajos – Sik Zoltán Nándor (2009): *A kritikus információs infrastruktúrák meghatározásának módszertana.* Budapest, ENO Advisory Kft.

Haig Zsolt – Kovács László – Ványa László (2008): Kritikus információs infrastruktúrák támadása, védelme. *Dunaújvárosi Főiskola Közleményei,* 29. évf. 1. sz. 265–273.

Haig Zsolt – Kovács László – Ványa László (2011): Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. *Felderítő Szemle,* 10. évf. 1–2. sz. 183–209.

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

Haig Zsolt (2015): *Információ, társadalom, biztonság.* Budapest, NKE Szolgáltató Kft.

Havass Miklós–Lengyel Veronika szerk. (1999): *Magyar válasz az Információs Társadalom kihívásaira. Szakértői anyag.* Forrás: http://members.iif.hu/lengyel/valasz (Letöltés ideje: 2017. 08. 25.)

Heise, Angie (2015): *Understanding the Enemy: The Advanced Persistent Threat.* Forrás: https://cyber.leidos.com/icsblog/understanding-the-enemy-the-advanced-persistent-threat (Letöltés ideje: 2017. 08. 25.)

Hern, Alex (2017a): Spam Email Operator's Faulty Backup Leaks 1.37bn Addresses. *The Guardian,* 2017. 03. 06. Forrás: www.theguardian.com/technology/2017/mar/06/email-addresses-spam-leak-river-city-media (Letöltés ideje: 2017. 08. 25.)

Hern, Alex (2017b): Google Acts against Fake News on Search Engine. *The Guardian,* 2017. 04. 25. Forrás: hwww.theguardian.com/technology/2017/apr/25/google-launches-major-offensive-against-fake-news#img-3 (Letöltés ideje: 2017. 08. 25.)

Herzberg, Ben – Bekerman, Dima – Zeifman, Igal (2016): *Breaking Down Mirai: An IoT DDoS Botnet Analysis*. Forrás: www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html (Letöltés ideje: 2017. 08. 25.)

History (2017): *The Death of Guy Fawkes.* Forrás: www.history.co.uk/this-day-in-history/31-january/the-death-of-guy-fawkes (Letöltés ideje: 2017. 08. 25.)

Hlács Ferenc (2017): Mindent megtesz a WannaCry-tűzoltásra a Microsoft. *HWSW.hu,* 2017. 05. 15. Forrás: www.hwsw.hu/hirek/57239/biztonsag-wannacry-ransomware-zsaroloszoftver-bitcoin.html (Letöltés ideje: 2017. 08. 25.)

Hunt, Troy (2017a): *Password Reuse, Credential Stuffing and Another Billion Records in Have I been Pwned.* Forrás: www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned (Letöltés ideje: 2017. 08. 25.)

Hunt, Troy (2017b): *Have I been Pwned?* Forrás: https://haveibeenpwned.com (Letöltés ideje: 2017. 08. 25.)

Hutchins, Eric M. – Cloppert, Michael J. – Amin, Rohan M. (2011): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Leading Issues in Information Warfare & Security Research,* No. 1. Forrás: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf (Letöltés ideje: 2017. 08. 25.)

HVG (2016): *Drónokat térít el egy magyar hekker.* Forrás: http://hvg.hu/tudomany/20160505_dronokat_terit_el_egy_magyar_hekker (Letöltés ideje: 2017. 08. 25.)

ICO (2017): *Preparing for the General Data Protection Regulation (GDPR): 12 Steps to Take Now.* Forrás: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf (Letöltés ideje: 2017. 08. 25.)

ICS-CERT (2016): *Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure.* Forrás: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (Letöltés ideje: 2017. 08. 25.)

ICS-CERT (2017): *Alert (ICS-ALERT-17-209-01) CAN Bus Standard Vulnerability.* Forrás: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-209-01 (Letöltés ideje: 2017. 08. 25.)

IEC (2017): *About IEC.* Forrás: www.iec.ch/about/?ref=menu (Letöltés ideje: 2017. 08. 25.)

IFLA (2017a): *About IFLA*. Forrás: www.ifla.org/about (Letöltés ideje: 2017. 08. 25.)

IFLA (2017b): *How to Spot Fake News.* Forrás: www.ifla.org/publications/node/11174 (Letöltés ideje: 2017. 08. 25.)

Inspire (2014): *Inspire Magazine.* Forrás: https://azelin.files.wordpress.com/2014/04/inspire-magazine-issue-12.pdf (Letöltés ideje: 2017. 08. 25.)

Internet World Stats (2017): *Internet Usage Statistics. The Internet Big Picture World Internet Users and 2017 Population Stats*. Forrás: www.internetworldstats.com/stats.htm (Letöltés ideje: 2017. 08. 25.)

Interpol (2017): *Cybercrime.* Forrás: www.interpol.int/Crime-areas/Cybercrime/Cybercrime (Letöltés ideje: 2017. 08. 25.)

ISACA (2017): *A Business Framework for the Governance and Management of Enterprise.* Forrás: www.isaca.org/cobit/Documents/COBIT-5-Introduction.pdf (Letöltés ideje: 2017. 08. 25.)

ISO 11898-1:2015: Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signalling. Forrás: www.iso.org/standard/63648.html (Letöltés ideje: 2017. 08. 25.)

ISO/IEC 27001:2005 ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements.

ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management.

ITBN (2017): *Történetünk.* Forrás: www.itbn.hu/index.php/hu/esemeny/tortenetunk (Letöltés ideje: 2017. 08. 25.)

ITMA Hungary (2017): *WannaCry zsarolóvírus.* Forrás: http://itma.blog.hu/2017/05/13/wannacry_zsarolovirus (Letöltés ideje: 2017. 08. 25.)

ITU (2005): *ITU Internet Reports 2005: The Internet of Things.* Forrás: www.itu.int/osg/spu/publications/internetofthings (Letöltés ideje: 2017. 08. 25.)

ITU (2008): *X.1205: Overview of Cybersecurity.* Forrás: www.itu.int/rec/T-REC-X.1205-200804-I (Letöltés ideje: 2017. 08. 25.)

ITU (2012): *ITU-T Recommendations.* Forrás: www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 (Letöltés ideje: 2017. 08. 25.)

ITU (2015): *Internet of Things Global Standards Initiative.* Forrás: www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (Letöltés ideje: 2017. 08. 25.)

ITU (2016): *ICT Facts and Figures 2016.* Forrás: www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf (Letöltés ideje: 2017. 08. 25.)

ITU (2017a): *About International Telecommunication Union (ITU).* Forrás: www.itu.int/en/about/Pages/default.aspx (Letöltés ideje: 2017. 08. 25.)

ITU (2017b): *Definition of Cybersecurity.* Forrás: www.itu.int/en/ITU-/studygroups/com17/Pages/cybersecurity.aspx (Letöltés ideje: 2017. 08. 25.)

ITU (2017c): *Global Cybersecurity Index (GCI) 2017.* Forrás: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (Letöltés ideje: 2017. 08. 25.)

Ivanov, Anton – Mamedov, Orkhan (2017): *In ExPetr/Petya's shadow, FakeCry ransomware wave hits Ukraine.* Forrás: https://securelist.com/in-expetrpetyas-shadow-fakecry-ransomware-wave-hits-ukraine/78973 (Letöltés ideje: 2017. 08. 25.)

Kaiser Tamás szerk. (2016): *Jó Állam Jelentés 2016.* Budapest, Dialóg Campus Kiadó.

Kaspersky (2016): *BlackEnergy APT Attacks in Ukraine Employ Spearphishing with Word Documents.* Forrás: https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440 (Letöltés ideje: 2017. 08. 25.)

Kaspersky (2017): *BlackEnergy APT Attacks in Ukraine*. Forrás: https://usa.kaspersky.com/resource-center/threats/blackenergy (Letöltés ideje: 2017. 08. 25.)

Khomani, Nadia – Solon, Olivia (2017): 'Accidental Hero' Halts Ransomware Attack and Warns: This is Not Over. *The Guardian,* 2017. 05. 13. Forrás: www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack (Letöltés ideje: 2017. 08. 25.)

KIBEV (2017): *Intézkedés-gyűjtemény az ipari rendszerek kiberbiztonságának fejlesztéséhez.* Forrás: www.kibev.hu/images/publikaciok/kibev_intezkedesek_tabla_2017_A0-v2.pdf (Letöltés ideje: 2017. 08. 25.)

Klimburg, Alexander ed. (2012): *National Cyber Security Framwork Manual.* Tallinn, NATO CCDCOE. Forrás: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (Letöltés ideje: 2017. 08. 25.)

Kormányzati Eseménykezelő Központ (2009): *PTA CERT-Hungary Központ, mint Nemzeti Hálózatbiztonsági Központ.* Forrás: www.cert-hungary.hu/node/65 (Letöltés ideje: 2017. 08. 25.)

Kormányzati Eseménykezelő Központ (2017): *Magunkról.* Forrás: www.cert-hungary.hu/node/1 (Letöltés ideje: 2017. 08. 25.)

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

Kovács László – Krasznay Csaba (2017): „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *NKE Stratégiai Védelmi Kutatóközpont Elemzések,* 2017/9.

Kovács, László – Nemeslaki, András – Orbók, Ákos – Szabó, András (2017): Structuration Theory and Strategic Alignment in Information Security Management: a Comprehensive Research Approach and Program. *AARMS,* Vol. 16, No. 1. 5–16.

Kovács László – Sipos Marianna (2010): A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. *Hadmérnök,* 5. évf. 4. sz. 163–172. Forrás: www.hadmernok.hu/2010_4_kovacs_sipos.pdf (Letöltés ideje: 2017. 08. 25.)

Kovács, László – Szentgáli, Gergely (2015): *National Cyber Security Organisation: Hungary.* Tallinn, NATO CCDCOE. Forrás: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_HUNGARY_2015-10-12.pdf (Letöltés ideje: 2017. 08. 25.)

Kovács László (2006): Az információs terrorizmus eszköztára. *Hadmérnök,* Robothadviselés 6. tudományos szakmai konferencia különszám. Forrás: http://zrinyi.zmne.hu/hadmernok/kulonszamok/robothadviseles6/kovacs_rw6.html ISSN 1788–1919 (Letöltés ideje: 2017. 08. 25.)

Kovács László (2011): Kiberháború? Internetes támadások a Wikileaks ellen és mellett. *Nemzet és Biztonság,* 4. évf. 1. sz. 3–8.

Kovács László (2012): Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése. *Hadmérnök,* 7. évf. 2. sz. 302–311.

Kovács László (2014): Az e-közszolgálat fejlesztés nemzetbiztonsági és hadtudományi kérdései. In Nemeslaki András szerk.: *E-közszolgálat fejlesztés: Elméleti alapok és tudományos kutatási módszerek.* Budapest, Nemzeti Közszolgálati Egyetem. 227–248.

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

KÖFOP (2015): *Közigazgatás- és Közszolgálat-fejlesztési stratégia 2014–2020.* Forrás: www.kormany.hu/download/8/42/40000/K%C3%B6zigazgat%C3%A1s_feljeszt%C3%A9si_strat%C3%A9gia_.pdf (Letöltés ideje: 2017. 08. 25.)

KSH (2017): *KSH statisztikai tükör.*

Kurzweil, Ray (2013): *A szingularitás küszöbén*. Budapest, Ad-Astra.

Lados Mihály szerk. (2011): *Smart Cities tanulmány.* Győr, MTA Regionális Kutatások Központja Nyugat-magyarországi Tudományos Intézet. Forrás: www-05.ibm.com/hu/download/IBM_SmarterCity_20110721.pdf (Letöltés ideje: 2017. 08. 25.)

Libicki, Martin (2017): *The Coming of Cyber Espionage Norms.* In Rõigas, Henri – Jakschis, Rais – Lindström, Lauri – Minárik, Tomaš eds.: *9th International Conference on Cyber Conflict: Defending the Core.* Tallinn, NATO CCD COE Publications. 7–23.

MacKeeper (2017): *Spammergate: The Fall of an Empire.* Forrás: https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire (Letöltés ideje: 2017. 08. 25.)

Magyar Információs Társadalom Stratégia – MITS (2003).

Magyar Szabványügyi Testület (2017): *Információbiztonság. MSZ/T ISO/IEC 27001:2014.* Forrás: www.mszt.hu/web/guest/informaciobiztonsag1 (Letöltés ideje: 2017. 08. 25.)

Makkay Imre – Seebauer Imre – Haig Zsolt – Vass Sándor – Ványa László, – Kovács László (2002): *Az információs társadalom veszélyforrásai: A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban.* Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem.

MalwareTech (2017): *Botnets.* Forrás: https://intel.malwaretech.com/WannaCrypt.html (Letöltés ideje: 2017. 08. 25.)

Maney, Kevin (2014): *Kevin Ashton, Father of the Internet of Things & Network Trailblazer.* Forrás: https://newsroom.cisco.com/feature-content?articleId=1558161 (Letöltés ideje: 2017. 08. 25.)

Megkezdődött az elektronikus egészségügyi szolgáltatási tér próbaüzeme. Forrás: www.kormany.hu/hu/emberi-eroforrasok-miniszteriuma/egeszsegugyert-felelos-allamtitkarsag/hirek/megkezdodott-az-elektronikus-egeszsegugyi-szolgaltatasi-ter-probauzeme (Letöltés ideje: 2017. 08. 25.) (2017)

Mella-Marquez, José M. – López-López, Asunción – Mella-Lopez, Victor (2014): *European Smart Cities: The Case Of Madrid (Spain).* Forrás: www.regionalstudies.org/uploads/EUROPEAN_SMART_CITIES_final.pdf (Letöltés ideje: 2017. 08. 25.)

Microsoft (2017a): *Korszakhatárhoz érkeztek a magyar nagyvállalatok.* Forrás: https://news.microsoft.com/hu-hu/2017/03/17/korszakhatarhoz-erkeztek-a-magyar-nagyvallalatok/#sm.000cm8tmb1aa4e1ksvd1n4ulfa4fy (Letöltés ideje: 2017. 08. 25.)

Microsoft (2017b): *Microsoft Update Katalógus.* Forrás: www.catalog.update.microsoft.com/Search.aspx?q=KB4012598 (Letöltés ideje: 2017. 08. 25.)

Mitnick, Kevin (2012): *Ghost in the Wires.* New York, Back Bay Books.

MTE (2016): *Hogyan viselkednek a magyar Facebookozók? Itt vannak a legújabb trendek és eredmények.* Forrás: http://mte.hu/_magyar_facebook_trendek (Letöltés ideje: 2017. 08. 25.)

MTI (2012): Dunaújvárosi tinit gyanúsítanak az Alkotmány márciusi átírásával. *Origo.hu,* 2012. 09. 08. Forrás: www.origo.hu/itthon/20120908-dunaujvarosi-tinit-gyanusitanak-az-alkotmany-marciusi-atirasaval.html (Letöltés ideje: 2017. 08. 25.)

Muha Lajos – Krasznay Csaba (2014): *Az elektronikus információs rendszerek biztonságának menedzselése*. Budapest, Nemzeti Közszolgálati Egyetem.

Muha Lajos szerk. (2002): *Az informatikai biztonság kézikönyve.* Budapest, Verlag und Dashöfer.

Munk Sándor (2007): *Katonai informatikai rendszerek interoperabilitásának aktuális hadtudományi kérdései*. MTA-doktori értekezés. Forrás: http://real-d.mtak.hu/86/1/Munk_Sandor.pdf (Letöltés ideje: 2017. 08. 25.)

NASK (2017): *About NASK.* Forrás: http://eng.nask.pl/en/about-nask/about-nask/250,Research-and-Academic-Computer-Network.html (Letöltés ideje: 2017. 08. 25.)

NATO (2002): *Prague Summit Declaration.* Forrás: www.nato.int/cps/en/natohq/official_texts_19552.htm (Letöltés ideje: 2017. 08. 25.)

NATO (2010): *A NATO 2010-es új stratégiai koncepciója: Aktív Szerepvállalás, Modern Védelem az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságáról.*

NATO (2016): *Warsaw Summit Communiqué.* Forrás: www.nato.int/cps/en/natohq/official_texts_133169.htm (Letöltés ideje: 2017. 08. 25.)

NATO (2017): *Cyber Defence*. Forrás: www.nato.int/cps/en/natolive/topics_78170.htm (Letöltés ideje: 2017. 08. 25.)

NATO ATC (2016): *Cybersecurity. A Generic Reference Curriculum*. Forrás: www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20161025_1610-cybersecurity-curriculum.pdf (Letöltés ideje: 2017. 08. 25.)

NEIH – Nemzeti Elektronikus Információbiztonsági Hatóság (2017): *Európai kiberbiztonsági hónap.* Forrás: http://neih.gov.hu/kiberhonap-2017 (Letöltés ideje: 2017. 08. 25.)

Nemeslaki András szerk. (2014): *E-közszolgálatfejlesztés. Elméleti alapok és tudományos kutatási módszerek.* Budapest, Nemzeti Közszolgálati Egyetem.

Nemzeti Infokommunikációs Stratégia (2014): *Az infokommunikációs szektor fejlesztési stratégiája (2014–2020) v7.0.* Forrás: http://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf (Letöltés ideje: 2017. 08. 25.)

Nemzeti Információs Társadalom Stratégia NITS (2001).

Nemzeti Kibervédelmi Intézet (2017): *Nemzetközi IT-biztonsági sajtószemle 2017. 30. hét*. Forrás: http://neih.gov.hu/sites/default/files/dlc/Sajt%C3%B3szemle_30.h%C3%A9t.pdf (Letöltés ideje: 2017. 08. 25.)

Newman, Lily Hay (2016): What We Know About Friday's Massive East Coast Internet Outage. *Wired.com,* 2016. 10. 21. Forrás: www.wired.com/2016/10/internet-outage-ddos-dns-dyn (Letöltés ideje: 2017. 08. 25.)

NIS Directive (2016): *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.*

NIST (2014): *Framework for Improving Critical Infrastructure Cybersecurity.* Forrás: www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf (Letöltés ideje: 2017. 08. 25.)

NIST (2017): *NIST Mission, Vision, Core Competencies, and Core Values.* Forrás: www.nist.gov/about-nist/our-organization/mission-vision-values (Letöltés ideje: 2017. 08. 25.)

NIST 800-53 (2013). Forrás: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (Letöltés ideje: 2017. 08. 25.)

NIST Cyber-physical System (2017): *NIST Cyber-physical System.* Forrás: www.nist.gov/el/cyber-physical-systems (Letöltés ideje: 2017. 08. 25.)

No More Ransom (2017): *No More Ransom.* Forrás: www.nomoreransom.org (Letöltés ideje: 2017. 08. 25.)

Norton (2017): *What is Social Engineering?* Forrás: https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html (Letöltés ideje: 2017. 08. 25.)

ObuCity (2017): *ObuCity.* Forrás: http://obucity.hu (Letöltés ideje: 2017. 08. 25.)

OECD (2015): *OECD Fixed Broadband Penetration and GDP Per Capita.* Forrás: www.oecd.org/sti/broadband/1_9-BBPenetration-GDPperCap-2016-06.xls (Letöltés ideje: 2017. 08. 25.)

OECD (2017): *OECD Broadband Statistics.* Forrás: www.oecd.org/sti/broadband/broadband-statistics (Letöltés ideje: 2017. 08. 25.)

Olson, Parmy (2012): *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency.* New York – Boston – London, Little, Brown and Co.

OpenSignal (2016): *Global State of Mobile Networks (August 2016).* Forrás: https://opensignal.com/reports/2016/08/global-state-of-the-mobile-network (Letöltés ideje: 2017. 08. 25.)

O'Sullivan, Dan (2017): The RNC Files: Inside the Largest US Voter Data Leak. *Upguard.* Forrás: www.upguard.com/breaches/the-rnc-files (Letöltés ideje: 2017. 08. 25.)

OWASP (2017a): *OWASP Internet of Things Project.* Forrás: www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main (Letöltés ideje: 2017. 08. 25.)

OWASP (2017b): *IoT Vulnerabilities.* Forrás: www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities (Letöltés ideje: 2017. 08. 25.)

Polityuk, Pavel – Vukmanovic, Oleg – Jewkes, Stephen (2017): Ukraine's Power Outage was a Cyber Attack: Ukrenergo. *Reuters.com,* 2017. 01. 18. Forrás: www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA (Letöltés ideje: 2017. 08. 25.)

Poulsen, Kevin (2010): Apple Bans Lame WikiLeaks App. *Wired.com,* 2010. 12. 21. Forrás: www.wired.com/2010/12/wikileaks-app (Letöltés ideje: 2017. 08. 25.)

Purser, Steve (2014): Standards for Cyber Security. In Hathaway, M. E. ed.: *Best Practices in Computer Network Defense: Incident Detection and Response.* Amsterdam, IOS Press. 97–106. Forrás: www.enisa.europa.eu/publications/articles/standards-for-cyber-security (Letöltés ideje: 2017. 08. 25.)

Reuters (2017): *FireEye researcher hacked; firm says no evidence its systems hit.* Forrás: https://cio.economictimes.indiatimes.com/news/digital-security/fireeye-researcher-hacked-firm-says-no-evidence-its-systems-hit/59856584 (Letöltés ideje: 2017. 08. 25.)

Riley, Michael – Dlouhy, Jennifer A. – Gruley, Bryan (2017): Russians Are Suspects in Nuclear Site Hackings, Sources Say. *Bloomberg.com,* 2017. 07. 07. Forrás: www.bloomberg.com/news/articles/2017-07-07/russians-are-said-to-be-suspects-in-hacks-involving-nuclear-site (Letöltés ideje: 2017. 08. 25.)

Riley, Michael – Robertson, Jordan (2017): Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known. *Bloomberg.com,* 2017. 06. 13. Forrás: www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections (Letöltés ideje: 2017. 08. 25.)

Rinaldi, Steven M. – Peerenboom, James P. – Kelly Terrence K. (2001): Identifying, Understanding and Analysing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine.*

S.1353 – Cybersecurity Enhancement Act of 2014 (US)

SANS (2016): *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Forrás: https://ics.sans.org/media/E-SAC_SANS_Ukraine_DUC_5.pdf (Letöltés ideje: 2017. 08. 25.)

Sarwar, Usman (2012): *Internet of Things: The Next Technology Revolution*. 3rd International Conference on Network Applications, Protocols and Services (NetAPPS).

Schmitt, Michael N. ed. (2013): *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York, Cambridge University Press.

Schmitt, Michael N. ed. (2016): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* New York, Cambridge University Press.

Schneier, Bruce (2010): Stuxnet. *Schneier.com,* 2010. 10. 07. Forrás: www.schneier.com/blog/archives/2010/10/stuxnet.html (Letöltés ideje: 2017. 08. 25.)

Schopp Attila (2014): *Okos város = élhető város.* Forrás: www.itbusiness.hu/Fooldal/hirek/ITB/Okos_varos_elheto_varos.html (Letöltés ideje: 2017. 08. 25.)

Shamieh, Luna – Szenes, Zoltán (2015): The Propaganda of ISIS/DAESH Through the Virtual Space. *DATR,* Vol. 7, No. 1. 7–31. Forrás: www.tmmm.tsk.tr/publication/datr/volume10/02-ThePropaganda_of_ISIS_DAESH_through_VirtualSpace.pdf (Letöltés ideje: 2017. 08. 25.)

Smart CEI Moncloa (2017): *Smart CEI Moncloa Dashboard.* Forrás: http://ceiboard.dit.upm.es/dashboard/sck_pub (Letöltés ideje: 2017. 08. 25.)

Schneider-electric (2015): *Smart City összetevői.* Forrás: https://blog.schneider-electric.com/wp-content/uploads/2015/08/Smart-Cities-Segments.jpg (Letöltés ideje: 2017. 08. 25.)

Solon, Olivia (2016): Team of Hackers Take Remote Control of Tesla Model S from 12 Miles Away. *The Guardian,* 2016. 09. 20. Forrás: www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes (Letöltés ideje: 2017. 08. 25.)

Statista (2017): *Most Famous Social Network Sites Worldwide as of September 2017, Ranked by Number of Active Users (in Millions).* Forrás: www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users (Letöltés ideje: 2017. 08. 25.)

Statista (2017b): *Forecast of Facebook User Numbers in Hungary from 2015 to 2022 (in Million Users).* Forrás: www.statista.com/statistics/568794/forecast-of-facebook-user-numbers-in-hungary (Letöltés ideje: 2017. 08. 25.)

Symantec (2016): *Destructive Disakil Malware Linked to Ukraine Power Outages Also Used against Media Organizations.* Forrás: www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations (Letöltés ideje: 2017. 08. 25.)

Szappanos, Gábor (2015): *Crooks Update their Exploits – Have You Updated Your Office?* Forrás: https://nakedsecurity.sophos.com/2015/12/18/crooks-update-their-exploits-have-you-updated-your-office (Letöltés ideje: 2017. 08. 25.)

Talyigás Judit szerk. (2000): *Tézisek az információs társadalomról.* Budapest, Miniszterelnöki Hivatal. Forrás: www.artefaktum.hu/kozgaz/tezisek.html (Letöltés ideje: 2017. 08. 25.)

Tarján M. Tamás (é. n.): *1605. november 5. Lelepleződik a „lőpor-összeesküvés" – Guy Fawkes elfogása.* Forrás: www.rubicon.hu/magyar/oldalak/1605_november_5_leleplezodik_a_lopor_osszeeskuves_guy_fawkes_elfogasa (Letöltés ideje: 2017. 08. 25.)

Tesla (2017): *Tesla Models.* Forrás: www.tesla.com/models (Letöltés ideje: 2017. 08. 25.)

TOR (2017): *Tor: Overview.* Forrás: www.torproject.org/about/overview.html.en (Letöltés ideje: 2017. 08. 25.)

Trend Micro (2016): *Operation Pawn Storm: Fast Facts and the Latest Developments.* Forrás: www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-pawn-storm-fast-facts (Letöltés ideje: 2017. 08. 25.)

Trend Micro (2017a): *2017 Midyear Security Roundup: The Cost of Compromise.* Forrás: www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup (Letöltés ideje: 2017. 08. 25.)

Trend Micro (2017b): *How Cyber Propaganda Influenced Politics in 2016.* Forrás: https://documents.trendmicro.com/assets/Appendix_how-cyber-propaganda-influenced-politics-in-2016.pdf (Letöltés ideje: 2017. 08. 25.)

Twitter (2017): *Anonymou5.* Forrás: https://twitter.com/OpHunAnon (Letöltés ideje: 2017. 08. 25.)

Ukrinform (2015): *Russian Hackers Plan Energy Subversion in Ukraine.* Forrás: www.ukrinform.net/rubric-crime/1937899-russian-hackers-plan-energy-subversion-in-ukraine.html (Letöltés ideje: 2017. 08. 25.)

UN DESA (2014a): *World Urbanization Prospects, The 2014 Revision.* Forrás: https://esa.un.org/unpd/wup (Letöltés ideje: 2017. 08. 25.)

UN DESA (2014b): *World Urbanization Prospects, Highlights.* Forrás: https://esa.un.org/unpd/wup/Publications/Files/WUP2014-Highlights.pdf (Letöltés ideje: 2017. 08. 25.)

UN DESA (2014c): *World Urbanization Prospects, The 2014 Revision. Urban Population at Mid-Year by Major Area, Region and Country, 1950–2050.* Forrás: https://esa.un.org/unpd/wup/CD-ROM/WUP2014_XLS_CD_FILES/WUP2014-F03-Urban_Population.xls (Letöltés ideje: 2017. 08. 25.)

UN DESA (2017): *World Population Prospects 2017.* Forrás: https://esa.un.org/unpd/wpp/Download/Standard/Population (Letöltés ideje: 2017. 08. 25.)

US DHS–FBI (2016): *US Department of Homeland Security and Federal Bureau of Investigation (2016): JAR-16-20296. GRIZZLY STEPPE – Russian Malicious Cyber Activity.* Forrás: www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (Letöltés ideje: 2017. 08. 25.)

US-CERT (2005): *Technical Cyber Security Alert TA05-189A: Targeted Trojan Email Attacks, July 2005.* Forrás: www.us-cert.gov/cas/techalerts/TA05-189A.html (Letöltés ideje: 2017. 08. 25.)

Valasek, Chris – Miller, Charlie (2014): *A Survey of Remote Automotive Attack Surfaces.* Forrás: www.ioactive.com/pdfs/IOActive_Remote_Attack_Surfaces.pdf (Letöltés ideje: 2017. 08. 25.)

Walz, Eric (2016): Automotive Networking: CAN-bus Topology. *Linkedin,* 2016. 07. 09. Forrás: www.linkedin.com/pulse/automotive-networking-can-bus-topology-eric-walz (Letöltés ideje: 2017. 08. 25.)

Webley, Kayla (2010): How the Nixon–Kennedy Debate Changed the World. *Time,* 2010. 09. 23. Forrás: http://content.time.com/time/nation/article/0,8599,2021078,00.html (Letöltés ideje: 2017. 08. 25.)

WikiLeaks (2014): *Vault 7: CIA Hacking Tools Revealed*. Forrás: https://wikileaks.org/ciav7p1/cms/page_13763790.html (Letöltés ideje: 2017. 08. 25.)

WikiLeaks (2015): *What is WikiLeaks.* Forrás: https://wikileaks.org/What-is-Wikileaks.html (Letöltés ideje: 2017. 08. 25.)

A Dialóg Campus Kiadó
a Nemzeti Közszolgálati Egyetem könyvkiadója.

Nordex Nonprofit Kft. – Dialóg Campus Kiadó • www.dialogcampus.hu
www.uni-nke.hu • 1083 Budapest, Ludovika tér 2. • Telefon: (30) 426 6116
E-mail: kiado@uni-nke.hu • A kiadásért felel: Petró Ildikó ügyvezető
Felelős szerkesztő: Kilián Zsolt • Olvasószerkesztő: Tar Krisztina
Korrektor: Bíró Csilla • Tördelőszerkesztő: Fehér Angéla
Nyomdai kivitelezés: Pátria Nyomda Zrt.
Felelős vezető: Simon László vezérigazgató

ISBN 978-615-5889-63-9 (nyomtatott)
ISBN 978-615-5889-64-6 (elektronikus)

A kibertér és benne az internet nemcsak a mindennapjaink részévé váltak, hanem óhatatlanul át is alakították a 21. század emberének életét. Megváltoztak a kommunikációs szokásaink, a gazdasági folyamatok, de még a politika és a kultúra sem képzelhető el a kibertér és az abban alkalmazott számítógépek nélkül. Ez komoly függőséget is jelent, hiszen addig, amíg néhány évtizede még csak néhány kiváltságos tudós élvezhette az akkor még csak a tudományos eredmények megosztására szolgáló hálózatokat, addig ma már Földünk népességének közel fele rendszeresen használja a kiberteret és annak valamely szolgáltatását. Így a kibertér biztonsága elengedhetetlen és megkerülhetetlen. A könyv ennek a biztonságnak a különböző kérdéseit járja körül átfogó módon, kezdve a kibertér szerepének bemutatásával, folytatva az abban megjelenő veszélyek és azok hatásainak elemzésével, egészen azoknak a megoldásoknak a felvillantásáig, amelyekkel a kibertér biztonságossá tehető.

A kiadvány
a KÖFOP-2.1.2-VEKOP-15-2016-00001
„A jó kormányzást megalapozó
közszolgálat-fejlesztés" című projekt
keretében került kiadásra.

Dialóg Campus

SZÉCHENYI 2020

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE