Dr. Krasznay Csaba

KIBERBIZTONSÁG A XX!. SZÁZADBAN

DR. KRASZNAY CSABA

KIBERBIZTONSÁG A XXI. SZÁZADBAN

Budapest, 2022.

Szerző:
Dr. Krasznay Csaba

Lektor:
Dr. Kassai Károly ezredes
Dr. Páll Orosz Piroska alezredes

Olvasószerkesztő:
Dr. Lángné Petruska Szidónia, Dr. Kenedli Tamás

Tördelőszerkesztő: Szabó Beatrix

A borító tervezője:
Perényi Attila

Felelős kiadó: Dr. Béres János altábornagy, főigazgató
Katonai Nemzetbiztonsági Szolgálat

A kiadó képviselője: Dr. Kenedli Tamás ezredes
Katonai Nemzetbiztonsági Szolgálat
Tudományos Tanács titkár

A kiadvány a Katonai Nemzetbiztonsági Szolgálat
Költségvetési Kutatóhely támogatásával készült.

A gyűjteményes műben megjelenő szolgálati művek tekintetében a Nemzeti Közszolgálati Egyetem (1083 Budapest, Üllői út 82.) engedélyt adott az újrakiadásra.

ISBN: 978-615-6128-11-9
ISBN: 978-615-6128-12-6 (PDF)

Nyomdai kivitelező:
Katonai Nemzetbiztonsági Szolgálat

TARTALOM

AJÁNLÓ

Tisztelt Olvasó!

Napi életünk mozzanataiba visszavonhatatlanul beépültek az elektronikus szolgáltatások. Napjainkban már az alapképzésbe integrált tudatosításra van szükség annak érdekében, hogy érthetőbb legyen az elektronikus információs környezet, az ezzel kapcsolatos egyéni, közösségi vagy társadalmi szintű hatások.

Egyre nehezebb felismerni az elektronikus szolgáltatásokat. A mobiltelefon szolgáltatások, az internet hozzáférés lassan alapszolgáltatásnak tekinthető életünkben. Ugyanakkor az egyszerű halandó számára nem érzékelhető, hogy a napi élet szolgáltatásai egyre jobban ráépülnek az elektronikus információs szolgáltatásokra.

Néha előfordul, hogy nem lehet kártyával fizetni a boltban, nem lehet pénzt felvenni az automatából karbantartás (vagy egyéb okok miatt), nincs internet, vagy egyéb formában nem áll rendelkezésre egy-egy megszokott szolgáltatás. Mindez rávilágít arra, hogy az elektronikus információs szolgáltatások által biztosított számtalan előny mellett rengeteg fenyegetés veszélyezteti a napi élet biztonságát, vagy a társadalmi vagy állami szempontból fontos szolgáltatásokat.

Példák részletezése nélkül is ismert, hogy nemzeti szinten is blokkolhatók - gátolhatók elektronikus szolgáltatások, országrészek borulhatnak sötétségbe, nemzeti egészségügyi rendszerek állíthatók le, regionális üzemanyagellátó rendszerek működése akadályozható, esetleg nukleáris létesítmény működése válik lehetetlenné a kibertéren keresztül történő kártékony beavatkozás eredményeképpen.

A kibertér biztonságával kapcsolatos kérdések vizsgálata napjainkban már nem tekinthető újdonságnak. Ezzel együtt az is megállapítható, hogy az egyre szélesebb körű nemzeti vagy nemzetközi vizsgálatok, publikációk nem egységes szempontrendszer vagy módszertan szerint világítják meg a kibertéri történéseket.

Az egységes, strukturált, teljes képet biztosító nemzetközi megközelítés vélhetően még jó ideig várat magára. Ennek ismeretében szükség van a kibertér nemzeti, nemzetbiztonsági, katonai vagy ágazati, esetleg egy-egy technikai vagy eljárási szempontú vizsgálatára.

Az apró lépések segíthetnek egy későbbi, nagyobb léptékű cél megvalósításában, illetve segítenek megérteni a fenyegetések stratégiai jelentőségét, az ellátási lánc biztonságot, vagy a függőség által kialakuló hiányosságokat.

A fenti gondolatok után érthető a Katonai Nemzetbiztonsági Szolgálat Tudományos Tanácsának törekvése a tudományos szempontból értékelhető, publikálható ismeretek menedzselésére. Ez a törekvés azonban nem keverhető össze a szerző bevezető gondolataival, vagy az egyes témák kifejtésére irányuló erőfeszítéseivel.

E ponton átadható a téma tárgyalása a Szerzőnek azzal az Olvasóknak címzett gondolattal, hogy a kibertér és a kibertér biztonság kérdéseinek összes problémáját ez a publikáció nem oldja meg. Ugyanakkor garantáltan hozzájárul ahhoz, hogy néhány területen olyan feldolgozott információkat biztosítson, melyek összegyűjtése sokkal bonyolultabb feladat, mint e publikáció élvezetes tanulmányozása.

A Katonai Nemzetbiztonsági Szolgálat Költségvetési Kutatóhely Tudományos Tanácsa ezennel kellemes kirándulást kíván a Tisztelt Olvasóknak a kibertér sejtelmes, specifikus szegmenseibe.

Budapest, 2022. november 28.

Dr. Béres János altábornagy
főigazgató

BEVEZETÉS

Kiberbiztonság. Egy olyan szó, ami lassan mindenkinek jelent valamit, mivel életünk egy jelentős része direkt módon a kibertérben zajlik. Jellemzően a közösségi hálózatokon, ahol egyre többen szereznek személyes tapasztalatot a kiberbűnözéssel kapcsolatban, igényelve azt, hogy a szolgáltató, az állam, vagy bárki más nyújtson megfelelő védelmet. Egy olyan szó, ami a politikusok szótárába is bekerült, hiszen társadalmunk, gazdaságunk, kritikus infrastruktúráink biztonságos működése nem biztosítható az azokat irányító számítógépes rendszerek megfelelő védelme nélkül. Végül egy olyan szó, ami az orosz–ukrán háború során mindennap elhangzik a médiában, figyelmeztetve a közvéleményt arra, hogy a kibertér műveleti tér, ahol valódi háború zajlik.

Az ember ritkán veszi észre, hogy történelmi időket él át, a 2000-es évek első néhány évtizedét viszont utódaink egészen biztosan az emberiség sorsfordító időszakai közé fogják sorolni. Ennek oka pedig elsősorban a digitalizáció, a gyors, nem helyhez kötött mobilhálózatok elterjedése, az okoseszközök (más néven a Dolgok Internete) megjelenése, a mesterséges intelligencia és az ezt lehetővé tevő nagy mennyiségű digitális adat rendelkezésre állása, valamint az automatizálás, az autonóm megoldások kialakulása. Mindezt nemes egyszerűséggel csak negyedik ipari forradalomnak nevezzük. Történelmi ismereteinkből pedig tudjuk, hogy minden ipari forradalom törvényszerűen átalakítja a társadalmat is. Ezt az átalakuló társadalmat először információs társadalomnak nevezték a tudósok, de valójában az ember maga is egy evolúciós ugrásban van.

De mi jöhet a homo sapiens után? A homo digitalis, amelynek agya képes a megnövekedett mennyiségű információt feldolgozni? A kiborgok, azaz a gép-ember hibridek? Esetleg a mesterséges intelligencia lesz a következő fejlődési lépcső az ember után? Ma még nem tudjuk, de az egészen biztos, hogy mind egyéni, mind társadalmi szinten új biztonsági modelleket kell kidolgozni, hiszen a homo sapiens számára a kibertéri veszélyek nem ismertek, nincsenek évtízezredes reflexei a védekezésre. A kiberbiztonság tehát egy új, egész társadalmat átható diszciplína, amely építkezhet a múltból, de egészen biztosan újszerű megoldásokkal kell dolgoznia.

Kiberbiztonsággal foglalkozó kutatóként régóta foglalkozom a negyedik ipari forradalmat kísérő kihívásokkal, fenyegetésekkel, kockázatokkal, trendekkel. A 2022. február 24-én kitört orosz–ukrán háború volt az elsődleges indokom arra, hogy korábbi írásaimat előszedjem és aktualizáljam, majd egy olyan gyűjteményes kötetet adjak ki, amely végig vezeti a Tisztelt Olvasót a kiberbiztonság fontosabb, stratégiai kérdésein. A kötetben először bemutatom azt a digitális ökoszisztémát, amelyben jelenleg élünk, kiemelve ezek kibertéri függőségeit, veszélyeit. Ezután áttekintem a digitális függőség kérdéskörét, rámutatva a nagyhatalmak elmúlt évtizedekben végrehajtott lépéseire, amelyek egyrészt hozzájárultak az információs társadalmak létrejöttéhez, másrészt viszont geopolitikai szintre emelték a kibertér uralmának kérdését. A harmadik fejezetben a hackercsoportok bevonását ismertetem a kiberhadviselésbe. Bár a választott téma túl szűknek hathat, mégis érdekes ezen keresztül megfigyelni, történelmileg hogyan váltak az internet „szabadságharcosai”, az állami elnyomás ellen küzdő civilek az egyes kormányzatok eszközeivé. Az

emberiség érdeke azonban azt kívánja, hogy a civilek védettek legyenek, a háborúkat elkerüljük, és a nagyhatalmak a diplomácia eszközével rendezzék vitáikat. Erre adna lehetőséget a kiberdiplomácia széleskörű alkalmazása, melynek kereteit és nemzetközi jogi hátterét, értelmezését a negyedik fejezet mutatja be. A negyedik ipari forradalom társadalmának biztonságát pedig a kiegyensúlyozott nemzetközi kapcsolatok mellett a kiberbiztonsági innováció eredményeképp létrejövő új termékek és szolgáltatások garantálhatnák, amelynek lehetőségeit az ötödik fejezet ismerteti. Az eredetileg megjelent szövegeket legfeljebb stilisztikai okok miatt változtattam meg, de azokat lábjegyzetekkel egészítettem ki, annak érdekében, hogy a Tisztelt Olvasó követni tudja a néhány év alatt bekövetkezett, időnként alapvető változásokat. A hatodik fejezetet ezeket kiegészítendő írtam, bemutatva 2022-es gondolataimat mindazzal kapcsolatban, ami a kibertér közeli jövőjére vonatkozik. A kutató felelőssége objektíven bemutatni múltbéli tapasztalatait, és ebből következtetni a jövőre. Bízom benne, hogy ezzel az összefoglalóval egy kicsit én is hozzá tudok járulni a biztonságosabb, élhetőbb kibertér létrehozásához.

A kötet megjelenéséért köszönettel tartozom mindenkinek, aki segítségemre volt. Dr. Muha Lajosnak, legfontosabb mentoromnak és barátomnak a szakmai jótanácsokért. Nagybátyámnak, dr. Tütő Lászlónak és Dajkó Pálnak a stilisztikai javaslatokért és a szerkesztésért. A Nemzeti Közszolgálati Egyetemnek, amely támogatta az itt feldolgozott írások eredeti megjelenését és engedélyezte azok újrakiadását, egyben lehetővé tette számomra azt, hogy kollégáimmal együtt Magyarország talán legjobb és leginspirálóbb, kiberbiztonsággal foglalkozó oktatási-kutatási környezetét hozzuk létre. A Katonai Nemzetbiztonsági Szolgálatnak és az ott dolgozó kollégáknak, akik támogatták a kötet megjelenését, lektorként, szerkesztőként és kiadóként. Végül és elsősorban köszönöm családomnak, Édesapámnak, Édesanyámnak, Feleségemnek és Gyermekeimnek, hogy mindenben támogattak. Nélkülük ez a könyv biztosan nem jelenhetett volna meg.

Budapest, 2022. október 2.

Dr. Krasznay Csaba

1. FEJEZET

OKOSESZKÖZÖK A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁKBAN[1]

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

1. BEVEZETÉS

A negyedik ipari forradalom a szemünk előtt zajlik. Ezt a fogalmat sokan Klaus Schwab nevéhez kötik, aki így foglalta össze a forradalmi változásokat:
„Mint ahogy az első ipari forradalom gőzzel működtetett gyárai, a másodiknál a tömeggyártás tudományának alkalmazása, továbbá a harmadik ipari forradalom során a digitalizáció elkezdése, addig a negyedik ipari forradalom olyan technológiái, mint a mesterséges intelligencia, a genomszerkesztés, a kiterjesztett valóság, a robotika és a 3D nyomtatás, gyorsan megváltoztatják azokat a folyamatokat és módszereket, ahogy az emberiség az értékeket létrehozza, cseréli és elosztja. Ahogy az az előző forradalmak során is történt, ez a változás is mélyen átalakítja az intézményeket, iparágakat és a magánszemélyeket is. Ennél is fontosabb azt észrevenni, hogy ezt a forradalmat az emberek ma meghozott döntései vezérlik. A világ 50–100 év múlva nagymértékben függ majd attól, hogy hogyan gondolkodunk ma ezekről a befektetésekről, és hogyan vezetjük be ezeket a nagy teljesítményű új technológiákat." [2]

Nagy Judit tanulmányában részletesen áttekintette a negyedik ipari forradalomra vonatkozó fogalmakat és így szintetizálta az egyes szerzők véleményét:
„A negyedik ipari forradalom alapja a digitalizáció és az adat, a számítógép csupán eszköz. Az internet és a technológia fejlődése megteremti az emberek, gépek és vállalatok folyamatos összeköttetésben lévő hálózatát, és az értékteremtő folyamatok adatainak folyamatos megosztásával elérhetővé válik a versenyképes, a vevő számára teljesen testreszabott termék előállítása. A versenyelőny forrása tehát nem csupán az összehangolt, vagy éppen teljesen új alapokra helyezett termelés (pl.

[1] Eredetileg megjelent: TÖRÖK, Bernát (szerk.): Információ- és kiberbiztonság: Fenntartható biztonság és társadalmi környezet tanulmányok V. Ludovika Egyetemi Kiadó, Budapest, 2020. pp. 121-147.

[2] SCHWAB, Klaus: The Fourth Industrial Revolution, Britannica, 2021. március 23. https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734

additív termelés) lesz, hanem a termékek digitális szolgáltatásokkal való körbeágyazása, valamint, hogy melyik vállalat hogyan válogatja ki a keletkező adatokból a releváns információt a döntéshozatal támogatásához"[3]

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

Ez az évtized kitermelt számos olyan okoseszközt is, amelyeknek a létjogosultságát sem feltétlenül értik azok, akik nem ebben a világban nőttek fel. Példaként lehetne kiemelni az okos vizes palackot, amelynek célja nem más, mint hogy ezt az eszközt összekötve az okostelefonnal és a fitneszkarkötővel, jelezze, hogy nem ittunk eleget, és figyelmeztessen minket az ivás fontosságára. Mivel a vízfogyasztás az ember alapvető biológiai szükséglete, felmerül a kérdés, hogy vajon mi indokolja egy ilyen eszköz létrehozását? Különös tekintettel arra, hogy nemcsak egy megoldás van jelen, hanem számos gyártó dobott piacra olyan terméket, amely ezt az igényt fedi le, ami azt is jelenti, hogy a fogyasztóknak feltehetőleg ténylegesen szüksége van ilyen eszközökre.[4]

2. A HÁLÓZATI TÁRSADALMAK

A választ a generációs különbségekben kell keresni. Jelen pillanatban hat különböző generáció él egymás mellett, és ez a hat különböző generáció különböző módon alkalmazkodott a technológiához, különböző módon élte meg az elmúlt 100 év technológiai fejlődését.[5]

- Az első generáció az *Építők generációja* (1946 előtt születettek), ahogy az amerikai terminológiában hívják, akik a második világháború után újjáépítették a világot, és kialakították azt a fogyasztói társadalmat, amelyet ma is ismerünk. A számítógépek ennek a generációnak köszönhetők.
- Utánuk következtek a *Baby Boomerek* (1946–1964 között születettek), akiket Magyarországon a Ratkó-gyerekeknek ismerünk. Az ő életükben változott át a gazdaság, az ipar számítógépesítetté, az ő idejük alatt jelent meg az első hálózatba kötött eszköz, a ma ismert internet elődje. Az ő idejükre tehető a harmadik ipari forradalom.
- Az *X generáció* (1965–1979 közöttiek), más néven a digitális bevándorlók világa hozta el az otthoni számítógépek korszakát, illetve az internetet olyan formában, ahogy azt ma ismerjük. Mivel fiatalkorukban érte őket a kétpólusú

[3] NAGY Judit: Az Ipar 4.0 fogalma és kritikus kérdései – vállalati interjúk alapján. Vezetéstudomány, 2019/1. DOI: 10.14267/VEZTUD.2019.01.02

[4] BONDOR, Mark: The best smart water bottles of 2020. MBReviews, 2020. április 14. https://www.mbreviews.com/best-smart-water-bottle/

[5] HOWE, Neil – STRAUSS, William: The next 20 years: how customer and workforce attitudes will evolve. Harvard Business Review, 2007/7-8. pp. 41-52.

világrend összeomlása, a globalizáció megjelenése, egyrészt érdeklődésből, másrészt munkahelyi kényszerből is elkezdték használni az informatikai eszközöket, amelyeket sokkal könnyebben tanultak meg, mint az előttük levő generációk.

- Az *Y generáció*, az 1980 és 1994 közöttiek generációja az, amely már ösztönszinten használta az informatikai vívmányokat. Az ő idejükben jelent meg például a Google vagy a Facebook, vált tömegessé a mobiltelefonok használata. Ők azok, akik fiatalkorukban tapasztalták meg először a kibertér árnyoldalait.
- Utánuk következett a *Z generáció*, az 1995 és 2009 között születetteké, akiket már digitális bennszülötteknek lehet nevezni. Életükben a kezdetektől jelen van az internet és a különböző digitális technológiák használata, így ők, a következő évtizedek dolgozói azok, akik a negyedik ipari forradalomhoz a legjobban tudnak alkalmazkodni.
- Végül az *Alfa generáció* tagjairól kell megemlékezni, a 2010 után született gyerekekről, akiknek a digitális élete már születésük előtt 6-8 hónappal elkezdődött, amikor édesanyjuk a közösségi hálózaton bejelentette, hogy a gyerek majd egyszer meg fog születni. Ők azok, akik már a tévét is megpróbálják úgy húzkodni, mint az okostelefonokat, hiszen azt látták, hogy a képernyő reagál arra, amit ők tesznek, és ők azok, akiknek az életéhez elválaszthatatlanul hozzátartoznak a digitális eszközök.

Látható tehát, hogy ahogy a generációkban haladunk előre, úgy a digitális technológiákhoz való hozzáállás is jelentős mértékben megváltozik, amely kikényszeríti azt, hogy a szolgáltatók is alkalmazkodjanak ügyfeleikhez. Ennek a következménye, hogy kialakult az úgynevezett hálózati társadalom, amelyet Manuel Castells, a fogalom megalkotója a következőképp határozott meg: *„egy olyan társadalom, amelynek társadalmi struktúráját a mikroelektronikai alapú információs és kommunikációs technológiák által táplált hálózatok alkotják”*.[6]

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

Nem véletlen, hogy a digitáliseszköz-használók a hagyományos értelemben vett okoseszközök használata mellett egyre inkább felokosítják a környezetüket is, azaz kialakulnak az okosotthonok, amelyek száma körülbelül 150 millióra tehető jelenleg világszerte. Ez a szám azonban hónapról hónapra növekszik, egyre többen döntenek úgy, hogy az otthonaikat is különböző okoseszközökkel látják el, ezzel

[6] CASTELLS, Manuel: Informationalism, Networks, and the Network Society: a Theoretical Blueprint. In: CASTELLS, Manuel (Ed.): The Network Society: A Cross-cultural Perspective. Edward Elgar UK, Cheltenham, 2004. pp. 3-45.

növelve a Dolgok Internetének méretét. Az okosotthonok létrehozása körülbelül 70 milliárd dolláros iparág.[78]

Természetesen az okosotthonok mellett az okosotthont kiszolgáló infrastruktúra megteremtése is egy fontos feladat. Az okosotthonok egyik legfontosabb építőköve az okos asszisztens, amelyből a legismertebbek közé tartozik az Amazon Echo, az Apple HomePod vagy a Google Home megoldása. Ezek olyan eszközök, amelyek az okosotthon középpontjaként a felhasználótól kapott szóbeli parancs vagy előre beállított feladat alapján irányítják, hogy mit csináljon az okosotthon, koordinálva a különböző okosotthon-felszereléseket. Az okoseszközök száma egyébként robbanásszerűen növekszik. 2017 és 2030 között a jóslatok szerint 27 milliárd eszközről várhatóan 125 milliárd eszközre fog növekedni a számuk.[9]

Feltehetőleg azonban ezek az adatok ma már el is avultak, hiszen napról napra újabb és újabb forradalmi megoldások jelennek meg. Az olyan társadalmat megrázó események, mint például a koronavírus-járvány például elősegítik az okoseszközök számának a növekedését, hiszen akár a gyógyászatban, akár a fertőzöttek követésében is elengedhetetlenül fontosak az embereket szolgáló és információkat szolgáltató eszközök. Így nem meglepő, hogy Kínában a koronavírus-járvány legyűrésében vitathatatlanul fontos szerepet játszottak a különböző okoseszközök is, illetve, hogy iparági elemzők az okos asszisztensek számának jelentős növekedését várják a járvány „mellékhatásaként".[10] Mindez európai szemmel komoly adatvédelmi és információbiztonsági kérdéseket vet fel, tekintettel arra, hogy az ilyen megoldások óhatatlanul sértik a személyek magánszféráját.

3. AZ IOT INFORMÁCIÓBIZTONSÁGI KIHÍVÁSAI

Az információbiztonság szempontjából tehát a kihívás adott. Egyre több hálózatba kapcsolt eszközt, egyre több okoseszközt látunk, amelyeknek tervezési szinten történő adatvédelme és információbiztonsága finoman szólva is megkérdőjelezhető. Hiszen gondoljunk csak bele abba, hogy ma már egy egyszerű kábel is sok esetben tartalmaz néhány mikroprocesszort, melyekről nem feltétlenül tudjuk, hogy konkrétan mit csinálnak, milyen adatokat forgalmaznak, hogyan hatnak működési környezetükre. Vagy gondoljunk egy modern önvezető autóra, amelynek

---

7 KEMP, Simon: Digital 2020: 3.8 Billion People Use Social Media. WeAreSocial, 2020. január 30. https://wearesocial.com/uk/blog/2020/01/digital-2020-3-8-billion-people-use-social-media/

8 A gyűjteményes kötet összeállításának idején ezek a számok jelentősen megváltoztak. Az emberiség létszáma 7,91 milliárd, 57% él városokban. A mobilfelhasználók száma érdemben nem nőtt (5,3 milliárd, 67,1%), de a Covid miatt az internetfelhasználók (4,95 milliárd, 62,5%) és a közösségi média résztvevőinek száma (4,62 milliárd, 58,4%) jelentősen megugrott. Az okosotthonok száma 263,4 millió, a teljes iparág 104,4 milliárd dollárra becsült. Forrás: https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/

9 IHS Markit: The Internet of Things: a movement, not a market. 2017. október 17. https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

10 SHEIN, Esther: COVID-19 pandemic impact pushing smart home voice control devices to predicted 30% growth. TechRepublic, 2020. április 1. https://www.techrepublic.com/article/covid-19-pandemic-impact-pushing-smart-home-voice-control-devices-to-predicted-30-growth/

működéséhez különböző beágyazott informatikai eszközök hálózatba kapcsolása szükséges, ezek irányítása pedig szoftveren keresztül történik. Ráadásul várhatóan nemsokára megjelennek majd az egymással, illetve a különböző forgalomirányító eszközökkel is kommunikáló önvezető autók, így egyértelmű, hogy egy hálózatba kapcsolt teljes ökoszisztémáról beszélünk, amelynek, ha bármelyik eleme is sérülékeny, az mindenképpen hatással lesz a teljes ökoszisztémára is.

Azt, hogy milyen fenyegetést jelentenek a hálózatba kapcsolt eszközök, a legjobban a Mirai botnet mutatja be, amely 2016-ban pusztította végig az internetet, és azóta is jelen van. Úgy működött, hogy különböző hálózatra kapcsolt okoseszközöket fertőzött meg, tipikusan IP-kamerákat, illetve sérülékeny routereket. A megfertőzött eszközök folyamatosan szkennelték az internetet, újabb és újabb gyenge eszközöket keresve találták meg azokat a réseket, sebezhetőségeket és tervezési hibákat, mint például a beépített gyenge jelszavakat, melyeket kihasználva fel tudták telepíteni saját magukat ezekre az eszközökre, majd a távolról jövő utasításokat elfogadva hajtottak végre olyan kibertámadásokat, amelyek hatással voltak olyan globális digitális szolgáltatásokra is, mint például a legnépszerűbb videostreaming szolgáltatás. Ez mutatja, mi történhet, hogyha tömegesen tud uralma alá hajtani valaki ilyen hálózatba kapcsolt okoseszközöket.[11]

További figyelmeztető jel a 2017-ben kiszivárgott Vault 7 nevű, a Wikileaksen megjelenő szivárogtatás, amely az amerikai Central Intelligence Agency, a CIA kibertevékenységébe adott bepillantást, és mutatta meg, hogy ez a hírszerző szervezet is aktívan keresi a sebezhetőségeket olyan okoseszközökben, mint például az okostelefonok, okostelevíziók, vagy éppen az önvezető autók. Ezek a példák is alátámaszthatják azt a trendet, hogy mind a kiberbűnözés, mind pedig az államilag támogatott kiberkémkedés vagy egyéb katonai kibertér-műveletek célpontjai lehetnek az okoseszközök. A jelen és a közeljövő igazi kihívása pedig az, hogy ezek a támadások hatással vannak nem csak a hétköznapi ember okosotthonaira, hanem a létfontosságú rendszerekre is, amelyek egyre több okoseszközt használnak.[12]

4. OKOSVÁROSOK BIZTONSÁGA

Bár a hétköznapokban kevésbé látszódik, az okosotthonok mellett kialakulóban vannak az okosvárosok is. Az okosvárosok, hasonlóan az okosotthonokhoz, okoseszközök hálózatba kapcsolását valósítják meg. Céljuk azonban nem az, hogy fel tudjuk húzni a redőnyünket szóban kimondott paranccsal, hanem az olyan közművek irányítása, mint például a villamosenergetikai ellátás, a gázellátás, az egészségügy, a közbiztonság, az épületvezérlés. Sallai Gyula így foglalja össze az okosváros koncepcióját, amely létrejöttének elsődleges kiváltója a túlzott urbanizáció miatt lassan élhetetlenné váló települések fenntarthatóságának biztosítása:
„Az okos város koncepció lényege a „smartintegráció”, egy olyan platform, amelyen a különféle területek megoldásai egymást erősítő rendszerré állnak össze, és a város erőforrásait hatékonyan, koordináltan használják fel. Ennek érdekében a

[11] BEDERNA Zsolt et. al.: Támadás hálózatba szervezve. In: AUER Ádám – JOÓ Tamás (Szerk.): Hálózatok a közszolgálatban. Dialóg Campus Budapest, 2019. pp. 223-247.
[12] WikiLeaks: Vault 7: CIA Hacking Tools Revealed. WikiLeaks, 2014. október 23. https://wikileaks.org/ciav7p1/cms/page_13763790.html

város életének minden releváns információját gyűjtik, elemzik, és egy közösen használt tudásbázist hoznak létre, amelynek bázisán adatvezérelt komplex megoldások valósíthatók meg. Egy város akkor nevezhető igazán okosnak, ha az IKT[13]*-megoldások segítségével a fizikai infrastruktúrák hatékony használatát és az életminőség javítását:*

- *a különféle erőforrások és szolgáltatások együttes, integrált kezelésével,*
- *adatvezérelve, adaptívan, a körülmények tényszerű változására reagálva,*
- *környezettudatosan, fenntarthatóan, energiatakarékosan,*
- *az érintett közösség aktív részvételével, érdekeltjeinek bevonásával,*
- *gazdaságilag önfenntartó módon éri el."*

A szerző 6+1 különböző kulcsterületet azonosít, amelyek az okosváros létrehozásához feltétlenül szükségesek. Ezek az okosváros-igazgatás, az okosvárosi környezet, az okosközlekedés, az okosenergetika, az okoséletvitel, az okos infokommunikációs infrastruktúra és az okosváros kiberbiztonsága, mint horizontális kulcsterület. Jelen tanulmány három kulcsterület, az okosközlekedés, az okosenergetika és az okosvárosi környezet példáján keresztül mutatja be, hogy az okosváros kiberbiztonsága miért kiemelkedően fontos. Az okosvárosi környezet körében jelenik meg az okos vízkezelés, azaz a víziközművek is. Az okos víziközművek megjelenése azt jelenti, hogy a víz kitermelése, tisztítása, célba juttatása, illetve szétosztása is egyre inkább „okossá válik", ezzel új, korábban nem látott lehetőséget, egyben biztonsági kihívást hozva a víziközmű-szolgáltatóknak.[14]

Az okosvárosok esetében biztonsági szempontból több különböző, egymással párhuzamosan mérlegelendő aspektust kell figyelembe venni. Egy közlekedési példával lehetne mindezt a legjobban illusztrálni. Gondoljunk bele abba, mi történik, hogyha egy önvezető autóban valamilyen sebezhetőség jelenik meg, amit a támadók ki tudnak használni, ezért azonnal frissíteni kell, hiszen hogyha egy Miraihoz hasonló kártékony kód elterjedne az okosközlekedés ökoszisztémájában, akkor az autóvezetés gyakorlatilag lehetetlenné válna. Az autókban azonban, hasonlóan bármilyen más önálló vagy beágyazott elektronikus információs rendszerhez, három különböző mérlegelési szempontot kell figyelembe venni: az üzembiztonság, az elektronikus információbiztonság, illetve az adatbiztonság. Hasonló helyzet történt a Wannacry kártékony kód elterjedésénél, amikor egy félnapon belül váltak működésképtelenné olyan kritikus rendszerek, mint például Nagy-Britannia egészségügyi informatikája.

Elektronikus információbiztonsági szempontból a probléma tehát az, hogy egy súlyos informatikai sebezhetőség jelenik meg az önvezető autókban, és hogyha egy olyan féreg típusú kártékony kód automatikusan tud a hálózaton keresztül terjedni, akkor a fertőzés perceken belül, globális méretekben szét tud terjedni a sebezhető gépjárművekben. Ez adott esetben több tízmillió autót is érinthet, ilyen esetben pedig, ahogy azt a Wannacry esetében is látni lehetett, a legtöbben azonnal frissíteni akarják az ezeken futó szoftvert. Itt azonban szóba kerülnek az üzembiztonsági kérdések is, hiszen egy informatikai eszközben egy új hibajavítás előre nem látható gondokat okozhat. Éppen ezért nem lehet menet közben frissíteni ezeket a gépjárműveket, meg kell várni, amíg leállnak. Az önvezető autókban ez egy

[13] Információs és Kommunikációs Technológiák

[14] SALLAI Gyula: Az okos város koncepciója. In: SALLAI Gyula (Szerk.): Az okos város (Smart City). Dialóg Campus, Budapest, 2018. pp. 13-34.

egyszerű állapotinformáció, ami interneten lekérdezhető, meg kell tehát néznünk, hogy áll-e az autó. Csakhogy itt előjönnek azok az adatvédelmi kérdések, amelyek korábban nem jelentettek problémát, hiszen hogyha a helyi adatokból és a szenzorokból kiderül, hogy mozgásban van az autó, az azt jelenti, hogy a gyártó figyelheti is az autó konkrét közlekedési helyzetét, ami adatvédelmi szempontból problémás lehet. Azaz, a kiberbiztonság és az elektronikus információbiztonság hatással van az üzembiztonságra, az üzembiztonság hatással van az adatvédelemre, és mindhárom szempontot egyenlően kell figyelembe venni az új típusú okosváros-megoldásoknál.

Természetesen az önvezető okosautók tömeges elterjedése még nem napjaink kihívása, de észre kell venni, hogy a technológia az ablakon kopogtat. A Society of Automotive Engineers (SAE) szövetség 2014-ben adott közre egy tanulmányt, amelynek címe J3016, Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems volt. Ebben írták le az autonóm autók hat különböző szintjével kapcsolatos követelményeket, amelyet Mester Gyula ezt így foglalta össze:[15]

- 0. szint: A hagyományos autó teljes mértékben emberi irányítás alatt áll, nincs automatizáltság, a vezetési környezetet az ember figyeli.
- 1. szint: Az autó teljes mértékben emberi irányítás alatt áll, autóvezetés támogatása kormányzás vagy fékezés/gyorsulás esetében, a vezetési környezetet az ember figyeli.
- 2. szint: Az autó teljes mértékben emberi irányítás alatt áll, részleges automatizáltság, az autóvezetés-támogató rendszer a kormányzási és a fékezési/gyorsítási műveleteket egyszerre átveheti, a vezetési környezetet az ember figyeli.
- 3. szint: Feltételes automatizáltság, az autót teljes mértékben ember irányítja, az autóvezetés-támogató rendszer a kormányzási és fékezési/gyorsítási műveleteket egyszerre átveheti, a vezetési környezetet az automata rendszer figyeli.
- 4. szint: Magas szintű automatizáltság, az automata autóvezető-rendszer irányítja az összes dinamikus vezetési műveletet, a vezetési környezetet az automata rendszer figyeli.
- 5. szint: Teljes automatizáltság, az automata autóvezető-rendszer folyamatosan irányítja az összes dinamikus vezetési műveleteket, a vezetési környezetet az automata rendszer figyeli, az autó ember nélkül is közlekedhet.

2020-ban a legtöbb új autó az 1. szinten meghatározott automatizálási fokon van, de kereskedelmi forgalomban már kaphatók a 2. szintet elérő gépjárművek is. A Tesla Autopilot megoldása például erre a szintre sorolható. Az első 3. szintet is elérő gépjárművet az Audi jelentette be, A8L modelljét tekinti a követelmények teljesítőjének. A Gartner elemzőcég Hype Cycle for Emerging Technologies, 2019 jóslata szerint a 4. szint két éven belül, az 5. szint 2–5 év múlva várható.[16][17] Az

[15] MESTER Gyula: Önvezető robot autók újdonságai és biztonsági kérdései. XII. Innováció és fenntartható felszíni közlekedés konferencia, XII. IFFK, Budapest, 2018.

[16] PANETTA, Kasey: 5 Trends Appear on the Gartner Hype Cycle for Emerging Technologies, 2019. Gartner, 2019. augusztus 29.

okosvárosok autókkal kommunikáló intelligens vezérlési rendszerei pedig egyelőre csak tesztpályákon léteznek. Kijelenthető tehát, hogy ha figyelembe vesszük a gépjárművek életciklusát és az átlagos városfejlesztési sebességet, a feljebb vázolt kiberbiztonsági kihívások inkább a 2030-as, mint a 2020-as évek problémáját fogják jelenteni.

Általánosságban is kijelenthető, hogy az okosvárosok kiépítése ugyan elkezdődött, de általánossá válásukra még jó pár évet várni kell. Hiányzik ugyanis néhány olyan infrastrukturális építőkő, amely nélkül a milliónyi okoseszköz kommunikációja és az általuk szolgáltatott adatok feldolgozása, majd ezek alapján a (fél)automata döntések nem valósíthatóak meg. A „hiányzik" ebben az esetben nem azt jelenti, hogy a technológia nem létezik, hanem azt, hogy még nem terjedt el, nem állt tömegesen a városok szolgálatába. Példa erre az ötödik generációs mobiltávközlés, az 5G hálózatok, amelynek technológiája, szabványai ismertek, de a frekvenciaengedélyek kiosztására Magyarországon 2019-ben, az első kereskedelmi szolgáltatás elindítására 2020-ban került sor. A szükséges városi lefedettség kiépítése pedig éveket vesz majd igénybe, melyet az olyan összeesküvés-elméletekből származó lakossági ellenállás is hátráltathat, mint hogy az 5G hálózatok terjesztik a koronavírust.[18]

De az adatfeldolgozás területén is számos akadályozó tényezőt lehet azonosítani, amelyek megint csak nem műszaki jellegűek. Az okosváros megoldások lényege, hogy a szenzoradatokból felépített Nagy Adat (Big Data) adatbázisok szolgálnak alapul a mesterséges intelligencia által segített döntéshozatalban. A legtöbb városi önkormányzat azonban még nem áll az ehhez szükséges érettségi fokon. Jelenleg jellemzően a szakapparátus és a politikai vezetés is a Baby Boomer vagy az X generáció tagja, így a negyedik ipari forradalom vívmányait véleményem szerint nehezebben fogadják be. Legalább még egy évtized kell, amikorra megjelenik az Y és a Z generáció a magas szintű döntéshozatalban, és általánossá válik az adatalapú, mesterséges intelligencia által támogatott várostervezés és önkormányzati működés.

Mindeközben az okosvárosokat ellátó közműszolgáltatók elkezdték az átállást az okosinfrastruktúrákra, de ez sem gyors folyamat. Az ipari irányítórendszerek életciklusa évtizedekben mérhető, így nem ritka, hogy 20–30 éves informatikai megoldások támogatják a létfontosságú rendszerelemek működését. Ez alapesetben nem okoz problémát, hiszen mindhárom vizsgált területen (villamosenergetika, víz, közlekedés) az üzembiztonság jelenleg a legfontosabb, és ezt gond nélkül meg tudják valósítani ezek a rendszerek. Hatékonysági okokból viszont ezeket folyamatosan hálózatba kötik, így elektronikus információbiztonsági szempontból védhetetlenné válnak. Nem ritkák az olyan SCADA/ICS[19] rendszerek, amelyeken Windows XP vagy még régebbi, már évek óta nem támogatott operációs rendszer

https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019

17 2022-ben még mindig a Level 3 szinten tart az iparág, a Level 4 gépjárművek egyelőre tesztelési fázisban vannak.

18 2022 első felében az 5G hálózat elérhető Budapesten, a Balaton-parton és a nagyobb városokban is.

19 Supervisory Control and Data Acquisition/Industrial Control System, Felügyeleti Ellenőrzés és Adatgyűjtés/Ipari Irányítórendszer

fut, így, ha ezek bármilyen módon hálózatra kerülnek, védelmük teljesen esélytelen a kibertéri veszélyekkel szemben. Ezeket tehát cserélni kell, a gyártói kínálatban pedig ma már az okosmegoldások dominálnak, érthető módon a Dolgok Internetének halmazába tartozó megoldásokat szeretnének a közműszolgáltatóknak értékesíteni. Ezek üzembiztonsági szempontból megfelelőek, az elektronikus információbiztonságot is jobban megvalósítják, mint régebbi társaik, ám egyrészt az adatvédelem továbbra sem szempont, illetve még évekig egy hálózatban fognak működni a hagyományos SCADA/ICS megoldásokkal, így az üzemeltetőknek egy hibrid infrastruktúra védelmére kell felkészülni. Tekintettel arra, hogy az ipari irányítórendszerek üzemeltetése jellemzően villamosmérnöki feladat üzembiztonsági fókusszal, itt is meg kell jelennie azoknak a mérnököknek, akik szélesebb látókörrel, elektronikus információbiztonsági szemléletmóddal is rendelkeznek. E szemléletmódváltás és az új üzemmérnök-generáció megjelenése is éveket fog igénybe venni, így a létfontosságú közművi információs rendszerek még jó darabig alacsonyabb védelmi szinten fognak működni, mint ahogy azt a kibertéri veszélyek indokolttá tennék.

5. KIBERBIZTONSÁG AZ OKOS VÍZIKÖZMŰVEKNÉL

Ma már tehát egyetlen ipari irányítástechnikai rendszerrel foglalkozó mérnök számára sem lehet kérdés, hogy az üzemeltetett infrastruktúra esetén nem csak az üzembiztonság, hanem az elektronikus információbiztonság, tágabban véve a kiberbiztonság is olyan szempont, amit figyelembe kell venni. Nehéz viszont felmérni, hogy valójában mekkora a fenyegetettség az olyan kritikus infrastruktúrák, mint például a víziközművek esetén. A következőkben ismertetésre kerülnek azok a kihívások, amelyek mind a klasszikus SCADA/ICS-rendszerekre, mind pedig az új típusú okosinfrastruktúrákra vonatkoznak, kiemelve mind a biztonságpolitikai, mind pedig a műszaki jellegű kihívásokat.

Orbók az okosvárosok biztonsági kihívásait így foglalja össze:
„A kibertér biztonsági kockázatainak befolyása a fizikai világra jelentősen megnövekszik, így közvetlenül hatással lesznek majd a személyes biztonságunk és a közösség biztonságának minden területére, függőségünk és a kiszolgáltatottságunk jelentősen megnő.”[20]

Ennek a kiszolgáltatottságnak a mértékét azonban egyelőre csak sejtjük, a bizonyosságot a következő évtizedek fogják elhozni. Az amerikai U.S. Department of Homeland Security The Future of Smart Cities: Cyber-Physical Infrastructure Risk című tanulmánya azonban megpróbálja előrejelezni, hogy mi vár a legfontosabb közművek üzemeltetőire a digitális átalakulás folyományaként. A kiadvány a közlekedés, az energiaellátás és a víziközművek területén mutatja be azt, hogy milyen kockázatokkal fognak szembesülni ezek az alapvető infrastruktúrák.

A víziközművek területén az okos vízkezelésben két példát hoz a tanulmány a kibertámadásra. Az egyik lehetőség, hogy kibertámadás éri a vízkezelő központot, és ezen keresztül olyan hatást érnek el a támadók, amely hathat a közegészségügyre. A másik példa az, hogy az információs rendszereken keresztül a támadó tönkreteszi

[20] ORBÓK Ákos: Az okos város kiberbiztonsága. In: SALLAI Gyula (Szerk.): Az okos város (Smart City). Dialóg Campus, Budapest, 2018. pp. 187-202.

a vízbázist, és ezzel okoz környezeti katasztrófát. A következő ilyen példa az okos vízelosztásnál jelentkezik. Az első az, hogy egy rosszindulatú támadó távolról behatol a rendszerbe, és lekapcsolja az érzékelő szenzorokat, így szennyezett víz kerül a háztartásokba, a másik példa pedig az, hogy a támadó rendkívüli időjárási helyzetben teszi lehetetlenné a felgyűlt csapadékvíz elvezetését. Az okos víztárolásnál a példatámadások úgy szólnak, hogy egy rosszindulatú támadó távolról manipulálja a víztárolók berendezéseit, ezzel áradást okoz, illetve egy rosszindulatú támadó az internetről behatolva zavarja meg a biztonsági berendezéseket, ezzel fedve el a potenciális vészhelyzetet.[21]

Mindegyik példa nagyon jól mutatja, hogy milyen problémákat tud okozni az okoseszköz a víziközművekben. De ha stratégiai szinten vizsgáljuk a közeljövőt, akkor célszerű kitérni az államilag szervezett kibertámadásokra is. E kihívások közül is érdemes figyelembe venni azt, hogy a negyedik ipari forradalommal párhuzamosan számos olyan, korábban nem látott lehetőség nyílik a nagy befolyással rendelkező, elsősorban gyártó államok számára a kibertéri befolyásolásra, amelyekre sem a víziközműveknél, sem általában a kritikus infrastruktúrák esetében sem vagyunk felkészülve. Gondoljunk itt például az ötödik generációs mobilhálózatok kérdéskörére, amelyben a kínai gyártókkal szembeni kérdések és kétségek elsősorban azért merülnek föl, mert az okosvárosok, így az okosközművek kommunikációját ezeken az ötödik generációs mobilhálózatokon keresztül lehet a legideálisabban megoldani. Márpedig hogyha egy államnak lehetősége van az állam területén belül működő gyártókon keresztül hatni az okosváros-infrastruktúrákra, akkor nyilvánvalóan ez egy előre nem látott nemzetbiztonsági kihívást jelenthet majd

Emellett a gyártók is okozhatnak nem várt elektronikus információbiztonsági problémákat. Példaképp lehet említeni azt, hogy a korábban említett okosasszisztensek mindegyikéről kiderült az, hogy a gyártó nem az információbiztonság és az adatvédelem alapvető eljárásai szerint működik, hiszen az okosasszisztenseknek mondott parancsok több gyártó esetében is megismerhetővé váltak valós személyek számára. Állítólagos minőségbiztosítási okokból ugyanis a gyártók munkatársai hallgatták végig azt, hogy mi minden történik a háztartásokon belül, így a gyártók korábbi ígérete, miszerint csak a mesterséges intelligencia dolgozza föl a hangot, több esetben bizonyítottan nem teljesült. Gondoljunk csak bele, milyen kihívást jelenthet az, hogy ha az okosvárost felépítő alapinfrastruktúrákban is ilyen tervezési hibák vannak, akár szándékosan, akár nem szándékosan, amellyel a gyártó is hathat az okos infrastruktúra működésére! Gondoljuk csak végig, milyen kockázatot jelentene az, ha az okosvárost építő infrastruktúraelemek mögött egy rosszindulatú országot vagy egy rosszindulatú gyártó állna![22]

---

[21] Office of Cyber and Infrastructure Analysis: The Future of Smart Cities: Cyber-Physical Infrastructure Risk. 2015. augusztus https://www.cisa.gov/uscert/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf

[22] A Solarwinds támadás világosan megmutatta, milyen kockázatot rejt magában az, ha a gyártón keresztül támadják meg a célpontot. Ebben az esetben orosz támadók helyeztek el hátsókaput a Solarwinds Orion szoftverben, amelyet frissítésen keresztül terítettek több

6. KIBERBIZTONSÁG AZ OKOS VILLAMOSENERGETIKÁBAN

Az energiatermelés, -átvitel, -elosztás és -fogyasztás forradalmi változása mutatja meg talán legjobban az okoseszközök helyét ebben a közműszektorban. A világ energiafelhasználása évről évre kétségtelenül egyre nagyobb, miközben az energiatermelés módszereinek mindenképpen változnia kell, hiszen a klímaváltozás kikényszeríti a szénhidrogén alapú energiatermelés visszaszorítását. Mindez elősegíti a kisebb, megújuló energiatermelő rendszerek előretörését, például a szélerőművek, napenergiafarmok megépítését. Ezek azonban, jellegüknél fogva, akkor termelnek, amikor fúj a szél és süt a nap. Sajnálatos módon Európa középső részén a téli időszakban, amikor a legnagyobb az energiafogyasztás, jellemzően nem süt a nap és szélcsend van, így a nem megújuló forrásokra épülő erőművek még addig velünk fognak élni, ameddig a nagy volumenű energiatárolás meg nem valósul. A „régi" és az „új" megoldásoknak tehát együtt kell működniük, egyszerre kell a létrehozott energiát úgy irányítani, hogy néhány jól tervezhetően működő alaperőmű és sok tízezer, környezeti hatásoktól függő kis energiatermelő megbízhatóan 230 V és 50 Hz feszültséget adjon a háztartási aljzatokban. Ez összehangolt informatikai háttér nélkül nem lenne lehetséges.

Mindeközben a felhasználói oldal energiafogyasztása is változik. Ma már nem a nagy fogyasztású hűtőszekrény kiszámítható, egész napos fogyasztása a meghatározó, hanem az éjszakára a töltőkre tett okoseszközöké, amelyekbe a legnagyobb fogyasztók, mint az elektromos autók is beleértendők. Az okoseszközök hatását jól lehet mérni azzal, hogy a koronavírus miatti otthoni munkavégzés és a távolléti oktatás alatt az energiafogyasztás szerkezete érdemben változott meg. A MAVIR[23] adatai alapján az Energiaklub kimutatta, hogy jelentősen kevesebb energiát fogyasztottak a kijárási korlátozás első két hetében Magyarországon (6000–6200 MW helyett 5700–5800 MW-ot), illetve az is kimutatható, hogy a korábban reggel 8 óra körül jelentkező első napi terhelési csúcsok dél körülre tolódtak el, és többször meghaladták a korábban rendre magasabb, este 7 óra körül mutatkozó második napi terhelési csúcsokat. Mindeközben 2020. április 16-án termelési csúcsot sikerült elérni a napenergia-termelés területén, aznap 942,8 MW-ot mértek, melyből a háztartási kiserőművek akár 30-40%-kal is részesülhettek, hiszen ezek együttes teljesítménye 460,77 MW volt ebben az időszakban a közlés szerint.[24,25]

A változó termelés és fogyasztás kezelésének a megoldása az okoshálózatokban, azaz smart gridekben rejlik. Definíció szerint: *„A smart grid (SG) elképzelés kiindulópontja az, hogy az intelligens, oda-vissza vezérelt és ellenőrzött fogyasztás decentralizált erőművi mikrorendszereket képes integrálni. A smart grid technikával a jelenlegi hálózati túlterheltség, a nagy hálózati veszteség és az erőművek rugalmatlansága részben orvosolható, növelhető továbbá az*

ezer felhasználó felé. 2021-ben ezért az ellátási láncok támadását (supply chain attack) tartották az egyik legkomolyabb kiberbiztonsági fenyegetésnek.

23 Magyar Villamosenergia-ipari Rendszerirányító

24 MAVIR: Újabb rekordok születhetnek a folyamatos napos időben. 2020. április 16. https://www.mavir.hu/web/mavir/kozlemenyek/-/asset_publisher/FPi3DcWJuTiD/content/ujabb-rekordok-szulethetnek-a-folyamatos-napos-idoben

25 Ez a csúcs azóta folyamatosan emelkedik, 2022 márciusában éppen 1725 MW a napi csúcs, de ez nyilván tovább fog nőni.

energiahatékonyság, illetve a megújulók integrációja [lehetővé válik]. (...) A harmadik lépésben kezdődik el a valódi smart grid kiépítése, miközben a már megszokott rendszer öregszik. A hatásfokok romlanak, a veszteségek emelkednek. Az új struktúrában már lehetőség lesz kisebb erőművi termelők lokális hálózatra kapcsolására. Fontos kiemelni, hogy a smart grid, amely lényegét tekintve egy irányítási technika, a hagyományos hálózatra építve képzelhető el, és nem izolációs célként"[26]

Az okoseszközök megjelenésének első példája a háztartási villamosenergetikában az okosmérő, azaz a smart meter. Ez Haddad Richárd összefoglalója szerint azt jelenti, hogy: *„Az okos mérési rendszerek lehetőséget adnak arra, hogy a szolgáltatók és a hálózatüzemeltetők a végfogyasztókra lebontva képesek egyedi adatszolgáltatásra. Ennek az egyik legfontosabb előnye, hogy a fogyasztók az elfogyasztott energiával, valamint a hálózatban lévő energia költségével arányosan fizetik meg a felhasznált energiát. Mint ismeretes, a különböző napszakokban más és más energiaforrások (különböző költségen termelő egységek) érhetők el. Az okos mérési rendszerek transzparenssé tudják tenni a felhasználás és a költség mértékét."*[27]

A smart metering eszközök valójában hálózatra kapcsolt informatikai megoldások, azaz a Dolgok Internetének részei. Elsődleges funkciójuk, hogy a fogyasztási adatokat elküldjék a szolgáltatóknak. Azonban logikus lépés lenne, hogy ne csak a szolgáltató, hanem a fogyasztó is percre pontosan értesüljön az aktuális fogyasztásáról, hiszen ezen adatok alapján ő is optimalizálni tudja otthona energiafelhasználását. Ha tehát a smart metering megoldás felkerül az otthoni vezetéknélküli hálózatra, és az adatokat az okosasszisztens számára is rendelkezésre bocsájtja, az az előre meghatározott fogyasztási szabályok alapján tudja ki- és bekapcsolni az okosotthon eszközeit. További lépés lenne, ha ezek az adatok az otthont segítő mesterséges intelligencia számára is elérhetővé válnának, így a szabályokon túlmenően még rugalmasabb, jobb döntéseket tudna hozni az okosotthon, jelentős energiamegtakarítást lehetővé téve. Ez az úgynevezett „edge AI", azaz a „peremhálózaton", az otthonokban levő eszközökön megjelenő mesterséges intelligencia is 2–5 éven belül valósággá válik a Gartner már idézett elemzése szerint.[28] Az okosközmű és az okosotthon tehát összeér, az elektronikus információbiztonság és főleg az adatvédelem emiatt elkerülhetetlenné válik a szolgáltatói oldalon, hiszen, ha nem terveznek megfelelően, nem csak saját létfontosságú rendszereik, de felhasználóik is veszélybe kerülhetnek.

---

[26] BARANYA Gábor – CSERNUS Ildikó (Szerk.): A fenntartható fejlődés és az állam feladatai. Dialóg Campus, Budapest, 2018.

[27] HADDAD Richárd: Okoseszközök a kritikus információs infrastruktúrákban, villamosenergetikai fókusszal. In: DEÁK Veronika (Szerk.): Kritikus információs infrastruktúrák védelme – Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyszámára – 2019. Nemzeti Közszolgálati Egyetem, Budapest, 2019. pp. 72-113.

[28] Elég csak arra gondolni, hogy 2022-ben például az Apple M1 chipjeiben komoly mesterséges intelligenciát támogató képességek vannak, amelyek lehetővé teszik az edge AI megjelenését a hétköznapokban.

A U. S. Department of Homeland Security okosváros-biztonsággal foglalkozó tanulmányában jól nyomon követhető, hogy mely pontok lehetnek sérülékenyek az okos villamosenergetikában. Az első ilyen felület az okoserőművek körében fedezhető fel. A kutatók három példát említenek. Az első szerint a támadó hozzáférést szerez a SCADA/ICS-rendszerhez azok nem megfelelő hálózati szegmentációja miatt. A második példát az élet számos esetben igazolta, és a későbbiekben vissza fogunk rá térni. Eszerint a támadó jogosulatlan hozzáférést szerez az erőmű hagyományos IT-rendszereihez. A harmadik példa pedig a már említett „régi" és „új" rendszerek nem megfelelő együttműködését említi, amelyek komoly rendelkezésre állási és sértetlenségi hiányosságokhoz vezethetnek. Az okos elosztás és átvitel a smart grid problémakörét mutatja be. A két példa szerint egy rosszindulatú támadó kompromittálja az átviteli rendszert, ezzel megfosztva a felhasználókat az áramellátástól, azaz klasszikus rendelkezésre állási problémát okoz. A másik forgatókönyv szerint egy rosszindulatú támadó manipulálja az energiaárakat mutató adatokat, emiatt a rendszer inkonzisztens módon irányítja a megtermelt energiát, felhívva ezzel a figyelmet arra, hogy az energiatermelésben nem néhány szereplő van csak, mint korábban, hanem a háztartások tömegei is eladnak áramot az országos hálózatba az általuk megtermelt, de nem felhasznált napenergia segítségével. A kutatók az okos mérőhelyek támadásaival is foglalkoztak. Elképzelésük szerint az ellenük irányuló támadással a háztartások áram nélkül maradnak, illetve sikeres támadás esetén a támadó akár a háztartások belső informatikai hálózatába is be tud jutni.

7. AZ OKOSKÖZLEKEDÉS KIBERBIZTONSÁGI SZEMPONTJAI

Az okosközlekedés kialakítása talán a legégetőbb a három, mintaként kiválasztott terület közül. A nagyvárosok közlekedése – ami a városi légszennyezés elsődleges forrása is – ugyanis már ma is a legtöbb helyen élhetetlen helyzetet teremt, ezzel a városlakók fizikai egészsége mellett a mentális jólétüket is veszélyezteti. Az önvezető autók mellett számos más innovatív megoldás is segíti az okosközlekedés kialakítását, például az autómegosztó szolgáltatások, vagy éppen a közlekedési viszonyokat másodperces pontossággal figyelő navigációs applikációk. Mindezt az ökoszisztémát együttesen Intelligens Közlekedési Rendszernek (Intelligent Transport System – ITS) nevezik, amely kialakításának fontosságát mi sem jelzi jobban, hogy az Európai Unió külön irányelvben szorgalmazta azt már 2010-ben. Lásd: az Európai Parlament és a Tanács 2010/40/EU irányelve (2010. július 7.) az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről.

Bódi Antal összefoglalója szerint: *„Az intelligens közlekedési rendszerek nagyvárosi alkalmazásának operatív célja a várost érintő hazai, adott esetben nemzetközi tranzitforgalom, a nagyvárosi agglomerációs forgalom és a városon belüli forgalom egyenletesebb, kevesebb zavarral járó és kontrollált, ezáltal biztonságosabb és kevesebb környezeti terheléssel járó lebonyolítása. Ezzel párhuzamos távlati, stratégiai célja pedig a közlekedők környezetkímélőbb közlekedési módok használatára való ösztönzése, az új közlekedési formákra való*

váltás kedvező feltételeinek megteremtésével, illetve ezen közlekedési módok szolgáltatási színvonalának emelésével."[29]
Jelenleg talán ez a legösszetettebb ökoszisztéma, kiberbiztonsági szempontból viszont talán kevésbé van szem előtt, mint a másik két ágazat.

Ettől függetlenül természetesen az US Department of Homeland Security okosváros biztonsággal foglalkozó tanulmány itt is megemlít néhány példát, melyeket célszerű komolyan venni. A kiadvány rögtön az autonóm közlekedés veszélyeivel kezd, megemlítve, hogy az informatikai vezérelt járműveket kibertámadás útján el is lehet téríteni, illetve, ha egy kártékony kód tönkreteszi az autonóm jármű szenzorait, akkor az irányíthatatlanná válik, működése nem biztosítható tovább. Az intelligens közlekedésirányító rendszerek esetében elképzelhető, hogy egy rosszindulatú támadó egy természeti katasztrófa idején úgy befolyásolja az eszközöket, hogy azok ne működjenek megfelelően, ezzel csapdába ejtve az embereket, illetve lehetséges, hogy a támadó manipulálja a rendszer adatait, ezzel aláásva a hosszútávú biztonságot és megbízhatóságot. A gépjárművek közötti, úgynevezett vehicle-to-vehicle (V2V), és a gépjárművek és működésüket segítő infrastruktúra-elemek közötti, azaz vehicle-to-infrastructure (V2I) kommunikáció esetén a példák szerint előfordulhat, hogy egy rosszindulatú támadó manipulálja a V2V- és V2I-jeleket, illetve nem elképzelhetetlen, hogy a gépjármű-tulajdonosok vagy –gyártók egy kiberbűnöző áldozatává válnak, aki zsarolóvírussal fertőzi meg ezeket az eszközöket.

8. A SCADA/ICS-KÖZMŰRENDSZEREK FENYEGETETTSÉGE

A jövő kihívásait a múlt eseményeivel lehet a legjobban szemléltetni. A közművek ipari irányítási rendszerei elleni kibertámadások ugyanis nem új keletűek. 2009-ben szerzőtársammal, Dr. Kovács Lászlóval tartottam több előadást „Digitális Mohács" címmel, amelyben egy elképzelt, összehangolt kibertámadás forgatókönyvét mutattuk be Magyarország ellen. Ez az előadás folyóiratcikk formájában is megjelent, és a következő mondattal zárult: *„Gyakran elhangzó vélemény jelen tanulmány szerzőitől is: nem az a kérdés, hogy egy ilyen támadássorozat bekövetkezik-e, hanem az, hogy mikor fog bekövetkezni."*[30] Az egyik ilyen előadás után egy víziközműnél dolgozó, információbiztonsággal foglalkozó kolléga jött oda hozzánk, és csak ennyit mondott: *„Ez nem az a téma, amit a nyilvánosság előtt kéne kibeszélni, ne adjunk ötleteket az ellenfeleinknek."* Eltelt több mint 10 év, megjelent a Digitális Mohács 2.0, az élet pedig folyamatosan igazolta vissza mindazt, amit az eredeti tanulmányunkban feszegettünk. Célszerűnek tűnik tehát, hogy minél nagyobb nyilvánosság előtt beszéljünk arról, mi is történt az elmúlt 10 évben, mik azok az okok, amelyek miatt a létfontosságú rendszerek védelme során a szakmának oda kell figyelnie a kiberbiztonságra!

A következő történet nem sokkal a Digitális Mohács tanulmányunk megírása után kezdődött. Pontosabban került nyilvánosságra. Középpontjában a Stuxnet nevű kártékony kód áll, amely izraeli–amerikai közös katonai műveletként évekkel

[29] BÓDI Antal – MAROSI Dóra: A komplex ITS ökoszisztéma alapjai. Acta Periodica. 17. kötet, 2019. pp. 48-70.
[30] KOVÁCS László – KRASZNAY Csaba: Digitális Mohács – Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, 2010/1. pp. 44-56.

korábban indult útjára, célja pedig az volt, hogy megakadályozza, vagy legalábbis hátráltassa Irán nukleáris ambícióit.[31] A Stuxnet kártékony kód működése, a részletekbe nem belemenve, azt a célt szolgálta, hogy az iráni urándúsító centrifugákat különböző, az optimálistól jelentősen eltérő fordulatszámon hajtva, azokat a lehető leghamarabb tönkretegye, így lehetetlenné téve a fegyvertisztaságú urán létrehozását. A kód azt a Windows operációs rendszert fertőzte meg, amelyen az ipari vezérlő szoftver futott, ezen keresztül közvetlenül a PLC[32]-ket irányította, miközben az operátorok által figyelt képernyőn látszólag a megfelelő adatok jelentek meg, tehát elfedte a valódi üzemi adatokat a szoftverben. Mivel az üzemeltetők a szemüknek, azaz a meghamisított adatoknak hittek, sokáig nem értették, mi okozhatja a leállásokat. A művelet amerikai–izraeli szempontból totális siker volt: Irán feladta nukleáris fegyverkezési programját anélkül, hogy emberek haltak volna meg (legalábbis nyílt háborúban, a titkos műveletek áldozatairól még sejtésünk sem lehet).

A SCADA/ICS-rendszereket használó mérnökök számára a Stuxnet volt az első olyan szemnyitogató támadás, amelynél a korábban alaptézisként szolgáló elveket felül kellett vizsgálni. Először is, a támadás közvetlenül hatott a vezérlésre, a humán-gép interfész (Human-Machine Interface – HMI) nem mutatott eltérést, így megdőlt a rendszer megbízhatóságába vetett hit. Másodszor, a rendszer nem volt elérhető az internet felől, egy szigorúan védett katonai objektumba tudtak kártékony kódot bejuttatni, ami autonóm módon, éveken keresztül működött. Harmadszor, kiderült, hogy van az az anyagi és emberi erőforrás, amivel egy ennyire speciális rendszert is lehet kompromittálni. Ami pedig talán a legtragikusabb felismerés volt, hogy az üzembiztonság erőteljesen függ az elektronikus információs rendszerek biztonságtól, tágabb értelemben véve a kiberbiztonságától, holott erre az ipari környezetben sem az üzemeltetők, sem pedig az üzemeltetett rendszerek nem voltak felkészülve.

Természetesen a kiberfizikai rendszerek biztonságának kérdése nem új keletű dolog, a 2010-es években viszont számos olyan incidens történt, amelynek eredményeképpen a termelésirányító rendszerekkel foglalkozó mérnökök eljutottak oda, hogy kénytelenek az elektronikus információbiztonsági kérdésekkel is foglalkozni. Az OT (operational technology) és az IT (information technology) olyan szoros szinergiát alakított ki, annyira elválaszthatatlan egymástól, hogy a szakterületek együttműködése elkerülhetetlen. Különös tekintettel arra, hogy a negyedik ipari forradalom hatásaként a közművek területén is sorra jelennek meg azok az okosmegoldások, szenzorok, hálózatba kapcsolt ipari eszközök (Industrial Internet of Things – IIoT), amelyek kiberbiztonsági hatásai egyelőre felmérhetetlenek. A tudományos közösség aktívan foglalkozik a témával, a Google Scholar tudományos keresőbe beírva a „cyber attack water" keresőszót például 54.000 potenciálisan érdekes cikket találhatunk, a gyakorlat azonban egyáltalán nem érte utol a tudósok elméleti eszmefuttatásait.

De ki és miért támadna közműveket a kibertérből? Mi az az indok, amiért országok vállalják, hogy súlyosan megsértik a nemzetközi humanitárius jog azon pontját, amely a civil objektumok védelméről szól, ahogy az az orosz–ukrán háború

[31] KOVÁCS László – SIPOS Marianna: A Stuxnet és ami mögötte van: tények és a cyberháború hajnala. Hadmérnök, 2010/4. pp. 163-172.

[32] Programmable Logic Controller, Programozható Logikai Vezérlő

első napjaiban megtörtént, amikor az orosz fél pusztító kártékony kód (wiper) támadást indított ukrán civil célpontok ellen?[33,34] Hiszen az elektronikus információs rendszereken keresztül történő beavatkozások olyan hatásokkal járhatnak, amelyek akár a vízbázist, a biztonságos vízellátást vagy éppen a villamosenergia-ellátást veszélyeztetik, amelyek nélkül a modern társadalom működésképtelen. Számos olyan esettanulmány létezik, amelyek bemutatják a kritikus infrastruktúrák kitettségét. Két példán keresztül szeretném bemutatni azokat az okokat, ami miatt a vizes szakma sem aludhat nyugodtan. Az első eset még 2013-ban történt, amikor iráni hackerek jutottak be egy New York melletti gát vezérlőrendszerébe.[35] Az eset nem kavart túl nagy vihart a közvéleményben, holott egy nagyobb, komplexebb képbe illik bele. A már említett Stuxnet mellett számos olyan, kiberteret érintő esemény történt, amely az amerikai–iráni relációt terhelte. Iráni részről a Twitter-fiókok feltörésétől kezdve, amelyeken propagandát terjesztettek, a kifinomult, kőolajtermelést érintő kibertámadásokig (Shamoon vírus szaúdi célpontok ellen) különböző intenzitású, de saját stratégiai céljukat szolgáló műveleteket láthattunk, amelyeket hatékonyan (jó hatásfokkal) hajtottak végre, de érezhetően egy bizonyos komplexitást már nem tudtak átlépni. Az amerikaiak eközben 2019-ben képesek voltak iráni katonai célpontokat semlegesíteni pusztán kiberműveletekkel, illetve olyan iráni katonai vezető célzott likvidálására is sor került, aki a kiberbiztonsági terület felelős vezetője volt.

Ennek az adok-kapoknak a sorába illeszkedett ennek a bizonyos gátnak, a Bowman Damnek a számítógépes rendszerébe történő behatolás. A híradások mellett a különböző szakkonferenciák előadásaiból lehet rekonstruálni, hogy mi is történt valójában. A banálisan egyszerű probléma az volt, hogy ez a gát egy viszonylag jelentéktelen közmű volt, amelyet természetesen nem őriztek 24 órában, hanem interneten keresztül tudtak belépni a vezérlő-számítógépre, ha erre szükség volt. Az iráni támadó véletlenül, egy egyszerű Google-kereséssel talált rá a számítógépre, amelynek belépési felhasználóneve és jelszava az admin/admin volt. Bár a manipulációra nem nagyon volt lehetőség, az iráni propaganda mégis hatalmas győzelemként tudta eladni ezt a hacket a hazai közönségnek. A támadó haszna ebben az esetben tehát a propagandagyőzelem volt, illetve egy újabb figyelmeztető jelet sikerült küldeni az amerikai kormányzatnak arról, hogy a kritikus infrastruktúráik közel sem sérthetetlenek.

A második eset ennél lényegesen komolyabb és figyelmeztetőbb. Az érintett országok Oroszország és Ukrajna, az időpont 2018. A Krím-félsziget annektálása és Kelet-Ukrajna elszakadási törekvéseinek támogatása miatt ekkor már negyedik éve folyt a se nem béke, se nem háború a két ország között. Oroszország az USA és Kína mellett az az ország, amelynek kiberképességei messze a többi ország fölé emelkednek. A híradások szerint az ország keleti felében, Dnyipropetrovszk megyében lévő Auliban működő klórdesztillációs állomást érte a támadás a hálózati

[33] A Microsoft Special Report: Ukraine című jelentése szerint „kormányzati, IT, energetikai és pénzügyi szervezetek” voltak a célpontok.

[34] ICRC: Rule 9. Definition of Civilian Objects 2020. április 22. https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule9

[35] FRANCESCANI, Chris: U.S. Infrastructure Can Be Hacked With Google, Simple Passwords. NBC News, 2016. március 24. https://www.nbcnews.com/news/us-news/u-s-infrastructure-can-be-hacked-google-simple-passwords-n548661

rendszeren keresztül. A támadás hátterében a VPNFilter nevű kártékony kód állt.[36] A támadást az ukrán biztonsági szervek meghiúsították. A VPNFilter többfunkciós támadó kód, amely otthoni és kisvállalati routereket fertőz, amelyeket gyakran használnak közművek adatátviteli rendszereiben. Funkciói az adatgyűjtés, mely segít megérteni, hogyan működik az adott kritikus infrastruktúra, a beavatkozás, amelynek segítségével bizonyos hálózati elemek elérhetetlenné válnak, illetve feltehetően a router teljes törlése, amely után az adott hálózati szegmens működésképtelenné válik.[37]

Bár nincsenek olyan bizonyítékok, hogy a klórdesztillációs állomás támadásával tömegkatasztrófát akartak volna előidézni, az bizonyosnak látszik, hogy a kártékony kód segítségével a feltehetően orosz támadó törekedett az ukrán kritikus infrastruktúrák működésének teljes feltérképezésére, ahogy azt egyébként tette más országokban is. Legalábbis a brit és az amerikai kormányzatok közzététele alapján orosz felderítő tevékenységet fedeztek fel az országok villamosenergia rendszereiben, amely akár egy későbbi támadás megalapozásaként is értelmezhető. Az is biztos, hogy 2015-ben és 2016-ban komolyabb áramkimaradások történtek Ukrajnában orosz eredetű kibertámadásoknak köszönhetően. A 2015-ös BlackEnergy támadás után például 230.000 ember maradt áramellátás nélkül decemberben.[38] A 2015-ös esemény különösen szofisztikált támadás volt. 2015. december 23-án, tehát a karácsony előtti napon, kora délután indult az akció, a nyugat-ukrajnai, tehát az orosz–ukrán konfliktusban az Oroszország szempontjából ellenérdekelt területen. A Kyivoblenergo nevű áramszolgáltatónál az ügyeletes üzemmérnökök azt tapasztalták, hogy az alállomási távkezelésért felelős számítógépes rendszerbe valaki távolról belépett, és megpróbálja lekapcsolni a lakossági áramellátást biztosító alállomásokat. Végül összesen 30 darab, 110 kV-os és 35 kV-os alállomást sikerült kiiktatni.[39] Mi a támadó motivációja? Nyilvánvalóan a nyomásgyakorlás, a biztonságérzet csökkentése oly módon, hogy ne lehessen egyértelműen kijelenteni, háborús cselekmény történt.[40] Az orosz–ukrán háború objektív értékelhetőségére még sokat kell várni, de a fejezet írásának idején erősen feltételezhető, hogy ezek a támadások orosz katonai műveletek voltak, amelyek a hibrid műveletek körébe tartoztak.

---

36 BOLCSÓ Dániel: Orosz kibertámadást hiúsított meg Ukrajna. Index.hu, 2018. július 11. https://index.hu/tech/2018/07/11/orosz_kibertamadast_hiusitott_meg_ukrajna/

37 Symantec: VPNFilter: New Router Malware with Destructive Capabilities. 2018. június 1. https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware

38 LIPOVSKY, Robert– CHEREPANOV, Anton: Industroyer: Biggest threat to industrial control systems since Stuxnet. WeLiveSecurity.com, 2017. június 12. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

39 PONGRÁCZ Péter: Kibertámadások villamosenergetikai környezetben. In: DEÁK Veronika (Szerk.): Kritikus információs infrastruktúrák védelme – Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyszámára – 2019. Nemzeti Közszolgálati Egyetem, Budapest, 2019. pp. 113-138.

40 Az orosz–ukrán háború kitörésekor számos szakértő számított arra, hogy hasonló, kritikus infrastruktúrákat érő kibertámadások érkeznek orosz részről. Ezek viszont elmaradtak. Ennek okait valószínűleg hosszú időn át fogják elemezni a kutatók, amikor a „háború köde" felszáll, és megbízható információkhoz lehet jutni.

A katonai tevékenységeknek tehát velejárója lehet a kibertéri műveletek összessége. Nem véletlen, hogy a NATO 2016-ban a kiberteret a negyedik műveleti térnek ismerte el, jelezve, hogy a föld, a víz és a levegő mellett itt is számítani kell mind védelmi, mind támadó jellegű képességfejlesztésre.[41] A már most is komoly képességekkel rendelkező országok pedig nem félnek felhasználni a kiberteret saját céljaik elérésének támogatásához. Bár a sajtó elsősorban Kína és Oroszország tevékenységével foglalkozik, egyre többet enged láttatni az Egyesült Államok is saját képességeiből, de például Nagy-Britannia is saját kiberműveleteit emelte ki az ISIL/Daesh terrorszervezet visszaszorításával kapcsolatban. A jövő pedig még több kihívást tartogat, a katonai műveleteken túl is. Gondoljunk itt csak arra, hogy a már említett IIoT elterjedésének alapfeltétele az 5G kommunikációs hálózatok kiépítése, márpedig aki kontrollálja az átviteli hálózatot, az kontrollálja többek között az „okos" közműveket is. A kínai Huawei körüli polémiát és az amerikai aktivitást ezen a területen érdemes tehát ebben a kontextusban is vizsgálni. Nem is beszélve arról, hogy a kiberbűnözői csoportok is egyre nagyobb érdeklődést mutatnak az iránt, hogy hogyan lehet az alapvető infrastruktúrákat sikeresen támadni.

9. AZ SCADA/ICS-RENDSZEREK BIZTONSÁGA

A probléma nagyságát jól illusztrálja a BlackCell Kft. nemrég publikált tanulmánya, amely ICS/OT[42] snapshot 2019 címmel jelent meg, és részletesen áttekinti, milyen állapotban vannak a magyarországi ipari infrastruktúrák kibervédelmi szempontból.[43] A tanulmány írói a shodan.io szolgáltatás, az „ipari rendszerek Google-ja" segítségével keresték meg azokat az interneten elérhető ICS/SCADA-rendszereket, amelyek Magyarországon vannak. Összesen 2013 ilyen rendszert találtak. A feltárt eszközök között megtalálhatók PLC-k és egyéb kontrollerek, HMI-eszközök és webes felületek, különböző kiegészítő modulok, webes menedzsment és monitoring eszközök, ipari switchek, átalakítók, illetve egyéb eszközök, amelyek felhasználása köthető valamilyen ipari, vagy más vezérléstechnikai (pld. épületvezérlés) tevékenységhez. Ezek közül számos eszköz tűnt sebezhetőnek elavult firmware, gyenge kriptográfia vagy akár nem megfelelő hitelesítés miatt. A vízellátással és energiával kapcsolatos protokollokat többször is említi a tanulmány. Egyrészt a DNP3-protokollt nevesíti, amely szabványos kommunikációs eljárást használó eszközök közül tizenkettőt találtak az interneten a kutatók, mindegyiket Budapesten, másrészt felsorol néhány gyártót, mint például a Saia-Burgess Controls (SBS) nevű céget, amelynek 134 termékét találták meg, kivétel nélkül sebezhető firmware-t futtatva, illetve a Siemens S7 családot, amelyből 75 darabot találtak az interneten. A napelemek vezérlésére használt Fronius megoldást 82 hazai helyen telepítették. Nem maradt ki a közlekedési szektor sem, az elektromos gépjárművek töltésében használt Etrel megoldásból 6 volt elérhető Magyarországon a nyílt hálózat felől. A shodan.io egyébként több mint 6000 találatot ad ki a „water", és 3000 találatot az „energy" szóra keresve.

Természetesen mindez nem jelenti azt, hogy az ipari rendszerek triviálisan törhetők lennének. Eleve érdemes észrevenni, hogy a példaként hozott támadások általában olyan rendszereket értek, melyek informatikai szempontból könnyen

41 2019 végétől a világűr is műveleti térnek számít a NATO-terminológiában.
42 Operational Technology, Operatív Technológia
43 KOCSIS Tamás: ICS/OT snapshot 2019. Black Cell Magyarország Kft.

hozzáférhetők, tehát a HMI-gépek, amelyek jellemzően valamilyen, többnyire elavult, nem frissített Windows operációs rendszert futtatnak, vagy pedig a hálózat olyan elemei, amelyek Linux alapúak. A célrendszerek, a PLC-k és azok speciális protokolljai egyelőre olyan nehezen áttörhető akadályt jelentenek, amelyet csak felkészült, megfelelő emberi és anyagi erőforrással rendelkező titkosszolgálatok és hadseregek tudnak megugrani. Természetesen ez nem azt jelenti, hogy ne lenne példa ilyen támadásokra, hiszen a Stuxnet után folyamatosan jelentek meg hírek olyan kártékony kódokról, amelyek „beszélnek SCADA-ul". A 2016-os ukrán áramkimaradást okozó Industroyer nevű kártékony kód például az IEC 60870-5-101, IEC 60870-5-104, IEC 61850 és az OLE for Process Control Data Access (OPC DA) protokollok mindegyikén tudott kommunikálni.[44]

A kiberbiztonsági szakértő szemében tehát az HMI és az oda vezető hálózat a legkritikusabb. Egy olyan infrastruktúra, ami szélsőséges esetben nem más, mint egy elektronikus információbiztonsági szempontból rosszul megírt szoftver, mely egy frissítés nélküli, elavult operációs rendszeren fut, látszólag szeparáltan, légréssel védve, de valójában az internetről elérhető módon, egy olyan tagolatlan hálózatban, ahol minden eszköz egy szegmensben van, amihez ráadásul az üzemeltetés miatt harmadik felek is hozzáférnek távolról. A HMI után következő infrastruktúra-elemek pedig a szenzorokkal, PLC-kkel egy olyan világot tárnak fel, ahol nagyon sok esetben esély sem mutatkozik az információbiztonsági alapelvek teljesítésére, hiszen egy víruskereséssel, vagy akár csak egy logüzenet legenerálásával sem lehet az üzembiztonságot veszélyeztetni, hiszen minden, ami információbiztonság, akár milliszekundumos késleltetést is jelenthet, és ez sokszor nem megengedhető.

A támadási eljárások megértéséhez a DragonFly 2.0 kampányt hozom példának, amely energetikai szereplőket támadott, gyaníthatóan orosz háttérrel.[45] Az alábbi lépések pontosan bemutatják, mi mindent kell tennie a támadónak a sikeres betöréshez. A hét felsorolt lépés egyébként a kiberbiztonsági szakterületen gyakran használt „Cyber Kill Chain" modellt is ismerteti, gyakorlatilag minden támadás ezt követi. Mindez azonban azt is jelzi, milyen sok lehetősége van egy potenciális áldozatnak a védelem kialakítására.

1. szakasz – Felderítés: ekkor történik az áldozat feltérképezése. A konkrét esetben például a támadók letöltöttek egy kis fényképet az egyik áldozat nyilvánosan elérhető HR oldaláról. A kinagyított kép egy nagy felbontású fotó volt, amely a vezérlőrendszerek berendezéseinek modelljeit és az állapotinformációkat jelenítette meg a háttérben.

2. szakasz – Fegyverkészítés: ez a konkrét támadó kód kialakítását jelenti. Példánkban a támadók egy speciális e-mail-mellékletet állítottak össze, így használták ki a Microsoft Office legális funkcióit. Ezzel a módszerrel dokumentumokat tudtak letölteni egy távoli kiszolgálóról az SMB (Server Message Block) protokoll használatával. Az ismert támadások nagyjából felében a dokumentumokat folyamatirányítással, ICS-sel vagy kritikus infrastruktúrával kapcsolatos kereskedelmi kiadványokban és információs webhelyeken helyezték el.

[44] LIPOVSKY, Robert– CHEREPANOV (2017.): i. m.

[45] Symantec: Dragonfly: Western energy sector targeted by sophisticated attack group 2017. október 20. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

Ezen lépéssel tudták felderíteni a potenciális áldozatok körét és az általuk használt informatikai megoldásokat.

3. szakasz – Kézbesítés: ebben a fázisban történik a konkrét támadó kód célzott eljuttatása. Célzott adathalász e-mailekben általános szerződési megállapodásnak tűnő témát használtak (a „SZERZŐDÉS & Bizalmas" tárgysorral), amely egy általános PDF dokumentumot tartalmazott, amelynek neve document.pdf volt. A dokumentum rövidített URL-t tartalmazott, amelyre kattintva a felhasználók egy olyan webhelyre érkeztek, ahol e-mail-címet és jelszót kértek a felhasználótól. Az e-mail-üzenetek ipari vezérlőberendezésekre és protokollokra való hivatkozásokat tartalmaztak. Bizonyos esetekben az e-mailek olyan rosszindulatú Microsoft Word-mellékleteket használtak, amelyek valódinak tetsző önéletrajzoknak tűntek az ipari irányítórendszerrel foglalkozó munkatársak számára, valamint meghívókat és szabályzatokat tartalmazó dokumentumokat is küldtek, rávéve a felhasználót arra, hogy megnyissák a mellékletet.

4. szakasz – Kihasználás: ilyenkor történik a rosszindulatú kód futtatása. A célpont fertőzésére a támadók rosszindulatú .docx fájlokat használtak, amelyekben a kártékony kód a felhasználói hitelesítő adatok rögzítésére szolgált. Amikor egy felhasználó megkísérelte hitelesíteni magát a hálózatban, a támadó által üzemeltetett külső szerver megkapta a jelszó lenyomatát (hash-ét).

5. szakasz – Telepítés: a támadó ekkor veti meg a lábát hosszabb távra a számítógépen. A támadók a kompromittált hitelesítő adatokat használták az áldozatok hálózatainak eléréséhez, de csak ott, ahol nem a kétlépcsős hitelesítést alkalmazták. A hozzáférés fenntartása érdekében a támadók helyi adminisztrátori fiókokat hoztak létre a célpont-hálózatban, és rosszindulatú fájlokat helyeztek el a feltört gépeken.

6. szakasz – Irányítás és vezérlés: ekkor történik a kommunikáció, a feladatok kiadása a kompromittált hálózaton. A támadók távoli elérést lehetővé tevő szoftvereket, ún. remote shelleket telepítettek a nyilvánosan elérhető e-mail- és webszervereken.

7. szakasz – Célokkal kapcsolatos tevékenységek: miután a támadók a kiszemelt célhálózatban voltak, kiemelt jogosultságot szereztek, és ezt használták fel az áldozat domain-vezérlőjének kompromittálására, általában RDP-protokollon keresztül. A támadók többször is hozzáfértek olyan munkaállomásokhoz és szerverekhez a vállalati hálózaton, amelyek az energiatermelő létesítmények vezérlőrendszereiből származó adatokat tartalmaztak. A támadók hozzáfértek az ICS/SCADA-rendszerekhez kapcsolódó fájlokhoz is.

Ha pedig sikerül eljutni erre a szintre, akkor már bármi megtörténhet. 2018-ban az NCC Group nevű kiberbiztonsági cég egyik ügyfele megbízásából hajtott végre tesztet egy energetikai ipari irányítási környezetben. A cél az volt, hogy kipróbálják, mekkora károkat okozna a NotPetya kiberfegyver, ha bejutna egy ilyen infrastruktúrába. Az ICS Cybersecurity Blog így foglalta össze a teszt eredményét:
„A módosított malware-t egy mérnöki hálózatban engedték szabadon és semmilyen jogosultságot nem kapott a hálózaton található eszközökön. Első körben a módosított malware három, az EternalBlue sérülékenység ellen nem patch-elt számítógépet talált. A malware-be kódolt exploit-ot használva a NotPetya mindhárom sérülékeny számítógépen kernel szintű jogosultságot szerzett, majd ezzel a jogosultsággal megfertőzte ezeket a számítógépeket. Tíz percen belül az első

három számítógépről szerzett felhasználónevekkel és jelszavakkal a teljes mérnöki hálózatot átfésülte további megfertőzhető eszközöket keresve. Két további perccel később a malware átvette az uralmat a teljes tartomány felett. A módosított NotPetya nagyjából 45 perc alatt 107 számítógép felett szerzett irányítást, mielőtt az NCC Group ügyfele aktiválta volna a beépített leállító és eltávolító funkciót."

Mindez jól illusztrálja, miért fontos a mérnöki hálózat kiemelt védelme, (mikro)szegmentációja az élesüzemi hálózattól. A módosított kártékony kód egyáltalán nem érintette a SCADA/ICS-hálózatot, pusztán a HMI-gépeket pusztította volna el, ha a hatásmechanizmus az eredeti.

10. A KIBERBIZTONSÁG EURÓPAI SZABÁLYOZÁSA

A megfelelően biztonságos okosinfrastruktúra kiépítése tehát nem csak a közműszolgáltató érdeke, hanem nemzetbiztonsági kihívás is. Sőt, egyes közművek – mint például a villamosenergia-rendszerek – komplex hálózata európai szinten értelmezhető. Nem csoda, hogy az Európai Unió 2013-ban kelt kiberbiztonsági stratégiájában célul tűzte ki az európai létfontosságú rendszerek egységesen magas kiberbiztonsági szintjének elérését. A Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér című dokumentum az alábbi célokat fogalmazza meg:

„A Bizottság:

- *az európai kritikus infrastruktúrák hálózat- és információbiztonsági sebezhetőségeinek azonosítása és ellenálló rendszerek kifejlesztésének ösztönzése érdekében folytatja tevékenységeit, amelyeket a Közös Kutatóközpont a tagállamok hatóságaival és a kritikus infrastruktúrák tulajdonosaival és üzemeltetőivel szoros együttműködésben lát el.*
- *2013 elején a botnetek és rosszindulatú programok elleni küzdelemmel kapcsolatos uniós finanszírozású kísérleti projektet indít el a tagállamok, a magánszektorbeli szervezetek, például az internetszolgáltatók és a nemzetközi partnerek közötti koordináció és együttműködés keretének megteremtése érdekében.*

A Bizottság az alábbiakra kéri az ENISA-t:

- *A tagállamok támogatása az erős nemzeti képességek kialakításában a kibertámadásokkal szembeni ellenálló képesség területén, főleg az ipari vezérlőrendszerek, a szállítás és az energiaipari infrastruktúra biztonságával és ellenálló képességével kapcsolatos ismeretek összegyűjtése révén.*
- *Az ipari vezérlőrendszerekre szakosodott uniós hálózatbiztonsági incidenskezelő csoportok (SCIRT) megvalósíthatóságának vizsgálata 2013-ban.*
- *A tagállamok és az uniós intézmények további támogatása rendszeres páneurópai kiberbiztonsági gyakorlatok megrendezésével, amelyek az Unió nemzetközi kiberbiztonsági gyakorlatokban való részvételének működési alapjául is fognak szolgálni.*

A Bizottság az alábbiakra kéri az Európai Parlamentet és a Tanácsot:

- *Az uniós közös, magas szintű hálózat- és információbiztonságra (NIS) vonatkozó irányelvjavaslat minél hamarabbi elfogadása, amely a nemzeti képességekkel és felkészültséggel, az uniós szintű együttműködéssel, a kockázatkezelési gyakorlatok elterjedésével és a NIS-sel kapcsolatos információk megosztásával foglalkozik.*

A Bizottság az alábbiakra kéri az ágazatot:

- *Vezető szerep vállalása a magas szintű kiberbiztonságba való beruházásban és bevált gyakorlatok, valamint ágazati szintű és a hatóságokkal való információmegosztás kidolgozása abból a célból, hogy biztosítsa az eszközök és egyének hatékony és megbízható védelmét, főleg az állami és a magánszektor partnerségei, például az EP3R és a Digitális élet iránti bizalom"*[46]

A stratégia eredményeképpen egy három pilléren nyugvó európai kiberbiztonsági szabályozás alakult ki, amelynek elemei Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, azaz a NIS Direktíva, Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet (Kiberbiztonsági Jogszabály) hatályon kívül helyezéséről, továbbá ezek mellett, fontos pillérként Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), amely GDPR-ként ismert.

A 2013-ban kiadott stratégiát 2017-ben vizsgálták felül, a Közös közlemény az Európai Parlamentnek és a Tanácsnak Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése című anyagban. Ebben ekképpen értékelték az Európai Unió előrehaladását:
„A kibertámadásokkal szembeni uniós ellenálló képességhez elengedhetetlen, hogy az irányelvet valamennyi tagállam 2018 májusáig teljeskörűen végrehajtsa. A folyamatot a tagállamok kollektív munkája támogatja, ami 2017 őszére iránymutatást fog eredményezni az összehangoltabb végrehajtás támogatására, különösen az alapvető szolgáltatások üzemeltetői tekintetében. A Bizottság közleményt fog kiadni az említett kiberbiztonsági csomag részeként, hogy azzal támogassa a tagállamok erőfeszítéseit, az irányelv végrehajtására vonatkozó bevált gyakorlatokat a tagállamoknak átadva és útmutatással szolgálva arról, hogy az irányelvnek miként kellene a gyakorlatban működnie. (…) Erősíteni kell a bizalmat a közszféra és magánszféra közötti partnerségek iránt, hogy meg lehessen alapozni a több ágazat közötti szélesebb körű együttműködést és információcserét. Az információcsere és -elemző központok szerepe különösen fontos abban, hogy kiépítsék a szükséges bizalmat a közszféra és a magánszféra közötti információcsere

[46] Európai Bizottság: Közös Közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér. 2013. február 7.

iránt. Történtek bizonyos első lépések egyes kritikus ágazatok tekintetében, mint például a repülés terén az Európai Repülési Kiberbiztonsági Központ, illetve az energetikában az információcserei és -elemző központok létrehozásával. A Bizottság teljes mértékben hozzájárul ehhez a megközelítéshez az ENISA által nyújtott támogatás révén, jóllehet fel kell gyorsítani a folyamatot, különösen a kiberbiztonsági irányelvben azonosított alapvető szolgáltatásokat végző ágazatok tekintetében."

A 7 évvel ezelőtti stratégiában foglalt, kritikus információs infrastruktúra-védelemmel kapcsolatos elvárások tehát lassabban teljesülnek, mint az kívánatos lenne. Elsősorban a NIS Direktíva felgyorsítása lenne célszerű[47], amelyet Tikos Anita így foglal össze.
„Az irányelv célja, hogy megteremtse a gyors és hatékony európai szintű kiberbiztonsági együttműködés és (incidenskezelés és -elemzés szintű) reagálóképesség alapjait, amely remélhetőleg hatékonyan alkalmazható lesz valamennyi lényeges biztonsági esemény és kockázat kezelésére. Annak érdekében, hogy egy ilyen hatékony és gyors együttműködési mechanizmus létrehozható legyen, a legkiemelkedőbb szektorokban meg kell teremteni a hálózati és információs rendszerek biztonsága általános védelmének alapjait Unió-szerte. Ezért az irányelv ezen szektorokra vonatkozóan megfogalmazza a legfontosabb védelmi szempontokat és minimumelvárásokat, valamint az EU-s együttműködési mechanizmusok megfelelő működéséhez szükséges nemzeti szakosított szervezeteket és azok minimumfeladatait, -képességeit."[48]

Az irányelv hatálya egyébként kétfajta szolgáltatóra terjed ki, az alapvető szolgáltatókra, ahova víziközművek is tartoznak, és a digitális szolgáltatást nyújtó szolgáltatókra, mint például az online piacterek.

Az okosvárosok kiberbiztonsági szabályozása egyébként direkt módon nem következik egyébként a NIS Direktívából, indirekt módon viszont egyértelmű, hogy hosszú távon kikerülhetetlen lesz az okosinfrastruktúra és az európai követelmény összehangolása. A pontos meghatározás szerint a NIS irányelv alá tartoznak *„A 98/83/EK tanácsi irányelv (17) 2. cikke 1. pontjának a) alpontjában meghatározott emberi fogyasztásra szánt víz szolgáltatói és elosztói, kivéve azokat az elosztókat, amelyek esetében az emberi fogyasztásra szánt víz elosztása csupán egy részét teszi ki az egyéb, alapvető szolgáltatásoknak nem tekinthető közszolgáltatások és áruk elosztására irányuló általános tevékenységüknek"*. E szolgáltatók kijelölése a nemzeti hatóságok feladata. Viszont ahogy ezek a szolgáltatók áttérnek az okosinfrastruktúra használatára, a kiberbiztonsági és elektronikus információbiztonsági szempontok figyelembevétele elkerülhetetlenné válik.

További lehetőséget biztosít a Kiberbiztonsági Jogszabályban megfogalmazott Európai Kiberbiztonsági Tanúsítási Keretrendszer létrehozása is. Eszerint az Európai Unióban csak olyan informatikai termékek hozhatók forgalomba, amelyek teljesítik az alapvető információbiztonsági eljárásokat. Tóth Tamás összefoglalója

[47] A NIS Direktíva megújítása, a NIS2 Direktíva várhatóan 2022-ben kerül elfogadásra.

[48] TIKOS Anita: A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései. In: DEÁK Veronika (szerk.): Kritikus információs infrastruktúrák védelme – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára – 2019. Nemzeti Közszolgálati Egyetem, Budapest, 2019. pp. 11-39.

szerint: *„Az igényeknek megfelelően kialakított stratégiai cél, hogy létrejöjjön az egységes európai IKT-biztonsági tanúsítási keretrendszer, amely megszünteti a tagállami és ágazati eljárások általi széttagoltságot, az elfogadott kiberbiztonsági tanúsítási szakpolitikai javaslat alapján biztosítottá válik. Az új keretrendszer a lehető legharmonikusabban fog illeszkedni a nemzetközi szabványokhoz, bizonyos nemzeti érdekeket is figyelembe véve annak érdekében, hogy csökkenjenek a kereskedelmi akadályok. Az uniós kiberbiztonsági tanúsítási keretrendszer alapvető célja igazolni, hogy a meghatározott kiberbiztonsági kritériumoknak maximálisan megfelelnek az e keretrendszer részeként elfogadott nemzeti tanúsítási eljárások során tanúsított IKT-termékek, -szolgáltatások és -folyamatok. Ez a tevékenység javítja az IKT-termékek és -szolgáltatások biztonságosságát a biztonsági paraméterekről szóló kielégítő tájékoztatást, ezáltal növelve a fogyasztók termékekbe és szolgáltatásokba vetett bizalmát."*[49]

Bár ez az előírás sem mondja ki explicit módon azt, hogy az okoseszközöket és konkrétan az okosvárosokat alkotó Dolgok Internetét biztonsági tanúsításnak kell alávetni, az évtized második felétől nyilvánvalóan az a szakpolitikai cél, hogy a kiberbiztonság egész Európában egységesen, az okosotthonoktól kezdve az okosvárosokig magasabb legyen.[50]

11. VÉDELMI LEHETŐSÉGEK

Mint a Dragonfly támadásnál felsorolt lépésekből látszódik, az ICS/SCADA-protokollok nem sérültek, a támadás mégis komolyan hozzájárult ahhoz, hogy a támadók fel tudták térképezni az amerikai és más országok energiarendszereit. Ezt a kockázatot természetesen a magyar jogszabályalkotók sem hagyhatták figyelmen kívül, ráadásul az európai direktívákat is honosítani kellett, így az elmúlt években több olyan szabályozás is elfogadásra került, amelyek – hol finomabban, hol keményebben – presszionálják a létfontosságú rendszerek üzemeltetőit az elektronikus információbiztonság megvalósítására.

A releváns szabályozások Magyarországon az alábbiak:

- a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, amely felsorolja, hogy melyek a kiemelten védendő infrastruktúra-elemek,
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény,
- 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 szóló 41/2015. (VII. 15.) BM rendelet, amely részletesen leírja, hogyan is kell ezen kijelölt létfontosságú információs rendszerek és rendszerelemek információbiztonságát megvalósítani.

[49] TÓTH Tamás: Az Európai Unió tervezett kiberbiztonsági tanúsítási keretrendszerének bemutatása. Szakmai Szemle, 2019/1. pp. 97-115.

[50] Az IoT eszközök kiberbiztonsági tanúsításának elterjesztése deklarált cél 2022-ben.

A 2013. évi L. törvény és a 41/2015. (VII. 15.) BM rendelet elsősorban hagyományos elektronikus információs rendszerekre (IT, azaz az irodai jellegű rendszerek) vannak kitalálva, így a gyakorlatban e követelmények műszaki teljesíthetősége kérdéses OT (SCADA/ICS) -rendszerek esetén. A humán és anyagi erőforrásokban szűkölködő közműszektoroknak már a hagyományos informatikai rendszerek védelme is komoly kihívás. Mégis érdemes felkészülni erre a kihívásra is, hiszen, mint láthattuk, ez nem a jövő kihívása, hanem a jelen fenyegetése, ráadásul a változó európai kiberbiztonsági szabályozás a NIS2 direktíván keresztül előbb-utóbb kikényszeríti az OT-rendszerek védelmét is. Éppen ezért a felkészülést érdemes az iparági ajánlások szerint elkezdeni. Az amerikai víziközmű-szolgáltatók kiberbiztonsági szervezete, a WaterISAC ajánlása például jó kiindulási alapot jelent. A szöveg 15 pontban szedi össze a javasolt intézkedéseket.

1. Legyen egyértelmű leltár az információs rendszerekről.
2. Mérjük fel a kockázatokat.
3. Minimalizáljuk a vezérlőrendszerek kitettségét.
4. Kényszerítsünk ki felhasználói hozzáférés-kontrollt.
5. Legyen védelem a nem jogosult fizikai hozzáféréssel szemben.
6. Telepítsünk független kiberfizikai biztonsági rendszereket.
7. Legyen folyamatunk a sebezhetőségek kezelésére.
8. Alakítsuk ki a kiberbiztonság kultúráját.
9. Legyenek kiberbiztonsági szabályaink és folyamataink, és ezeket tartsuk is be.
10. Alakítsunk ki fenyegetés-észlelési és -monitorozási folyamatot.
11. Legyen tervünk az incidensek, vészhelyzetek és katasztrófák kezelésére.
12. Számoljunk a belső fenyegetéssel.
13. Biztosítsuk az ellátási láncunkat.
14. Foglalkozzunk az összes okos megoldás biztonsági kérdésével.
15. Vegyünk részt az információmegosztásban, tartsunk kapcsolatot ezekkel a szervezetekkel.[51]

Ez utóbbi ponthoz kapcsolódóan a magyarországi közművek számára kijelölt kibervédelmi hatóság az Országos Katasztrófavédelmi Főigazgatóság, az incidenskezeléssel pedig a Nemzeti Kibervédelmi Intézet foglalkozik.[52] Személy szerint viszont a 8. pontot, a kultúra kialakítását tartom a legfontosabbnak. Nem csak a jogszabályi követelmények miatt, hanem a józan előrelátás érdekében is célszerű, ha a közműszolgáltatónál van elektronikus információs rendszer biztonságáért felelős személy. A jogszabály alapján képzésüket a Nemzeti Közszolgálati Egyetem látja el.

[51] WaterISAC: 15 Cybersecurity Fundamentals for Water and Wastewater Utilities. 2019. június 3. https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20(WaterISAC).pdf

[52] A jogszabályváltozás miatt a kritikus információs infrastruktúrák kiberbiztonsággal kapcsolatos hatósági feladatait a könyv írásának idején már a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet látja el.

12. ÖSSZEFOGLALÁS

2019 nyarán a Tripwire magazin megkérdezett néhány kiberbiztonsági szakértőt, hogy véleményük szerint hogyan fog alakulni a SCADA/ICS-rendszerek biztonsága a következő 5-10 évben. Az összes megszólaló kivétel nélkül kiemelte a digitális transzformációt, az IIoT előretörését, a hálózatosodást, illetve azokat a kibertéri veszélyeket, amelyeket elsősorban állami szereplők felől kell várni. Patrick Miller, az Archer Energy Solutions szakértője így foglalta össze mindezt:
„*Más szavakkal: a folyamat adatokat generál, majd ezek az adatok elhagyják a folyamatot vezérlő hálózatot, és bárhová/mindenhová eljutnak (pl. felhő, köd, tó, helyi adatközpont, távoli adatközpont), elemzésre kerülnek, újból felhasználhatók lesznek és a végén visszajutnak a folyamatba. Mindez olyan új kockázatokat vet fel a folyamatok azon adataira és az ezekhez kapcsolódó rendszerekre nézve, melyek a vezérlő/folyamathálózatokon kívül kerülnek, amelyet most kezdünk csak megérteni.*”[53]

Biztosak lehetünk azonban abban, hogy a megelőzés minden körülmények között olcsóbb, mint hogyha utólag kellene a biztonságot beleépíteni az okosváros-infrastruktúrákba. Ehhez viszont szemléletváltásra van szükség. Először is, a legfontosabb a tudatosság, azaz az okoseszközök beszerzésénél legyünk tisztában a kiberbiztonság kiemelt szerepével, és az anyagi megfontolások mellett mindenképpen tervezzünk az elektronikus információbiztonsággal is. Második fontos szempont a szabályozás megléte. A NIS Direktíva fontos kötelezettséget ró az alapvető szolgáltatások üzemeltetőire, emiatt a külső kényszer miatt az érintett szektorokban elkerülhetetlen az elektronikus információbiztonsággal tervezni. Fontos emellett, hogy olyan belső szabályozás is létrejöjjön a víziközmű- és más közműszolgáltatóknál, amely tervez a tanulmányban említett kibertéri veszélyekkel, azaz a kiberbűnözéssel, a kiberkémkedéssel, a hacktivista és kiberterrorista csoportokkal és a kiberhadviseléssel. A harmadik lépés pedig a műszaki védelem megvalósítása, hiszen egyre több olyan szolgáltatás, illetve termék érhető el, amelyek ezekben a speciális közműszolgáltatói szektorokban is tudják emelni a kiberbiztonsági szintet. Emellett ki kell emelni, hogy az átalakuló, „okosodó” közművek esetében a végfelhasználóknak is komoly felelősségük van, hiszen például az energiaszolgáltatásban az okosmegoldások üzemeltetői sokszor nem a szolgáltatók, hanem például a napelemeket üzemeltető ingatlantulajdonosok lesznek.

[53] PETTIT, Joe: Ask the Experts: What Will Have the Greatest Impact on ICS Security in the Next 5-10 Years?. Tripwire, 2019. július 24. https://www.tripwire.com/state-of-security/greatest-impact-ics-security

Felhasznált irodalom:

- BARANYA Gábor – CSERNUS Ildikó (Szerk.): A fenntartható fejlődés és az állam feladatai. Dialóg Campus, Budapest, 2018.
- BEDERNA Zsolt et. al.: Támadás hálózatba szervezve. In: AUER Ádám – JOÓ Tamás (Szerk.): Hálózatok a közszolgálatban. Dialóg Campus Budapest, 2019. pp. 223-247.
- BÓDI Antal – MAROSI Dóra: A komplex ITS ökoszisztéma alapjai. Acta Periodica. 17. kötet, 2019. pp. 48-70.
- BOLCSÓ Dániel: Orosz kibertámadást hiúsított meg Ukrajna. Index.hu, 2018. július 11. https://index.hu/tech/2018/07/11/orosz_kibertamadast_hiusitott_meg_ukrajna/
- BONDOR, Mark: The best smart water bottles of 2020. MBReviews, 2020. április 14. https://www.mbreviews.com/best-smart-water-bottle/
- CASTELLS, Manuel: Informationalism, Networks, and the Network Society: a Theoretical Blueprint. In: CASTELLS, Manuel (Ed.): The Network Society: A Cross-cultural Perspective. Edward Elgar UK, Cheltenham, 2004. pp. 3-45.
- Európai Bizottság: Közös Közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér. 2013. február 7.
- FRANCESCANI, Chris: U.S. Infrastructure Can Be Hacked With Google, Simple Passwords. NBC News, 2016. március 24. https://www.nbcnews.com/news/us-news/u-s-infrastructure-can-be-hacked-google-simple-passwords-n548661
- HADDAD Richárd: Okoseszközök a kritikus információs infrastruktúrákban, villamosenergetikai fókusszal. In: DEÁK Veronika (Szerk.): Kritikus információs infrastruktúrák védelme – Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyszámára – 2019. Nemzeti Közszolgálati Egyetem, Budapest, 2019. pp. 72-113.
- HOWE, Neil – STRAUSS, William: The next 20 years: how customer and workforce attitudes will evolve. Harvard Business Review, 2007/7-8. pp. 41-52.
- https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/
- ICRC: Rule 9. Definition of Civilian Objects 2020. április 22. https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule9
- IHS Markit: The Internet of Things: a movement, not a market. 2017. október 17. https://cdn.ihs.com/www/pdf/IoT_ebook.pdf
- KEMP, Simon: Digital 2020: 3.8 Billion People Use Social Media. WeAreSocial, 2020. január 30. https://wearesocial.com/uk/blog/2020/01/digital-2020-3-8-billion-people-use-social-media/

- KOCSIS Tamás: ICS/OT snapshot 2019. Black Cell Magyarország Kft.
- KOVÁCS László – KRASZNAY Csaba: Digitális Mohács – Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, 2010/1. pp. 44-56.
- KOVÁCS László – SIPOS Marianna: A Stuxnet és ami mögötte van: tények és a cyberháború hajnala. Hadmérnök, 2010/4. pp. 163-172.
- LIPOVSKY, Robert– CHEREPANOV, Anton: Industroyer: Biggest threat to industrial control systems since Stuxnet. WeLiveSecurity.com, 2017. június 12. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/
- MAVIR: Újabb rekordok születhetnek a folyamatos napos időben. 2020. április 16. https://www.mavir.hu/web/mavir/kozlemenyek/-/asset_publisher/FPi3DcWJuTiD/content/ujabb-rekordok-szulethetnek-a-folyamatos-napos-idoben
- MESTER Gyula: Önvezető robot autók újdonságai és biztonsági kérdései. XII. Innováció és fenntartható felszíni közlekedés konferencia, XII. IFFK, Budapest, 2018.
- NAGY Judit: Az Ipar 4.0 fogalma és kritikus kérdései – vállalati interjúk alapján. Vezetéstudomány, 2019/1. DOI: 10.14267/VEZTUD.2019.01.02
- Office of Cyber and Infrastructure Analysis: The Future of Smart Cities: Cyber-Physical Infrastructure Risk. 2015. augusztus https://www.cisa.gov/uscert/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf
- ORBÓK Ákos: Az okos város kiberbiztonsága. In: SALLAI Gyula (Szerk.): Az okos város (Smart City). Dialóg Campus, Budapest, 2018. pp. 187-202.
- PANETTA, Kasey: 5 Trends Appear on the Gartner Hype Cycle for Emerging Technologies, 2019. Gartner, 2019. augusztus 29. https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019
- PETTIT, Joe: Ask the Experts: What Will Have the Greatest Impact on ICS Security in the Next 5-10 Years?. Tripwire, 2019. július 24. https://www.tripwire.com/state-of-security/greatest-impact-ics-security
- PONGRÁCZ Péter: Kibertámadások villamosenergetikai környezetben. In: DEÁK Veronika (Szerk.): Kritikus információs infrastruktúrák védelme – Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyszámára – 2019. Nemzeti Közszolgálati Egyetem, Budapest, 2019. pp. 113-138.
- SALLAI Gyula: Az okos város koncepciója. In: SALLAI Gyula (Szerk.): Az okos város (Smart City). Dialóg Campus, Budapest, 2018. pp. 13-34.
- SCHWAB, Klaus: The Fourth Industrial Revolution, Britannica, 2021. március 23. https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734

- SHEIN, Esther: COVID-19 pandemic impact pushing smart home voice control devices to predicted 30% growth. TechRepublic, 2020. április 1. https://www.techrepublic.com/article/covid-19-pandemic-impact-pushing-smart-home-voice-control-devices-to-predicted-30-growth/
- Symantec: Dragonfly: Western energy sector targeted by sophisticated attack group 2017. október 20. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
- Symantec: VPNFilter: New Router Malware with Destructive Capabilities. 2018. június 1. https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware
- TIKOS Anita: A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései. In: DEÁK Veronika (szerk.): Kritikus információs infrastruktúrák védelme – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára – 2019. Nemzeti Közszolgálati Egyetem, Budapest, 2019. pp. 11-39.
- TÓTH Tamás: Az Európai Unió tervezett kiberbiztonsági tanúsítási keretrendszerének bemutatása. Szakmai Szemle, 2019/1. pp. 97-115.
- TÖRÖK, Bernát (szerk.): Információ- és kiberbiztonság: Fenntartható biztonság és társadalmi környezet tanulmányok V. Ludovika Egyetemi Kiadó, Budapest, 2020. pp. 121-147.
- WaterISAC: 15 Cybersecurity Fundamentals for Water and Wastewater Utilities. 2019. június 3. https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20(WaterISAC).pdf
- WikiLeaks: Vault 7: CIA Hacking Tools Revealed. WikiLeaks, 2014. október 23. https://wikileaks.org/ciav7p1/cms/page_13763790.html

2. FEJEZET

A KIBERTÉR TECHNOLÓGIAI VONATKOZÁSAI, AMERIKAI–KÍNAI VERSENGÉS BUDAPESTRŐL NÉZVE[1]

1. BEVEZETÉS

A hardver kínai, a szoftver rajta amerikai. Ha egy rövid mondatban kellene megfogalmazni, hogy Európa, és benne Magyarország digitális szuverenitása szempontjából mi a XXI. század egyik legaggasztóbb trendje, akkor valószínűleg a legtöbb technológiával foglalkozó szakember ezt mondaná. De természetesen – ahogy látni fogjuk –, ha ezt a mondatot elkezdjük kibővíteni és a valós összefüggések mélyére ásni, akkor a helyzet nem ennyire fekete vagy fehér. Kivéve, hogy Európának és benne Magyarországnak ténylegesen kicsi és egyre szűkülő tere van negyedik ipari forradalom alapjait jelentő technológiák kialakításában.

Nem véletlen, hogy az Európai Bizottság 2020-ban megválasztott új vezetőinek politikai programjában kiemelt szerepet kapott Európa digitális függetlenségének visszaszerzése. Ennek fontos lépése volt a 2021 júliusában bejelentett két iparági megállapodás, a Processzorok és Félvezető Technológiák Szövetsége (Alliance for Processors and Semiconductor technologies), valamint az Ipari Adat, Peremhálózat és Felhő Európai Szövetsége (European Alliance for Industrial Data, Edge and Cloud). Ahogy azt Margrethe Vestager, az Európai Bizottság digitális korszakért felelős ügyvezető alelnöke elmondta:
„*A felhő- és peremhálózati technológiák óriási gazdasági potenciált jelentenek a polgárok, a vállalkozások és a közigazgatás számára, például a megnövekedett versenyképesség és az ágazatspecifikus igények kielégítése szempontjából. A mikrocsipek minden manapság használt eszközünk középpontjában állnak. A mobiltelefonoktól az útleveleinkig ezek a kis alkatrészek rengeteg lehetőséget kínálnak a technológiai fejlődésre. Ezért e kritikus ágazatokban az innováció támogatása kulcsfontosságú, és segíthet Európának előrelépni a hasonló gondolkodású partnerekkel együtt.*”[2]

A bejelentés mögött valós, jól felismert geostratégiai érdekek állnak, megvalósításuk azonban nem triviális, köszönhetően a több évtizedes lemaradásnak, a gazdasági megfontolások miatt Ázsiába kiszervezett gyártásnak és elsősorban az USA irányába történő sikeres agyelszívásnak. Ez utóbbira példa lehet Andy Grove, az Intel egyik alapítója, később fejlesztési igazgatóhelyettese, a mikrocsipek gyártási forradalmának egyik kidolgozója, aki Gróf András István néven született Budapesten, majd 1956-ban elhagyta hazánkat, hogy az Egyesült Államokban új életet kezdjen. Illetve példaként állhat itt jelen sorok szerzőjének számos egyetemi évfolyamtársa a 2003-ban végzett műegyetemista villamosmérnök és informatikus évfolyamból, akik szintén az USA-ban találták meg szakmai számításaikat. Komoly kihívás tehát Európa vezetőinek az, hogyan lehet a trendeket megfordítani, hol

[1] Eredetileg megjelent az Ütközőpályán című kötetben, 2022-ben.

[2] European Commission: Digital sovereignty: Commission kick-starts alliances for Semiconductors and industrial cloud technologies. European Commission, 2021. július 19. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3733

lehetnek a beavatkozási pontok? Különösen egy olyan helyzetben, amikor mind az Egyesült Államok, mind Kína arra törekszik, hogy az Európai Uniót, illetve annak egyes országait saját érdekei szerint mozgassa, csorbítva ezzel az önálló mozgástér kialakításának lehetőségét. Az USA ezt a multilaterális kapcsolatok helyreállításával, megerősítésével, Kína pedig a látszólag kedvező befektetési megállapodásokkal kívánja elérni.[3]

2. A NYERSANYAGOK GEOPOLITIKÁJA

Kezdjük talán a hardverek alapanyagainak kérdésével, végletekig leegyszerűsített formában! A negyedik ipari forradalom, a modern digitális társadalom alapját a mindenhol jelenlevő informatika, az IoT jelenti. Már a 2020-as évek elején is közel 20 milliárd hálózatra kötött informatikai eszköz vesz minket körül, az egyértelműen látható számítógépektől és okostelefonoktól kezdve az otthonunkat ellepő okos robotporszívókon és internetképes mosógépeken át, egészen a hétköznapi ember számára láthatatlan, gyártást, közüzemi működést segítő érzékelő szenzorokig bezárólag. Ezek gyártásának előfeltétele, hogy rendelkezésre álljanak azok a nyersanyagok, amelyekből a termékek létrehozhatók, legyen tudás ahhoz, hogy a hardverelemeket meg lehessen tervezni, és végül, legyen gyártási kapacitás, ahol egyrészt az egyes hardverelemeket hozzák létre, másrészt pedig a hardverelemek összességéből előáll a késztermék.

A mikrocsipek gyártásához két fontos alapanyag kell: szilícium és tiszta víz. Látszólag mindkét alapanyag végtelen mennyiségben áll rendelkezésre a Földön, de valójában a komoly tisztasági követelmények miatt már ezen alapanyagok megszerzése is akadályokba ütközik. A kettő közül talán a szilícium előállítása az egyszerűbb, hiszen az oxigén után a második leggyakoribb kémiai elem a Földön. Az Egyesült Államok Földtani Szolgálatának éves gyorsjelentéseiben jól követhető, hogy a mikrocsipek gyártásához használt szilíciumból évente 8.000 tonna kerül feldolgozásra. Ebből a 2020-as évben egyedül Kína 5.400 tonnát vállalt magára, ami jól mutatja azt a hatalmas nyersanyagéhséget, ami a keleti nagyhatalmat jellemzi.[4] Az Egyesült Államok 290 tonnát jegyez, ezzel Oroszország, Brazília, Norvégia után az ötödik helyen áll. A tiszta vízhez való jutás azonban már nem ennyire egyszerű Kína esetében. Nem véletlen, hogy egyes szakértők az Indiával való határvillongások hátterében a Himalája vízkészletét is sejtik, hiszen az onnan eredő források kiválóan ki tudnák szolgálni a gyártási igényeket. Kasmír, Akszaj Chin és Ladakh tartományok a bőséges vízforrások, a Takla-Makán sivatag pedig a homok miatt kiválóan alkalmasak komoly gyártási infrastruktúra létrehozására.[5]

Fontos alapanyagként szokták még emlegetni a ritkaföldfémeket, azaz a szkandiumot, az ittriumot, a lantánt, a cériumot, a prazeodímiumot, a neodímiumot,

---

[3] MÁRTONFFY Balázs – NYSTROM, Dwight: „Kimért multilateralizmus": Előrejelzés a bideni külpolitikáról. Külügyi Szemle, 2021/1. pp. 43-59., DOI: 10.47707/Kulugyi_Szemle.2021.1.03

[4] SCHNEBELE, Emily K.: Silicon. U.S. Geological Survey, 2021. január. https://pubs.usgs.gov/periodicals/mcs2021/mcs2021-silicon.pdf

[5] Manish Tewari: War of the chips. Deccan Chronicle, 2021. május 23. https://www.deccanchronicle.com/opinion/columnists/220521/manish-tewari-war-of-the-chips.html

a prométiumot, szamáriumot, az európiumot, a gadolíniumot, a terbiumot, a diszpróziumot, a holmiumot, az erbiumot, a túliumot, az itterbiumot és a lutéciumot. Nevükkel ellentétben, ezek a fémek jelentős mennyiségben állnak rendelkezésre a Földön, széles körben használják is ezeket az elektronikai termékek, így az okostelefonok és a viselhető okoseszközök gyártása során is. A leggyakrabban emlegetett felhasználási területen, a tartós akkumulátorok gyártásánál azonban nem ezek a fémek kellenek elsősorban, hanem lítium, mangán és kobalt, hiszen ezekből készül a lítium-ionos akkumulátor.[6]

A valódi ritkaföldfémek bányászata a 2000-es évek elejétől kezdve valóban gyakorlatilag kínai monopólium volt, az évezred elején a világ termelésének 90–95%-a Kínában történt. 2010-ben azonban egy japán–kínai incidens után, amikor a japán hatóságok letartóztatták egy vitatott tengerszakaszon hajózó kínai halászhajó legénységét, Kína visszafogta az exportját, ami érezhető fennakadásokat okozott világszerte. A Kereskedelmi Világszervezet, a WTO keretein belül, hosszas tárgyalás után, 2016-ra állt vissza az eredeti kínai exportmennyiség. Ez arra ösztönözte a kitett országokat, hogy diverzifikálják a kitermelést. 2020-ban, változatlan termelés mellett, Kína már csak a globális mennyiség 58%-át adja, az Egyesült Államok 16%-kal a második, őket követi Mianmar, Ausztrália és Madagaszkár.[7] Hosszú távon pedig Brazília és Vietnám akár át is veheti Kína helyét, ezzel csökkentve a rövid távon valóban jelentős hegemóniáját.[8]

A kobalt és a lítium kitermelése viszont valóban körülményes, ugyanis földrajzilag igen koncentráltan fordulnak elő. A lítium esetében a legnagyobb források Dél-Amerikában érhetők el, az Argentína–Bolívia–Chile által határolt háromszögben találhatók a legnagyobb tartalékok. Utánuk következik Ausztrália, amely jelenleg a legnagyobb kitermelő, majd utána Kína, amelynek vállalatai azonban egyre nagyobb részvényessé válnak a dél-amerikai régió bányatársaságaiban. Ausztrália jelenleg 40.000, Chile 18.000, Kína 14.000 tonnát termel ki, míg a világ teljes bányászati volumene 82.000 tonna.[9] A legnagyobb kobaltbányák pedig a Kongói Demokratikus Köztársaságban vannak – szintén főleg kínai tulajdonban. A kongói kobaltexport 86,5%-át Kína kontrollálja, így elsősorban saját iparát látja el ezzel a fémmel, akadályozva az alapanyaghoz jutást más országok vállalatai számára.[10] Ez az adat – annak a fényében, hogy a világ 2020-as termelése összesen 140.000 tonna volt, amiből csak a Kongói Demokratikus

6 GORRILL, Lindsay: Lithium-ion Batteries: "Rare Earth" vs Supply Chain Availability. Battery Power Online, 2019. szeptember 12. https://www.batterypoweronline.com/news/lithium-ion-batteries-rare-earth-vs-supply-chain-availability/

7 DAIGLE, Brian – DECARLO, Samantha: Rare Earths and the U.S. Electronics Sector: Supply Chain Developments and Trends. Office of Industries, 2021. június. https://www.usitc.gov/publications/332/working_papers/rare_earths_and_the_electronics_sector_final_070921_2-compliant.pdf

8 ERDEY László et. al.: China Does Not Want a Trade War – The Case for Rare Earth Elements. Polgári Szemle,. 2019/4-6. pp. 281-295., DOI: 10.24307/psz.2019.1218

9 JASKULA, Brian W.: Lithium. U.S. Geological Survey, 2021. január. https://pubs.usgs.gov/periodicals/mcs2021/mcs2021-lithium.pdf

10 RAPOZA, Kenneth: China's Rare Earths 'Slump' A Sign Of Domestic 'Hoarding' For EV Batteries, And More. Forbes, 2021, január 17. https://www.forbes.com/sites/kenrapoza/2021/01/17/chinas-rare-earths-slump-a-sign-of-domestic-hoarding-for-ev-batteries-and-more

Köztársaság 95.000 tonnát termelt – jól mutatja, hogy mennyire fontos az alapanyagok forrásainak birtoklása még a XXI. században is, és mennyire tudatosan vonta kontroll alá ezt Kína, részben a saját bányáira építve, részben pedig, akár a világ túlsó részén, nagyvállalatok megvásárlásával.[11,12,13]

Beláthatjuk tehát, hogy stratégiai szempontból nem elsősorban a ritkaföldfémek és a ritka fémek hiánya fenyeget, sokkal inkább az ezekhez való hozzáférés válhat nehézzé, köszönhetően az ugyan egyre csökkenő, de még mindig igen komoly kínai kontrollnak. Európai szemszögből nézve a digitális szuverenitás egyik alapja tehát az lenne, hogy ha vannak gyártási képességeink, akkor legyenek alapanyagok is ehhez. A ritkaföldfémek esetében ugyan a Dániához tartozó Grönlandot lehetne példaként említeni, mint hatalmas tartalékokkal rendelkező országot, de talán célszerűbb a kontinentális Európát áttanulmányozni, ahol a kutatások szerint jelentős lelőhelyek lehetnek, például Magyarországon is, ahol a nagyharsányi bauxit lelőhelyen már a 70-es években komoly koncentrációt jeleztek.[14] A lítiumkitermelés is több országban megkezdődött, Portugáliából már most is 900 tonna fém származik, de további beruházásokat terveznek Finnországban, Németországban, Ausztriában és az Egyesült Királyságban is.[15] Kobalt bányászatára is van lehetőség, hiszen jelenleg 25 európai országban 509 forrás ismert, ám ezekből jelenleg csak Finnországban folyik kitermelés három bányában. További jelentős készletek vannak Svédországban, Norvégiában, Lengyelországban, Németországban, a Balkánon és Törökországban.[16] A szilíciumtermelésben pedig Franciaországban, Izlandon, Norvégiában, Spanyolországban és Ukrajnában vannak világszinten is értelmezhető bányászati kapacitások.[17]

A bányászat azonban hagyományosan igen környezetszennyező iparág, így, ha el is indulna a fokozott kitermelés Európában, borítékolhatóan lakossági tiltakozással kellene szembenézni. Ezért megfontolandó inkább az újrahasznosítás felé fordulni. Jowitt és szerzőtársai 2018-as tanulmánya szerint például a ritkaföldfémeknek mindösszesen 1%-át hasznosítják csak újra, aminek számos oka között szerepel a megfelelő technológia hiánya és a gazdaságos kitermelés kérdése is.[18] Ha azonban a digitális szuverenitás oldaláról nézzük a kérdést, akkor hosszú

11 SHEDD, Kim B.: Cobalt. U.S. Geological Survey, 2021. január. https://pubs.usgs.gov/periodicals/mcs2021/mcs2021-cobalt.pdf

12 KALANTZAKOS, Sophia: The Race for Critical Minerals in an Era of Geopolitical Realignments. The International Spectator, 2020/3. pp. 1-16. DOI: 10.1080/03932729.2020.1786926

13 BIHARI Katalin: Kína növekvő befolyása a világgazdaságban. Pro Publico Bono – Magyar közigazgatás, 2020/4. pp. 26-35., DOI: 10.32575/ppb.2020.4.3

14 GOODENOUGH, Kathryn M. et al.: Europe's rare earth element resource potential: An overview of REE metallogenetic provinces and their geodynamic setting. Ore Geology Reviews, 2016/1. pp. 838-856., DOI: doi.org/10.1016/j.oregeorev.2015.09.019.

15 SCOTT, Alex: Europe is poised to begin lithium mining. Chemical and Engineering News, 2021. június 2. https://cen.acs.org/business/inorganic-chemicals/Europe-poised-begin-lithium-mining/99/i21

16 HORN, Stefan: Cobalt resources in Europe and the potential for new discoveries. Ore Geology Reviews, Vol. 130, 2021. 103915. DOI: 10.1016/j.oregeorev.2020.103915.

17 SCHNEBELE (2021): i. m.

18 JOWITT, Simon M. et al.: Recycling of the rare earth elements. Current Opinion in Green and Sustainable Chemistry, Vol. 13, 2018. pp. 1–7., DOI: 10.1016/j.cogsc.2018.02.008.

távon megérheti a szükséges reciklálási, azaz újrahasznosítási innovációba fektetni, hiszen még az európai éllovasok között szereplő Magyarországon is csupán az e-hulladék 51,1%-át hasznosítják újra, miközben az európai átlag csak 40%. A Dolgok Internetének megjelenésével pedig e-hulladékból egyre több lesz, így érdemes az elsődleges, környezetszennyező bányászat helyett a már kibányászott alapanyagok visszanyerésére koncentrálni. Az Európai Unió szabályozási rendszere ebbe az irányba tart, hiszen például az Európai Parlament 2021. február 10-i állásfoglalása a körforgásos gazdaságról szóló új cselekvési tervről vagy a konfliktusövezetből származó ásványokra vonatkozó európai behozatali tilalom – az emberi jogok és a környezetvédelem alapértékeibe csomagoltan – fokozatosan korlátozza a Kína által kontrollált elsődleges alapanyagok importjának lehetőségét.[19] Kérdéses persze, hogy az import korlátozásával párhuzamosan megoldhatóvá válik-e az európai ipar számára szükséges erőforrások megfelelő mennyiségének belpiacon történő előállítása. A megfelelő ellátási lánccal akár olyan sikerek is elérhetők, mint amit az amerikai Apple Termékkörnyezeti Jelentéséből lehet kiolvasni. Eszerint az iPhone 12 okostelefonban található ritkaföldfémek 98%-a újrahasznosított.[20] Ehhez természetesen előfeltétel, hogy az Apple-höz hasonló globális vállalatok jöhessenek létre, amelyek a teljes ellátási láncot kontrollálni tudják. A végfelhasználói piacon erre jelenleg csak az amerikai és a kínai cégek képesek, bár az utóbbiaknál a fenntarthatóság még nem kiemelt szempont.

3. A HARDVERGYÁRTÁS FÖLDRAJZA

A digitális függetlenség következő lépése az, hogy a nyersanyagból alkatrész, majd késztermék legyen. Folytatva az előző gondolatmenetet, a szilíciumból csipet kell gyártani, a lítiumból és a kobaltból akkumulátort, a ritkaföldfémekből pedig többek között szenzort, hangszórót és kijelzőt. Ezek tervezése és gyártástechnológiája viszont nagyon speciális ismereteket kíván meg, nem véletlen tehát, hogy bármelyik alkatrészt is vesszük alapul, jelentős gyártói koncentráció tapasztalható. Ahogy viszont látni fogjuk, mindegyik vizsgált területen az USA és a Kínán kívüli ázsiai országok dominálnak, így az alkatrésztervezés és -gyártás jelenleg sokkal kevésbé függ Kínától, mint ahogy az a híradások alapján talán érződik.

A mikrocsip-, kicsit általánosabban a félvezetőgyártás 15 legnagyobb bevételű vállalata között egyetlen kínai cég sincs. A legnagyobb vállalat az Intel, amelyet a dél-koreai Samsung és a tajvani TSMC követ. A 15 legnagyobb vállalat listáján nyolc amerikai, kettő-kettő dél-koreai, tajvani és európai, valamint egy japán található.[21] Mivel ez a lista a bevételt mutatja, így elsősorban a tervezési és értékesítési képességeket mutatja be. Ha azonban a gyártásra koncentrálunk, azt

[19] Európai Parlament: Elektronikai hulladék az EU-ban: tények és adatok. 2020. december 23. https://www.europarl.europa.eu/news/hu/headlines/society/20201208STO93325/elektronikai-hulladek-az-eu-ban-tenyek-es-adatok-infografika

[20] Apple: Product Environmental Report – iPhone 12. 2020. október 13. https://www.apple.com/environment/pdf/products/iphone/iPhone_12_PER_Oct2020.pdf

[21] FLAHERTY, Nick: Boom quarter for top 10 semiconductor companies. eeNews Europe, 2021. május 25. https://www.eenewseurope.com/news/boom-quarter-top-10-semiconductor-companies

láthatjuk, hogy a világ mikrocsipellátása egy kis szigettől, Tajvantól függ. A világ gyártási kapacitásának 63%-a itt található, 54%-ot pedig egyetlen cég, a TSMC tesz ki ebből. A második helyezett Dél-Korea 18%-kal, amely szinte teljes egészében a Samsungot jelenti. Kína 6%-kal, ezen belül a legnagyobb félvezetőgyártó, az SMIC 5%-kal szerepel. A legnagyobb amerikai gyártó, aki jelentős európai kapacitással is rendelkezik, a GlobalFoundries 7%-kal részesül a globális termelésből.[22]

Nem meglepő tehát, hogy a Covid19 járvány egyik legfontosabb gazdaságpolitikai hozadéka a globális félvezetőhiánnyal való szembesülés után a beszerzési láncok diverzifikálása, illetve a jelenlegi beszerzési források, azaz konkrétan Tajvan védelme. Csiki Varga Tamás és Tálas Péter elemzése a Biden-kormányzat külpolitikai stratégiájáról világosan rámutat Tajvan fontosságára:
„*A Washington és Peking közötti stratégiai versengés leginkább kézzelfogható példája és akut eszkalációs pontja pedig Tajvan, ahol a Biden-adminisztráció a diplomáciai offenzívától Peking provokációján, megszégyenítésén át a katonai erődemonstrációig több eszközzel és a korábban látottaknál nagyobb intenzitással, új minőségben lépett fel a feltartóztatás jegyében*."[23]

A szerzők részletesen nem térnek ki ennek okaira, de megjegyzik, hogy a biztonságpolitikai, nemzetközi kereskedelmi, pénzügyi és fejlesztési szempontok mellett az ellátási láncok védelme és a technológiai versengés is fontos szempont. Egy esetleges Kína és Tajvan közötti konfliktus ugyanis azonnali problémát jelentene a világ gazdaságában, hiszen a félvezetőgyártás több mint fele kiesne. Ennek hatását el lehet képzelni akkor, amikor a pandémia miatt „csak" a nehezebbé vált logisztika és a szórakoztatóelektronikai termékek keresletének bővülése eredményeképpen a magyarországi gépjárműgyárak többször is leálltak, mivel nem tudták időben beszerezni a modern autókhoz nélkülözhetetlen elektronikai alkatrészeket.[24]

A diverzifikálás tehát elkerülhetetlen, ám nem egyszerű és főleg nem olcsó. Csak a tajvani TSMC egyedül több mint 100 milliárd dollárnyi értékű innovációt hajtott végre a saját gyáraiban, így a Samsunggal együtt ketten képesek a legfejlettebb mikrocsipek előállítására. A mikrocsipek gyártástechnológiai mérőszáma a csíkszélesség, amelyet nanométerben mérnek. A TSMC 2018-tól kezdve képes 7 nanométeres, 2020-tól 5 nanométeres gyártásra, és már léteznek 3 nanométeres csipjei is fejlesztési fázisban. A Samsung szintén 2020-ban kezdte el az 5 nanométeres mikrocsipek gyártását. Az Intel eközben 2018 óta tud 10 nanométert, a 7 nanométeres csíkszélességet várhatóan csak 2023-ra éri el.[25] Eközben a kínai

---

22 LEE, Yen Nee: 2 charts show how much the world depends on Taiwan for semiconductors. CNBC, 2021. március 15. https://www.cnbc.com/2021/03/16/2-charts-show-how-much-the-world-depends-on-taiwan-for-semiconductors.html

23 CSIKI VARGA Tamás – TÁLAS Péter: Erő és diplomácia. Az Egyesült Államok stratégiai érdekei és lehetőségei a Biden-kormányzat időszakában. Stratégiai Védelmi Kutatóintézet, 2021. július 27. https://svkk.uni-nke.hu/document/svkk-uni-nke-hu-1506332684763/SVKI_Elemzesek_2021_13_Ero%20es%20diplomacia.pdf

24 hvg.hu: Sorra állnak le világszinten az autógyárak a chiphiány miatt. 2021. szeptember 3. https://hvg.hu/cegauto/20210903_Sorra_allnak_le_vilagszinten_az_autogyarak_a_chiphiany_miatt

25 SUN, Leo: Why Intel's Foundry Plans Don't Make Any Sense. The Motley Fool, 2021. május 3. https://www.fool.com/investing/2021/05/03/why-intel-foundry-plans-dont-make-any-sense/

SMIC célja, hogy mintegy 9 milliárd dolláros beruházással létrehozzanak egy olyan gyárat, amely képes lesz a 12 nanométeres csíkszélesség gyártására.[26] Ez a cég egyébként szerepel a legfrissebb amerikai tiltólistán, így a beruházást amerikai technológia nélkül kell elvégeznie.[27] Az európai képességek jelenleg a 16 nanométeres gyártást teszik lehetővé, de a Processzorok és Félvezető Technológiák Szövetségének célja minél előbb 10 nanométer alá jutni, hosszú távon pedig a 2-5 nanométert célozták meg.[28] Hozzá kell tenni, hogy a legtöbb eszköz nem igényli az ilyen kis csíkszélességet, tehát van haszna az olcsóbb, de kevésbé fejlett technológiába történő befektetésnek is.

A lítium-ion akkumulátorok piacán szintén ázsiai fölényt tapasztalhatunk, de szintén nem Kínában összpontosul a gyártás. Sőt, ez az a terület, ahol Európa időben lépett, és elsősorban a fejlett autóiparának köszönhetően, sikerrel veheti fel a versenyt ázsiai versenytársaival. Legalábbis a gyártási kapacitásokat illetően, ugyanis a legnagyobb gyártók között egyetlen európai sincsen, csak a gyárakat telepítik hatalmas ütemben Európába, ahogy az történik az SK Innovation nevű dél-koreai vállalat esetében is, amely Dunaújváros mellett, Iváncsán építi fel Magyarország történetének legnagyobb zöldmezős beruházása keretében azt a gyártóbázisát, amely nagyságrendileg akkora lesz, mint a világ jelenlegi legnagyobbja, a Tesla Gigafactory az USA-ban.[29] Ez utóbbi gyárnak is köszönhetően egyébként az egyik legnagyobb gyártó jelenleg az amerikai Tesla és a technológiát szállító japán Panasonic, akik mellett a dél-koreai LG Chem és Samsung SDI, valamint a kínai CATL és BYD számít a legfontosabb szereplőnek.[30]

Elsősorban az autógyártásnak és a zöld forradalomnak köszönhetően tehát dinamikusan növekszik a lítium-ion akkumulátorok gyártása, előrejelzések szerint a jelenlegi 500 GWh teljesítményhez képest 2030-ban már 3.000 GWh összteljesítményt tudnak a vállalatok forgalomba hozni. Jelenleg Kína ebből 72,5%-kal, Európa 5,4%-kal, Észak-Amerika pedig 9,2%-kal részesül, de az előrejelzés szerint a 2030-as évre Kína részesedése 66,9%-ra csökken, míg Európa 16,7%, az USA pedig 11,9%-ot tudhat majd magáénak. Ennek érdekében pedig jelentős gazdaságpolitikai lépések is történnek, hiszen, ahogy a magyar kormány is támogatta az SK Innovation beruházását, a svéd NorthVolt Németországban, a francia SAFT pedig Franciaországban tervez komoly fejlesztést kormányuk bátorításával.[31] Az Egyesült Államokban egy elnöki rendelet nyomán végzett

---

26 HONG, Iris: SMIC spending $9 bn to build China's most-advanced wafer plant. Asia Financial, 2021. február 9. https://www.asiafinancial.com/smic-spending-9-bn-to-build-chinas-most-advanced-wafer-plant

27 The White House: Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China. 2021. június 3.

28 European Commission (2021a)

29 HIPA: SK Innovation - Minden idők legnagyobb zöldmezős beruházása Iváncsán. 2021. január 29. https://hipa.hu/giga-beruhazast-indit-az-sk-innovation-minden-idok-legnagyobb-zoldmezos-beruhazasa-ivancsan

30 ULRICH, Lawrence: The Top 10 EV Battery Makers. IEEE Spectrum, 2021. augusztus 25. https://spectrum.ieee.org/the-top-10-ev-battery-makers

31 MOORES, Simon: The Global Battery Arms Race: Lithium-Ion Battery Gigafactories and Their Supply Chain. The Oxford Institute of Energy Studies, 2021. február https://www.oxfordenergy.org/wpcms/wp-content/uploads/2021/02/THE-GLOBAL-BATTERY-ARMS-RACE-LITHIUM-ION-BATTERY-GIGAFACTORIES-AND-THEIR-SUPPLY-CHAIN.pdf

felmérés eredményeképpen vált stratégiai beavatkozási területté a gyártási kapacitás fejlesztése.[32]

Az elektronikai termékek végül az összeszerelő üzemekben nyerik el végső formájukat. A megbízásra dolgozó vállalatok piacának összefoglaló neve electronic manufacturing services (EMS), a legnagyobb 50 vállalat bevételének 90%-a pedig Ázsiában keletkezik. Közülük is a legnagyobb a tajvani bázisú Foxconn, amelynek legnagyobb gyárai Kínában vannak. Ezekben állítják össze a legismertebb márkák termékeit, mint például az Apple iPhone telefonját is. Fontos szereplők még a szintén tajvani Pegatron, Wistron, New Kinpo Group, az amerikai Jabil, Sanmina, az amerikai-szingapúri Flex, a kínai BYD Electronics, USI és a kanadai Celestica.[33] E vállalatok közül többnek is van magyarországi érdekeltsége, illetve a Videoton európai szinten is az egyik legnagyobb összeszerelő üzemmel rendelkezik. Ezen a területen már kevésbé szükséges a szellemi tőke megléte, az üzemek jellemzően ott jönnek létre, ahol a legolcsóbban lehet gyártani, így a kínai munkabérek emelkedésével elkezdődött az üzemek átszivárgása olyan más ázsiai országokba, mint Vietnám, Indonézia vagy Thaiföld. Mint azt Magyarországon többször is meg lehetett tapasztalni, az ilyen gyárakat aránylag könnyen át lehet költöztetni más országokba, így a stratégiai függőség szempontjából kevésbé fontosak.[34] Igaz, a logisztikai problémák jelentős fennakadást tudnak okozni akkor is, ha nem Kínából, hanem más ázsiai országból érkeznek az áruk, mint ahogy azt meg lehetett tapasztalni akkor, amikor az Ever Given teherhajó eltorlaszolta a Szuezi-csatornát 2021 májusában. Éppen ezért aggasztó Kína tevékenysége a Dél-kínai-tengeren, illetve a Malaka-szoros biztonsága, hiszen, ha ezt a hajózási szakaszt lezárják, az összeszerelt késztermékek nem, vagy csak hosszabb idő után tudnak eljutni Európába.

4. SZOFTVEREK, ADATOK, FELHŐ

A Dolgok Internetének alapját a hardverelemek adják, amelyek tehát – akár az alkatrészek, akár a végtermékek eredetét vizsgáljuk – elsősorban ázsiai, ezen belül is főként tajvani bázisú gyártóktól érkeznek. Ám ezek mit sem érnek, ha nincs olyan szoftveres ökoszisztéma, ami lehetővé teszi a működésüket, és ha nincsen olyan hálózati kapcsolat, amely a Dolgok Internetét becsatornázza a valódi internet felé. Ezek hiányában nem válik lehetővé a negyedik ipari forradalom legfontosabb alapja, és nem lehet a gépek által létrehozott digitális adatokat megfelelően feldolgozni a felhőben. Ezt a láncolatot végigkövetve pedig arra jutunk, hogy a kulcsfontosságú területeken szinte teljes az amerikai dominancia.

---

32 Department of Energy: DOE Announces Actions to Bolster Domestic Supply Chain of Advanced Batteries. 2021. június 8. https://www.energy.gov/articles/doe-announces-actions-bolster-domestic-supply-chain-advanced-batteries

33 CLARKE, Peter: Top ten EMS contract manufacturers boost revenues in 2020. eeNews Europe, 2021. április 16. https://www.eenewseurope.com/news/top-ten-ems-contract-manufacturers-boost-revenues-2020

34 Mordor Intelligence: Electronics Manufacturing Services Market - Growth, Trends, Covid-19 Impact, and Forecasts (2021-2026). 2021 https://www.mordorintelligence.com/industry-reports/electronics-manufacturing-services-market

Azt talán minden végfelhasználó tudja, hogy a hardverek működését az operációs rendszerek teszik lehetővé. A számítógépek világában ezek jellemzően a Microsoft Windows, a nyílt forráskódú, ezért számtalan formában létező Linux és a piaci szegmensét tekintve alig használt, mégis nagy presztízsű Apple macOS. Az okostelefonok, tabletek esetében a Google Android és az Apple iOS a legnépszerűbb. Az egyéb okoseszközök tipikusan valamilyen Linux verzióra épülnek, az ipari folyamatirányítási rendszerek pedig jellemzően Windows vagy Linux alapúak. Természetesen vannak ettől eltérő megoldások is, de ezek marginálisan vannak csak jelen. A felsorolt szoftverek gyártói közül a Microsoft, az Apple és a Google amerikai, a Linux pedig közösségi fejlesztésű, ám az alapját jelentő kernelt viszont még mindig első programozója, a finn–amerikai Linus Torvalds végső engedélyével lehet csak módosítani. Jól illusztrálja azt, hogy ez a helyzet mennyire előnyös az amerikai kormányzat számára, hogy miután 2019-ben megtiltották a Google számára az Android licencének átadását a kínai Huawei számára, az kénytelen volt saját operációs rendszerrel előállni. Ez volt a Harmony OS, amelynek piaci részesedése mérhetetlen, a felhasználók pedig széles körben elutasították a használatát. Ez olyan mértékű csapás volt a Huawei számára, hogy a Honor nevű okostelefonos márkáját kénytelen volt eladni egy, az anyavállalattól független, kormányzati hátterű cégnek annak érdekében, hogy túléljen a piacon. Miután ez megtörtént, visszakapták az Android licencengedélyét, ami jól mutatja az amerikai szoftverek megkerülhetetlenségét.[35]

A XX. század végén, az internet hajnalán az operációs rendszerek feladata a felhasználói szoftverek futtatása volt. Számos megkerülhetetlennek tűnő, hatalmas szoftverfejlesztő konglomerátum alakult ki, amelyek az ezredforduló internetboomjának idején sok esetben teljesen eljelentéktelenedtek, helyüket az új, dinamikus, elsősorban adatokra épülő digitális szolgáltatást építő vállalkozások vették át. 20 évvel a forradalom után érdekes összevetni a hagyományos szoftverek és az adatokra építő vállalatok közötti különbséget. A 2020-as év bevételi adatai alapján a legnagyobb hagyományos szoftvercég a Microsoft, 118,2 milliárd dolláros bevétellel, 946 milliárd dolláros piaci kapitalizációval. Az utána következő, második helyezett, szintén amerikai Oracle cég már „csak” 39,6 milliárd dollár bevétellel és 186 milliárd dolláros kapitalizációval rendelkezik. A Top10-es listán egyébként 8 amerikai, egy francia és egy német cég szerepel, és a legtöbben pénzügyi, vállalatirányítási szoftverek fejlesztésével foglalkoznak.[36] Eközben a világ legértékesebb cégeinek listáját az Apple vezeti, a fejezet írásának időpontjában 2.550 milliárd dolláros piaci kapitalizációval, utána következik a Microsoft 2.263 milliárd dollárral (több mint kétszeres értékkel, mint 2020-ban), majd az Alphabet, azaz a Google van a harmadik helyen, 1.924 milliárd dollárral. Az első, nem technológiai cég a listán a Saudi Aramco olajvállalat, értéke 1.870 milliárd dollár. A 20 legértékesebb cég közül 11 kötődik a digitális világhoz, ebből kettő kínai.[37,38]

---

35 PORTER, Jon: Honor confirms Google’s apps will return to its phones with new 50 series. The Verge, 2021. június 16. https://www.theverge.com/2021/6/16/22536512/honor-50-series-pro-release-date-news-features-google-mobile-services-apps-play-store

36 Bizwibe: Top 10 Largest Software Companies in the World by Revenue 2020, Software Industry Factsheet. 2020. április 8. https://blog.bizvibe.com/blog/top-software-companies

37 CompaniesMarketCap.com: Largest Companies by Market Cap. 2021. szeptember 4. (aznapi állapot) https://companiesmarketcap.com/

38 A gyűjteményes kötet megírásának idején a háborús helyzet jelentős felfordulást okozott a tőzsdén, de a legnagyobb vállalatok köre érdemben nem változott.

Jól mutatja a világ félvezetőéhségét, hogy e vállalatok közül négy a mikroelektronikai gyártás világából érkezett. Ez azonban valószínűleg csak szezonális kilengés, az adatokkal és a felhőinfrastruktúrák üzemeltetésével foglalkozó vállalatok viszont kitartóan, évek óta őrzik helyüket a legértékesebb vállalatok listáján. Az Apple, a Microsoft, a Google és az Amazon birtokolja a világ felhő-számítástechnikai kapacitásának jelentős részét, a Google, az Amazon és a Facebook pedig a digitális adatok legnagyobb tárházával rendelkezik. A Tencent és az Alibaba kínai vállalatként szintén elsősorban az adatokra és a felhőre építik szolgáltatásukat. Az Ipari Adat, Peremhálózat és Felhő Európai Szövetsége létrehozásának indokolásában az Európai Bizottság ki is emelte, hogy jelenleg a felhőszolgáltatások bevételének kevesebb, mint 1%-a kerül európai szolgáltatókhoz, azok gyakorlatilag mérhetetlenek a piacon.[39]

Az adatok átvitele a felhőbe és az ott történő új tudás előállítása még két technológia említését kívánja meg. Ezek az 5G, azaz az ötödik generációs mobiltávközlés és a mesterséges intelligencia, amelyek kiemelt szerepét Magyarország 2020-ban kiadott Nemzeti Biztonsági Stratégiája is megemlíti: „*A hatalmi vetélkedés mindinkább kiterjed a globális közjavakra is: fokozódó küzdelem folyik a nemzetközi vizek és az ott található erőforrások, az északi sarkvidék és a világűr ellenőrzéséért, valamint a kibertér dominanciájáért. Az emberiség technológiai szintjének rohamos fejlődésével [digitalizáció, ötödik generációs vezeték nélküli hálózat (5G), űrtechnológia, stb.] folyamatosan új lehetőségek és kihívások jelennek meg, amelyek hatást gyakorolnak hazánk biztonságára. Az 5G jelentette technológia olyan forradalmi fejlesztéseket tehet lehetővé perspektivikusan, amelyek számottevő változásokat generálhatnak társadalmunk és gazdaságunk viszonylatában.*”, illetve *„A forradalmi technológiák fejlesztése stratégiai fontosságú kérdés. Hazánk biztonsága megkívánja, hogy a kulcsfontosságú területeken – mint például a kibervédelem, a mesterséges intelligencia, az autonóm rendszerek, a biotechnológia – kiemelt figyelmet fordítsunk a kutatás-fejlesztésre és annak védelmi összetevőjére.”*[40].

Az amerikai–kínai technológiai verseny leginkább látható konfrontációja is az adat–5G–mesterséges intelligencia háromszögben mutatkozik. Az 5G ugyanis a Dolgok Internetének „autópályája”, az az alapinfrastruktúra, melyre a digitális gazdaság épülni tud. A mesterséges intelligencia működésének alapja pedig az adat. Aki tehát birtokolja ezt a három technológiát, az uralja a negyedik ipari forradalmat. A nemzetközi diplomáciában ezért az USA kormánya a legjelentősebb nyomást a kínai 5G vállalatok kiszorítására helyezte. Konkrétan a Huawei és a ZTE vállalatok ellehetetlenítése a cél a nemzetbiztonságot veszélyeztető gyakorlatuk miatt.[41] Ennek a gyanúsításnak a pontos részleteit nem osztották meg a közvéleménnyel, de számos szövetséges ország csatlakozott a kínai 5G technológia tiltásához, ezzel igyekezve elzárni a kínai kormányt attól, hogy a következő évtizedekben befolyásolni tudja a

[39] European Commission: In-depth reviews of strategic areas for Europe’s interests. 2021. május 5. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy/depth-reviews-strategic-areas-europes-interests_en#semiconductors

[40] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

[41] SHEPARDSON, David: U.S. FCC votes to advance proposed ban on Huawei, ZTE gear. Reuters, 2021. június 18. https://www.reuters.com/technology/us-fcc-votes-launch-further-crackdown-huawei-zte-equipment-2021-06-17/

modern gazdaságokat. Kevésbé látható módon, de a mesterséges intelligenciát érintő technológiák esetében a két ország kölcsönösen exportkorlátozást vezetett be, jelenleg pedig aktívan folyik a mesterséges intelligencia felhasználásának szabályozása is.[42] Az adataggregátor cégek esetében valódi függés nem mutatható ki a két ország között, hiszen az olyan amerikai szolgáltatások, mint a Google keresőmotorja vagy a Facebook közösségi oldala nem rendelkeznek valós kínai jelenléttel, mint ahogy a Baidu keresőfelületét vagy a WeChat közösségi hálózatát sem igazán használják Kínán és a kínai nemzetiségű embereken kívül. A kínai ByteDance TikTok nevű közösségi szolgáltatása viszont elkezdett terjedni Nyugaton is, illetve a Tencent és az Alibaba megoldásait is széles körben használják, így Trump elnök időszakában komolyan felmerült ezen vállalatok tiltólistára tétele.[43]

5. AZ USA ÉS KÍNA TECHNOLÓGIAI VERSENYE BUDAPESTRŐL NÉZVE

Magyarország külgazdasági mutatóit böngészve látható, hogy Kína Németország után a legfontosabb partner a behozatal szempontjából. Ez nem meglepő, tudva, hogy a magyar gazdaság számára fontos alapanyagok forrása elsősorban Kína. A kivitelt tekintve viszont erős passzívum mutatkozik (7.926,6 millió euró import és 1.813,5 millió euró export), a Kína irányába történő export volumenét számos európai országé is megelőzi. Az Egyesült Államok tekintetében eközben pozitív a mérleg, 2.042,7 millió euró import mellett 3.133 millió euró export mutatkozott 2020-ban. Németország, a legjelentősebb kereskedelmi partner mellett eközben 24.372,9 millió euró import és 29.253,7 millió euró export szerepel.[44]

A puszta számok tehát azt mutatják, hogy az Egyesült Államok kevésbé fontos kereskedelmi partnere Magyarországnak, érdemes inkább a kínai lehetőségeket vizsgálni. Ha azonban az ellátásbiztonsági és nemzetbiztonsági kérdések szempontjából vizsgáljuk a kérdést, lényegesen bonyolultabb képet kapunk. Technológiai szempontból ugyanis Magyarország sokkal inkább kitett az amerikai digitális termékeknek és szolgáltatásoknak, ráadásul a szövetségi rendszerünkből és nyugati orientációnkból adódóan lényegesen több a bizalom és az ismeret az amerikai megoldások irányába, illetve több az ismeret azokról. Az alábbiakban tételesen áttekintjük és elemezzük a korábban vizsgált területeket, Magyarország biztonságának szemszögéből, figyelembe véve az európai stratégiákat.

5.1. A nyersanyagok kérdése

Az Európai Unió listáján 30 olyan nyersanyag szerepel, amely kritikus a gazdaság szempontjából. Ezen minden korábban említett anyag, így a szilícium, a

[42] Reuters: U.S. government limits exports of artificial intelligence software. 2020. január 3. https://www.reuters.com/article/us-usa-artificial-intelligence-idUSKBN1Z21PT

[43] ALPER, Alexandra – PAMUK, Humeyra: Trump administration shelves planned investment ban on Alibaba, Tencent, Baidu: sources. Reuters, 2021. január 13. https://www.reuters.com/article/us-usa-trump-china-tech-idUSKBN29I2RW

[44] Központi Statisztikai Hivatal: 17.1.1.8. A külkereskedelmi termékforgalom értéke euróban és értékindexei a fontosabb országok szerint [folyó áron]. https://www.ksh.hu/stadat_files/kkr/hu/kkr0008.html

ritkaföldfémek, a kobalt és a lítium is szerepel.[45] Azonban miközben az ipar igénye exponenciálisan nő, a ritkaföldfémek EU-s forrása 98%-ban Kína, a kobalt globális exportjának 70%-a pedig korlátozások alá esik, például az emberi jogi visszaélések miatt. Az ipar igénye eközben exponenciálisan nő. A témával a Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Reziliencia a kritikus fontosságú nyersanyagok terén: a nagyobb biztonsághoz és fenntarthatósághoz vezető út feltérképezése című dokumentum foglalkozik, amely 10 lépésből álló intézkedési tervet határoz meg.

Magyarország számára a gyártáshoz szükséges nyersanyagok beszerzése elsősorban az akkumulátorok területén fontos, hiszen erre jelentős gyártási kapacitás épül hazánkban. Kitettségünk csökkentése érdekében számos lépést lehet tenni az európai intézkedések támogatása érdekében:

- A 3. intézkedés szerint el kell indítani a kritikus fontosságú nyersanyagokkal kapcsolatos kutatást és innovációt 2021-ben a hulladékfeldolgozás, a fejlett anyagok és a helyettesítés területén, az Európai horizont keretprogramra, az Európai Regionális Fejlesztési Alapra és a nemzeti kutatási és innovációs programokra támaszkodva. Mivel Magyarországon igen magas az e-hulladék újrafeldolgozásának aránya, érdemes ezt a lehetőséget kihasználni.
- A 4. intézkedés szerint feladat az EU-ban található készletekből és hulladékokból kinyerhető másodlagos kritikus fontosságú nyersanyagok potenciális készletének feltérképezése és életképes hasznosítási projektek azonosítása 2022-ig. Itt érdemes a magyarországi ritkaföldfémek kinyerésének lehetőségeit felmérni.
- A 6. intézkedés felhívja a figyelmet a bányászati, kitermelési és feldolgozási technológiákkal kapcsolatos szakértelem és készségek továbbfejlesztésére 2022-től az átalakulóban lévő régiókban a kiegyensúlyozott átmeneti stratégia részeként. Mivel Magyarországon évszázados hagyománya van a bányászati felsőoktatásnak, érdemes lehet célzottan szakot, szakirányt indítani a ritkaföldfémek kinyerésével kapcsolatos tudás átadására, illetve fejleszteni az újrahasznosításhoz kapcsolódó képzéseket.[46]

E lehetőségek közül a hulladék újrahasznosítás szerepel a Nemzeti Intelligens Szakosodási Stratégia (S3[47]) – 2021-2027 tervben. Az erőforráshatékony gazdaságprioritás szerint cél *„a környezeti terhelés mérséklése érdekében a körforgásos gazdaság erősítését, a hulladékminimalizálást célzó KFI tevékenység erősítése és az ilyen irányú innovációk terjedésének erősítése és jó gyakorlatok*

[45] European Commission: Critical raw materials. 2020 https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials_en

[46] Európai Bizottság: Reziliencia a kritikus fontosságú nyersanyagok terén: a nagyobb biztonsághoz és fenntarthatósághoz vezető út feltérképezése. 2020. szeptember 3. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020DC0474&from=EN

[47] A Smart Specialization Strategy angol megnevezésből adódó rövidítés.

adaptációja."[48] Ki kell emelni, hogy a nyersanyagok tekintetében ez nem csak a környezeti terhelés csökkentése, hanem az ellátásbiztonság érdekében is fontos. A bányászati képességek erősítése nem szerepel a prioritások között, így ezt érdemes intézményi szinten fejleszteni, az érintett egyetemek nemzetközi innovációs projektben való részvételével.

5.2. A hardvergyártás lehetőségei

A Processzorok és Félvezető Technológiák Szövetségének létrehozása világosan mutatja, hogy az európai szándék a saját félvezetőgyártási képesség (újra)felépítése. A TSMC és a SMIC korábban említett példája azonban azt mutatja, hogy ez több milliárd eurós beruházást jelent. Ráadásul nincsen meg az a tudás, amivel ezt a képességet létre lehetne hozni, hiszen azok az európaiak, akik a tudás birtokában vannak, nyilvánvalóan azoknál az amerikai vállalatoknál dolgoznak, ahol a legújabb technológiákat használják. Az Európai Unió tehát elsősorban a képességfejlesztés irányába tesz lépéseket. Törekszik az elvesztett tudás megszerzésére, olyan vállalatok felvásárlására, ahol a know-how elérhető, illetve az ellátási láncok biztosítására.[49]

A lítium-ion akkumulátorok esetében a cél elsősorban az alapanyagokhoz való biztosabb hozzáférés és a gyártási képességek fejlesztése. Az Európai Akkumulátor Szövetség 2017-ben alakult, több mint 600 tagja van. A magyar részvétel marginális, összesen 3 magyar vállalat vesz részt a munkában, viszont egyetlen kínai cég sem tagja a szövetségnek. Európában csak 2019-ben 60 milliárd eurót fektettek az elektromobilitásba, ami háromszorosa a kínai befektetéseknek. Az Európai horizont keretprogramban 1 milliárd eurót terveznek kutatás-fejlesztésre fordítani. Talán ezen a területen vannak a legjobb esélyek arra, hogy az európai tudás vezetővé válik.

Az összeszerelés kérdését az Európai Unió nem említi stratégiai függőségi kérdésként. Európában, így Magyarországon ugyanis számos összeszerelő üzem települt, amelyeket a pandémia okozta ellátásilánc-zavar után nem valószínű, hogy a felszámolás veszélye fenyeget. Észre kell azonban venni, hogy a modern összeszerelés-technológiával kapcsolatos tudás megszerzése a magyar gazdaság számára kulcsfontosságú. Ezért törekedni kell az európai szintű képzésekre. Emellett – összhangban a Nemzeti Intelligens Szakosodási Stratégiával – támogatni kell az új típusú anyagok és gyártástechnológiák területén történő kutatásokat. Ez a tudás reálisan európai együttműködésben szerezhető meg, összhangban az európai fejlesztési törekvésekkel.

Magyarország gazdaságának egyik legfontosabb forrása az összeszerelés, amely közvetlenül az itt megtelepedett elektronikai összeszerelő üzemeken keresztül, és közvetve például a gépjárműgyártók mikrocsip-felhasználása miatt is erősen függ a kínai–amerikai vitáktól, de elsősorban Tajvan függetlenségének kérdésétől, másodsorban pedig Dél-Korea helyzetétől. Mivel mindkét ország biztonsága nagyban függ az Egyesült Államok támogatásától, nem lehet figyelmen

[48] Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal: Nemzeti Intelligens Szakosodási Stratégia (S3) – 2021-2027. 2021. július 26. https://nkfih.gov.hu/hivatalrol/nemzeti-intelligens/nemzeti-intelligens-szakosodasi-strategia-2021-2027

[49] European Commission (2021b)

kívül hagyni a térségbeli amerikai ténykedést és a szövetségesi felkéréseket. Eközben ezen a területen eközben Magyarország Kína felé történő kitettsége jóval alacsonyabb, ezen a területen nem is igazán lehet a másik két ázsiai országhoz hasonló nagybefektetést felmutatni. Emellett meg kell jegyezni, hogy bár a sokat vitatott Fudan Egyetemmel kapcsolatos híradások szerint természettudományos és mérnöki karok is kerülhetnének Magyarországra, technológiai szempontból jelenleg nincsen olyan bázis hazánkban, ahol az ott tanított tudás a gyakorlatban hasznosítható lenne.

5.3. Adatgazdaság Magyarországon, a két nagyhatalom között

A negyedik ipari forradalom szemszögéből a legérdekesebb, egyben legfontosabb stratégiai kérdés, hogy kié lesz az adatokból származó információ, illetve az abból nyert tudás. Az Egyesült Államok szempontjából a helyzet azért aggasztó, mert míg korábban egyértelműen az amerikai technológiai cégek uralták ezt a területet, a 2010-es években a kínai versenytársak olcsóbb és nem egyszer jobb minőségű termékekkel és szolgáltatásokkal álltak elő – nem ritkán az amerikai szellemi tulajdon megsértésének árán. Leegyszerűsítve, a két nagyhatalom szempontjából a kérdés az, hogy ki uralja az átviteli hálózatokat, kié a felhő, és ki tudja a legjobban kihasználni a mesterséges intelligenciát. Nem véletlen, hogy a leglátványosabb politikai küzdelem a kínai 5G szereplők kiszorítása és az amerikai adataggregátor cégek megregulázásának területén mutatkozik.[50] A felhő talán kevésbé van a látótérben, köszönhetően annak, hogy éppen egy új technológiai irányzat, az ún. peremfelhő (edge cloud) áttörését láthatjuk, mely az eddig ismert nagy (elsősorban amerikai) adatközpontok helyett a szervezeteken belül tartja az adatokat.

Az Európai Bizottság számítása szerint a generált adatok 80%-a 2025-re ilyen peremfelhőben kerül majd feldolgozásra, itt pedig jelenleg nincsenek domináns vállalatok. A Bizottság a peremfelhők mellett komoly lehetőséget lát a szoftveres szolgáltatások területén is, illetve a hibrid, különböző gyártók által szállított és épített 5G hálózatok is biztosíthatják a stratégiai függetlenséget. Ehhez viszont jelentősen növelni kell a beruházásokat, hiszen egyrészt az EU-ban évente 11 milliárd euróval kevesebb beruházás történik a felhőtechnológiába, mint az USA-ban vagy Kínában, másrészt eleve kevésbé használják ezt a technológiát az európai vállalatok, főleg a konzervatív fejlesztési mentalitás és a bizalmatlanság miatt. Az Ipari Adat, Peremhálózat és Felhő Európai Szövetségének megalapításával ez a helyzet változhat, de jelentős lemaradást kell pótolni, amely azonban talán egyszerűbb, mint a korábban felvázolt, földrajzi adottságokból eredő kihívások kezelése.[51]

Ez a terület Magyarország stratégiáiban hangsúlyos szerepet kap. A Nemzeti Intelligens Szakosodási Stratégia három részterülete (Gazdaság digitalizációja prioritás, Szolgáltatások prioritás, Kreatív ipar prioritás) is foglalkozik azokkal a felvetett problémákkal, amelyeket az EU is azonosított. Magyarország Nemzeti Biztonsági Stratégiája megemlíti az 5G és a mesterséges intelligencia jelentette

[50] BOROS Szilárd – KOLOZSI Pál Péter: Egy 21. századi geopolitikai összeütközés természetrajza Kína és az USA példáján keresztül. Polgári Szemle, 2019/4-6. pp. 258-280., DOI: 10.24307/psz.2019.1217

[51] European Commission (2021b)

kihívásokat. A kormány a Digitális Jólét Programon belül kiemelten foglalkozik az adatvagyonnal, az 5G-vel és a mesterséges intelligenciával. Ezek jellemzően a saját képességek fejlesztését hangsúlyozzák, összhangban az európai lépésekkel. Az ország eközben úgy függ az amerikai és kínai megoldásoktól, hogy valójában kiváló saját lehetőségekkel is rendelkezik.

Először is, Magyarország digitális adatvagyona jelentős, de többnyire kihasználatlan. Az állampolgárok által előállított digitális adatok elsődleges haszonélvezői jelenleg az amerikai adataggregátor cégek – csakúgy, mint Európa más országaiban. A hazai adatpiac kialakítása tehát gazdaságilag és a digitális autonómia szempontjából is kiemelten fontos. Az 5G hálózatok fejlesztése külföldi (német, brit, cseh) vállalatok kezében van, a felhasznált alaptechnológiák jellemzően kínaiak (Huawei és ZTE), de eközben jelen vannak az európai megoldások is (Ericsson, Nokia). Míg a Huaweinek „csak" az elsődleges európai gyártóközpontja van Magyarországon, az európai gyártók kutatás-fejlesztési központokkal is rendelkeznek hazánkban, így lényegesen magasabb hozzáadott értéket jelentenek a magyar gazdaság számára. A felhőszolgáltatások területén európai szinten is alacsony a magyar felhasználás, jelentős felhőkapacitások sincsenek az országban. Viszont számos olyan szoftveres szolgáltatóközpont (Shared Service Center – SSC) települt meg Magyarországon, amelyeket továbbfejlesztve részt tudunk venni a peremfelhők előretörésében. A mesterséges intelligencia esetében hasonló a helyzet. Érdemi képességekkel az ország nem rendelkezik, de az egykor világszintű matematikaoktatás romjain még mindig kiváló az adattudománnyal foglalkozó oktatásunk, így számos amerikai, adattal és mesterséges intelligenciával foglalkozó cég üzemeltet fejlesztőközpontokat Magyarországon, építve erre a szellemi tőkére.

6. KÖVETKEZTETÉSEK

Ha pusztán a stratégiai függőség szempontjából vizsgáljuk Magyarország helyzetét a kínai–amerikai küzdelemben, nem lehet kérdés, hogy kitől függ hazánk kibertere. Az alapanyagok kivételével a hardveres és szoftveres technológiák jelentős része amerikai tudásra épül, gyártástechnológiájuk pedig az USA-val szövetséges ázsiai országokból ered. Nem lehet elvitatni Kína jelentős előretörését a digitális technológiák világában, de az 5G kivételével – ahol jelentős, Magyarországon is jelenlevő európai gyártók is vannak – nem érzékelhető valós kínai részvétel sem hazánkban, sem Európában. Ha figyelembe vesszük az Egyesült Államok korlátozó intézkedéseit és az Európai Unió saját intézkedéseit, nem is valószínű, hogy a következő évtizedben ezen a területen jelentős változás állna be.

Felmerülhet a kérdés, hogy érdekében áll-e Magyarországnak kínai technológiával csökkenteni az amerikaiakkal szembeni technológiai függésünket. Ha azokat a példákat vizsgáljuk, amikor ez megtörtént – például a HIKVision megoldások a közterületi megfigyelésben, Huawei eszközök az országos segélyhívó rendszerben és az országos 5G hálózatokban –, gyakorlatilag kivétel nélkül olyan cégekkel találkozhatunk, akikkel szemben az USA embargót rendelt el, így fejlesztéseik során nem építhetnek az amerikai tudástőkére. Emellett rendszeresen felmerülnek nemzetbiztonsági aggályok is, legalábbis a hazai sajtó és az amerikai diplomácia erősen artikulálja ezeket a feltételezéseket.

Természetesen miért ne lehetne kínai megoldásokkal dolgozni, ha azok „olcsóbbak és jobbak”? Mivel a digitális technológia igen innovációigényes, így rendkívül nagy befektetések szükségesek, és egyre kevésbé lesz fenntartható az a kínai modell, hogy a termék egyszerre olcsó és jó is legyen. Az olcsóság előfeltétele nagyon sokáig az volt, hogy az alaptechnológiákat a kínai nagyvállalatok jogilag igen kérdéses megoldásokkal szerezték meg, nem feltétlenül tisztelve a szellemi tulajdont, illetve sokszor embertelen körülmények között, igen alacsony bérrel dolgoztak a munkavállalók a gyárakban. Eközben a legjobb kínai elmék amerikai egyetemeken pallérozódtak, és ez nem került a kínai oktatásnak pénzbe. A 2010-es évek közepére nyilvánvalóvá vált, hogy a három feltétel egyike sem tartható tovább. A szellemi tulajdon védelme kiemelt fontosságúvá vált, a kínai bérek emelkednek, a kínai egyetemek pedig saját jogon is innoválnak. Az árak pedig mindennek következtében emelkednek.

De vajon „jobbak” lesznek-e a kínai termékek, mint az amerikaiak? Ezt mindig a piac dönti el, a digitális technológiák piacát pedig jellemzően olyan szempontok befolyásolják, mint a kínai cégek által kevésbé jól használt marketing. Az USA, ezen belül is a Szilícium-völgy még nagyon sokáig fog rendelkezni két olyan képességgel, amivel Kína és Sencsen nem tudja felvenni a versenyt. Az egyik a multikulturális, kreatív közeg, amelyet más szempontból nevezhetünk sikeres agyelszívásnak is, a másik pedig a tőke rugalmas rendelkezésre állása, azaz a kapitalizmus maga. A kínai kultúra és politikai berendezkedés még hosszú ideig nem lesz alkalmas arra, hogy ezeket – az innováció szempontjából roppant fontos paramétereket – képes legyen reprodukálni. Korai tehát a nyugati technológiai fölény hanyatlását vizionálni és a keleti technológia fölényére tenni – ahogy ez igaz minden más szempontra is az amerikai–kínai versenyben.[52,53]

[52] GYŐRFFY Dóra: Amerika vagy Kína hanyatlik? In: ÁGH, Attila (szerk.): Az új világrend kialakulása – Az EU–USA–Kína hatalmi háromszög. Budapest, Magyarország: Noran Libro (2021) pp. 145–167., 23 p.

[53] Ezek a következtetések természetesen nem csak Magyarországra igazak. Az orosz–ukrán háború egyik hozadéka, hogy Oroszország soha korábban nem látott szankciókkal kénytelen szembesülni, mely a modern technológiához való hozzáférést is akadályozza. A kötet szerkesztésének idején még tart a háború, így korai messzemenő következtetéseket tenni, de valószínű, hogy mivel Oroszországban nincsen semmilyen érdemi képesség a XXI. század technológiájának gyártására, a szankciók fenntartása évtizedekkel veti vissza az ország fejlettségét. A digitális autonómiatörekvéseket így célszerű ebben a kontextusban is figyelemmel kísérni!

Felhasznált irodalom:

- Központi Statisztikai Hivatal: 17.1.1.8. A külkereskedelmi termékforgalom értéke euróban és értékindexei a fontosabb országok szerint [folyó áron]. https://www.ksh.hu/stadat_files/kkr/hu/kkr0008.html
- 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
- ALPER, Alexandra – PAMUK, Humeyra: Trump administration shelves planned investment ban on Alibaba, Tencent, Baidu: sources. Reuters, 2021. január 13. https://www.reuters.com/article/us-usa-trump-china-tech-idUSKBN29I2RW
- Apple: Product Environmental Report – iPhone 12. 2020. október 13. https://www.apple.com/environment/pdf/products/iphone/iPhone_12_PER_Oct2020.pdf
- BIHARI Katalin: Kína növekvő befolyása a világgazdaságban. Pro Publico Bono – Magyar közigazgatás, 2020/4. pp. 26-35., DOI: 10.32575/ppb.2020.4.3
- Bizwibe: Top 10 Largest Software Companies in the World by Revenue 2020, Software Industry Factsheet. 2020. április 8. https://blog.bizvibe.com/blog/top-software-companies
- BOROS Szilárd – KOLOZSI Pál Péter: Egy 21. századi geopolitikai összeütközés természetrajza Kína és az USA példáján keresztül. Polgári Szemle, 2019/4-6. pp. 258-280., DOI: 10.24307/psz.2019.1217
- CLARKE, Peter: Top ten EMS contract manufacturers boost revenues in 2020. eeNews Europe, 2021. április 16. https://www.eenewseurope.com/news/top-ten-ems-contract-manufacturers-boost-revenues-2020
- CompaniesMarketCap.com: Largest Companies by Market Cap. 2021. szeptember 4. (aznapi állapot) https://companiesmarketcap.com/
- CSIKI VARGA Tamás – TÁLAS Péter: Erő és diplomácia. Az Egyesült Államok stratégiai érdekei és lehetőségei a Biden-kormányzat időszakában. Stratégiai Védelmi Kutatóintézet, 2021. július 27. https://svkk.uni-nke.hu/document/svkk-uni-nke-hu-1506332684763/SVKI_Elemzesek_2021_13_Ero%20es%20diplomacia.pdf
- DAIGLE, Brian – DECARLO, Samantha: Rare Earths and the U.S. Electronics Sector: Supply Chain Developments and Trends. Office of Industries, 2021. június. https://www.usitc.gov/publications/332/working_papers/rare_earths_and_the_electronics_sector_final_070921_2-compliant.pdf
- Department of Energy: DOE Announces Actions to Bolster Domestic Supply Chain of Advanced Batteries. 2021. június 8. https://www.energy.gov/articles/doe-announces-actions-bolster-domestic-supply-chain-advanced-batteries
- ERDEY László et. al.: China Does Not Want a Trade War – The Case for Rare Earth Elements. Polgári Szemle,. 2019/4-6. pp. 281-295., DOI: 10.24307/psz.2019.1218

- Európai Bizottság: Reziliencia a kritikus fontosságú nyersanyagok terén: a nagyobb biztonsághoz és fenntarthatósághoz vezető út feltérképezése. 2020. szeptember 3. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020DC0474&from=EN
- Európai Parlament: Elektronikai hulladék az EU-ban: tények és adatok. 2020. december 23. https://www.europarl.europa.eu/news/hu/headlines/society/20201208STO93325/elektronikai-hulladek-az-eu-ban-tenyek-es-adatok-infografika
- European Commission: Critical raw materials. 2020 https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials_en
- European Commission (2021a): Digital sovereignty: Commission kick-starts alliances for Semiconductors and industrial cloud technologies. European Commission, 2021. július 19. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3733
- European Commission (2021b): In-depth reviews of strategic areas for Europe's interests. 2021. május 5. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy/depth-reviews-strategic-areas-europes-interests_en#semiconductors
- FLAHERTY, Nick: Boom quarter for top 10 semiconductor companies. eeNews Europe, 2021. május 25. https://www.eenewseurope.com/news/boom-quarter-top-10-semiconductor-companies
- GOODENOUGH, Kathryn M. et al.: Europe's rare earth element resource potential: An overview of REE metallogenetic provinces and their geodynamic setting. Ore Geology Reviews, 2016/1. pp. 838-856., DOI: doi.org/10.1016/j.oregeorev.2015.09.019.
- GORRILL, Lindsay: Lithium-ion Batteries: "Rare Earth" vs Supply Chain Availability. Battery Power Online, 2019. szeptember 12. https://www.batterypoweronline.com/news/lithium-ion-batteries-rare-earth-vs-supply-chain-availability/
- GYŐRFFY Dóra: Amerika vagy Kína hanyatlik? In: ÁGH, Attila (szerk.): Az új világrend kialakulása – Az EU–USA–Kína hatalmi háromszög. Budapest, Magyarország: Noran Libro (2021) pp. 145–167., 23 p.
- HIPA: SK Innovation - Minden idők legnagyobb zöldmezős beruházása Iváncsán. 2021. január 29. https://hipa.hu/giga-beruhazast-indit-az-sk-innovation-minden-idok-legnagyobb-zoldmezos-beruhazasa-ivancsan
- HONG, Iris: SMIC spending $9 bn to build China's most-advanced wafer plant. Asia Financial, 2021. február 9. https://www.asiafinancial.com/smic-spending-9-bn-to-build-chinas-most-advanced-wafer-plant
- HORN, Stefan: Cobalt resources in Europe and the potential for new discoveries. Ore Geology Reviews, Vol. 130, 2021. 103915. DOI: 10.1016/j.oregeorev.2020.103915.

- hvg.hu: Sorra állnak le világszinten az autógyárak a chiphiány miatt. 2021. szeptember 3. https://hvg.hu/cegauto/20210903_Sorra_allnak_le_vilagszinten_az_autogyarak_a_chiphiany_miatt
- JASKULA, Brian W.: Lithium. U.S. Geological Survey, 2021. január. https://pubs.usgs.gov/periodicals/mcs2021/mcs2021-lithium.pdf
- JOWITT, Simon M. et al.: Recycling of the rare earth elements. Current Opinion in Green and Sustainable Chemistry, Vol. 13, 2018. pp. 1–7., DOI: 10.1016/j.cogsc.2018.02.008.
- KALANTZAKOS, Sophia: The Race for Critical Minerals in an Era of Geopolitical Realignments. The International Spectator, 2020/3. pp. 1-16. DOI: 10.1080/03932729.2020.1786926
- LEE, Yen Nee: 2 charts show how much the world depends on Taiwan for semiconductors. CNBC, 2021. március 15. https://www.cnbc.com/2021/03/16/2-charts-show-how-much-the-world-depends-on-taiwan-for-semiconductors.html
- Manish Tewari: War of the chips. Deccan Chronicle, 2021. május 23. https://www.deccanchronicle.com/opinion/columnists/220521/manish-tewari-war-of-the-chips.html
- MÁRTONFFY Balázs – NYSTROM, Dwight: „Kimért multilateralizmus": Előrejelzés a bideni külpolitikáról. Külügyi Szemle, 2021/1. pp. 43-59., DOI: 10.47707/Kulugyi_Szemle.2021.1.03
- MOORES, Simon: The Global Battery Arms Race: Lithium-Ion Battery Gigafactories and Their Supply Chain. The Oxford Institute of Energy Studies, 2021. február https://www.oxfordenergy.org/wpcms/wp-content/uploads/2021/02/THE-GLOBAL-BATTERY-ARMS-RACE-LITHIUM-ION-BATTERY-GIGAFACTORIES-AND-THEIR-SUPPLY-CHAIN.pdf
- Mordor Intelligence: Electronics Manufacturing Services Market - Growth, Trends, Covid-19 Impact, and Forecasts (2021–2026). 2021 https://www.mordorintelligence.com/industry-reports/electronics-manufacturing-services-market
- Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal: Nemzeti Intelligens Szakosodási Stratégia (S3) – 2021-2027. 2021. július 26. https://nkfih.gov.hu/hivatalrol/nemzeti-intelligens/nemzeti-intelligens-szakosodasi-strategia-2021-2027
- PORTER, Jon: Honor confirms Google's apps will return to its phones with new 50 series. The Verge, 2021. június 16. https://www.theverge.com/2021/6/16/22536512/honor-50-series-pro-release-date-news-features-google-mobile-services-apps-play-store
- RAPOZA, Kenneth: China's Rare Earths 'Slump' A Sign Of Domestic 'Hoarding' For EV Batteries, And More. Forbes, 2021, január 17. https://www.forbes.com/sites/kenrapoza/2021/01/17/chinas-rare-earths-slump-a-sign-of-domestic-hoarding-for-ev-batteries-and-more

- Reuters: U.S. government limits exports of artificial intelligence software. 2020. január 3. https://www.reuters.com/article/us-usa-artificial-intelligence-idUSKBN1Z21PT
- SCHNEBELE, Emily K.: Silicon. U.S. Geological Survey, 2021. január. https://pubs.usgs.gov/periodicals/mcs2021/mcs2021-silicon.pdf
- SCOTT, Alex: Europe is poised to begin lithium mining. Chemical and Engineering News, 2021. június 2. https://cen.acs.org/business/inorganic-chemicals/Europe-poised-begin-lithium-mining/99/i21
- SHEDD, Kim B.: Cobalt. U.S. Geological Survey, 2021. január. https://pubs.usgs.gov/periodicals/mcs2021/mcs2021-cobalt.pdf
- SHEPARDSON, David: U.S. FCC votes to advance proposed ban on Huawei, ZTE gear. Reuters, 2021. június 18. https://www.reuters.com/technology/us-fcc-votes-launch-further-crackdown-huawei-zte-equipment-2021-06-17/
- SUN, Leo: Why Intel's Foundry Plans Don't Make Any Sense. The Motley Fool, 2021. május 3. https://www.fool.com/investing/2021/05/03/why-intel-foundry-plans-dont-make-any-sense/
- The White House: Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China. 2021. június 3.
- ULRICH, Lawrence: The Top 10 EV Battery Makers. IEEE Spectrum, 2021. augusztus 25. https://spectrum.ieee.org/the-top-10-ev-battery-makers

3. FEJEZET

A PROXYCSOPORTOK ALKALMAZÁSÁNAK TAKTIKÁJA: A HACKTIVISTÁK[1]

1. BEVEZETÉS

A 2007-es Észtország ellen végrehajtott kibertámadás sok tekintetben egészen új helyzetet teremtett a kibertéri műveletek világában. Jelen fejezet szempontjából talán az attribúció körüli polémiát érdemes kiemelni. A nemzetközi sajtó és a politika ugyanis szinte azonnal Oroszországot, mint államot vélte felfedezni a támadás mögött, az orosz kormányzat viszont akkor, és azóta is folyamatosan tagadja a részvételét a műveletben. Rain Ottis, Észtország egyik legismertebb kiberbiztonsági szakértője 2008-ban így fogalmazta meg a rendelkezésre álló tényeket:
„Az orosz kormány folyamatosan tagadta direkt részvételét az Észtországot 2007 tavaszán ért kibertámadásban. A szerző tudomása szerint ez az állítás igaz. De meg kell jegyezni, hogy semmilyen bizonyíték nem áll rendelkezésre arra vonatkozóan, hogy az orosz kormányzat bármit is tett volna a helyzet megoldása érdekében. Az észt nyomozással kapcsolatos együttműködés hiánya arra utal, hogy az orosz kormány nem volt érdekelt a támadók kilétének felfedésében, így röviden szólva, védte őket. Más szavakkal a politikai elit által alkalmazott ellenséges retorika arra ösztönözte az embereket, hogy támadják Észtországot és semmit nem tettek annak érdekében, hogy ezt a támadást leállítsák. Ez a csendes támogatás pedig úgy értelmezhető, mint egyfajta implicit állami támogatás, mivel a retorziótól való félelem hiányában szabadon lehetett támadni az észtországi célpontokat.”[2]

Ottis azt is hozzáteszi, hogy a támadás végrehajtásával kapcsolatos információkat orosz nyelvű fórumokon osztották meg egymás között a résztvevők. Ezeken pontosan meg volt határozva a célpont, az időzítés, a végrehajtás módja, valamint az ideológiai motiváció is. A támadást végül a Nasi („Mieink”) ifjúsági mozgalom aktivistája, Konsztantyin Goloszkokov vállalta magára, tagadva, hogy bármilyen utasítást kapott volna az orosz hivatalos szervektől.[3] Érdekesség, hogy 2016-ban az ukrán biztonsági szervek, mármint az orosz katonai titkosszolgálat, a GRU, azaz az Oroszországi Föderáció Fegyveres Erői Vezérkarának Felderítő Főcsoportfőnöksége tisztjeként hivatkoznak Goloszkokovra.[4]

---

1 Megjelenés alatt: KRASZNAY Csaba (Szerk.): Taktikák és stratégiák a kiberhadviselésben

2 OTTIS, Rain: Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Cooperative Cyber Defence Centre of Excellence, 2008. március 2. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

3 LOWE, Christian: Kremlin loyalist says launched Estonia cyber-attack. Reuters, 2009. március 13.

4 UCMC Press Center: Security Service of Ukraine possesses audio records of Krasnov’s conversations with his Russian supervisor. Ukraine Crisis Media Center, 2016. március 3.

A Meduza nevű orosz oknyomozó portál tényfeltáró riportja a támadás végrehajtásának koordinátoraként Pjotr Levasovot nevezi meg, aki „főállásban" az egyik legnagyobb kéretlen levélküldő szolgáltatást, a Kelihoszt üzemeltette, amíg 2017-ben az FBI nyomozása után le nem tartoztatták Barcelonában. A Medusa forrásai szerint Levasov legalább 2005 óta együttműködött az orosz állami szervekkel, és aktívan támogatta bizonyos műveleteit a Kelihosz infrastruktúráját felhasználva.[5,6] Ezért cserébe érinthetetlen volt, így bár az amerikai nyomozóhatóság már 2007-ben vádat emelt ellene, 10 éven keresztül lehetetlen volt elfogni.[7]

Érdemes még megemlíteni Danyiil Turovszkij, a Meduza újságírójának orosz hackerekről szóló könyvének egy bekezdését, ahol a 2000-es évek közepének történéseit dolgozza fel, beleértve a 2007-es incidenst is. Ebben az időben egy Anton Moszkal nevű szentpétervári programozót keresett fel a belbiztonsági és kémelhárítási feladatokat ellátó Szövetségi Biztonsági Szolgálat, az FSZB munkatársa, és arról beszélt neki, hogyan lehetne küzdeni a „terrorista weboldalak ellen", illetve mit jelent számára a patriotizmus. Bár a megkeresés nem érte el a célját, a fentiek egyértelműen jelzik, hogy a 2000-es évek közepétől az orosz biztonsági szervek aktívan keresték a kapcsolatot a hazafias érzelmeket tápláló hackerekkel és kiberbűnözőkkel.[8]

2. A HACKTIVIZMUS ALAPVETŐ FOGALMAI

Játsszunk el egy pillanatra azzal a gondolattal, hogy ismerve az események utáni közel 15 év történetét és az orosz kibertéri műveletek fejlődését, talán a 2007-es esemény mégis egyfajta offenzív katonai kiberművelet volt, és nem tisztán az állampolgári elégedetlenség szülte azt! Tételezzük fel, hogy az orosz katonai vezetés már a korai 2000-es években felismerte annak lehetőségét, hogy az ország stratégiai érdeke megkívánja az információs műveletek során azokat az akciókat, amelyeket nem lehet közvetlenül összekötni a kormányzattal, hanem azokat látszólag független személyekre és csoportokra bízza! Amennyiben így történt, Oroszország sikerrel alkalmazta a proxycsoportok taktikáját, amelyet a fizikai hadviselésből jól ismerhetünk. Ráadásul nem is elsőként tette ezt, ahogy látni fogjuk, de a téma megértéséhez tisztázni szükséges néhány alapfogalmat.

Proxycsoportok a kibertérben: Michael N. Schmitt és Liis Vihul, a kiberhadviselés legismertebb nemzetközi jogi szakértői szerint akkor beszélhetünk proxycsoportokról a kibertérben, ha egy nem állami szereplő az adott állam utasításai szerint cselekszik, vagy az adott állam kontrollálja, illetve irányítja a nem

---

5 TUROVSZKIJ, Danyiil: 'It's our time to serve the Motherland' How Russia's war in Georgia sparked Moscow's modern-day recruitment of criminal hackers. Meduza, 2018. augusztus 7. https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland

6 Department of Justice: Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses. Department of Justice Office of Public Affairs, 2018. szeptember 12. https://www.justice.gov/opa/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer-crime

7 United States District Court: United States Versus Peter Yuryevich Levashov. United States District Court, 2017. április 4. https://www.justice.gov/opa/press-release/file/956511/download

8 TUROVSZKIJ, Danyiil: Orosz hekkerek. Athenaeum Kiadó, Budapest, 2020. p. 143.

állami szereplő cselekedeteit, kivéve akkor, ha az állami szereplő túllépi a hatáskörét, és úgy befolyásolja a nem állami szereplőket. Ha tehát „rendes ügymenet" szerint egy állami titkosszolgálat kontrollál vagy irányít egy hackert, kiberbűnözői csoportot, laza, informális csoportot, vállalatot, vagy akár egy terrorista, felkelő csoportosulást, proxy műveletről beszélhetünk. A lényeg, hogy bár mindezt esetileg kell megítélni, legyen egyértelmű irányítási kapcsolat az állam és a nem állami szereplő között.[9]

Hacktivizmus: A fogalom magyarázatára számos forrást lehet találni, de érdemes visszamenni az ősforrásig, amely így határozza meg a hacktivizmust: *„Az emberek felhatalmazásának célként való kitűzése, hogy a világ tudomást szerezzen az igazságtalanságokról, az emberi jogok megsértéséről. Más szóval, az információáramlás megszervezése világszerte, korlátozások és cenzúra nélkül. Ez a hacktivizmus."* Oxblood Ruffin visszaemlékezése szerint a hacktivizmus szó Omegától származik, a fogalmat pedig Count Zero írta le. Oxblood Ruffin így egészítette ezt ki: *„a technológia használata az elektronikus médián keresztül az emberi jogok fejlesztése érdekében."* Mindhárman a Cult of the Dead Cow (cDc) nevű hackercsapat tagjai voltak, a fogalom maga pedig az 1990-es évek közepén alakult ki, amikor a cDc igen aktív közéleti tevékenységet is folytatott.[10]

Hacktivista: Az előző gondolatmenet alapján következik, hogy a hacktivista az, aki részt vesz a hacktivizmusban. A '90-es évek óta viszont annyiféle megjelenését láttuk a hacktivista mozgalmaknak, hogy érdemes tágabban értelmezni a résztvevőket. Tim Jordan és Paul Taylor hacktivizmust feldolgozó könyvében így írja le a jelenséget:
„A hacktivizmus a népszerű politikai akciók tovább fejlődése, embercsoportok saját akciói a kibertérben. A politikai tiltakozások és a számítógépes hackelés kombinációja. A hacktivisták a kibertér keretein belül működnek, küzdenek a virtuális életben technikailag lehetséges dolgokért, és kinyúlnak a kibertérből, a virtuális erők felhasználásával alakítják az offline életet. A társadalmi mozgalmak és a népi tiltakozás a huszonegyedik századi társadalmak szerves részét képezik. A hacktivizmus tulajdonképpen az aktivizmus elektronikussá válása."[11]

Hacktivista tehát az, aki egy politikai ideológia mentén szervezett kibertéri akcióban vesz részt, amelynek hatása van a fizikai világra is.

Patrióta vagy hazafias hacker: A katonai kiberműveletek szempontjából nagyon fontos csoportot alkotnak a hacktivistákon belül a patrióta vagy hazafias hackerek. Athina Karatzogianni hacktivizmusról szóló könyvében úgy írja körbe a patrióta hackereket, mint akik a nemzetük tisztaságáért küzdenek az online média ügyes felhasználásával. Paradox módon tehát a nacionalizmus, mint politikai

9 SCHMITT, Michael N.– VIHUL, Liis: Proxy Wars in Cyberspace. Fletcher Security Review, 2014/2. pp. 54-73.

10 Oxblood Ruffin: Hacktivism: From Here to There. Threatpost, 2010. december 9. https://threatpost.com/hacktivism-here-there-120910/74759/

11 JORDAN, Tim– TAYLOR, Paul A.: Hacktivism and Cyberwars. Rebels with a cause?. Routledge, New York, 2004. p. 1.

ideológia jelenik meg a klasszikus hacktivista akciók mögött, kihasználva az internetet, mint globális médiát.[12]

Hacktivista cselekmény: A hacktivista akciók eszköztára közel sem annyira összetett, mint amit egy kiváló műveleti tervező képességekkel rendelkező állami szereplő kivitelezni tudna. A hacktivista csoportok ereje ráadásul a láthatóságban van, így nem érdekeltek abban, hogy a művelet rejtve legyen, illetve tipikusan csoportosan követik el a cselekményt, sokszor egymást nem is ismerve, akár nagyon eltérő földrajzi helyekről. A konspiráció tehát nem feltétlen cél. Romagna összefoglalója alapján így egy hacktivista cselekmény jellemzően az elosztott túlterheléses támadásokra (DDoS[13]), a weboldalak átírására (defacement) és az adatlopásra korlátozódik. Időnként előfordulhat kártékony kódok alkalmazása, de ennek meglehetősen negatív visszhangja van a közösségben.[14]

3. HACKTIVIZMUS A TALLINNI KÉZIKÖNYV SZERINT

A proxycsoportok alkalmazásának tilalma a kibertéri műveletek során egyértelműen megjelenik az ENSZ 2012-2013 között működő kormányzati szakértői munkacsoportjának (GGE[15]) záró jelentésében. A GGE feladata a tagállamok konszenzusát elérni bizonyos alapvető kibertéri szabályok és normák tekintetében. Az A/68/98 számú ENSZ határozat 23. pontja világosan megfogalmazza ezt az elvárást:
„Az államoknak teljesíteniük kell a nemzetközi jogot sértő, nekik tulajdonítható cselekményekkel kapcsolatos nemzetközi kötelezettségeiket. Az államok nem használhatnak proxykat a nemzetközi jogot sértő cselekmények elkövetésére. Az államoknak törekedniük kell annak biztosítára, hogy a területeiket ne használhassák olyan nem állami szereplők, akik jogellenesen használják az infokommunikációs technológiákat."[16]

Természetesen az ördög a fenti követelmény esetén is a részletekben rejlik. Egyrészt nem egyértelmű, hogy hol is van a határa a nemzetközi jogot sértő cselekményeknek, legalábbis az, hogy hol kezdődik a politikai akarat a nemzetközi jogot sértő cselekmények deklarálására. Másrészt igen nehezen bizonyítható, hogy az állam ténylegesen kontrollálta-e a nem állami szereplőt a cselekmény végrehajtása során. Harmadrészt az internet határtalan, tehát elképzelhető, hogy a proxycsoportok nem abban az országban működnek, ahonnan az utasításokat kapják, a fogadó ország pedig nem rendelkezik olyan képességekkel, amelyekkel meg tudja

12 KARATZOGIANNI, Athina: Firebrand Waves of Digital Activism 1994-2014: The Rise and Spread of Hacktivism and Cyberconflict. Palgrave Macmillan, Basingstoke, 2015. p. 22.
13 Distributed Denial of Service
14 ROMAGNA, Marco: Hacktivism: Conceptualization, Techniques, and Historical View. In: HOLT, T. – BOSSLER, A. M. (Eds.): The Palgrave Handbook of International Cybercrime and Cyberdeviance. https://doi.org/10.1007/978-3-319-90307-1_34-1
15 Group of Governmental Experts
16 ENSZ: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Document A/68/98 2013. június 24.
https://undocs.org/Home/Mobile?FinalSymbol=A%2F68%2F98&Language=E&DeviceType=Desktop&LangRequested=False

akadályozni a nemzetközi jogba ütköző cselekmény végrehajtását, esetleg nem is tud ezekről a cselekményekről.

A Tallinni Kézikönyv azért kísérletet tesz arra, hogy pontosítsa a proxycsoportok, ezen belül is a hacktivisták alkalmazásának definícióját. Legpontosabban a nem állami szereplőkkel foglalkozó 17. szabály fogalmazza meg azt a követelményt, amelyet korábban már ismertettünk, egyben a GGE határozat lényegét is tartalmazza. Eszerint tehát a kiberműveleteket végrehajtó nem állami szereplők tevékenysége akkor attribútálható egy államnak, amikor az az állami szereplő utasításai szerint cselekszik, illetve annak irányítása és kontrollja alatt áll, valamint az állami szereplő tudomásul veszi és felhasználja a műveletet saját céljai érdekében.[17]

A 69. szabály próbálja meghatározni, hol kezdődik a nemzetközi jogot sértő cselekmények határa. Eszerint a kiberműveletek erőszakos cselekménynek minősülnek, amennyiben azok mértéke és hatása összehasonlítható az erőszakos cselekménynek minősülő nem-kibertéri műveletekkel. A magyarázatban az szerepel, hogy például egy hacktivista csoportnak pusztán a finanszírozása nem minősül erőszakos cselekménynek, abban az esetben, ha az adott csoport egy felkelés részese egy másik ország ellen.[18] Ez magyarázatot ad arra, hogy miért lehet hasznos az olyan országon belüli hacktivista csoportok támogatása, mint például a Cyberberkut, amely egy Ukrajnán belül működő oroszbarát csoportosulás, és amely aktívan kivette a részét a Kelet-Ukrajnában zajló fegyveres konfliktus kibertéri részéből.[19] Ha azonban a politikai akarat megvan arra, hogy egy kiberműveletet egy országnak attribútáljanak, akkor a finanszírozás ténye bizonyíték lehet a kontroll megvalósulására, ez pedig fontos szempont lehet akkor, ha Oroszországgal szemben eljárást kezdeményez a nemzetközi közösség az orosz–ukrán háború után.

A 82. szabály magyarázata fegyveres konfliktus idején elemzi azt, hogy hol van a helye mindebben a hacktivista csoportoknak. Fegyveres konfliktusról akkor beszélünk, amikor ellenséges cselekmények történnek két állam között, beleértve ebbe akár a pusztán kiberműveleteket alkalmazó akciókat is. A szabály magyarázatában a nem állami szereplő fölött gyakorolt kontrollra megjelenített példa szerint az Észtországgal szemben végrehajtott művelet nem minősül fegyveres cselekménynek, mivel nincsen bizonyíték arra, hogy az abban résztvevő személyek valamely állam iránymutatása szerint cselekedtek volna, illetve valamely állam szervezte vagy jóváhagyta volna a műveletet. Ráadásul kérdéses, hogy egyáltalán volt-e fegyveres konfliktus, tehát a bevetett eszközök kiberfegyvernek minősülnek-e. A magyarázatból látszódik, hogy bár számos jel utal titkosszolgálat által összehangolt műveletre, a bizonyítékok és a fegyveres támadás hiányában a nemzetközi jog alapján nem lehetett eszkalálni a válaszadást.[20]

---

17 SCHMITT, Michael N. (Szerk.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge, 2017. p. 94.

18 SCHMITT (2017): i m. p. 330.

19 KOVAL, Nikolay: Revolution Hacking. In: GEERS, Kenneth (Ed.): Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCD COE Publications Tallinn, 2015. pp. 55-58.

20 SCHMITT (2017): i m. p. 379.

A 95. szabály szerint ráadásul egy fegyveres konfliktusban, azaz ius in bello idején mindaddig civilnek kellene tekinteni egy személyt, ameddig egyértelműen be nem bizonyosodik, hogy az illető nem civil. Egy hacktivista esetében éppen ezért különösen nehéz bármilyen ellenintézkedést foganatosítani mindaddig, amíg direkt módon részt nem vesz az ellenséges tevékenységben.[21] A 97. szabály szerint viszont a direkt részvétel megfosztja őt a civil státusztól. A magyarázat szerint, ha például egy hacktivista többször egymás után is megpróbál megtámadni egy vezetési pontot, mindaddig támadható marad, ameddig a támadásokat elköveti, tehát nem csak a konkrét támadás idején, hanem a támadások között is. Sőt, amennyiben fennáll a lehetősége annak, hogy támadásait folytatni fogja hosszabb kihagyás után is, mindaddig célpont maradhat, ameddig a műveleti képessége fennmarad. A Tallinn Manual példája szerint egyértelműen közvetlen részvételnek minősül a fegyveres konfliktushoz kapcsolódó kibertámadások végrehajtása, valamint minden olyan cselekmény, amely lehetővé teszi a konkrét támadásokat, például a célzott rendszer sebezhetőségének azonosítása vagy rosszindulatú szoftverek tervezése bizonyos sebezhetőségek kihasználása érdekében. A további egyértelmű példák közé tartozik az ellenséges műveletekre vonatkozó információk kibereszközökkel történő gyűjtése és azok továbbítása a saját állam fegyveres erői számára, valamint DDoS-műveletek végrehajtása az ellenséges külső katonai rendszerek ellen.[22,23]

4. A HACKTIVIZMUS GYÖKEREI

Ahogy láthattuk, a Tallinni Kézikönyv a nemzetközi jog alapján meg tudja fogalmazni a hacktivista csoportok offenzív kibertéri felhasználásának definícióját, az ehhez vezető út azonban hosszú volt. Érdemes tehát röviden áttekinteni, hogyan alakult ki a hacker szcéna, milyen fázisokon ment át a hacktivizmus, és hogyan kapcsolódtak ezek a csoportok az állami szereplőkhöz. Ahogy a történelmi áttekintésben látni fogjuk, Oroszország katonai szervei egyáltalán nem véletlenül kerültek közel ezekhez a csoportokhoz, de nem elsőként használták ki a bennük rejlő potenciált.

Maga a hackelés fogalma több évtizedre tekint vissza. A „hacking” szó eredeti jelentése valaminek a véletlenszerű levágását jelenti nehéz ütésekkel, és már az 1200-as évek Angliájában használták a szót. Modern értelmében először 1955-ben írták le a Massachusetts Institute of Technology (MIT) modellvasút klubjának jegyzőkönyvében: *„Mr. Eccles kéri, hogy bárki, aki az elektromos rendszeren dolgozik vagy azt hackeli, legyen szíves lekapcsolni az áramot, hogy a biztosíték ne égjen le”*.[24] A „hackelés” ezen az egyetemen ettől kezdve azt jelentette, hogy valaki egy technikai problémán dolgozik szokatlan, kreatív megoldásokat keresve. Magyarul talán a buherálás, berhelés szavakkal lehetne a legjobban lefordítani. Nem meglepő módon a kifejezést elsősorban a „Signals and Power Subcommitte”-ban, azaz az irányítástechnikai csoportban használták, a hackinget a modellvasút minél hatékonyabb irányításának kifejezésére alkalmazták. Mivel a számítógépek civil

[21] SCHMITT (2017): i m. 424.
[22] SCHMITT (2017): i m. 428.
[23] Ezek fényében érdemes megvizsgálni az Anonymous csoport és más hackercsoportok tevékenységét az orosz–ukrán háborúban.
[24] YAGODA, Ben: A Short History of “Hack”. The New Yorker, 2014. március 6. https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack

környezetben elsők között az MIT-n jelentek meg, ezekhez pedig elsősorban azok a diákok fértek hozzá, akik szabadidejükben a modellvasutakat „programozták", törvényszerűen a hackelés kifejezés tőlük ragadt át az informatika világára is. Nekik köszönhetjük egyébként a hacker etikát és az egész „cyber életérzést" is. Mivel az MIT diákjai között kialakult egy sajátos nyelvezet, amit kívülálló nem igazán értett, megírták a The Jargon File-t, amely az általuk használt kifejezések magyarázatát tartalmazta. Ebben találhatjuk a hacker definícióját is.

1. Olyan személy, aki élvezi a programozható rendszerek részleteinek feltárását és a képességei kibővítését, szemben a legtöbb felhasználóval, akik inkább csak a szükséges minimumot tanulják meg. Az RFC1392 szerint olyan személy, aki örömmel ismeri meg a rendszer, különösen a számítógépek és a számítógépes hálózatok belső működését.
2. Aki lelkesen (akár rögeszmésen) programoz, vagy aki sokkal inkább élvezi magát a programozást, mint a programozásról való elmélkedést.
3. Olyan személy, aki képes értékelni a hack értékét.
4. Olyan ember, aki jól tud gyorsan programozni.
5. Egy adott program szakértője, vagy aki gyakran dolgozik a programon vagy annak segítségével (ld. a „Unix hacker" definícióját).
6. Bármilyen szakértő vagy rajongó. Lehet valaki például csillagász hacker is.
7. Aki élvezi a korlátok kreatív legyőzésének vagy megkerülésének intellektuális kihívását.
8. [elavult] Rosszindulatú beavatkozó, aki kényes információkat próbál felfedezni próbálkozással. Ezek a jelszó-hackerek vagy hálózati hackerek. Ma már a helyes kifejezés ezekre a cracker.[25]

A 70-es években a hacker szubkultúra folyamatosan terjedt, elsősorban a Szilícium-völgyben és a nagy amerikai műszaki egyetemeken. Ennek folyamatát és történetét Steven Levy 1984-es könyve írja le, egyben itt található meg a Hacker Etika leírása is, ami szerint az ősi hackerek a világhoz viszonyultak.

1. A számítógépekhez való hozzáférésnek – és bárminek, ami megtaníthat valamit arról, hogy a világ hogyan működik – korlátlannak és totálisnak kellene lennie.
2. Minden információnak hozzáférhetőnek kellene lennie.
3. Ne bízz a hatóságban – támogasd a decentralizációt!
4. A hackereket az általuk elkövetett tettek alapján kellene megítélni, nem pedig iskolai végzettség, kor, faj, vagy pozíció alapján.
5. Művészetet és szépséget kreálhatsz a számítógépeden.
6. A számítógépek jobbá tehetik az életedet.[26]

Érdemes kiemelni, hogy a negyedik pont szerint a hatóságokkal való együttműködés nem kívánatos, ami annak is köszönhető, hogy ekkoriban jelent meg az amerikai büntetőjogban az első olyan passzus, amely szankcionálta a

[25] RAYMOND, Eric S.: The Jargon File, version 4.4.8. Eric S. Raymond's Home Page, 2004. október 1. http://catb.org/jargon/

[26] LEVY, Steven: Hackers: Heroes of the Computer Revolution. Anchor Press/Doubleday, Garden City, 1984. p. 458.

számítógépes bűncselekményeket. Ezután a hackerközösség tagjai egyre gyakrabban kerültek szembe a törvénnyel és a bűnüldöző szervekkel. Ennek tragédiáját fogalmazza meg Loyd Blankenship, a Legion of Doom hackercsoport tagjának nagy hatású írása, A hacker kiáltványa, amelynek utolsó sorai így hangzanak Voyager2 fordításában: *„Igen, bűnöző vagyok. A bűnöm a kíváncsiság. A bűnöm az, hogy azután ítélem meg az embereket, amit mondanak és gondolnak, és nem a külsejük alapján. A bűnöm, hogy okosabb vagyok, mint ti, ez olyan dolog, amit soha nem fogtok nekem megbocsátani. Hacker vagyok, és ez a kiáltványom. Megállíthatjátok az egyént, de nem állíthattok meg minket... végül is, mind egyformák vagyunk."*[27]

Nem tett jót az állam és a hackerek közötti kapcsolatnak az sem, hogy a hatósági érdeklődés pont 1984-ben erősödött fel. George Orwell világhírű regényének címe és tartalma, valamint az aktuális évszám és a közösséget érő csapások közötti látszólagos összefüggések ugyanis nagy hatást tettek az arra érzékeny közönségre, és nem javították az USA kormányával szembeni bizalmat. Lassan 40 éves távlatból viszont úgy látszódik, hogy sokkal inkább véletlen egybeesések alakították ezt a viszonyt. Az 1980-as évek elejétől az amerikai háztartásokban is széles körben elérhetővé váltak a számítógépek, fiatalok százezrei ismerkedtek meg a programozás alapjaival. 1983-ban megjelent a Háborús játékok című film, amely széles körben ismertté tette a hackereket. 1984-ben megtartották az első hackerkonferenciát, a Hackers Conference-t, elindult az első hacker magazin, a 2600, illetve ehhez kapcsolódóan megjelent Steven Levy már említett könyve. A „hacker" fogalom tehát bekerült az amerikai közbeszédbe, aminek a hatására létrejöttek az első szervezett hackercsoportok, amire viszont már lépnie kellett a jogalkotónak és meg kellett szabnia azokat a határokat, amiket a számítógépes tevékenységek nem léphetnek át. Ez viszont érdekellentétet és meglehetős bizalmatlanságot szült.

5. AZ ELSŐ HACKTIVISTA CSOPORTOK

Az amerikai hackercsoportok gondolkodásában eközben egyre inkább megjelentek az ideológiai vonások is. Ez egyenesen következik a keleti és nyugati parti amerikai egyetemek klasszikus szabadelvűségéből és a korszellemből, amely előbb a vietnámi háborúval, majd később a Ronald Reagan nevével fémjelzett mély konzervatív gondolkodással való szembenállásban manifesztálódott az amerikai fiataloknál. A hacker nem bízott az államban, és meg akarta mutatni, hogy az állam hazudik. Éppen ezért, ahogy a hacker etika második pontjában olvashatjuk is, az információt sokan hozzáférhetővé akarták tenni. Beleértve ebbe az állam titkait is. Ezt a mozgalmat az „Information wants to be free", azaz az információ szabad akar lenni mottóval indították el, amelynek eredete az MIT modellvasút klubjának két tagjához, Jack Dennishez és Peter Samsonhoz nyúlik vissza. A kifejezést viszont Stewart Brand alkotta meg, aki 1984-ben, a Hackers Conference-en ezt mondta:
„Egyrészt az információ drága akar lenni, mert nagyon értékes. A megfelelő információk a megfelelő helyen egyszerűen megváltoztatják az életedet. Másrészt az

[27] The Mentor: The Conscience of a Hacker. Phrack Inc., Vol.1., Issue 7., Phile 3 of 10, 1986. http://phrack.org/issues/7/3.html

információ ingyenes akar lenni, mert a kinyerésének költsége folyamatosan csökken. Tehát ez a kettő harcol egymás ellen."[28]

A 80-as évek közepén, 90-es évek elején számos hackercsoport jött létre, így volt táptalaja ennek a gondolkodásnak. A legnagyobb ilyen csoportok a Cult of the Dead Cow, amely 1984-ben, Texasban alakult meg, a Legion of Doom, szintén 1984-es alapítással, amely szerte az USA-ban rendelkezett tagokkal, a Masters of Deception, amely a 80-as évek végétől New Yorkban működött és a bostoni L0pht Heavy Industries, 1992-es indulással. Ahogy korábban olvasható volt, a cDc tagjai megalkotják a hacktivizmus kifejezést, a hackercsoportok pedig egyre többször szerepelnek a nyilvánosság előtt. Talán a legemlékezetesebb ebből az időszakból a L0pht kongresszusi meghallgatása volt 1998-ban, amelyet az első, széles körben ismertté vált kiberbiztonsági ülésként tartanak számon. Ennek témája az USA kibertéri kitettsége volt. A hackerek segítettek rávilágítani arra, hogy milyen súlyos sebezhetőségek vannak az interneten és a kritikus infrastruktúrákban.[29] Érdekesség, hogy a meghallgatáson komoly szerepet játszott Peiter "Mudge" Zatko, a L0pht tagja, aki 2004-től kezdve hosszabb ideig a DARPA-nak[30] dolgozott katonai kibervédelmi projekteken.

A hacktivizmus ekkoriban találkozott a digitális aktivizmussal, és ugyan nagyon hasonló eszköztárral ugyan, de nagyon különböző háttérrel két irányzat erősödött meg. Az egyiket tömegmozgalmi hacktivizmusnak nevezték, és sokkal inkább a politikai aktivizmus jegyeit mutatta, de már kihasználta az internetben rejlő lehetőségeket. Az első ilyen mozgalmat Ricardo Dominguez alapította, aki művész és író volt. Mozgalmának neve The Electronic Disturbance Theater volt, és 1997-ben indította el. Ez volt az első olyan polgárjogi mozgalom, amely számítógépeket használt aktivista tevékenysége során. Legismertebb akciójuk a FloodNet volt, melynek segítségével DDoS támadást indítottak a mexikói zapatista felkelők támogatása érdekében. A célpontok között volt a mexikói és az amerikai elnökök weboldala is.[31]

A másik irányzatot digitálisan korrekt hacktivizmusnak hívták. Ez a Cult of the Dead Cow-ból indult mozgalom volt, Oxblood Ruffin vezetésével.[32] Elsődleges célkitűzése az információhoz való hozzáférés és a szólásszabadság biztosítása volt az interneten. 2001. július 4-én, a Függetlenség Napján adták ki a Hacktivismo Declaration-t, amelyben az internet szabadságának alapértékeit fogalmazták meg, amelyek máig hatnak. Ebben többek között foglalkoznak az internet-hozzáférés szabadságával, az elektronikus információ cenzúrájának kérdésével és a

---

28 DOCTOROW, Cory: Saying information wants to be free does more harm than good. The Guardian, 2010. május 18. https://www.theguardian.com/technology/2010/may/18/information-wants-to-be-free

29 TROPEANO, Rosemary: Landmark Senate Hearings Exposed Risks and Threats That Are Still Being Confronted. National Security Archive, 2019. január 9. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2019-01-09/cybersecurity-when-hackers-went-hill-revisiting-l0pht-hearings-1998#_edn1

30 Defense Advanced Research Projects Agency, az Egyesült Államok Védelmi Minisztériumának kutatásokért felelős részlege

31 JORDAN – TAYLOR (2004): i. m. p. 69.

32 Uo. p. 98.

szólásszabadsággal is.[33] Ők kezdték el propagálni az anonim kommunikációs megoldások használatát az információ szabad áramlása érdekében, amely a 2020-as évek elejére annyira általánossá vált, hogy már a nemzetbiztonságot fenyegeti ezen platformok lehallgathatatlansága.

A 90-es évek végén az amerikai hacktivista csoportok már a globális biztonságpolitikába is belekeveredtek, valószínűleg nem is sejtve, hogy ezzel elindítják a proxycsoportok alkalmazásának taktikáját a 2000-es években. Az egyik komoly visszhangot kiváltó akciót az utókor Blondie Wong és a Hong Kong Blondes néven ismeri. Az 1995-1998 között zajló eseménysorozat lényege, hogy állítólag Oxblood Ruffin kapcsolatba került egy kínai disszidens csoporttal, akik a kínai triádok segítségével csempésztek Nyugatra olyan másként gondolkodókat, akik szembe kerültek a kínai kormánnyal. A Blondie Wong néven ismert kapcsolattartó és a Hong Kong Blondes-nak nevezett csoportja Ruffin segítségével kapcsolatba került a cDc-vel és más hackercsoportokkal is, akik segítségével egyrészt sajtónyilvánosságot kaptak, másrészt elsajátították hackertechnikákat, és hozzáfértek olyan támadóeszközökhöz, mint például a Back Orifice 2000 nevű, távoli hozzáférést lehetővé tevő szoftverhez, amelynek használatával sikeresen támadtak kínai célpontokat. A részletek nem ismertek, de Ruffin évekkel későbbi beszámolója arra enged következtetni, hogy a művelet nem nélkülözte a titkosszolgálati jelleget.[34] Már ha megtörtént egyáltalán, és nem a cDc hatalmas médiahackje volt, a kínai szakirodalomban ugyanis nyoma sincs mindennek.[35] Az amerikai média mindenesetre felkapta a történetet, és így széles körben ismertté vált a hacktivizmus.

A másik ilyen akcióra 1998 végén került sor, amikor a Legions of the Underground nevű csoport kiberháborút hirdetett Kína és Irak ellen az emberi jogok megsértése miatt. A felhívás lényege az volt, hogy néhány napon keresztül a közösség tagjai célzottan támadták a két ország informatikai infrastruktúráját, ezzel ellehetetlenítve az országok normális működését. Ez hatalmas vihart kavart, a legjelentősebb hackercsoportok, mint a cDc, a L0pht vagy a német Chaos Computer Club közös közleményben határolódott el a felhívástól, jelezve azt, hogy elfogadhatatlannak tartják az ilyen beavatkozást más országok működésébe.[36] A beszámolók szerint egyébként a Legions of the Underground is tagadta, hogy köze lenne a felhíváshoz. A felhívást a csoport egyik tagjának, Staktonnak tulajdonították, viszont ő saját bevallása szerint a felhívás idejében két hétig nem volt online, a nevében nyilatkozott valaki, aki felől utána soha többet nem hallottak.[37] A támadást végül nem hajtották végre, a történeti visszatekintésekben viszont egyre többször merül fel, hogy az érintett titkosszolgálatok beépültek ezekbe a közösségekbe. Ezt

33 Cult of the Dead Cow: Hacktivismo Declaration. 2001. július 4. https://blog.9while9.com/manifesto-anthology/2001.html

34 RUFFIN, Oxblood: Blondie Wong And The Hong Kong Blondes. Medium, 2015. március 23. https://medium.com/emerging-networks/blondie-wong-and-the-hong-kong-blondes-9886609dd34b

35 HONKER, Wei: cDc Created Hong Kong Blondes and 'Hacktivism' as a Media Hack. seclist.org, 2012. május 3.

36 International Coalition of Hackers: "Hackers Don't Go To War". 1999. január 7. https://seclists.org/fulldisclosure/2012/May/30

37 GLAVE, James: Confusion Over 'Cyberwar'. Wired, 1999. január 12. https://www.wired.com/1999/01/confusion-over-cyberwar/

erősíti meg az FBI-tól kikért akták sokasága is, amely szerint legkésőbb az 1995-ös DefCon hackerkonferencián már műveleti célból vettek részt FBI ügynökök.[38] Ezen az eseményen azóta is rendszeres programpont a „Spot the Fed", azaz a „Szúrd ki az Ügynököt" játék.

6. HACKTIVIZMUS A KELETI NAGYHATALMAKBAN

Turovszkij orosz hackerekről szóló könyvéből az olvasható ki, hogy nagyon más fejlődési úton ugyan, de a 2000-es évek elejére Oroszországban is kialakult egy olyan közösség, amely a hacktivizmus útját járta. Az orosz hacker-szcéna kezdetei a számítógépekhez való szabad hozzáféréssel vette kezdetét a 90-es évek elején, majd az IRC-csatornák, az orosz nyelvű Hacker magazin, és nem utolsósorban a kiváló matematikaoktatás folyamatosan kitermelte az erre fogékonyak közül az első generációs hackereket. Az orosz vadkapitalizmus során ezek a fiatalok elsősorban klasszikus kiberbűncselekményeket követtek el, nyugati, elsősorban amerikai áldozatok bankszámláit és kártyáit csapolták meg. Az orosz hatóságok egy ideig képtelenek voltak ellenük bármit is tenni, majd megszületett az a hallgatólagos megállapodás, hogy ameddig nem hazai célpontokat támadnak, addig nem is tesznek hatalmas erőfeszítéseket az elkövetők kézre kerítése érdekében. Ami rossz Amerikának, de nem fáj Oroszországnak, az elfogadható, azaz az ellenségem ellensége a barátom. Ez az évtizedek során azt eredményezte, hogy a külföldön elkövetett gazdasági bűncselekmények elkövetésének „elnézése" fejében ezeket a kiberbűnözői csoportokat és a támadó infrastruktúráikat egyre gyakrabban használták fel proxyként az Oroszország érdekében álló műveletek végrehajtása során, ahogy azt az Észtország elleni támadás során is láthattuk.[39]

Az orosz állampolgár és az orosz államhatalom közötti, évszázadok alatt kialakult sajátos kapcsolat miatt a hacktivizmus itt nem a liberális, szólásszabadságot támogató és az állami túlhatalmat ellenző irányban jelent meg hangsúlyosan – bár ilyen irányzatokkal is lehet találkozni –, hanem kitermelte a hazafias hackerek irányzatát. Ez hangsúlyosan a második csecsen háborútól érződik, amikor önszerveződő csoportok kaukázusi internetes célpontok ellen hajtottak végre támadásokat, majd 2005-től egyértelműen megjelennek azok a szervező erők a fórumokon, amelyekre 2007-ben már támaszkodni lehetett.

A nyugati olvasók számára talán kevésbé ismert, de a kínai hacktivista csoportok létrejötte és politikai célok mentén történő aktivizálódása megelőzte orosz társaikét. Scott J. Henderson könyvében részletesen feldolgozta a kínai hackerközösség történetének első évtizedét, amelyből kiderül, hogy a kínai internet 1994-es indulása után szinte azonnal megjelentek azok a fórumok, ahol a téma iránt érdeklődő tízezrek egymásra tudtak találni. Az első szervezettebb csoport a Zöld Hadsereg (Green Army) volt, amelyet az első kommunista katonai akadémia, a Whampoa Academy után neveztek el. Nem sokkal ezután indult a Kínai Sasszövetség (China Eagle Union). Mindkét csoport indulása 1997-re datálható.

---

[38] BROWN, JPat: FBI files on DEF CON show "Spot the Fed" contest a sore spot for Feds. Muckrock, 2015. május 6. https://www.muckrock.com/news/archives/2015/may/06/def-cons-spot-fed-contest-sore-spot-feds/

[39] TUROVSZKIJ (2020): i. m. pp. 27-59.

A legjelentősebb csoportosulás azonban a 90-es évek végén, különböző csoportok egyesülése után jött létre. Az önmagát Vörös Hackerek Szövetségnek (Red Hacker Alliance) nevező csoport több tízezer tagot számlált, és kimondottan a patrióta hackerek jellemzőit viselte magán. A csoport első komoly hacktivista tevékenysége 1998-ra tehető, amikor tömeges deface támadásokat intéztek indonéz kormányzati célpontok ellen, mivel ebben az időben a kínai kisebbséget jelentős támadás érte az indonéz többség részéről. Később célponttá vált Tajvan és Japán is, minden esetben a kínai nacionalizmust sértő lépések miatt.

A Vörös Hackerek Szövetsége valószínűleg a kínai kormányzattól függetlenül jött létre, ráadásul az is valószínű, hogy a kínai kultúra sajátossága miatt a kínai titkosszolgálatok nem vettek részt aktívan az első hacktivista akciók szervezésében, azt a kínai hackerek ténylegesen saját patrióta beállítottságuk miatt hajtották végre. Az azonban Henderson kutatásai szerint biztosnak tűnik, hogy a csoport felbomlásának idején, 2005-ben a kínai hadsereg már aktívan toborzott a tagok között, illetve a 2000-es évek elején már létezett olyan kiberhadviseléssel foglalkozó csoport a Kínai Népi Felszabadító Hadseregen belül, amely az amerikai és izraeli példa alapján szerveződött.[40] Ezzel véget is ért a kínai hacktivizmus első generációjának időszaka, de jöttek a következő generációk, amelyeknek egyre inkább a kontrollált kínai interneten kellett működniük, az érdeklődés azonban nem csökkent, éppen ellenkezőleg, nőtt a hackerizmus iránt.[41]

7. KÖVETKEZTETÉSEK

Jelen fejezet a 2000-es évek első felében hagyja abba a hacktivista csoportok történetének bemutatását, nem foglalkozik az Anonymous vagy a LulzSec csoportokkal, nem részletezi a Wikileaks tevékenységét, és Edward Snowden vagy Bradley (ma már Chelsea) Manning szerepét sem elemzi. Ennek oka az, hogy a 2007-es észtországi események teljesen új világot teremtettek a kibertéri műveletek területén, és a nagyhatalmak inkább az ilyen proxycsoportok integrálására törekedtek. Ennek oka egyrészt a nemzetközi kapcsolatokban keresendő, de valószínűleg nagyobb súllyal esett latba az, hogy a hackerek kevéssé kontrollálhatóak, egyáltalán nem biztos, hogy egy titkos művelet nem kerül napvilágra egy sértett hacker miatt. Ha ugyanezek az emberek egy fegyveres testületen belül, annak szabályait követve dolgoznak, valószínűleg sokkal hatékonyabbak is.

Ha megnézzük a nagyhatalmak hozzáállását a hacktivista csoportokhoz, ugyanazt az utat látjuk. Az Egyesült Államokban az első generációs hacktivisták eltűntek, sokan közülük valószínűleg Mudge-hoz hasonlóan kormányzati szolgálatba álltak. Az biztos, hogy az Anonymous csoportra már rendvédelmi problémaként tekintettek az amerikai rendvédelmi szervek, és a szétzüllesztésére és felszámolására törekedtek. Az USA-ra egyébként sem volt jellemző a hacktivisták proxyként való

[40] HENDERSON, Scott J.: The Dark Visitor. Inside the World of Chinese Hackers. Scott Henderson, 2007.

[41] WEBBER, Craig– YIP, Michael: The Rise of Chinese Cyber Warriors: Towards a Theoretical Model of Online Hacktivism. International Journal of Cyber Criminology. 2018/1. pp. 230-254.

felhasználása.[42] Oroszország a hibrid hadviselése során továbbra is széles körben alkalmaz proxykat, de ezek ma már szinte kizárólag magánbiztonsági cégek. Ezek közül talán a legismertebb az Internet Research Agency, amelyet a 2016-os amerikai elnökválasztás befolyásolási kísérlete során használtak, de számos más, hasonló cég megtalálható az amerikai embargós listán, amelyet az őket ért kiberincidensek nyomán bővítenek. Emellett természetesen minden lehetőséget kihasználnak, így Julian Assange, a Wikileaks vezetőjének gyakori szereplése az orosz RT nevű propagandatévében sem véletlen. Kína esetében pedig a hacktivisták és az állam motivációi sosem álltak egymástól távol, így aránylag könnyen integrálták és integrálják jelenleg is a hackerizmus iránt érdeklődő fiatalokat a hadseregbe.

A hacktivisták proxyként való felhasználása offenzív kiberműveletekben tehát inkább a 2000-es évekre jellemző, de ez nem jelenti azt, hogy a hacktivizmus kora leáldozott volna. Mindig lesznek olyan lánglelkű fiatalok, akik rendszerkritikusságukat vagy éppen hazafiságukat a hackerizmus eszközeivel élik meg. Amennyiben egy ország tudatosan törekszik e fiatalok honvédelembe való integrálására – hasonlóan a nagyhatalmakhoz –, akár rövid távon is megvalósítható az offenzív kiberképességek létrehozása. Egy 2012-es felmérés szerint Magyarországon az információbiztonságban dolgozó vagy az iránt érdeklődő személyek 59%-a akár ingyen is szolgálná a hazáját, míg 27%-uk pénzt kérne ezért. Csupán 14% válaszolt úgy, hogy nem venne részt a honvédelemben.[43] Bár a felmérés régi, feltehetően továbbra is sikerrel lehetne meríteni a magyar hackerek közül, ami tudatos tervezéssel a magyar katonai kibertéri műveleti képességek fejlesztésének egyik fontos eleme lehet.

Felhasznált irodalom:

- BROWN, JPat: FBI files on DEF CON show "Spot the Fed" contest a sore spot for Feds. Muckrock, 2015. május 6. https://www.muckrock.com/news/archives/2015/may/06/def-cons-spot-fed-contest-sore-spot-feds/
- Cult of the Dead Cow: Hacktivismo Declaration. 2001. július 4. https://blog.9while9.com/manifesto-anthology/2001.html
- Department of Justice: Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses. Department of Justice Office of Public Affairs, 2018. szeptember 12. https://www.justice.gov/opa/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer-crime

[42] Az orosz-ukrán háború során az Anonymous aktívan részt vett a műveletekben, így ha a „háború köde" felszáll, elképzelhető, hogy ez az állítás pontosításra fog szorulni.

[43] KRASZNAY Csaba – VARGA-PERKE Bálint: Ifjúságvédelem a hacker szubkultúrában. In: BÍRÓ A Zoltán – GERGELY Orsolya (Szerk.): Ártalmas vagy hasznos internet? A média hatása a gyermekekre és fiatalokra. Státus Kiadó, Csíkszereda, 2013. pp. 179–202.

- DOCTOROW, Cory: Saying information wants to be free does more harm than good. The Guardian, 2010. május 18. https://www.theguardian.com/technology/2010/may/18/information-wants-to-be-free
- ENSZ: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Document A/68/98 2013. június 24. https://undocs.org/Home/Mobile?FinalSymbol=A%2F68%2F98&Language=E&DeviceType=Desktop&LangRequested=False
- GLAVE, James: Confusion Over 'Cyberwar'. Wired, 1999. január 12. https://www.wired.com/1999/01/confusion-over-cyberwar/
- HENDERSON, Scott J.: The Dark Visitor. Inside the World of Chinese Hackers. Scott Henderson, 2007.
- HONKER, Wei: cDc Created Hong Kong Blondes and 'Hacktivism' as a Media Hack. seclist.org, 2012. május 3.
- International Coalition of Hackers: Hackers Don't Go To War. 1999. január 7. https://seclists.org/fulldisclosure/2012/May/30
- JORDAN, Tim– TAYLOR, Paul A.: Hacktivism and Cyberwars. Rebels with a cause?. Routledge, New York, 2004. p. 1.
- KARATZOGIANNI, Athina: Firebrand Waves of Digital Activism 1994-2014: The Rise and Spread of Hacktivism and Cyberconflict. Palgrave Macmillan, Basingstoke, 2015. p. 22.
- KOVAL, Nikolay: Revolution Hacking. In: GEERS, Kenneth (Ed.): Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCD COE Publications Tallinn, 2015. pp. 55-58.
- KRASZNAY Csaba – VARGA-PERKE Bálint: Ifjúságvédelem a hacker szubkultúrában. In: BÍRÓ A Zoltán – GERGELY Orsolya (Szerk.): Ártalmas vagy hasznos internet? A média hatása a gyermekekre és fiatalokra. Státus Kiadó, Csíkszereda, 2013. pp. 179–202.
- KRASZNAY Csaba (Szerk.): Taktikák és stratégiák a kiberhadviselésben (Megjelenés alatt)
- LEVY, Steven: Hackers: Heroes of the Computer Revolution. Anchor Press/Doubleday, Garden City, 1984. p. 458.
- LOWE, Christian: Kremlin loyalist says launched Estonia cyber-attack. Reuters, 2009. március 13.
- OTTIS, Rain: Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Cooperative Cyber Defence Centre of Excellence, 2008. március 2. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
- Oxblood Ruffin: Hacktivism: From Here to There. Threatpost, 2010. december 9. https://threatpost.com/hacktivism-here-there-120910/74759/

- RAYMOND, Eric S.: The Jargon File, version 4.4.8. Eric S. Raymond's Home Page, 2004. október 1. http://catb.org/jargon/
- ROMAGNA, Marco: Hacktivism: Conceptualization, Techniques, and Historical View. In: HOLT, T. – BOSSLER, A. M. (Eds.): The Palgrave Handbook of International Cybercrime and Cyberdeviance. https://doi.org/10.1007/978-3-319-90307-1_34-1
- RUFFIN, Oxblood: Blondie Wong And The Hong Kong Blondes. Medium, 2015. március 23. https://medium.com/emerging-networks/blondie-wong-and-the-hong-kong-blondes-9886609dd34b
- SCHMITT, Michael N. (Szerk.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge, 2017. p. 94.
- SCHMITT, Michael N.– VIHUL, Liis: Proxy Wars in Cyberspace. Fletcher Security Review, 2014/2. pp. 54-73.
- The Mentor: The Conscience of a Hacker. Phrack Inc., Vol.1., Issue 7., Phile 3 of 10, 1986. http://phrack.org/issues/7/3.html
- TROPEANO, Rosemary: Landmark Senate Hearings Exposed Risks and Threats That Are Still Being Confronted. National Security Archive, 2019. január 9. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2019-01-09/cybersecurity-when-hackers-went-hill-revisiting-l0pht-hearings-1998#_edn1
- TUROVSZKIJ, Danyiil: 'It's our time to serve the Motherland' How Russia's war in Georgia sparked Moscow's modern-day recruitment of criminal hackers. Meduza, 2018. augusztus 7. https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland
- TUROVSZKIJ, Danyiil: Orosz hekkerek. Athenaeum Kiadó, Budapest, 2020. p. 143.
- UCMC Press Center: Security Service of Ukraine possesses audio records of Krasnov's conversations with his Russian supervisor. Ukraine Crisis Media Center, 2016. március 3.
- United States District Court: United States Versus Peter Yuryevich Levashov. United States District Court, 2017. április 4. https://www.justice.gov/opa/press-release/file/956511/download
- WEBBER, Craig– YIP, Michael: The Rise of Chinese Cyber Warriors: Towards a Theoretical Model of Online Hacktivism. International Journal of Cyber Criminology. 2018/1. pp. 230-254.
- YAGODA, Ben: A Short History of "Hack". The New Yorker, 2014. március 6. https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack

4. FEJEZET

NEMZETKÖZI KAPCSOLATOK A KIBERTÉBEN[1]

1. BEVEZETÉS

A kibertér a 2010-es évek végére minden kétséget kizáróan a valós, fizikai tér mellett második életterünkké vált. Amellett, hogy az emberiség közel fele napi szinten használja az internetet magán- és hivatalos teendőinek elvégzésére, a vállalatok és az állami szervezetek is függenek infokommunikációs rendszereik megbízhatóságától. Ez a függés pedig már régen tovább jutott annál a szintnél, amelyet egy szervezet saját hatáskörén belül kezelni tud, mert egymagában nem tudja megoldani a működéséhez szükséges elektronikus információs rendszereinek védelmét. A digitális ellátási láncolatok hihetetlen komplexitása alakult ki, amelynek sérülékenységét teljes egészében egyelőre el sem tudjuk képzelni. Márpedig ez az évtized bebizonyította, hogy akár egy véletlen számítógépes hiba, akár egy jól megtervezett kibertámadás az ellátási láncban komoly gazdasági károkat, sőt emberéleteket veszélyeztethet. Ilyen körülmények között pedig az egyes államhatalmaknak reagálniuk kell, meg kell védeniük nemzetük biztonságát.

Az internet tömeges elterjedésével együtt tehát az egyes államok folyamatosan törekedtek arra, hogy belső biztonságukat a kibertérben is szavatolni tudják. Kialakultak azok a rendészeti, titkosszolgálati eljárásrendek, illetve az ezeket szabályozó jogi normák, amelyek segítségével a digitális úton elkövetett bűncselekményeket kezelni lehetett. Felállították azokat a szervezeteket, amelyek műszaki úton is képesek voltak az információbiztonságot veszélyeztető eseményeket elhárítani. A kiberbűncselekmények számának és főleg az okozott kárnak az emelkedésével azonban minden szakember számára világossá vált, hogy a nemzetközi szervezett bűnözés felfedezte magának ezt a területet is, így nemzetközi rendészeti együttműködések szükségesek ahhoz, hogy a virtuális létet egyre nagyobb számban felfedező állampolgárok biztonsága szavatolható legyen. Megjelent tehát az igény arra, hogy az egyes nemzetállamok közösen lépjenek fel a kibertér fenyegetéseivel szemben. Az Európa Tanács Budapesten elfogadott, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye volt az első olyan jelentős nemzetközi megállapodás, amely ezt a közös fellépést segítette.

A közös fellépés azonban nem minden esetben érdeke a kormányzatoknak. A számítógépes bűnözés visszaszorítása kivétel nélkül minden ország célja, de nem feltétlenül áll érdekükben annak teljes megszüntetése.

[1] Eredetileg megjelent: DEÁK Veronika (Szerk.): Az IBTV. gyakorlata. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára. Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, Budapest, 2020. pp. 6–36., 31 p.

Bizonyos esetekben ugyanis a bűnözői csoportok által használt eszközök és technikák jól hasznosíthatók az állami érdekek szolgálatában is.[2] Már a 2007-es, Észtországot ért kibertámadás is fontos jelzés volt arra, hogy ezek a csoportok és az ő erőforrásaik jól használhatók abban az esetben, ha egy kormányzat nem kíván közvetlenül részt venni egy nyomásgyakorló akcióban, de mégis érvényesíteni kívánja saját érdekeit. Ezek a proxy csoportok jól használhatók akkor is, ha egy ország a pénzügyi egyensúlya fenntartásának érdekében a klasszikus kiberbűnözési módszerekhez nyúl, ahogy azt a 2017-es Wannacry kártékony kód kampány során is lehetett tapasztalni. A nemzetközi rendészeti együttműködés rendszerét pedig felkészületlenül érte az a tény, hogy a bűncselekmények károsultjai és elkövetői földrajzilag nem azonos országban, sőt sokszor nem is egy földrészen vannak, így rá vannak szorulva az elkövető tartózkodási helyén működő bűnüldözők támogatására, de ezt a támogatást nem mindig kapják meg. Míg ugyanis a hagyományos alvilággal jellemzően szembe tudnak szállni a fizikai térben, itt sokszor olyan bűnözői csoportokkal találkoznak, akik bizonyos szempontból védelem alatt állnak. A digitális térben elkövetett visszaélések így sokszor büntetlenül maradnak, a kiberbűnözők és az államilag támogatott titkosszolgálati és katonai csoportok között pedig elmosódott a határ.[3]

Tovább bonyolítja a helyzetet az, hogy mind a hírszerzés, mind a katonai műveletek terén, amelyek állami monopóliumnak számítanak, hangsúlyosan jelenik meg napjainkban a kibertér adta lehetőségek maximális kihasználása. Ez teljesen természetes akkor, amikor az információk szinte kivétel nélkül digitális formában keletkeznek és léteznek teljes életciklusuk során. Ez az emberiség történelme során korábban nem tapasztalt információbőség, illetve az infokommunikációs rendszerektől való függés egyes kormányzatokat arra csábított, hogy stratégiai érdekeik érvényesítése érdekében túllépjen azokon a határokon, amelyet az erkölcs, a jóérzés és az etika egyébként megkövetelt volna. Hangsúlyosan nem a nemzetközi jog és az évszázados normák, hiszen a nagyhatalmak versengésében a kibertér egyfajta Vadnyugatnak számított, ahol senki nem törekedett a közös játékszabályok kialakítására, a meglevő nemzetközi normák pedig nem adtak egyértelmű útmutatást arra vonatkozóan, hogy mit szabad és mit nem, legalábbis számos esetben az érdekelt országok nem kívánták a kibertérre alkalmazni az évszázados normarendszert. Emellett nem is állt rendelkezésre az a kényszerítő erő, amivel a szabályrendszert be lehetett volna tarttatni a normaszegő országokkal. Ez csak a 2010-es évek elejétől változott, amikor a nyugati szövetségi rendszerek és az ENSZ is deklarálta, hogy a nemzetközi jog érvényes a kibertérben is.

Az elmúlt évtizedben a nemzetközi kapcsolatok rendszere a kibertérben egy olyan területté vált, amelyet a széles közvélemény is érzékel, globális hatása van a nemzetközi kapcsolatok rendszerére, a biztonságpolitika egészére, tudományos háttere azonban csak kevesek számára ismert, súlyához mérten kisszámú szakértő

[2] Ezt egyébként az orosz–ukrán háború során Oroszország ellen végrehajtott hacktivista akciók után kikerült információk is bizonyíthatják, amelyek során információk kerültek napvilágra arról, hogy az orosz állam és a Conti nevű kiberbűnözői csoport között kapcsolat van.

[3] Ezzel kapcsolatban érdemes megnézni az FBI Cyber's Most Wanted listáját, amelyen számos kiberbűncselekménnyel állami szereplőket kötnek össze, illetve annak ellenére, hogy ismert az elkövető személye, ők nem kerülnek kiadatásra. Emellett az állítást alátámasztja Turovszkij korábban idézett könyvének számos oknyomozó fejezete is.

foglalkozik vele a nyilvánosan elérhető tudományos szakirodalomban. Magyarországon, a hazai perspektívából pedig gyakorlatilag semmilyen publikáció nem született a témában. Jelen tanulmány ezt a hiányt igyekszik bepótolni, bemutatva mindazokat az eredményeket, amelyek a nemzetközi szaksajtóban elérhetők, összefoglalva a tudományos diskurzus jelenlegi állapotát, egyben irányt mutatva a nemzetközi joggal és biztonságpolitikával foglalkozó közösségnek a kibertér kihívásainak megismeréséhez.

2. NORMÁK A KIBERTÉRBEN

„A nemzetközi jog a nemzetközi közösség tagjai – elsődlegesen és döntő mértékben az államok – közötti kapcsolatokat, viszonyokat szabályozó jogi normák rendszere. A nemzetközi jog tehát azoknak a magatartási szabályoknak az összessége, amelyek a nemzetközi jog alanyai közötti kapcsolatokat rendezik.” – foglalja össze Cserny és Téglási a nemzetközi jog fogalmát a magyar szakirodalom alapján. Majd így folytatják:
„A nemzetközi eredetű normák és a belső jogszabályok viszonyával kapcsolatban elmondható, hogy:

- *a szabályszerűen megkötött nemzetközi szerződések arra kötelezik az államot, hogy a belső jogalkotást a nemzetközi szerződéseknek megfelelően alakítsa.*
- *A belső jogszabállyal kihirdetett nemzetközi szerződések a belső jogszabály formájának megfelelő szinten helyezkednek el a jogszabályok hierarchiájában, azzal, hogy az azonos formában elfogadott szabályok között a nemzetközi eredetű megelőzi a belső eredetű jogszabályt.*
- *Minthogy nemzetközi szerződést nem lehet alkotmányként kihirdetni, a nemzetközi szerződés szabálya nem mondhat ellent az alkotmánynak (Alaptörvénynek), de más belső jogszabállyal kihirdetett nemzetközi szerződés ellentmondhat az azonos vagy alacsonyabb szintű belső jogszabályoknak.*
- *A belső jogszabállyal kihirdetett nemzetközi szerződés a belső jog integráns része lesz.”*[4]

De mi történik akkor, ha robbanásszerűen megjelenik egy új technológia, amelyre a nemzetközi kapcsolatok rendszere nem tudott felkészülni, azonban feszültséget szül a nemzetállamok és nemzetközi közösségek között? Pontosan ezzel a dilemmával szembesült a nemzetközi közösség az információs rendszerek elterjedése miatt. Miközben már az ezredfordulón is voltak jelei annak, hogy egyes országok kormányzati szervezetei előszeretettel támadnak nem egyértelműen állami hírszerzési célpontnak minősülő információs rendszereket információszerzési vagy pusztítási szándékkal, először 2011-ben, a Müncheni Biztonságpolitikai Konferencián beszéltek nagy nyilvánosság előtt arról vezető politikusok, hogy ezzel a problémával valamit kezdeni kell. Ban Ki-moon ENSZ főtitkár hangsúlyozta, hogy a nemzetközi közösségnek közösen kell fellépnie a kibertámadások ellen. A felszólalók arról is szót ejtettek, hogy a határ a kiberbűnözés, a kémkedés és a

[4] CSERNY Ákos – TÉGLÁSI András: Jogforrástan: nemzetközi és uniós jog. Nemzeti Közszolgálati Egyetem, Budapest, 2014.

terrorizmus között kezd elmosódni az interneten.[5] Lattmann így foglalta össze a 2010-es évek első felének jogalkalmazási problémáját:
„Jelenleg nincsenek egyértelműen kötelező, írott hadijogi szabályok, amelyek az informatikai hadviselésre alkalmazhatók lennének. E hiányosságnak több oka van. Egyrészt a létező humanitárius jogi szabályaink kodifikációjának idejében az informatikai hadviselés a mai formájában nem volt realitás. 1949-ben a Genfi egyezmények, vagy 1977-ben a két Kiegészítő jegyzőkönyv elfogadásakor a jogalkotó államok nem kellett, hogy ezzel a kérdéssel foglalkozzanak. Ennek eredményeképpen szerződésalkotó akaratuk nem terjedt ki e sajátos helyzetre, így a humanitárius nemzetközi jog alapelvei (és a hadijog szokásjogi normái) által fedett kérdéseken túlmenően nehezen érvelhető bármilyen kötelező erő.

Másik jelentős probléma a „megfogható" tér, mint elem hiánya. Mi az a „kibertér", és hogyan tudjuk szabályozási területként kezelni? Az egész modern nemzetközi jogrendünk a területük felett szuverenitást gyakorló államokon nyugszik, ennek eredményeképpen mind az erő alkalmazását szabályozó jogrend, mind pedig a humanitárius nemzetközi jog elválaszthatatlan az államterület kérdésétől. Márpedig az informatikai hadviselés területén bajosan tudunk a területiségre alapozni: míg a fizikai csatatereken vannak valamiféle vonalak és államhatárok, ezek nehezen értelmezhetők a kibertérben, ami számos problémára vezethet.

A fentiekből következik, hogy nehezen dönthető el, mi minősül jogszerű katonai célpontnak, valamint hogy ki minősül jogszerű harcosnak, utóbbiakkal szemben pedig milyen intézkedéseket tartunk megengedhetőnek az államok részéről. Ehhez kapcsolódó probléma az esetleges jogsértésekkel szembeni fellépés nehézsége – a tényleges, „fizikai" hadviselés során például a harcokba közvetlenül bebocsátkozó civil személy cselekményének jogsértő jellege a genfi egyezmények meghatározta kritériumok hiányában a helyszínen könnyen felismerhető, valamint a vele szemben való büntetőjogi fellépés az egyezmények szabta keretek között biztosítható. Ám több száz, vagy akár ezer kilométeres távolságból ez nehezen elképzelhető."[6]

A NATO a 2014-es walesi csúcsán egyértelmű választ adott ezekre a kérdésekre. A csúcs zárónyilatkozatának 72. pontjában így fogalmaznak:
„Politikánk szintén elismeri, hogy a nemzetközi jog, így a nemzetközi humanitárius jog és az ENSZ Alapokmány érvényes a kibertérben is."[7]

A nyugati, elsősorban angolszász országok nyilatkozataiban azóta folyamatosan visszaköszön az, hogy a kibertér is hasonló a fizikai térhez, a nemzetközi jogi normák pedig itt is érvényesek. Ez természetesen egy fontos politikai állásfoglalás, azonban számos gyakorlati problémát vet fel, amelyek megoldására valószínűleg évtizednyi időre lesz szükség.

---

5 Munich Security Conference: MSC 2011 Summary. 2011. február https://securityconference.org/en/ (Letöltés ideje:)

6 LATTMANN Tamás: A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén. In: CSAPÓ Zsuzsanna (Szerk.): Emlékkötet Herczegh Géza születésének 85. évfordulójára: A ius in bello fejlődése és mai problémái. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2013. pp. 209-220.

7 NATO: Wales Summit Declaration. 2018. augusztus 30. https://www.nato.int/cps/ic/natohq/official_texts_112964.htm

A NATO CCD COE 2008-ban kezdte meg azt a munkát, melynek során ajánlásokat tett a nemzetközi jog alkalmazására a kibertérben. Ennek eredménye lett az úgynevezett Tallinn Manual, azaz Tallinni Kézikönyv, amelynek első kiadása 2013-ban, második (bővített) kiadása 2017-ben jelent meg.[8] Ez természetesen nem kötelező jellegű, mégis fontos munka abból a szempontból, hogy támpontot, vitaalapot jelent az egyes nemzetállamoknak azzal kapcsolatban, hogyan lehet értelmezni a fennálló nemzetközi jogi kereteket. A jog azonban a közösen elfogadott normákból következik, így először a viselkedési játékszabályokban kell megállapodni. Tekintettel arra, hogy minden ország kivétel nélkül sebezhető az információs rendszerein keresztül, ez a kiegyezés néhány éven belül meg kell, hogy történjen. Anna-Maria Osula és Henry Rõigas kétfajta normát különböztet meg. Egyrészt vannak olyan normák, amelyek jogilag kötelező érvényű kötelezettségek, például a nemzetközi egyezmények. Másrészt vannak olyan nemzetközi normák, amelyek referenciapontként szolgálnak az elvárt viselkedéssel kapcsolatban, idővel kötelező érvényűvé válnak, de kezdetben nem kötelező érvényű jogi aktusok, és elsősorban diplomáciai megállapodásokban érhetők tetten.[9]

A normák kialakítása történhet kétoldalú, úgynevezett bilaterális és többoldalú, úgynevezett multilaterális megállapodások keretében. A kibertér jellegéből adódóan összekapcsolt, komplex, egymástól függő információs rendszereket jelent, amelyek egyes elemei különböző országokban lehetnek, az egyes kibertéri eseményeknek mégis nemzeti hatása lehet. Munk ezt a következőképp fogalmazza meg:
„A harmadik kérdés úgy fogalmazható meg, hogy a kibertér globális jellegű, vagy egy adott szereplő szempontjából értelmezett, körülhatárolt. A legtöbb meghatározásban nincs utalás a szereplő-orientált megközelítésre, így ezek – bár nem zárják ki a másik változatot – a globális jelleget sugallják. Több esetben találkozhatunk azonban a szereplő-orientált megközelítéssel is, amelyek nemzeti kibertérről beszélnek. A két megközelítés nem zárja ki egymást, ugyanis egy szereplő-orientált kibertér nyilvánvalóan a globális kibertér valamely szempontok alapján körülhatárolt része, azonban egy meghatározásból – ha nem tartalmaz jelzős megkülönböztetést – egyértelműen ki kell tűnnie, hogy melyik megközelítésre épül.”[10]

A kibertér esetében tehát mindkét megállapodástípusnak van létjogosultsága. Egyrészt a globális normákat szabályozni szükséges annak érdekében, hogy minden kibertéri szereplő elfogadjon bizonyos alapszabályokat. A Budapest Egyezmény egy jó példa arra a közös szándékra, ami egy multilaterális egyezményhez vezethet. De ugyanígy van indoka a bilaterális megállapodásoknak is, például, ha egyes nemzeti létfontosságú információs rendszerek vagy rendszerelemek a nemzeti határokon túl üzemelnek, mint ahogy Magyarország esetében ez a távközlési szektor esetében történik. Az egyes országok diplomáciai kapcsolatán túl tehát kiemelt fontossága van azoknak a nemzetközi szervezeteknek, amelyek a globális vagy régiós, multilaterális normák kialakításában vesznek részt.

---

8 A harmadik kiadás 2023-ra várható.

9 OSULA, Anna-Maria – RÕIGAS, Henry: Introduction. In: OSULA, Anna-Maria – RÕIGAS, Henry (Eds.): International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn, 2016. pp. 11-22.

10 MUNK Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. Hadtudomány, 2018/1. pp. 113-131.

3. A NEMZETKÖZI SZERVEZETEK SZEREPE A KIBERTÉR BIZTONSÁGÁNAK GARANTÁLÁSÁBAN

3.1. Egyesült Nemzetek Szervezete (ENSZ)

A globális biztonsági megállapodások létrehozásának elsődleges terepe az Egyesült Nemzetek Szervezete, az ENSZ. A 193 tagország folyamatos párbeszéde lehetőséget biztosít arra, hogy minden szempont és érvrendszer napvilágra kerüljön, szakosított intézményein keresztül pedig a fejlett országok számára egyébként rejtett kihívásokra is fény derülhet. Éppen ezért kiemelt fontosságú az ENSZ tevékenysége a globális kiberbiztonság megteremtésében.

Az ENSZ már az új évezred elejétől kiemelt célként tekint az infokommunikáció elterjesztésére. A 2000 és 2015 közötti időszakra megfogalmazott Millenniumi Fejlesztési Célok (MDG[11]) között is szerepel a hozzáférés segítése az új technológiákhoz, mérőszámként pedig a 100 főre jutó internetfelhasználók számát jelölték meg. Ezt követte a 2030 Menetrend a Fenntartható Fejlődésért (2030 Agenda for Sustainable Development) program, amely a fenntartható fejlődés érdekében 17 Fenntartható Fejlődési Célt (Sustainable Development Goal – SDG) jelöl meg. Ezek között nem szerepel direkt infokommunikációs cél, viszont minden egyes cél mögött ott van az informatika, mint a megvalósítást lehetővé tevő eszköz, illetve mint paradigmaváltó megoldás, amely hozzájárul a célok újszerű, innovatív eléréséhez. Ha tehát az informatika az alapköve a globális jólét biztosításának, akkor ennek az alapkőnek a biztonsága is fontos.

Az ENSZ kiberbiztonsággal kapcsolatos tevékenysége két fő csapásirány felé indult el. Tim Maurer ezt politikai-katonai és gazdasági irányoknak nevezte el, praktikusan a kiberhadviselés és a kiberbűnözés kezelése szerepel a nemzetközi szervezet napirendjén.[12] Ide tartozhat még az internetirányítással kapcsolatos tevékenység és a gyermekek online védelme is, bár ezek nem elsősorban kiberbiztonsággal kapcsolatos tevékenységek. A kiberbiztonsággal kapcsolatos érdemi tevékenység az ENSZ-ben 1998-ban kezdődött, amikor az orosz kormány kért állásfoglalást az ENSZ Közgyűlést támogató Első Bizottságtól, amely a Leszerelési és Nemzetközi Biztonsági Bizottság nevet viseli. A nézetkülönbségek már ekkor megjelentek az Egyesült Államok és az Orosz Föderáció között. Az USA mélyebb együttműködést várt volna el a kiberbűnözés területén, ez azonban az orosz álláspont szerint az alkotmányukba ütközne, hiszen idegen rendőri erők vizsgálnák a szuverén orosz kiberteret. Oroszország a kibertérben használatos fegyverek korlátozására vonatkozó kérelemmel állt elő, amerikai vélemények szerint azért, hogy megakadályozzák az USA erőfölényének kialakulását. Szintén problémás terület Biztonsági Tanács két tagja között az interneten megjelenő szólásszabadság kérdése, amely az orosz fél szerint politikailag destabilizálhatja az országot. Ez megegyezik Kína álláspontjával is, bár az ázsiai fél a két ország közötti vitában viszonylag ritkán nyilvánított véleményt. Az első határozatot egyébként 1999-ben

[11] Millennium Development Goals

[12] MAURER, Tim: Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security. Belfer Center for Science and International Affairs, 2011.

adták ki, 53/70, „Developments in the Field of Information and Telecommunications in the Context of International Security" címmel, orosz kezdeményezésre.

A téma komplexitását mutatja, hogy a kibertérben megjelenő normákkal kapcsolatban a hat bizottság közül három is javaslatot nyújtott be, az Első Bizottság mellett a Második Bizottság (Gazdasági és Pénzügyi Bizottság) és a Harmadik Bizottság (Szociális, Humanitárius és Kulturális Bizottság) is foglalkozott a kérdéssel. 2018-ig összesen öt, úgynevezett kormányzati szakértői csoport (Group of Governmental Experts – GGE) ült össze, hogy megvizsgálja az infokommunikációs technológiákban rejlő lehetséges veszélyeket. Ezek az ENSZ Közgyűlés 58/32 határozata alapján működtek, amelyet 2003-ban fogadtak el.

2009-től új lendületet kapott a korábban sikertelen GGE-testület, hiszen az észtországi kibertámadás, illetve a 2008-as grúziai háború megmutatta, milyen hatással lehetnek a nemzetközi kapcsolatokra a kibertérben történő műveletek. A rendszeressé váló, kétéves mandátumokkal rendelkező GGE-k az alábbi eredményeket érték el:

- 2010: A GGE együttműködést szorgalmazott a tagállamok, a privát szektor és a civil társadalom között, valamint ajánlásokat fogalmazott meg az infokommunikációs leállásokból fakadó félreértések elkerülése végett. Ezek magukba foglalták a bizalomerősítő és kockázatcsökkentő lépéseket, a nemzeti jogrendbe ültetett információmegosztást, a szabályalkotást és jógyakorlatok megosztását, valamint a kevésbé fejlett országok képesség-fejlesztését.
- 2012/2013: A Közgyűlés 66/24 számú határozatával a harmadik GGE is mandátumot kapott és 2013-ban egy konszenzusos nyilatkozatot tett közzé. Eszerint a nemzetközi jog, különösen az ENSZ Alapokmány érvényes a kibertérben is, az állami szuverenitást garantáló normák és kötelezettségek minden, a tagállamok által a kibertérben végrehajtott műveletre érvényesek, beleértve ebbe a tagállamok területén levő infokommunikációs infrastruktúrák használatát is. A GGE-tagok abban is megállapodtak, hogy nem megengedett a proxyk használata a szándékosan jogellenes cselekmények végrehajtásához, valamint ezen csoportok számára nem lehet átengedni a nemzeti kiberteret. A nyilatkozat felszólít a további párbeszédre, valamint a bizalomépítéssel és képességfejlesztéssel kapcsolatos ajánlásokat is tesz. Bátorítja továbbá a nemzeti eseménykezelő központos (CERT[13]-ek) együttműködését is.
- 2014/2015: A negyedik GGE a 68/243 számú határozat alapján alakult meg 20 taggal, konszenzusos beszámolóját 2015 júniusában adta közre. Épít a korábbi GGE-riportokra, de kiegészíti azokat az önkéntes, nem kötelező normák, szabályok és elvek alkalmazásának javaslatával. A korábbi nemzetközi jogi elveket kiterjesztve foglalkozik a hadijog kérdéseivel is a kibertérben. Az ENSZ Közgyűlés elfogadta a jelentést, és felhívta a tagállamokat az abban foglaltak betartására, amely minden korábbinál erősebb jelzés volt.

[13] Computer Emergency Response Team

- 2016/2017: Az ötödik GGE a 70/723 számú határozattal alakult meg, de nem sikerült konszenzusos nyilatkozatot tennie. Az Egyesült Államok nyilatkozata szerint a sikertelenség oka az volt, hogy a tagállamok nem tudtak megegyezni abban, hogyan vonatkozik a nemzetközi jog az államok válaszaira és ellenintézkedéseire a kiberbiztonsági incidensek során. Az USA álláspontja szerint, ha nem ismerik el jogosnak egy állam válaszát a rosszindulatú kibertevékenységekkel kapcsolatban, nem lehet a szükséges elrettentést megvalósítani a technológiák rosszindulatú használatának elkerülése érdekében. A másik oldalon a kubai delegáció fejezte ki azon félelmét, hogy egy ilyen felhatalmazással egyes országok egyoldalú akciókat indíthatnak kibertámadásokra hivatkozva, ezzel militarizálva a kiberteret. Valószínűleg az orosz és a kínai delegációk is ezt a véleményt osztották, bár az ő állásfoglalásuk nem került nyilvánosságra.[14,15]
- 2019/2021: A hatodik GGE a 73/266 számú határozat alapján indult el. Konszenzusos jelentése megerősíti, hogy a korábbi jelentésekben azonosított súlyos IKT-fenyegetések továbbra is fennállnak. Hangsúlyozza az alábbiakkal kapcsolatos komoly aggodalmakat: a kritikus infrastruktúrát érintő káros IKT-tevékenységek; az IKT-alapú titkos információs kampányok államok általi rosszindulatú felhasználásának növekedése egy másik állam folyamatainak, rendszereinek és általános stabilitásának befolyásolására; valamint a sebezhetőségek kihasználására irányuló rosszindulatú IKT-tevékenység. A GGE ebben a jelentésben megerősítette, hogy a normák és a hatályos nemzetközi jog egymás mellett állnak, a normák pedig a nemzetközi közösség elvárásait tükrözik, és olyan kereteket határoznak meg a felelős állami magatartásra vonatkozóan, amelyek idővel pedig a szokásjog részévé válnak. A csoport megbízásából a GGE 2015 13 önkéntes normájának további értelmezését is kidolgozta. Szintén megerősítették a nemzetközi jog, és különösen az ENSZ Alapokmányának teljes egészében az IKT-környezetre való alkalmazhatóságát. A csoport hangsúlyozta, hogy a nemzetközi humanitárius jog csak fegyveres konfliktusban alkalmazandó. Ugyanakkor a bevett nemzetközi jogi elvek, köztük az emberiesség, a szükségesség, az arányosság és a megkülönböztetés elveinek az IKT-k használatára való alkalmazása további tanulmányozást igényel. Emellett a bizalomépítő intézkedésekkel, a nemzetközi együttműködéssel és segítségnyújtással foglalkozik az IKT-biztonság és a kapacitásépítés terén.

A hatodik GGE mellett egy párhuzamos formátum, a Nyitott Munkacsoport (Open Ended Working Group – OEWG) is elkezdte a működését 2019-ben, amit elsősorban Oroszország támogatott. Az OEWG a nemzetközi biztonsággal összefüggésben az IKT-k területén bekövetkezett fejleményekkel foglalkozott. A csoport a harmadik és egyben utolsó érdemi ülésén elfogadta zárójelentését. A jelentés megerősítette a GGE korábbi jelentéseinek eredményeit, valamint azt, hogy

[14] Elaine Korzak: UN GGE on Cybersecurity: The End of an Era? The Diplomat, 2017. július 31. https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/

[15] Nuclear Threat Initiative: The UN Groups of Governmental Experts (GGE). 2016. január. https://www.nti.org/education-center/treaties-and-regimes/united-nations-groups-governmental-experts/

a nemzetközi jog, és különösen az ENSZ Alapokmánya a kibertérre is alkalmazandó. A normák nem helyettesítik vagy módosítják az államok nemzetközi jog szerinti kötelezettségeit vagy jogait – amelyek kötelező erejűek –, hanem inkább kiegészítő és konkrét útmutatást nyújtanak arra vonatkozóan, hogy mi minősül felelős állami magatartásnak az IKT-k használata során, illetve ezek idővel kötelező érvényűvé is válhatnak. A jelentés azt ajánlja, hogy az államok önkéntesen határozzák meg és fontolják meg a sajátos helyzetüknek megfelelő bizalomépítő intézkedéseket (Confidence-Building Measures – CBM), és működjenek együtt más államokkal azok végrehajtásában. A jelentés átfogó kapacitásépítési intézkedéseket is felvázol az IKT-biztonság területén. Az OEWG mandátumát a 2021–2025 közötti időtartamra meghosszabbították, új GGE jelen tanulmány írásakor még nem került megalakításra.

3.2. Nemzetközi Távközlési Egyesület (ITU)

A Nemzetközi Távközlési Egyesület (International Telecommunication Union – ITU) az ENSZ infokommunikációs technológiákra specializálódott szervezete. Kiemelt szerepe van az elektromágneses spektrumgazdálkodás és a műholdpályák globális kezelésében, emellett hatáskörébe tartozik az infokommunikációs területen az összekapcsolódást segítő interoperabilitási szabványok kiadása, és általánosságban a technológiához való hozzáférés elősegítése. Jelenleg 193 tagországa és közel 800 privát szektorba tartozó, illetve akadémiai tagja van. Székhelye Genfben található.

Mint az ENSZ szakosított szervezetének, elsősorban az ITU-nak a feladata a globális kibertérrel kapcsolatos műszaki megfontolások kezelése, így szerepet vállal a kiberbiztonság elterjesztésében is. Ennek fő hajtóereje a Connect 2020 Agenda for Global Telecommunication/ICT Development, amely a tagországok stratégiai céljait fogalmazza meg az infokommunikációs területen. Magyarország Connect 2020-szal kapcsolatos nemzeti vállalása a következő:
„Mindannyian büszkék vagyunk arra, hogy a közelmúltban indult két, az ágazatra vonatkozó kezdeményezés: a Nemzeti Infokommunikációs Stratégia és a Digitális Jólét Program. Mindkét stratégia négy pillérre épül – teljes összhangban az ITU stratégiai gondolkodásával. Ezek az elemek biztosítják majd azt, hogy az IKT ágazat szolgálni fogja a munkahelyteremtést, a kutatást és fejlesztést, a fenntartható gazdasági növekedést és a társadalmi szolidaritást. Az iparági tendenciák és a horizontális fejlesztési célok azonosítása alapján számos, a nemzeti stratégiákban megjelölt célkitűzés tökéletesen illeszkedik a Connect 2020 négy egymást kiegészítő céljához."[16]

A stratégiai célok között szerepel a fenntarthatóság, amely a telekommunikációs és IKT fejlődésből eredő kihívások kezelését hivatott megoldani. Ezen belül az egyik indikátor a kiberbiztonsági felkészültség 40 százalékkal történő javítása. Ennek érdekében az ITU számos, kiberbiztonsággal kapcsolatos programot indított el:

[16] ITU: On the road to implement the Connect 2020 Agenda. 2014. https://studylib.net/doc/12920596/on-the-road-to-implement-the-connect-2020-agenda

- A nemzeti eseménykezelő központok (Computer Incident Response Team – CIRT) közötti együttműködés támogatása, amelynek jelenleg 103 teljes jogú tagja van, köztük Magyarország.
- A Globális Kiberbiztonsági Index (Global Cybersecurity Index) évenkénti elkészítése, amely objektív szempontok alapján mutatja be a tagországok felkészültségét. Magyarország a 2017-es felmérésben az európai középmezőnybe került, ez azonban elsősorban az adatszolgáltatás hiányosságának köszönhető, nem a valós képet mutatja.[17]
- Az online gyermekvédelem (Protecting Children Online) elősegítése. Magyarország aktív részese az ITU vonatkozó kezdeményezésének.
- A nemzeti kiberbiztonsági stratégiák létrehozása, amelyet az ITU keretrendszere (Guide to Developing a National Cybersecurity Strategy) támogat. A magyar kiberbiztonsági stratégia jelenleg nincs összhangban ezzel a keretrendszerrel, nem véletlen, hogy a Nemzeti Biztonsági Stratégia elvárja egy új nemzeti kiberbiztonsági stratégia megalkotását.
- A kiberbiztonsággal kapcsolatos területek szabványosítása, amely a Study Group 17 csoporton belül történik és már közel 170 olyan ajánlást fogalmaztak meg, amely hozzájárulhat a biztonságosabb kibertér kialakításához.
- Az ITU történelmi mandátumához igazodva a rádiókommunikációs rendszerek biztonságának megerősítése is szerepel a kiberbiztonsággal kapcsolatos feladatok között.[18]

Ahogy korábban említésre került, az ENSZ 2030 Agenda for Sustainable Development programban megfogalmazott Fenntartható Fejlődési Céljainak nélkülözhetetlen hátteret jelentenek az infokommunikációs technológiák. Az ITU az információs társadalommal foglalkozó világ-csúcstalálkozó (World Summit on the Information Society Forum – WSIS) keretében ad teret a fenti célok és a technológia kapcsolatának megvitatására. A WSIS 2004 óta évente kerül megrendezésre, a globális információs társadalom fejlesztésének legjelentősebb globális fóruma, ahol állami és nem állami szereplők osztják meg egymással véleményüket. A WSIS úgynevezett Akcióvonalakat (Action Lines) jelöl ki, amelyek mentén a diskurzus halad. Ezek közül az ötödik foglalkozik a kiberbiztonsággal, pontos neve Bizalom és Biztonság építése az IKT technológiák használata során (Building Confidence and Security in the use of ICTs). Az itt folyó munkának a 2007-ben kiadott ITU Globális Kiberbiztonsági Agenda (Global Cybersecurity Agenda – GCA) ad alapot. Ennek öt stratégiai pillére a jogi, a technológiai és eljárásbeli, szervezeti, képességépítési és nemzetközi együttműködési kérdésekkel foglalkozik.

A kibertér nemzetközi kapcsolatrendszerében azonban a legfontosabb olyan töréspont, amiben az ITU-nak is szerepe van, az az internetirányítás, azaz internet governance kérdése. A WSIS a következőképpen határozta meg az internetirányítás fogalmát:

[17] A 2020-as felmérésen Magyarország a globális 35. helyet érte el, Európában a 22.
[18] ITU: ITU Cybersecurity Activities. 2018. július 5. https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

„Az internetirányítás azon fejlesztések és alkalmazások összessége, melyet a kormányok, a magánszektor és a civil társadalom saját szerepkörükben hajtanak végre, megosztott elvek, normák, szabályok, döntéshozatali eljárások és programok mentén az internet fejlődésének és használatának érdekében."[19]

Leegyszerűsítve viszont annak problémáját hozza felszínre, hogy valójában ki irányítja az internet működéséhez nélkülözhetetlen erőforrások szétosztását. Mivel az internet amerikai találmány, a történelmi hagyományok szerint az olyan nélkülözhetetlen információk kiosztása, mint a felsőszintű doménnevek, az IP-címek és tartományok, valamint az alkalmazásokhoz csatolt portszámok, jelenleg a Los Angelesben működő Internet Corporation for Assigned Names and Numbers (ICANN) nonprofit szervezet kezében vannak. Ezt egészen 1998-as haláláig Jon Postel amerikai informatikus irányította egyszemélyben. Bár az ICANN igyekezett függetlenül és átláthatóan működni, működésének jogi háttere elvileg lehetővé tette azt, hogy az USA kormányzatára szálljon át a felsőszintű doménnevek kezelése, ami elfogadhatatlan lett volna más nagyhatalmak számára. Ennek megoldására az ITU elindította az Internetirányítási Fórumot (Internet Governance Forum – IGF), amelynek célja egy globálisan elfogadható irányítási modell kidolgozása. 2016-ban végül az ICANN és az amerikai kormányzat közötti függőségi viszony megszűnt, jelenleg egy többszereplős testület irányítja a globális internetet. Az ITU-nak tehát kiemelten fontos szerepe van abban, hogy ENSZ szervezetként konszenzust tudjon kialakítani a nemzeti érdekek rengetegében, és az internet valóban egy globális, mindenki javát szolgáló szolgáltatás lehessen.

3.3. Európai Biztonsági és Együttműködési Szervezet (EBESZ)

Az Európai Biztonsági és Együttműködési Szervezet (EBESZ, angolul Organization for Security and Cooperation in Europe – OSCE) a világ legnagyobb, kizárólag biztonsággal foglalkozó kormányközi szervezete. Mandátumához tartozik többek között a fegyverzetellenőrzés, az emberi jogok támogatása, a sajtószabadság ellenőrzése és a választások tisztaságának kontrollja. Titkársága Bécsben működik. 57 tagja elsősorban Európából kerül ki, de részt vesznek benne az európai biztonságra hatással bíró nagyhatalmak, illetve a volt Szovjetunió több tagországa is. 11 társult tagországa van. Gyökerei 1973-ig nyúlnak vissza, amikor az Európai Biztonsági és Együttműködési Értekezlet (EBEÉ, angolul Conference on Security and Co-operation in Europe – CSCE) története megkezdődött. Jelenlegi formájában 1995-ben jött létre az 1994-es, Budapesten tartott kongresszus folyományaként.

Az EBESZ kiberbiztonsággal foglalkozó tevékenysége kiemelten fontos a kibertér globális biztonságának megteremtésében. Ugyan az itt kötött megállapodások jogilag nem kötelező érvényűek, a kialkudott normák önkéntesek, elsősorban politikai kötelezettséget jelentenek, de az egyes tagállamoknak így nagyobb mozgásterük van, mint például az ENSZ-ben. Az ilyen normákat bizalomerősítő intézkedésnek, azaz confidence-building measure-nek (CBM) nevezik, amelyek eredetileg a hidegháború feszültségének enyhítésére jöttek létre. A koncepció lényege, hogy a konfliktushelyzetben lévő mindkét (vagy több) fél támadástól való félelmének csökkentése érdekében tegyenek olyan lépéseket, amelyek segítenek az eszkaláció megelőzésében. Mivel a kibertérben történő akciók

[19] ITU: Report of the Working Group on Internet Governance. 2005. http://www.wgig.org/docs/WGIGREPORT.pdf

jellegüknél fogva hasonlóképp rontják az országok közötti bizalmat, mint ahogy azt a nukleáris fegyverkezés idejében láthattuk, a CBM-ek jó megoldást jelenthetnek egy kontrollálhatatlan kiberkonfliktus kitörésének megelőzéséhez is.

Az ENSZ korábban említett GGE jelentései közül a 2013-as és a 2015-ös is kiemeli az államok közötti transzparencia, együttműködés és stabilitás növelésének igényét a bizalomerősítő intézkedések útján. Mivel ez az EBESZ elsődleges küldetései közé tartozik, történelmileg pedig komoly eredményeket ért el a szervezet a hidegháború során az amerikai és szovjet felek között, azaz van tapasztalata a nagyhatalmak közötti közvetítésben, 2012-ben formálisan is felvállalta a kiberbiztonság kérdésének kezelését. Az EBESZ Állandó Tanácsa a PC.DEC/1039 számú döntésével indította útjára azt az informális munkacsoportot, amely a kibertérben történő bizalomépítést kapta feladatául. A határozat címe „Development of confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies" azaz Bizalomépítő intézkedések létrehozása az infokommunikációs technológiák használatából eredő konfliktusok kockázatának csökkentése érdekében. Ennek első eredményeit a 2013-ban kiadott PC.DEC/1106 határozatból ismerhette meg a nagyvilág, majd 2016-ban a PC.DEC/1202 tartalmazta a végső eredményeket. Az ebben szereplő CBM-ek a következők:

- Magatartással kapcsolatos CBM-ek:
  - Információmegosztás az IKT használatból adódó nemzeti és transznacionális kockázatokkal kapcsolatban (CBM 1);
  - Információmegosztás a nyílt, interoperábilis, biztonságos és megbízható internet létrehozásának érdekében tett lépésekről (CBM 4);
  - Információmegosztás a nemzeti szervezetekről, stratégiákról, szabályokról és programokról (CBM 7);
  - Az IKT-val kapcsolatos nemzeti terminológiák listája (CBM 9).

- Kommunikációval kapcsolatos CBM-ek:
  - Konzultációk tartása a politikai és katonai feszültségek csökkentése érdekében (CBM 3);
  - Az EBESZ, mint platform használata a párbeszédre, a jógyakorlatok cseréjére, a tudatosságnövelésre és a képességfejlesztéssel kapcsolatos információmegosztásra (CBM 5);
  - Nemzetközi munkacsoport létrehozása, amely évente legalább háromszor ülésezik, illetve további CBM-eket javasol (CBM 11);
  - Nemzeti kapcsolattartó kinevezése, akinél a vitás eseteket jelezni lehet (CBM 8);
  - A kommunikációs vonalak azonosítása és azok hatékonyságának ellenőrzése (CBM 13).

- Felkészültséggel kapcsolatos CBM-ek:
  - A releváns nemzeti szervezetek közötti együttműködés elősegítése (CBM 2);
  - Hatékony jogszabályalkotás a határokon túlnyúló műveletek támogatása érdekében azon hatóságok között, amelyek az IKT-eszközök segítségével végrehajtott terrorista és bűnözői tevékenységek elhárításával foglalkoznak (CBM 6);
  - Együttműködési tevékenységek azonosítása a kockázatcsökkentés érdekében (CBM 12);
  - A létfontosságú információs rendszerek védelmének megerősítése (CBM 15);
  - Az IKT sebezhetőségek jelentése, beleértve ebbe a privát szektort is (CBM 16).

Az EBESZ által kidolgozott CBM-ek hatékonyan segítik az ENSZ céljainak gyakorlati megvalósulását. Ezt támasztja alá az a tény, hogy az EBESZ tagok 90%-a, 52 delegált vesz részt egy vagy több CBM-ben. A CBM 8 alapján például mind az 52 tag kijelölt egy nemzeti kapcsolattartót, de a CBM 7 szerinti információmegosztás a nemzeti szervezetekről és jogszabályokról is 42 résztvevőt vonzott. Jelen kötet megjelenésének idején a PC.DEC/1039 által létrehozott informális munkacsoport vezetője Magyarország állandó képviselője.[20]

4. A NEMZETKÖZI JOG SZEREPE A KIBERTÉRBEN

A nemzetközi szervezetek fontos szerepet töltenek be az egyes államok viselkedési normáinak kialakításában, de ezek önkéntes, politikai szintű kötelezettséget jelentenek csupán, melyek fontosak ugyan, de a jogi garanciák nélkül nem tudják teljes értékűen garantálni a kibertér biztonságát. Ezeket a jogi garanciákat a már meglevő nemzetközi jogban kell keresni, hiszen a 2013-as GGE-jelentésben, és azóta is többször, többen kijelentették, hogy a nemzetközi jog érvényes a kibertérben is. A gyakorlatban azonban a kibertevékenységeknek vannak olyan sajátosságai, amelyek nem teszik egyértelművé a nemzetközi jog alkalmazását. A Tallinni Kézikönyv ezt a megértést hivatott segíteni, de ez egy fontos tudományos mű, nem az államok közötti együttműködés elfogadott kódexe. Lattmann a következőképp foglalja össze a Tallinni Kézikönyv szerepét:
„A kodifikált szabályok hiánya ugyanakkor nem jelent teljes szabályozatlanságot. A nemzetközi humanitárius jog szokásjogi alapon kötelező elveinek alapul vételével kialakíthatók olyan szabályok, amelyek alkalmazhatósága nehezen megkérdőjelezhető egy informatikai támadás, vagy akár egy átfogó „kiberháború" során. Ehhez alapként az 1977-ben elfogadott I. Kiegészítő jegyzőkönyvet lehet használni, amely számos olyan hadviselési normát foglalt írásos, nemzetközi szerződési formába, amelyek informatikai támadások esetében is alkalmazhatóak. E munka első eredménye a 2013-ban megjelent Tallinni kézikönyv, amely első alkalommal tett kísérletet e szabályok rendszerbe foglalt megjelenítésére, majd ezt 2017-ben egy újabb kiadás követte. Ezek a munkák olyan szakértői értelmezést jelentenek, amelyek célja, hogy a létező hadviselési jogi normák felhasználásával

[20] DÁN Károly: Promoting confidence in Cyberspace: The workings of the OSCE. Elhangzott: Nemzeti Közszolgálati Egyetem, 2018. 03. 12.

állítsanak elő egy olyan szabálygyűjteményt, ami egyrészt tükrözi a jelenleg létező alkalmazható szabályokat, másrészt pedig egy későbbi nemzetközi szerződés alapjául is szolgálhatnak akár. Nemzetközi jogi értelemben a kézikönyvek tartalma nem kötelezi az államokat – ám a szokásjogi erejű normák alkalmazásától nem térhetnek el."[21]

Michael N. Schmitt és Liis Vihul véleménye szerint két olyan területe van a nemzetközi jognak, ahol a kibertéri cselekmények értelmezése aránylag előrehaladott, legalábbis a Tallinni Kézikönyv ezeket a területeket tárgyalja részletesen. Ezek a háború indításának joga (jus ad bellum) és a nemzetközi humanitárius jog (jus in bello). Mindkét esetben olyan szabályozásokról beszélünk, amelyek már a második világháború után, évtizedekkel ezelőtt létrejöttek, bőven az infokommunikációs eszközök és a számítógépes hálózatok megjelenése előtt.[22] Alapelveik azonban adaptálhatók a virtuális térre is. Bódi, Kádár és Petruska történeti áttekintést is adva a jus ad bellumot és a jus in bello-t az alábbiak szerint foglalja össze:

„Az államközi viták erőszakos rendezése egyidős az államok alapításával. A klasszikus nemzetközi jogban a háború indításának joga (ius ad bellum) az állami szuverenitás részét képezte.

- *A hadüzenet átvételével a hadviselő országok között beállt a hadiállapot.*
- *Ultimátum küldése esetén az abban foglalt követelések teljesítésének elmaradása esetén állt be hadiállapot.*
- *A hadiállapot beálltakor a hadviselő felek közötti szerződések megszűntek és a diplomáciai kapcsolatok megszakadtak, még akkor is, ha tényleges harccselekményekre nem került sor. Minden kívülálló ország köteles volt semleges maradni. […]*

A II. világháború pusztításai és a nukleáris fegyverek megjelenése nyilvánvalóvá tették, hogy egy jövőbeni világháború akár az emberiség pusztulását is eredményezheti, ezért a háború indításának jogát mindenképpen korlátozni kellett. Az ENSZ Alapokmányának 2. cikk (4) bekezdése (államok közötti erőszak teljes tilalma) ezért kimondja, hogy „a szervezet összes tagjának nemzetközi érintkezései során más állam területi épsége vagy politikai függetlensége ellen irányuló, vagy az ENSZ céljaival össze nem férő bármely más módon megnyilvánuló erőszakkal való fenyegetéstől, vagy erőszak alkalmazásától tartózkodnia kell." […] Az ENSZ elismeri az államok önvédelemhez való jogát, azaz fegyveres erőik önvédelmi helyzetben való alkalmazását. Az ENSZ Alapokmányának alapján a nemzetközi béke és biztonság fenntartásának elsődleges felelőssége az ENSZ Biztonsági Tanácsánál van, amelynek hatásos és érdemi döntéséhez a megtámadott, önvédelmet gyakorló államnak is igazodnia kell."

A jus in bello összefoglalása a következő:

„A háború nemzetközi joga (ius in bello) a háborúskodással járó pusztítást az elkerülhetetlenül legcsekélyebb mértékűre korlátozta. A hadijog a szabályozás

---

[21] LATTMANN Tamás: Nemzetközi jogi szabályozás célzott kibertámadások esetén. In: DEÁK Veronika (Szerk.): Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszolgálati Egyetem, 2018.

[22] SCHMITT, Michael N.– VIHUL, Liis: The Nature of International Law Cyber Norms. In: OSULA, Anna-Maria, RÕIGAS, Henry (Eds.): International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn, 2016. pp. 23-48.

tárgya alapján két nagy csoportra (hágai és genfi jog) osztható fel mind a mai napig. A hágai jog a katonai célpontok és a bevethető fegyverek korlátozását írja elő. […] A hágai jog kötelezi az egyezményt aláírókon kívül azokat a hadban álló feleket is, akik ellenfele egyoldalú nyilatkozattal a rendelkezéseit elismeri, vagy legalábbis ténylegesen alkalmazza. A hágai jog előírta, hogy a háborút hadüzenetnek vagy ultimátumnak, azaz feltételhez kötött hadüzenetnek kell megelőznie. A semleges államok hadicselekményben nem vehetnek részt, sőt nem tehetnek semmilyen, valamelyik fél számára kedvező intézkedést (például felvonulási terület, repülőtér átengedése, rádióállomások telepítése). […] A hágai jog egyik pillére a harcosok (kombattánsok) megkülönböztetése a polgári személyektől ez utóbbiak kímélése érdekében. A IV. számú hágai egyezmény és az azt kibővítő 1949-es genfi jog értelmében a reguláris és irreguláris (önként fegyvert fogó lakosság, ellenálló szabadcsapatok, gerillák) csapatok bárhol kifejthetik harctevékenységüket, ha élükön felelős személy áll, messziről felismerhető megkülönböztető jelvényt viselnek, fegyvereiket nyíltan viselik, valamint hadműveleteik során a háború törvényeihez, szokásaihoz alkalmazkodnak. Egy partizánháború esetén a nyílt jelvény- és fegyverviselés elképzelhetetlen, azért az 1977-es I. számú kiegészítő jegyzőkönyv óta csak az összecsapás és az azt megelőző felfejlődéskor követeli meg a nyílt fegyverviselést a jog. A totális háborút a hágai egyezmények kizárják, és megtiltják az ellenséges tulajdon elpusztítását is, kivéve, ha azt a háború követelményei mindenképpen megkívánják. Katonai célpontok kizárólag azok az objektumok lehetnek, amelyek az ellenséges katonai erőfeszítéseket szolgálják. A „feleknek nincs korlátlan joguk az ellenségnek ártó eszközök megválasztásában”, ezért a megkülönböztetés nélkül ható, tömegpusztító, nem csupán katonai célpontok ellen használható nukleáris eszközök alkalmazását a nemzetközi jog eleve kizárja.

A genfi jog tárgya a háború áldozatainak védelme, amelynek rendezésére 1949-ben, Genfben négy átfogó egyezményt kötöttek: az elsőt a hadra kelt fegyveres erők sebesültjei és betegei helyzetének javítására, a másodikat tengeri haderők sebesültjei, betegei és hajótöröttjei helyzetének javítására, a harmadikat a hadifoglyokkal való bánásmódra, a negyediket pedig a polgári lakosság háború idején való védelmére. […] A genfi jog személyi hatálya a háborús áldozatokra terjed ki, akik alatt nem csupán a polgári személyeket, hanem azokat a személyeket is értjük, akik valamilyen ok miatt (például sebesülés, fogság, betegség) a fegyveres konfliktusból kiváltak (például hadifoglyok, sebesültek, hajótöröttek). A genfi jog alapelveit egyaránt be kell tartani államok közötti és államon belüli (polgárháború) fegyveres konfliktus során. A nem nemzetközi háborúk során is a konfliktusban közvetlen részt nem vevőkkel megkülönböztetés nélkül emberségesen kell bánni, tilos megölni, megcsonkítani őket, kegyetlenkedni velük. Tilos túszokat szedni, szükséges garanciák nélküli eljárás nélkül ítéletet hozni és azokat végrehajtani. A védett személyek nem mondhatnak le a genfi egyezmény által garantált jogokról (például hadifogoly státusz).”[23]

Ez a két rövid összefoglalás is számos olyan példát juttat a szakértő eszébe, amelyek rámutatnak a nemzetközi jog nagy körültekintést igénylő gyakorlati alkalmazhatóságára a kibertámadások során. A továbbiakban a teljesség igénye nélkül néhány olyan eset kerül felsorolásra, amely indokolttá teszi a nemzetközi jog gyakorlati alkalmazhatóságának alapos vizsgálatát a kibertámadások során:

[23] BÓDI Stefánia – KÁDÁR Pál – PETRUSKA Ferenc: Jogi alapismeretek honvéd tisztjelölteknek. Nemzeti Közszolgálati Egyetem, Budapest, 2014.

- A 2016-os amerikai elnökválasztás során az USA álláspontja szerint Oroszország beavatkozott a választási folyamatba, behatolt az egyes pártok és kampánystábok által használt elektronikus információs rendszerekbe, valamint a közösségi hálózatokon keresztül próbálta befolyásolni az amerikai választók döntését. Ezzel szemben Oroszország és Kína kiemelt lépéseket tesz azért, hogy az amerikai bázisú cégeket, mint a Facebook, a Google vagy az Apple kiszorítsa a hazai piacairól, de legalábbis elfogadtassa velük a honos jogukban elvárt normák betartását. Teszik mindezt attól a nem alaptalan félelemtől vezéreltetve, hogy az amerikai kormányzatnak ezeken a platformokon keresztül befolyásoló hatása lehet az orosz és kínai társadalmakra nézve. A „politikai függetlenség" biztosítása az államhatárokat nem ismerő szolgáltatások esetében tehát nem könnyen megvalósítható. Tovább bonyolítja a kérdést az, hogy a korábban említett cégeknek az államoktól függetlenül is van bizonyos szabadságfokuk, amivel sem a nemzetállami, sem a nemzetközi szabályozás nem tud egykönnyen mit kezdeni. A Facebook moderálási elvei, azaz a szólásszabadság foka ezen a platformon nem teljesen transzparens, nem tudja jól lekövetni a különböző kulturális kontextusokat, de mivel 1 milliárdnál is több ember használja, bizonyos esetekben döntő befolyása van fontos politikai döntések meghozatalában, dacára annak, hogy nem állami szereplő.[24]
- Talán a legtöbbet emlegetett kérdés az önvédelemhez való jog alkalmazásának lehetősége. Bár a laikusok számára úgy tűnhet, hogy a „kiberháború" már zajlik, amelynek során államok támadnak államokat, valójában ritkán lehet olyan támadásokkal találkozni, amelyek egy országot próbálnak ellehetetleníteni. Ilyen támadásnak minősülhet a 2007-es Észtország elleni támadás vagy a 2017-es NotPetya kampány. Viszont mindkét eset azt mutatta meg, hogy a gyakorlatban egyáltalán nem egyszerű az állami érintettséget bizonyítani a támadások mögött. Nem véletlen, hogy 2017-ig a támadó megnevezése a sajtó feladata volt, hivatalos politikai szereplők ezt nem tették meg, tekintettel az ezzel járó diplomáciai nehézségekre. Az attribúció komoly politikai döntés, melyet a rendelkezésre álló technológiai és hírszerzési információk alapján hoznak meg, mérlegelve az ezzel járó politikai előnyöket és hátrányokat. Az „önvédelemhez való jog" alkalmazására egy összetett kibertámadás után viszont még nem láttunk példát, bár az Egyesült Államok már évek óta lebegteti a kinetikus, azaz fizikai világban történő válaszadást egy információs rendszereket érintő támadásra.[25] Ezt megerősítve, körülbelül 2016-tól kezdve több ország is kilátásba helyezte a válaszadást, kiberbiztonsági vagy katonai stratégiájának elemeként. Ezt nevezzük elrettentésnek (deterrence), ami egyben mutatja több ország szándékát arra, hogy offenzív képességeket építsen. Az önvédelem megvalósítása erő nélkül ugyanis nem lehetséges.

[24] Bár ez a példa nem feltétlenül tartozik a korábban felsorolt nemzetközi jogi kérdések közé, de az orosz–ukrán háború során a közösségi médiaszolgáltatóknak platformszolgáltatóként komoly szerepe volt az információs műveletekben és az ellentevékenységekben.

[25] 2019. május 5-én Izrael megtorló csapást mért a Hamasz által működtetett szerverközpontra, így ez az állítás az eredeti szöveg megjelenése óta nem igaz. Forrás: https://www.theverge.com/2019/5/5/18530412/israel-defense-force-hamas-cyber-attack-air-strike

- Ius in bello esetében elvileg a kibertérben is csak katonai célpontokat lehetne támadni, békeidőben mégis több olyan államilag támogatottnak tekintett kártékony kód kampányról lehet tudni, amelyek szándékosan vagy véletlenül, de civil célpontok működését lehetetlenítették el, ezzel megsértve az egyes államok szuverenitását, de nem elérve azt a küszöbértéket, hogy az adott állam azt fegyveres konfliktusnak fogja fel. A 2015-ben és 2016-ban egyes ukrán erőműveket támadó BlackEnergy nevű trójai vírus mögött Oroszországot sejtik, a brit egészségügyi rendszert ellehetetlenítő WannaCry zsarolóvírust pedig Észak-Koreának tulajdonítják. Mindkét esetben olyan kritikus információs infrastruktúrák estek áldozatul, amelyek civil mivolta megkérdőjelezhetetlen. Különösen a WannaCry aggasztó ebből a szempontból, hiszen a támadó feltehetőleg nem szándékosan célozta meg az egészségügyi információs rendszereket, ráadásul ezt nem is katonai szándékkal tette, amennyiben azonban tényleg államilag motivált volt a támadás, az felveti a számonkérhetőség kérdését.
- Nem egyértelmű, hogy kik azok a nem állami szereplők, akik mégis állami célokat támogatnak? Bár egyre több hadsereg és hírszerző szervezet alkalmaz olyan informatikai szakembereket, akik a támadó műveletek végrehajtásában vesznek részt, a kiberkatonák többsége nem visel egyenruhát. A kibertérben különösen gyakran használnak olyan közvetítőcsoportokat, azaz proxykat, akik nem kötődnek a hadsereghez. Ezek lehetnek egyéni szereplők vagy kisebb-nagyobb bűnözői csoportok is, működhetnek a támadó ország határain belül, de akár azon kívül is, hiszen az internet nem ismer határokat. De a „támadó" lehet egy olyan végfelhasználó is, akinek az informatikai infrastruktúráját tudtán kívül használják, például egy botnet részeként. A fizikai világban viszonylag ritkán fordul elő, hogy egy harcos vagy egy bűnöző nem tud arról, hogy ő éppen egy harci cselekmény vagy bűncselekmény részese, a kibertérben viszont több millió olyan számítógép van, amely egy kártékony kód fertőzés után egy összetett művelet részese lehet. Nemzetközi jog szempontjából bonyolítja a helyzetet, hogy a felsorolt példák más megítélés alá esnek háború és békeidő esetén, ráadásul sokszor a büntetőjog a mérvadó vagy éppen az egyéni felelősséget kell vizsgálni.
- Ez utóbbihoz kapcsolódik a semleges országok területéről végrehajtott cselekmények kérdése. A 2007-es Észtország elleni támadás utólagos elemzése például bebizonyította, hogy a világ számos országából, így Magyarországról is érkeztek olyan hálózati forgalmak, amelyek hozzájárultak az észt infrastruktúra lebénításához. Természetesen a kor technológiája sokat segített abban, hogy az illetékes hatóságok le tudják kapcsolni a támadásban résztvevő számítógépeket, de a felhő számítástechnika (cloud computing) megjelenésével a nemzeti hatóságok feladata sokkal nehezebbé vált, hiszen egy támadó erőforrás, például virtuális gép a felhőszolgáltató bármelyik fizikai adatközpontjában lehet. Tehát az sem egyértelmű, hogy melyik ország tartozik felelősséggel a támadás megszüntetésében.

A sok alapvető kérdés közül talán a legfontosabb, hogy mit is jelent tulajdonképpen a támadás fogalma a kibertérben? Az incidensek mögött ugyanis több különböző motivációt találhatunk. A legtöbb esetben anyagi haszonszerzés motiválja az elkövetőket, a kiberbűnözés tehát az, amivel legtöbbször találkozunk. Ennek megítélése egyértelműen a Budapest Egyezmény körébe tartozik, nincsen vita

arról az államok között, hogy ez üldözendő cselekmény, bár az akarat nyugatról keletre, a képesség pedig északról délre csökken e bűncselekménytípus megfékezésére. Szintén gyakran lehet hallani információszerzési célzattal véghezvitt támadásokról. Amennyiben állami szereplő hajtja ezt végre, a cselekmény nemzetközi jogi megítélése szürke zónába tartozik, ahogy azt a későbbiekben látni fogjuk. Nagyon ritkán, de találkozhatunk a hacktivista, illetve elméletileg a kiberterrorista cselekedetekkel is, ilyenkor a csoport célja valamilyen politikai ideológia terjesztése, esetleg ennek az ideológiának a támogatására valamilyen kiberfizikai rendszeren keresztül pusztítás végrehajtása. Ezeket a nemzeti jog kezeli, az eddig ismert esetekben ugyanis vagy államoktól független csoportosulások, például az Anonymous csoport, vagy államokhoz nem egyértelműen, inkább patrióta alapon kapcsolódó csoportok, mint például a Szír Elektronikus Hadsereg (Syrian Electronic Army) tevékenységét lehetett megfigyelni. Katonai műveletek, azaz a nyilvánosság számára is ismert kiberhadviselés esetén azonban fontos annak megállapítása, hogy mikor beszélhetünk támadásról.

Schmitt és Vihul ezt a kérdést az ENSZ Alapokmány 51. cikkéből vezeti le, amely lehetővé teszi az államok számára az erőszak alkalmazását önvédelem céljából, fegyveres támadás esetén:
„A jelen Alapokmány egyetlen rendelkezése sem érinti az Egyesült Nemzetek valamelyik tagja ellen irányuló fegyveres támadás esetében az egyéni vagy kollektív önvédelem természetes jogát mindaddig, amíg a Biztonsági Tanács a nemzetközi béke és a biztonság fenntartására szükséges rendszabályokat meg nem tette. A tagok az önvédelem e jogának gyakorlása során foganatosított rendszabályaikat azonnal a Biztonsági Tanács tudomására tartoznak hozni és ezek a rendszabályok semmiképpen sem érintik a Biztonsági Tanácsnak a jelen Alapokmány értelmében fennálló hatáskörét és kötelességét abban a tekintetben, hogy a nemzetközi béke és biztonság fenntartása vagy helyreállítása végett az általa szükségesnek tartott intézkedéseket bármikor megtegye.”[26]

A legtöbb kibertámadás, ahogy láthattuk, nem éri el azt a szintet, hogy állam elleni támadásnak nevezhessük, habár egyértelműen nincs lefektetve az a határ sem, ahol már az egész államot érintő tevékenységről beszélhetünk, hiszen ennek a határnak a kijelölése mindig a megtámadott állam felelőssége. Általánosságban a tulajdon megsemmisülése vagy az ember sérülése lehet az a kulcsmomentum, ami kiválthatja az erő alkalmazását egy viszontválaszban, ami lehet kinetikus a fizikai világban vagy informatikai jellegű a kibertérben. De ez még mindig „nem háború”, azaz nem fegyveres konfliktus a szó jogi értelmében. Schmitt és Vihul arra is felhívják a figyelmet, hogy a „háború”, így a „kiberháború” fogalma is meghaladott a nemzetközi jog fogalmi keretei között, ugyanis a 20. század közepétől a „fegyveres konfliktus” szóhasználat terjedt el a négy Genfi Egyezménnyel párhuzamosan, a humanitárius jog szempontjából ugyanis nem számít, hogy a hadviselő felek betartották-e a hadüzenet formai követelményeit vagy sem. A katonai jellegű kibertámadások megítélése abban az esetben egyértelmű, amikor egy hagyományos fegyveres konfliktus kísérőjeként jelennek meg, ahogy történt az 2008-ban a grúz–orosz konfliktusban, vagy a szíriai polgárháborúban. Ezekben az esetekben minden hadviselő félnek be kell tartani a humanitárius jog szabályait. A kiberháborút tehát szerencsésebb „kibertérben történő fegyveres konfliktusnak”

[26] ENSZ: Az Egyesült Nemzetek Alapokmánya. 1945. június 26. http://www.grotius.hu/doc/pub/HBJFWJ/az%20ensz%20alapokm%C3%A1nya.pdf

nevezni, a nemzetközi jog szempontjából így megkülönböztetve azt a békeidőben végrehajtott kibertéri műveletektől a nemzetközi jog szempontjából.[27]

További kérdéseket vet fel a „támadás" fogalmának meghatározása. Míg mérnöki szempontból egyértelműen (informatikai) támadást hajtanak végre akkor, amikor az információk bizalmassága, sértetlensége és/vagy rendelkezésre állása sérül, esetleg, amikor a kritikus információs infrastruktúrák sértetlensége és rendelkezésre állása tekintetében következik be negatív esemény, a nemzetközi kapcsolatok nézőpontjából a támadás ennél mélyebb meghatározást igényel. Először is, a már idézett ENSZ Alapokmány 51. cikke a „fegyveres támadás" kifejezést használja, azonban ez a fogalom nincs részletesen meghatározva. Értelmezési segítséget jelent az ENSZ 3314. (XXIX) közgyűlési határozata, amely az „agresszió" fogalmát definiálja. Kajtár az alábbiak szerint foglalja össze az agresszió és a fegyveres támadás közötti kapcsolatot:
„A 3314. sz. határozat előkészítő munkálataiból egyértelmű, hogy az államok különbséget tettek az agresszió és a fegyveres támadás között, és a határozatban az előbbit kívánták meghatározni. Számos okból azonban a határozat mégis nagy jelentőségű. Egyrészt a fegyveres erőszak legtipikusabb formáit sorolja fel, ha csak példálózva is. Másrészt jelzi, hogy a fegyveres erőszak különböző formái és különösen intenzitása jogilag is relevánsak. Az agresszió definíciójából egyértelműen kiderül, hogy minden agresszió egyben fegyveres erőszak, de ez fordítva már nem igaz (vagyis az agresszió a fegyveres erőszak teljes részhalmaza). Ez már a határozat preambulumából is világosan kiderül, amely a következőképpen fogalmaz: „az agresszió az erő jogtalan alkalmazásának[28] legkomolyabb és legveszélyesebb formája". Harmadrészt egyértelművé teszi, hogy fegyveres erőszakot közvetett módon is el lehet követni, azaz nem csupán a fegyveres erőszak közvetlen formái sértik a 2. cikk (4) bekezdését. Negyedrészt világossá teszi a határozat, hogy – mint minden más, a 2. cikk (4) bekezdéséhez kapcsolódó erőszakfogalomnál – itt is államközi erőszakfogalomról van szó. Illeszkedve a 2. cikk (4) bekezdésének logikájához, a határozat 1. cikkében lévő fogalom meghatározás szerint agresszió „fegyveres erő alkalmazása valamely állam részéről…". Az agresszió államközi jellegét a 2. cikk ismét megerősíti: „Fegyveres erőnek az Alapokmány megsértésével elsőként való alkalmazása valamely állam részéről – első megítélésre – agresszió bizonyítékának tekintendő…"[29]

Kovács könyvében idézi a közgyűlési határozat pontos szövegét is, amely segít megérteni azokat a példákat, amelyek agressziónak minősülnek:
„Az agresszió fegyveres erőszak alkalmazása egy állam által más állam szuverenitása, területi integritása vagy politikai függetlensége ellen, illetve az Egyesült Nemzetek Alapokmányával össze nem férő bármely más módon."

Ezt követi a közgyűlési határozatban felsorolt tényállások listája. Agresszió tehát, függetlenül attól, hogy volt-e hadüzenet,

---

27 Az orosz–ukrán háború valószínűleg sok tudományos kérdést fog tisztázni gyakorlatban, amely alapot jelenthet egy majdani pontos, nemzetközileg is elfogadott definícióhoz.

28 Helyesen: az erőszak jogtalan alkalmazása.

29 KAJTÁR Gábor: Az önvédelem jogával kapcsolatos dilemmák a terrorizmus elleni háború korában. In: NAGY Marianna (Szerk.): Ünnepi konferencia az ELTE megalakulásának 375. évfordulója alkalmából. Jogi Tanulmányok, II. kötet, 2010. pp. 293-308.

- i) ha egy állam fegyveres erői inváziót vagy támadást hajtanak végre más állam területe ellen, vagy mindenfajta katonai megszállás, bármilyen ideiglenes is, amely ilyen invázió vagy támadás következménye, vagy más állam területének erő alkalmazásával történt annektálása;
- ii) ha egy állam fegyveres erői bombázzák más állam területét, vagy ha egy állam bármiféle fegyvert használ más állam területe ellen;
- iii) ha egy állam kikötőit vagy partvidékét más állam fegyveres erői blokád alá veszik;
- iv) ha egy állam fegyveres erői megtámadják más állam szárazföldi, tengeri vagy légierőit, tengeri és légiflottáját;
- v) ha egy állam fegyveres erőit, amelyek más állam területén tartózkodnak a fogadó állammal történt megegyezés alapján, az egyezményben foglalt feltételek megszegésével használja fel, vagy ha azok az egyezmény lejárta után tovább tartózkodnak az illető területen;
- vi) ha egy állam megengedi, hogy területét, amelyet egy másik állam rendelkezésére bocsátott, a másik állam agressziós cselekmény elkövetésére használja fel harmadik állam ellen;
- vii) ha egy állam fegyveres bandákat, csoportokat, önkénteseket vagy zsoldosokat küld – vagy a nevében ilyeneket küldenek – más állam ellen fegyveres cselekmények végrehajtására, amelyek oly súlyosak, hogy kimerítik a fent felsorolt cselekményeket, illetve ha egy államnak komoly része van ebben.[30]

A Tallinni Kézikönyv a fenti jogforrások alapján javaslatot tesz a „kibertámadás" meghatározására, amely merőben eltér attól a fogalomtól, ami a köznyelvben, sajtóban terjedt el. A Kézikönyv 68. Szabálya ekképpen fogalmaz:
„Jogellenes az olyan kibertéri művelet, amely bármely állam területi integritása vagy politikai függetlensége elleni erőszakkal való fenyegetést vagy erőszak alkalmazását jelenti, vagy bármely más módon ellentétes az Egyesült Nemzetek céljaival."

A Kézikönyv 92. szabálya ezt így egészíti ki:
„Egy kibertámadás olyan kiberművelet, legyen az akár támadó, akár védelmi jellegű, mely alapján személyek sérülése vagy halála, illetve objektumok megrongálódása vagy megsemmisülése megalapozottan várható."

E forrás 103. szabálya szerint a kiberhadviselés eszközei a kiberfegyverek és a hozzájuk tartozó kiberrendszerek, módszerei pedig azok a kibertaktikák, technikák és eljárások, amelyekkel az ellenséges tevékenységet végrehajtják.[31]

A kiberháború, kibertámadás és kiberfegyver szavak gyakori használata a nemzetközi jog mélyebb megismerése után tehát inkább az újságírók, semmint a nemzetközi jogászok szokása, az utóbbi szakma képviselői sokkal szűkebb fókusszal

[30] KOVÁCS Péter: A nemzetközi jog fejlesztésének lehetőségei és korlátai a nemzetközi bíróságok joggyakorlatában. Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar, Budapest, 2010.

[31] SCHMITT, Michael N. (Ed.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge, 2017.

hivatkoznak erre a kifejezésre, mint az előbbiek. Ez azért is megnyugtató, mert ha egy tisztán informatikai úton megvalósuló támadást a szó jogi értelmében is támadásnak minősítenének, az jogalapot adna a NATO Észak-atlanti Szerződés V. cikkelyének alkalmazására. A Szerződés szövege ugyanis ezt írja:
„A Felek megegyeznek abban, hogy az egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek; és ennélfogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. cikke által elismert egyéni vagy kollektív védelem jogát gyakorolva, támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Felekkel egyetértésben, azonnal megteszi azokat az intézkedéseket – ideértve a fegyveres erő alkalmazását is –, amelyeket a békének és biztonságnak az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart. Minden ilyen fegyveres támadást és az ennek következtében foganatosított minden intézkedést azonnal a Biztonsági Tanács tudomására kell hozni. Ezen intézkedések akkor zárulnak le, ha a Biztonsági Tanács meghozta a nemzetközi béke és biztonság helyreállítására és fenntartására szükséges rendszabályokat."[32]

Az V. cikkely alkalmazásának lehetősége már a 2007-es Észtország elleni művelet idején felmerült, akkor azonban nem éltek vele a felek. Elkezdődött azonban egy komoly gondolkodás arról, mik lehetnek azok a kiváltó okok, amelyek mellett a kollektív védelmet alkalmazni kell és lehet akkor is, ha a támadás tisztán a kibertérből érkezik, a fizikai térben azonban semmilyen más művelet nem kíséri azt. Az Észak-atlanti Szerződés Szervezete folyamatosan elemzi ezt a kérdést, de megnyugtatóan csak a saját információs rendszerek védelméről intézkedett a 2000-es évek elejétől kezdve, a kollektív védelem gyakorlata nem alakult ki. Veenendaal és szerzőtársai 2016-ban foglalták össze, milyen lépéseket kell tennie a NATO-nak annak érdekében, hogy erre a kérdésre választ kapjon. A szerzők az alábbi javaslatokat tették:

- A NATO ismerje el a kiberteret, mint a katonai műveletek lehetséges terét. Ezt a katonai szövetség a 2016-os varsói csúcson megtette. Tálas összefoglalója szerint: *„Az állam és kormányfők azzal, hogy a kibervédelmet a NATO kollektív védelmi feladatai közé sorolták, az operatív hadviselés területét pedig kiterjesztették a kibertérre is, lehetővé tették, hogy egy tagállama elleni koordinált kibertámadást a NATO a szövetség egésze elleni támadásnak tekintsen. Deklarálták azt is, hogy a NATO támogatni fogja a kiberhadviselés fenyegetéseinek elhárításával és a kibervédelemmel összefüggő kutatásokat, illetve a tagállamok védelmi iparának együttműködését e téren."* [33]
- Különböztesse meg a békeidőre szóló, hálózati védelemre vonatkozó mandátumot a katonai műveletekre és a kollektív védelemre szóló mandátumtól és vizsgálja meg egy olyan szabályozás létrehozását, amely lehetővé teszi a szövetségeseknek a képességek teljes spektrumának felhasználását az elrettentés és védelem céljából, bármilyen kibertérből érkező fenyegetésre.

[32] NATO: Az Észak-Atlanti Szerződés. 1949. április 4. https://www.nato.int/cps/ic/natohq/official_texts_17120.htm?selectedLocale=hu
[33] TÁLAS Péter: A varsói NATO-csúcs legfontosabb döntéseiről. Nemzet és Biztonság. 2016/2. pp. 97-101.

- Hozzon létre olyan doktrínát és eljárásrendet, amely lehetővé teszi a kiberképességek használatát katonai műveletekben.[34,35]

Annak a küszöbértéknek a meghatározása, amelyet már a nemzetközi jog alapján is fegyveres támadásnak lehet minősíteni, minden esetben a megtámadott ország joga. Az például továbbra sem ismert a nyilvánosság előtt, hogyan reagálna a NATO egy komoly hatással rendelkező, kibertérből érkező incidensre, hiszen ilyen esetben a tagállamok együttesen döntenének, egy tagállam kezdeményezésére. Ez különösen aggasztó az Ukrajnában végrehajtott kiberműveletek sorozatának fényében, amelyek erősen feszegetik az agresszió fentiek szerint leírt megfogalmazását. Az ukrán kibervédelemmel foglalkozó szervezetek gyakorlatilag havonta szembesülnek, vagy legalábbis hoznak nyilvánosságra olyan incidenseket, amelyek jogi elemzésének eredményeképpen a műveletet fegyveres támadásnak lehetne minősíteni, függően az adott állam döntésétől. 2018 júliusában például arról adtak tájékoztatást, hogy gyaníthatóan oroszországi támadók az ivóvízellátást veszélyeztették a tisztítórendszerek informatikai rendszereinek támadásával.[36,37]

A NATO mindenesetre legalább a kibervédelmi gyakorlatai során teszteli az V. cikkely alkalmazhatóságát. A rendszeresen megrendezésre kerülő CyberCoalition gyakorlat, amely az egyes NATO tagországok kiberbiztonsági együttműködését teszteli egy szimulált kibertámadás során, illetve a Locked Shields gyakorlat a NATO CCDCOE[38] rendezésében, amely minden évben olyan helyzetbe próbálja hozni a csapatokat, hogy felvessék a kollektív védelem lehetőségét. A már idézett Veenendaal egy interjúban arról számolt be, hogy míg a 2016-os Locked Shields gyakorlaton nem került sor az V. cikkely alkalmazására, a 2017-es gyakorlaton az egyik résztvevő csoport olyan módon tudta a forgatókönyv határait kifeszíteni, hogy a gyakorlat végeredményeként kérelmezni tudták a NATO beavatkozását.[39]

A fokozódó kibertéri kihívások és a gyakorlatok eredményei teszik lehetővé, hogy a katonai-szakmai felkészüléssel párhuzamosan a politikai támogatás is megjelenjen a NATO tagországainak részéről. Kis lépésekkel ugyan, de évről évre tovább merészkedik az a politikai állásfoglalás, amelyet az aktuális csúcstalálkozó után tesznek közzé. A 2018-as brüsszeli csúcs zárónyilatkozata például reagál mindazokra a változásokra, amelyek a 2016-os varsói csúcs óta történtek, amikor is

---

34 VEENENDAAL, Matthijs– KASKA, Kadri– BRANGETTO, Pascal: Is NATO Ready to Cross the Rubicon on Cyber Defence? NATO CCDCOE, 2016. június. https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf

35 Ezek a kívánalmak 2022-re megvalósultak.

36 MARTIN, Alexander J.: Russian hackers targeted Ukraine's water supply, security service claims. Sky News, 2018. július 11. https://news.sky.com/story/russian-hackers-targeted-ukraines-water-supply-security-service-claims-11432826

37 Az orosz-ukrán háború első hónapjának tapasztalatai alapján egyébként az ukrán kibervédelem, feltehetően jelentős nyugati támogatással megfelelően felkészült a kibertéri harcászati tevékenység elhárítására.

38 Cooperative Cyber Defence Centre of Excellence, Egyesített Kibervédelmi Kiválósági Központ

39 CALATAYUD, Jose Miguel: Locked Shields: The world's largest cyber-war game. Al Jazeera, 2017. június 18. https://www.aljazeera.com/features/2017/6/18/locked-shields-the-worlds-largest-cyber-war-game

a kiberteret műveleti területté nyilvánították. Így különösen érdekes megvizsgálni az alábbi pontokat:

- „*Képesnek kell lennünk olyan hatékonyan működni a kibertérben, ahogy tesszük azt a levegőben, a vízen és a tengeren, így megerősítve és támogatva a Szövetség általános elrettentési és védelmi szempontjait*.” Ez a rész utal arra, hogy a kibertérben NATO-szinten is szükséges az offenzív képességeket fejleszteni, egyben a védelmi szemszögű megközelítés mellé az elrettentés is felzárkózik. Kiemeli továbbá azt a tényt, hogy a katonai műveleteket a kibertérben is végre lehet hajtani, megerősítve ezzel a 2016-os állásfoglalást.
- „*Egyetértettünk abban, hogyan integráljuk a szuverén kiberképességeket a Szövetség műveleteibe és misszióiba, melyet önkéntesen ajánlanak fel a Szövetségesek, erős politikai felügyelet keretében.*” Ez egyben azt is jelenti, hogy a NATO-tagországok saját képességeket fejlesztenek, amelyek összessége adja a NATO kiberképességeit. Ennek köszönhetően indult el például Magyarországon is a kiberképességek kiemelt fejlesztése.
- „*A NATO védelmi mandátumának megerősítése mellett eltökélt szándékunk képességeink teljes körének felhasználása, beleértve ebbe a kiberképességeket is, a kiberfenyegetések teljes spektrumának elrettentésére, kivédésére és válaszadásra, ideértve ebbe azokat a fenyegetéseket is, melyeket hibrid kampányok részeként hajtanak végre.*” Ez fontos üzenet Oroszország felé, hiszen a NATO jelzi, nem hagyja annyiban a kibertámadásokat, még azokat sem, amelyek a hibrid hadviselés részeként nem érték el a fegyveres beavatkozás szintjét. A teljes képességek emlegetésével a hagyományos, kinetikus válaszadást is elvileg lehetővé teszik.
- „*Az egyes szövetséges tagállamok szükség esetén megfontolhatják a kártékony kibertevékenységek attribúcióját és a koordinált válaszadást, az attribúciót szuverén nemzeti előjogként elismerve.*” Miután az Egyesült Államok, majd több ország is hivatalosan élt az attribúció lehetőségével, azaz egy bizonyos országot nevesített egy kibertámadás elkövetésével kapcsolatosan, a katonai szövetség állást foglalt arról, hogy elismeri az attribúciót, mint szuverén jogot, de ezzel egyelőre nem kíván szövetségi szinten élni.[40]
- „*Megerősítjük elkötelezettségünket abban, hogy mindenkor a nemzetközi jog, így az ENSZ Alapokmány, a nemzetközi humanitárius jog és az emberi jogok keretében cselekszünk, amennyiben ezek alkalmazhatók.*” A NATO ezzel kijelöli azt a nemzetközi joganyagot, amelyet érvényesnek tart a kibertérben, ahogy tette azt 2014-ben is, de meghagyja azt a kiskaput, hogy bizonyos esetekben ezek a keretrendszerek nem lesznek alkalmazhatók a virtuális térben.[41]

[40] Az Albániát 2022-ben ért kibertámadás után a NATO Iránt attribútálta elkövetőként. Ld. https://www.nato.int/cps/en/natohq/official_texts_207156.htm

[41] NATO: Brussels Summit Declaration. 2018. augusztus 30. https://www.nato.int/cps/en/natohq/official_texts_207156.htm

5. KIBERKÉMKEDÉS

Míg a kiberhadviselés, azaz a kibertérben történő katonai műveletek nemzetközi joggal összefüggő elemzése meglehetősen előrehaladott, miközben a gyakorlatban ritkán találkozunk vele, addig a kiberkémkedés, azaz az elektronikus információs rendszerekben tárolt információk hírszerzési célú megszerzése napi gyakorlatnak számít az államok eszköztárában, viszont nemzetközi jogi szabályozása minimális. A Tallinni Kézikönyv 32. szabálya is ezt emeli ki:
„Bár a békeidőben történő állami kiberkémkedés önmagában nem sérti a nemzetközi jogot, a módszer, amivel kivitelezik, már lehet, hogy az előírásokba ütközik."[42]

Nem meglepő tehát, hogy a szakmai közvélemény először a kibertérben történő hírszerzéssel találkozhatott a kibertéri konfliktusok sorából. Ilyen tevékenységekről már az 1990-es évek második felében lehetett hallani, például a gyaníthatóan Oroszország által végrehajtott Moonlight Maze akciót 1999-ben tárta fel a sajtó. Emlékezzünk vissza az ENSZ kiberbiztonsági tevékenységéről szóló korábbi fejezetre, amely szerint először 1998-ban Oroszország kezdett el a kibertéri tevékenységekkel foglalkozni a nemzetközi szervezetben. A jelek tehát arra utalnak, hogy a nagyhatalmak, kiemelten az Egyesült Államok és Oroszország már az 1990-es évek végén aktívan használták a kiberteret titkos műveletek végrehajtására. A valószínűleg Kína által végrehajtott Titan Rain művelet pedig 2003-ban indult, így a képességfejlesztés valószínűleg ott is az 1990-es évek végén vette kezdetét. A nemzetközi kapcsolatokat befolyásoló kiberműveletek tehát már jóval azelőtt részesei voltak az állami gyakorlatoknak, mielőtt a közvélemény erről tudomást szerzett volna.

Ez nem meglepő annak tudatában, hogy az informatika széles körű elterjedésével a hírszerzés sosem volt olyan könnyű, mint a XXI. században. A hírszerzés célja Izsa szerint: „*a (politikai és katonai) döntéshozók támogatása információkkal. A politikai jelentőséggel bíró döntéseket bonyolult helyzetben, hiányos informáltság mellett, a várható következmények részleges ismeretében, kockázatokat vállalva hozzák meg az illetékesek. Az informáltság növeli a döntések megalapozottságát és esélyeit a kedvezőbb eredmény bekövetkezésének elősegítésére. Ám ennek alapvető feltételeként az információknak összhangban kell lenniük a tényekkel.*"[43]

Tekintettel arra, hogy az információk napjainkban szinte kizárólagosan digitális formában keletkeznek, tárolódnak, továbbítódnak és kerülnek feldolgozásra, a hírszerzéssel foglalkozó szakemberek elsődleges feladata azoknak a számítástechnikai eszközöknek a fellelése, amelyek a döntéshozatalhoz releváns információkat kezelik. Ehhez pedig nem feltétlenül kell elhagyni a saját országukat, hiszen a határtalan internet lehetőséget biztosít a biztonságos körülmények között végrehajtott információszerzésre is, a határok átlépése nélkül.

Tovább könnyíti a helyzetet, hogy az információk jelentős része eleve nyilvánosan jelenik meg. A nyílt forrású hírszerzés integráns része a hírszerzési eljárásoknak, de az olyan szolgáltatók, mint a Google vagy a Facebook lehetővé tették a személyekről, intézményekről, történésekről szóló információk szinte

[42] SCHMITT (2017): i. m.
[43] IZSA Jenő: A hírszerzés céljáról és rendszeréről. Hadtudomány. 2009/1-2, pp. 72-83.

korlátlan begyűjtését. Ferenczy megfogalmazásában a nyílt forrású hírszerzés „*olyan információgyűjtő eljárás, amely során a nyilvánosan (a publikum számára) elérhető forrásokból az információkat felkutatják, elemzik, értékelik és felhasználják egy adott cél elérése érdekében, általában a parancsnok és annak közvetlen törzse által feltett kérdés megválaszolására. Más szavakkal az információszerzés kipróbált eljárásainak alkalmazása a széles körben hozzáférhető nyílt adatforrásokra. A nyílt forrású információszerzés nem kizárólag katonai felderítési vagy információszerzési kategória, mivel ezt a tevékenységet a civil szférában is folytatják.*”[44]

A társadalom digitalizálódásával ráadásul olyan különleges metaadatokhoz is hozzá lehet férni, amelyek kontextuális információt is tudnak szolgáltatni a nyílt forrásból megszerzett információkhoz. Bányász a közösségi médiába beleérti az okoseszközök használatát is, így egy olyan kiterjesztett teret határoz meg, amely a metaadatok széles körét kínálja a felkészült hírszerzők számára a következőképpen: „*Nem csak az esetleges, akár már a gyártósoron feltelepített kémprogramok jelentenek veszélyeket, hanem az egyes feltelepített alkalmazások is, hiszen használatuk érdekében különböző hozzáféréseket biztosítunk személyes adatainkhoz. A Facebook például az alábbi adatokhoz kér hozzáférést: személyes adatok (névjegyadatok), tartózkodási hely (hálózatalapú és GPS alapú helymeghatározás), hálózati kommunikáció (teljes internet hozzáférés), fiókok adatai (üzenetek olvasása), tárhely (lehetőség az USB-tároló tartalmának módosítására vagy törlésére), telefonhívások, hardvervezérlők (fénykép és videókészítés, hangrögzítés), rendszereszközök (szinkronizálás). Természetesen eldönthetjük, hogy feltelepítjük-e az alkalmazást a telefonunkra, de hasonló engedélyeket kér a Google is a szolgáltatásai használataiért cserébe, már pedig egy Androidos telefon esetében nincs döntési lehetőségünk, nem távolíthatjuk el a telefonról a Google alkalmazásait.*”[45]

A döntéshez szükséges információk tehát gyaníthatóan elérhetők az interneten vagy az internetről elérhető elektronikus információs rendszerekben. Nyilvánvalóan kiberkémkedési tevékenységről az utóbbi, internetről nem elérhető rendszerek esetében beszélünk, azaz a nem nyilvános információk jogosulatlan vagy a hírszerzést szabályozó nemzeti jog alapján történő megszerzése tartozik ebbe a fogalomkörbe.

Buchan az államilag támogatott kiberkémkedés és a nemzetközi jog kapcsolatában kiemeli, hogy nincs egyetlen nemzetközi egyezmény sem, amely a kiberkémkedést szabályozná, egyben olyan egyezmény sincs, amely a kémkedést szabályozza, és egyértelműen adaptálni lehetne a kiberkémkedésre, legalábbis békeidő esetén. Mivel azonban a nemzetközi rend az államok szuverén egyenlőségére épít, e cselekmény szembekerülhet a nemzetközi jog általános elveivel, egyben kijelenthető, hogy a nemzetközi kapcsolatokban a kibertéri hírszerző tevékenységek elsősorban a szuverenitás szempontjából vizsgálhatók. Fegyveres konfliktus során a Genfi Egyezmény I. Kiegészítő Jegyzőkönyvének 46.

[44] FERENCZY Gábor Zoltán: Internet alapú nyílt információszerzés elvi rendszertechnikai megvalósítása. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007.

[45] BÁNYÁSZ Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. Nemzetbiztonsági Szemle, 2015/2. pp. 21-36.

cikkelye vonatkozik a hírszerzési tevékenységekre, történjenek azok akár a fizikai, akár a virtuális világban.[46]

A területi szuverenitás a kibertérben kétféleképpen értelmezhető. Egyrészt a kibertér egy olyan környezet, mely egyetlen ország területéhez sem tartozik, hasonlóan például a világűrhöz. Ebben az esetben azokat a joggyakorlatokat kéne alkalmazni, amelyeket a semleges területekre már korábban megalkottak. Az egyes államok azonban határozottan kinyilvánították igényüket arra, hogy szuverenitást gyakoroljanak a saját kiberterük felett, ezért napjainkban ezt a virtuális, emberek által létrehozott képződményt is hasonlóan kezelik, mint a saját fizikai területüket. Így történt ez Magyarországon is. A 2013-ban elfogadott Nemzeti Kiberbiztonsági Stratégia kinyilvánítja azt az igényt, hogy a nemzeti kibertér felett Magyarország szuverenitást kíván gyakorolni. Suba ezt ekképp fogalmazta meg:
„*A kibertér nincs tekintettel az állami határokra, eszközeit és infrastruktúráját meghatározó mértékben az üzleti szektor szereplői tulajdonolják, működtetik és ellenőrzik. […] A fentiek figyelembevételével került meghatározásra a kibertér fogalma, miszerint 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. Magyarország kibertere a Magyarországon található, a globális kibertér részét képező elektronikus információs rendszerekből és ezen elektronikus információs rendszereken keresztül adatok és információk formájában Magyarországra irányuló és hazánkban megjelenő társadalmi és gazdasági folyamatok összességéből áll.*”[47]

A nemzeti kibertér feletti szuverenitás alapját az adja, hogy a kibertér nem lenne elképzelhető fizikai infrastruktúrák, azaz hálózatok, szerverek, végpontok és hasonló informatikai alkotóelemek nélkül. Amennyiben tehát ezek az alkotóelemek az ország területén helyezkednek el, az ezeken tárolt információk ellen végrehajtott hírszerzési tevékenység önmagában nem ütközik a nemzetközi jogba, a módszer azonban, amivel végrehajtják, nemzetközi jogba ütközhet a beavatkozás tilalmának megsértése vagy az adott ország szuverenitásának megsértése esetén. Nem véletlen tehát, hogy egyre több kormányzat igyekszik az érzékeny információkat kezelő rendszereit minden tekintetben a belső határok között tartani. Magyarország sem kivétel ez alól, a 2013. évi L. törvény az állami és önkormányzati szervezetek elektronikus információbiztonságáról elvárja, hogy a jogszabály alá tartozó intézmények az országhatáron belül kezeljék a magyar közigazgatás adatvagyonát, illetve azt csak kockázatelemzés és hatósági engedély beszerzése után tehessék külföldi szerverre, ekkor is csak az Európai Unió határain belül.

Vannak azonban olyan esetek, amikor az információ nemzeti határon belül tartása nem egyszerű. Már említettük a felhőszolgáltatók jelentette kihívásokat, amikor egyáltalán nem lehet biztosan megmondani, hogy az információ pontosan

[46] BUCHAN, Russell: The International Legal Regulation of State-Sponsored Cyber Espionage. In: OSULA, Anna-Maria – Henry RÕIGAS (Eds.): International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn, 2016. pp. 65-86.

[47] SUBA Ferenc: Nemzeti Kiberbiztonsági Stratégia. In: DOBÁK Imre (Szerk.): A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem, Budapest, 2014. pp. 110-115.

melyik ország területén található, köszönhetően a szolgáltatók adatközpontjai közötti folyamatos adatszinkronizálásnak. De még nehezebb megoldást találni az adatátvitelt érintő támadásokra. Az internet működését az úgynevezett routing, azaz útválasztó protokollok segítik, ezek teszik lehetővé a kliens és a szerver közötti megbízható adatkapcsolat létrejöttét és fenntartását. Az egyik ilyen alapvető protokoll a Border Gateway Protocol, röviden BGP. Ennek manipulálása elvileg lehetővé teszi, hogy a teljes internetforgalmat „eltérítsék", azaz a legkézenfekvőbb útvonal helyett egy bizonyos ország felé irányítsák. Ez történt 2017 decemberének közepén, amikor a Google, a Facebook, az Apple és a Microsoft szerverei felé irányuló forgalom 3 percig minden műszaki logika nélkül Oroszország területén található infrastruktúraelemeken keresztül folyt át. A feltételezések szerint ebben a 3 percben az orosz hírszerző szervezetek hozzájutottak az amerikai informatikai mamutvállalatok felé haladó teljes globális forgalomhoz, amely nagyon értékes információforrás lehet, még akkor is, ha a tartalom maga titkosított, és valószínűleg jelenleg nincs meg a képesség annak dekódolásához. De a metaadatok elemzése, illetve a robbanásszerűen fejlődő informatika mellett a kriptográfiai lehetőségek előrehaladása elvileg lehetővé teszi értékes információk megszerzését ebből a hatalmas adathalomból, akár rövid távon is.[48]

Ilyen esetekben a területi szuverenitás nyilvánvalóan nem értelmezhető. Figyelembe lehet azonban venni a be nem avatkozás elvét, amely a nemzetközi jog azon próbálkozása, hogy az állami szuverenitást megvédje bármilyen külső hatástól. Ez az elv két pilléren nyugszik. Egyrészt egy ország megsérti a be nem avatkozás elvét akkor, ha olyan cselekményt hajt végre, mely hatással van egy másik állam szuverén cselekedeteire, másrészt, ha a cselekmény természeténél fogva kényszerítő erejű. Buchan az első pillért a kibertér vonatkozásában úgy magyarázza, hogy például amennyiben egy ország a minősített adatait egy külföldi ország kiberinfrastruktúráján tárolja vagy továbbítja, akkor ezt az információt tiszteletben kell tartani a nemzeti szuverenitás részeként abban az esetben, ha ez az információ hozzájárul az állam közfeladatainak ellátásához. Üzleti titkoknál ez az érvelés már nem áll fenn. Ha például egy ország külképviseleti szerveinek elektronikus információs rendszereit támadják információszerzési céllal, az megalapozza a be nem avatkozás elvének megsértését az első pillér szerint.[49] Ilyen támadások pedig gyakran előfordulnak. A kelet-európai régió kitettsége ebből a szempontból kiemelkedő, a 2010-es években számos kártékony kód támadta meg az itt működő nagykövetségeket. A WhiteBear, más néven Turla csoport tevékenysége például kifejezetten ezekre az intézményekre fókuszál, és a célpontok kiválasztása Oroszország információéhségét hivatott kielégíteni. Meg lehet említeni továbbá a Ke3chang csoportot is, melyet az elemzések szerint Kínában kell keresni, és szintén a diplomáciai célpontok állnak érdeklődése középpontjában. De Edward Snowden szivárogtatásai szerint az amerikai National Security Agency, az NSA is rutinszerűen figyelte meg más országok, így közeli szövetségeseinek diplomáciával kapcsolatos informatikai forgalmát.

---

48 GOODIN, Dan: Suspicious" event routes traffic for big-name sites through Russia. Ars Technica, 2017. december 13. https://arstechnica.com/information-technology/2017/12/suspicious-event-routes-traffic-for-big-name-sites-through-russia/

49 BUCHAN, Russell: The International Legal Regulation of State-Sponsored Cyber Espionage. In: OSULA, Anna-Maria – RÕIGAS, Henry (Eds.): International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn, 2016. pp. 65-86.

A másik feltétel a kényszerítő erő alkalmazása. Ez azt jelenti, hogy egy ország olyan tevékenységet hajt végre, amely komolyan befolyásol egy másik országot jogszabályalkotásában vagy állami gyakorlatában, olyan tevékenységekre kényszeríti, amelyet szabad akaratából az nem tett volna meg. Erre sokkal nehezebb példát hozni a nyilvánosságra került kiberbiztonsági incidensek sorából, jellegüknél fogva ugyanis az ilyen kényszerítések csak jóval később kerülnek a nyilvánosság elé. Kiindulva viszont abból, hogy az információk szinte kizárólagosan digitális formában léteznek napjainkban, nem zárható ki, hogy már a 2010-es évtizedben is képesek voltak egyes országok más országok döntéseit befolyásolni oly módon, hogy a területükön kívül megszerzett minősített információk felhasználásával megsértették a beavatkozás tilalmának elvét. Amíg azonban ilyen esetek nem kerülnek napvilágra, és nincsen róla a hágai Nemzetközi Bíróság által hozott ítélet, csak elméletben állapíthatjuk meg, hogy a kiberkémkedés bizonyos esetekben a nemzetközi jogba ütközhet. A gyakorlat azt mutatja, hogy ez a megfelelő képességekkel rendelkező országok napi rutinja, amelynek egyelőre még a nemzetközi normák rendszere sem szab határt.

A fedett információszerzés tehát elfogadott szokásjog az államok kapcsolatában. A hírszerzés legtöbbször a biztonságos saját országból történik. Előfordul viszont, hogy a hírszerzők „terepen" dolgoznak, azaz a célország területéről hajtják végre az elektronikus információs rendszerek elleni támadásokat. Ez érthető, hiszen számos esetben a megcélzott rendszer zárt hálózaton működik, internetről nem elérhető, így fizikailag kell hozzáférni a rendszerhez, ahogy történt ez a Stuxnet kártékony kód bejuttatása esetén is a szigorúan védett busehri nukleáris telepre. Az ilyen cselekményeket a szokásjog alapján minden állam igyekszik kivédeni, esetleg észlelése után számára kedvező módon befolyásolni, például hamis információk átadásával. Ritkán azonban, de előfordul, hogy a közvélemény számára is látható módon szakítanak meg egy hírszerzési műveletet. Amennyiben saját állampolgár vagy nem diplomáciai fedésben dolgozó hírszerző vesz részt a felszámolt műveletben, az adott ország büntető törvénykönyve alapján történik a számonkérés, diplomáciai akkreditációval rendelkező személyek esetén pedig jellemzően kiutasítják az országból az illetőt. A 2016-os amerikai elnökválasztásra tett befolyásolási kísérlet miatt Barack Obama leköszönő elnök 35 orosz diplomatát utasított ki az Egyesült Államok területéről, és bezáratott két orosz diplomáciai létesítményt. Tekintettel arra, hogy ez röviddel a befolyásolási kísérlet nyilvánosságra kerülése után történt, bizonyosak lehetünk abban, hogy az amerikai elhárító szervezetek hosszabb ideje tudatában voltak azon személyek kilétének, akik amerikai földről vettek részt a műveletben.

Fegyveres konfliktus idején a kémek jogállása megváltozik. Ahogy a Tallinni Kézikönyv 89. szabálya fogalmaz, „*A fegyveres erők azon tagja, aki kiberkémkedési tevékenységben vesz részt az ellenséges területen, elveszíti a hadifoglyoknak járó jogokat és kémnek tekinthető, mielőtt csatlakozna azon fegyveres erőhöz, melyhez tartozik.*" Így bár a kiberkémkedés fegyveres konfliktus esetén sem tiltott tevékenység, az ebben résztvevők nagyobb kockázatot vállalnak, mintha azt békeidőben tennék. Libicki így foglalja össze a kiberkémkedés dilemmáját, amelyet akár békeidőben, akár fegyveres konfliktus idején érdemes megfontolni:
„*A lecke, amit meg kell fontolni az, hogy milyen üzenetet hordozzon a kiberkémkedési tevékenységed, ha és amennyiben azt felfedezik. Amennyiben nem akarod, hogy feszültséget szüljön, duplázd meg a műveleti biztonságot, de ne számíts sikerre. Emellett kerüld el a katonai célpontok elleni hírszerzést krízis esetén, vagy*

legalábbis olyan technikákkal közelítsd meg ezeket, hogy azok biztosan elkülöníthetők legyenek egy kibertámadás előkészítésétől. Amennyiben viszont a képességeidet szeretnéd megvillantani vagy jelzésértékű szándékaid vannak, olyan narratívát készíts elő, amely számít a felfedezésre. De mindezt gondold végig alaposan a művelet előtt."[50]

6. KIBERDIPLOMÁCIA

A kibertér, ahogy láthattuk, roppant komoly értelmezési kihívást jelent a kialakult nemzetközi biztonságpolitikai környezetben. Évtizedek óta folynak állami hátterű műveletek, amelyekre valamilyen módon reagálni kell. A válaszadás természetesen csak végső esetben lehet katonai jellegű, a feszültségeket lehetőség szerint bilaterális és multilaterális keretek között, diplomáciai eszközökkel kell csökkenteni. Rácz megfogalmazása szerint *„[a] diplomácia az államközi (külpolitikai) kapcsolatok nemzetközi jog által szabályozott, intézményes formája. Elsődleges tartalma az államok, mint a nemzetközi jog alanyai, azaz egyenjogú és szuverén entitások (önálló és cselekvőképes egységek) érdekeinek képviselete azok összehangolt, békés és civilizált módon történő érvényesítése céljából, az együttműködés és a kapcsoltfejlesztés útján. Az érdekképviselet gyakorlati módja az államok külpolitikai céljainak, szándékainak, törekvéseinek az érintettek részére történő – két- és többoldalú keretben megvalósított – világos, érthető, pontos, artikulált kifejtése az előírt speciális (diplomáciai) udvariassági szabályok betartásával úgy, hogy az még az esetleges nézeteltérések, potenciális konfliktusok fennállása mellett is biztosítsa a felek közötti folyamatos konzultációt, tárgyalást, megoldáskeresést, kompromisszumos (kölcsönösen elfogadható) végkifejlethez vezető együttműködést. Mindezt egy sajátos intézményi keretben, a külképviseleti munkát végző személyek és szervezetek működési és tevékenységi feltételeinek meghatározott módon történő – kölcsönösségen alapuló – biztosítása mellett."*[51]

Ennek megfelelően a diplomácia területén kialakult egy új szakterület, amelyet kiberdiplomáciának neveznek. Barrinha és Renard meghatározása szerint *„a kiberdiplomácia a kibertérben megjelenő diplomácia, más szavakkal a diplomáciai erőforrások használata, valamint a diplomáciai funkciók kiaknázása a nemzeti érdekek kibertérben történő érvényesítése céljából. Ezeket az érdekeket általánosságban a nemzeti kibertér vagy kiberbiztonsági stratégia fogalmazza meg, mely jellemzően hivatkozik a diplomáciai agendára. A kiberdiplomácia legfontosabb témái között megtalálható a kiberbiztonság, a kiberbűnözés, a bizalomerősítés, az internet-szabadság és az internet-irányítás kérdései."*[52]

A kibertér legfontosabb multilaterális intézményei diplomáciai szempontból az ENSZ, az EBESZ és az ITU, de például a Délkelet-ázsiai Nemzetek Szövetsége (Association of Southeast Asian Nations – ASEAN) is egy kiemelkedően fontos

[50] LIBICKI, Martin C.: Drawing Inferences from Cyber Espionage. In: MINÁRIK, T.– JAKSCHIS, R.– LINDSTRÖM, L. (Eds.): 2018 10th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinn, 2018. pp. 109-122.

[51] RÁCZ Lajos: Diplomácia – Katonadiplomácia. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2010.

[52] BARRINHA, André– RENARD, Thomas: Cyber-diplomacy: the making of an international society in the digital age. Global Affairs, 2017/4-5. pp. 353-356.

regionális szervezet, ahol a kiberbiztonság regionális kérdéseiről születnek többoldalú megállapodások, vagy a Visegrádi Négyek (Csehország, Lengyelország, Szlovákia, Magyarország) közötti regionális együttműködést is érdemes megemlíteni.

Magyarország kiberdiplomáciai tevékenysége során az ország a Nemzeti Kiberbiztonsági Stratégiájában foglalt értékeket képviseli:
„Magyarország a globális kibertér minden Magyarországgal hasonló értékrendet valló állami és nem állami szereplőjével kölcsönös bizalmon alapuló együttműködés kialakítását és fenntartását célozza meg, továbbá szövetségi és nemzetközi kapcsolati rendszerén, különösen az EU és a NATO, továbbá az Európai Biztonsági és Együttműködési Szervezet (EBESZ), az ENSZ, az Európa Tanács és más nemzetközi szervezeti tagságán keresztül törekszik a globális kibertér szabad és biztonságos használatának szavatolására. Magyarország tudatában van annak, hogy a kibertérben megjelenő fenyegetések és támadások elérhetnek egy olyan szintet, ami szövetségesi együttműködést tehet szükségessé, ezért kiemelten fontosnak tartja, hogy a kiberbiztonság kérdése bekerült a NATO Alapító Okmányának 5. cikkelye alá tartozó kollektív védelem körébe. E szövetségesi nemzetközi együttműködésben Magyarország saját biztonsága miatt is érdekelt. Magyarország különös figyelemmel tekint a közép- és kelet-európai régióra, melynek kiberbiztonságát regionális együttműködések keretében tovább erősíthetőnek látja.”[53]

Bilaterális módon, azaz két állam között sok esetben akkor történik kiberdiplomáciai együttműködés, ha az adott országok érdekei kölcsönösen sérülnek az egymással szembeni kibertevékenységek miatt. A legismertebb példa erre az Amerikai Egyesült Államok és Kína közötti 2015-ös megállapodás. Ekkor Barack Obama és Hszi Csin-ping állapodott meg a kiberbűnözés elleni kölcsönös fellépésben, valamint a kibertérben történő, gazdasági célú hírszerzés korlátozásában. Egy forródrót létrehozásáról is döntöttek, amely segíti a kérdéses esetek gyors tisztázását, elkerülve ezzel egy esetleges incidens eszkalálódását. Történt mindez azután, hogy az amerikai államot és vállalatokat súlyosan érintette a kibertérben történő kínai hírszerzés, amely során kínai vállalatokhoz jutott az amerikai iparban keletkezett szellemi tulajdon, ezzel tisztességtelen előnyhöz juttatva a kínai felet. A találkozó eredményeképp drasztikusan visszaestek a Kínának tulajdonított kibertámadások az Egyesült Államokban.

A kiberdiplomácia fogalma gyakran keveredik a digitális diplomácia fogalmával, holott ez utóbbi a digitális eszközök és szolgáltatások használatát jelenti a diplomáciai kapcsolatok fenntartása során. A Twitter szolgáltatás például igen gyakran jelent hivatkozási alapot napjainkban, elég csak Donald Trump amerikai elnök online tevékenységére gondolni. Fontosságát jelzi, hogy a diplomáciai szakzsargonban elterjedt a „Twiplomacy” kifejezés, utalva a néhány száz karakterben nyilvánosságra hozott állami üzenetek fontosságára. A kommunikáció felgyorsulásával ezek a digitális eszközök is fontosak, azonban a kommunikáció stílusa miatt a hagyományos diplomáciai kapcsolattartás szabályai gyakran sérülnek, amiatt pedig újszerűen kell hozzáállni az évszázadok óta létező diplomáciai protokollhoz. Mivel aránylag új jelenségről van szó, ezek a szabályok kialakulóban

[53] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

vannak, még a fogalmi rendszer sem egyértelmű. Manor a cikkében áttekintette a digitális diplomácia szakirodalomban elterjedt definícióit, majd arra jutott, hogy ezek közül egyik sem fedi le teljesen a gyakorlati jelenséget, így ő a „diplomácia digitalizálódását" javasolja fogalomként használni, amely többet jelent a Facebook, a Twitter, az okostelefon és egyéb, a hétköznapokban elterjedt eszközök használatánál az állami kommunikációban. Ez megfogalmazása szerint *„olyan kifejezés, mely a digitális technológiák normatív és időleges hatását helyezi a középpontba. Ebben benne van az a hosszú távú folyamat is, melynek hatása messze túllépi az innovatív technológiák hatását."*[54]

Több, mint pusztán imázsépítés a közösségi médiában, mint a Twitter használata a kommunikációban, hiszen egyes tudósok már arról cikkeznek, vajon kitörhet-e egy fegyveres konfliktus egy rosszul sikerült Twitter-bejegyzés miatt. A kiberdiplomácia pontos feladatkörét mutatja az Európai Unió Kiberdiplomáciai Eszköztára (EU Cyberdiplomacy Toolbox). A Tanács 2019. május 17-én létrehozott egy olyan keretet, amely lehetővé teszi az EU számára, hogy célzott korlátozó intézkedéseket hozzon az EU-t vagy tagállamait érő, külső fenyegetést jelentő kibertámadások megakadályozására és az azokra való reagálásra, ideértve a harmadik államok vagy nemzetközi szervezetek elleni kibertámadásokat, ahol korlátozott intézkedések szükségesek a közös kül- és biztonságpolitika (KKBP) céljainak eléréséhez. Eszerint az új szankciórendszer akkor alkalmazható, ha egy számítógépes támadás jelentős hatással van és:

- az EU-n kívülről hajtják végre,
- vagy az EU-n kívüli infrastruktúrát használnak, vagy
- az EU-n kívül letelepedett vagy működő személyek, illetve szervezetek hajtják végre.

Ez a szankciórendszer a potenciálisan jelentős hatással bíró kibertámadásokra is kiterjed. Főbb elvei a következők:

- az EU, tagállamai és polgáraik integritásának és biztonságának védelmére szolgál,
- figyelembe veszi az EU és az érintett állam közötti külkapcsolatok tágabb kontextusát,
- gondoskodik az Európai Unióról szóló szerződésben meghatározott KKBP-célkitűzések eléréséről és az azok megvalósításához szükséges megfelelő eljárásokról,
- a tagállamok között elfogadott, közös helyzettudatosságon alapul, és megfelelnek a konkrét helyzet szükségleteinek,
- arányos a számítógépes tevékenység terjedelmével, méretével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásával,
- tiszteletben tartja az alkalmazandó nemzetközi jogot, és nem sértheti az alapvető jogokat és szabadságot.

[54] MANOR, Ilan: The Digitalization of Diplomacy: Toward Clarification of a Fractured Terminology. Exploring Digital Diplomacy, 2017. augusztus https://digdipblog.files.wordpress.com/2017/08/the-digitalization-of-diplomacy-working-paper-number-1.pdf

A kiberdiplomácia tehát az állami kapcsolatokról szól a kibertérben, mégis van egy speciális eleme, amely megkülönbözteti minden más diplomáciai ágazattól. A kibertérben ugyanis vannak olyan vállalati szereplők, amelyek helyet követelnek maguknak az államközi együttműködésekben, hiszen az általuk működtetett infrastruktúrák globálisan meghatározóak. Az olyan több milliárd felhasználóval rendelkező szereplők, mint a már sokszor emlegetett Facebook, Microsoft vagy Google meghatározó résztvevői a multilaterális kapcsolatoknak, és bár nem szuverén szereplők, hiszen alapvetően amerikai joghatóság alatt állnak, együttműködésük nélkül a kibertér békéje nem megvalósítható. Az együttműködés természetesen a vállalatok érdeke is, hiszen nem egyszer előfordult már, hogy akaratukon kívül részeseivé váltak a geopolitikai folyamatoknak.

A Microsoft a 2017-es WannaCry kártékony kód kampány idején került a figyelem középpontjába, tekintettel arra, hogy az automatikusan terjedő zsarolóvírus, úgynevezett féreg típusú kód a Microsoft Windows rendszerekben megtalálható EternalBlue nevű sérülékenységet használta ki, amely legalább 20 éve része volt ezeknek az operációs rendszereknek. Habár a 2017. május végén elindult fertőzést meg lehetett volna előzni a cég által márciusban kiadott javítással, az ezt a hibát kihasználó támadás nem került volna nyilvánosságra, ha az amerikai titkosszolgálat, az NSA azt nem fedezi fel évekkel korábban, nem használja fedett műveletekben, és nem kezeli olyan hanyagul, hogy utána a Shadow Broker hackercsoport azt meg tudja szerezni. Mivel a Microsoft már annak az évnek az elején tisztában volt azzal, hogy ez a sebezhetőség komoly károkat okozhat a későbbiekben – és úgy általában komoly üzleti kockázatot látott abban, hogy állami szereplők az általuk készített szoftverek sebezhetőségeire építik műveleteiket anélkül, hogy ezekre a hibákra figyelmeztetnék a gyártókat –, előálltak a Digitális Genfi Egyezmény (Digital Geneva Convention) című javaslatukkal, ezzel aktív részesei lettek a kiberdiplomáciai tevékenységnek. Javaslatuk gyakran hivatkozott kiadvány lett a nemzetközi diplomáciai körökben, később a francia kormány fel is karolta a kezdeményezést és Párizsi Felhívás (Paris Call for Trust and Security in Cyberspace) néven hivatalosan is a diplomáciai agendába emelte a javaslatok nagyrészét.

A Digitális Genfi Egyezmény az alábbiakat javasolja az államok felé, kifejezve a digitális ipar szereplőinek elvárásait a termékeikkel és szolgáltatásaikkal kapcsolatos felelős viselkedéssel kapcsolatban:

- Ne támadjanak olyan rendszerek ellen, amelyek megsemmisítése hátrányosan befolyásolná a biztonságot (azaz a létfontosságú infrastruktúrákat, például kórházakat, energiaszolgáltató vállalatokat).
- Ne támadjanak olyan rendszerek ellen, amelyek megsemmisítése károsíthatja a globális gazdaságot (például a pénzügyi tranzakciók sértetlensége) vagy egyéb jelentős globális zavarokat okozhatnak (például felhőalapú szolgáltatások támadása esetén).
- Tartsák távol magukat az újságírók és a választási folyamatokban résztvevő magánszemélyek személyes fiókjainak vagy személyes adatainak meghackelésétől.

- Ne használjanak információs és kommunikációs technológiát a magánvállalkozások szellemi tulajdonának ellopásához, ideértve a kereskedelmi titkokat vagy más bizalmas üzleti információkat azért, hogy más vállalatoknak vagy kereskedelmi szektoroknak versenyelőnyt szerezzenek.
- Ne illesszenek be vagy ne követeljenek meg "backdoorokat", azaz hátsó kapukat tömegpiaci kereskedelmi technológiai termékekben.
- Értsenek egyet a sérülékenységek megszerzésével, megtartásával, biztosításával, használatával és jelentésével kapcsolatos egyértelmű szabályozással, ami tükrözi azt az erőteljes követelményt, hogy a megtalált sebezhetőségeket jelenteniük kell a gyártók felé – a tömegpiaci termékek és szolgáltatások terén.
- Tanúsítsanak önmérsékletet a kiberfegyverek kifejlesztésének terén, biztosítsák azt, hogy ezek korlátozottak, pontosak legyenek, és ne lehessen újra használni őket. Az államoknak azt is biztosítaniuk kell, hogy a fegyvereiket biztonságos környezetben, megfelelő kontroll mellett kezelik.
- Elfogadják a kiberfegyverek elterjedésének korlátozását. A kormányok nem terjeszthetnek, és nem engedélyezhetik mások számára sem a számítógépes fegyverek terjesztését, egyben hírszerzési, bűnüldözési eszközöket és pénzügyi szankciókat alkalmaznak azok ellen, akik ennek a követelménynek nem tesznek eleget.
- A kibertérben zajló támadó műveletekben való részvételt korlátozzák a civil infrastruktúrák és létesítmények tömeges károsodásának elkerülése érdekében.
- Részt vesznek a magánszektor azon erőfeszítéseiben, amelyek a kibertámadások észleléséhez, korlátozásához, illetve a reagáláshoz és a helyreállításhoz szükségesek. Kifejezetten rendelkezésre bocsájtják a válaszadáshoz és helyreállításhoz szükséges alapvető képességeiket vagy eljárásaikat, beleértve az eseménykezelő központokkal (Computer Emergency Response Team – CERT) való együttműködést. A magánszektor válaszába és a helyreállításban való részvételbe való beavatkozás hasonló lenne a katonai kórházak orvosi személyzetének támadásához.[55]

A kiberdiplomáciai szakértelem jellemzően az egyes országok külügyminisztériumában található. Nincs ez másképp Magyarországon sem, a tanulmány írása idején hatályos 19/2016. (VIII. 31.) KKM utasítás a Külgazdasági és Külügyminisztérium Szervezeti és Működési Szabályzatáról szerint a minisztérium Erőforrás-diplomácia és Új Típusú Biztonsági Kihívások Főosztályon működő Kibertér Koordinátor feladata ennek a szerepkörnek a betöltése.[56] Tiirmaa-Klaar hangsúlyozza, hogy ez a szerep jelentősen különbözik más külügyi pozícióktól, hiszen *„az infokommunikációs technológiák átfogó ismerete szükséges*

[55] Microsoft: A Digital Geneva Convention to protect cyberspace. 2017. április 13. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH

[56] A jelenleg hatályos 4/2019. (III. 13.) KKM utasítás a Külgazdasági és Külügyminisztérium Szervezeti és Működési Szabályzatáról szerint a kibertér koordinátor a Biztonságpolitikai és Non-proliferációs Főosztályhoz tartozik.

hozzá, így át kell látni a fejlesztési folyamatokat, a számítógépes és hálózati biztonságot, az internet-irányítást, a nemzetközi biztonságpolitikát, a kiberbűnözést, a kibertérben történő hírszerzést stb. Ezen tárgyak jó részét nem tanítják a diplomáciai akadémiákon vagy a külkapcsolati iskolákban. Eközben viszont a diplomatáknak gyorsan meg kell tanulniuk kibernyelven beszélni, mivel a téma gyorsan fejlődik."[57]

2014-ben kelt cikkében a kiberdiplomácia főbb kihívásai között a következőket említi: nemzetközi biztonság és bizalomerősítés a kibertérben, a kiberbűnözés elleni küzdelem, az emberi jogok védelme a kibertérben és az internet-irányítás kérdése. Bár ezek a prioritások folyamatosan fejlődnek, az elfogadásra váró amerikai kiberdiplomáciai törvény (Cyber Diplomacy Act of 2017) is hasonló fókuszterületeket fogalmaz meg az USA kiberkapcsolataival összefüggésben.

7. ESETTANULMÁNY: A NOTPETYA KAMPÁNY

A kiberteret érintő kártékony cselekmények sora végtelen hosszú, de vannak olyan események, amelyek fordulópontot, egyben hivatkozási alapot jelentenek a kutatóknak. A 2007-es Észtország elleni támadás, a Stuxnet kártékony kód bevetése, Edward Snowden információszivárogtatása mind olyan történések voltak, amikor át kellett értékelni a kibertérről alkotott véleményünket. Jelen tanulmány szempontjából a NotPetya kártékony kód kampány az a fordulópont, amely megmagyarázza a nemzetközi jog és a nemzetközi kapcsolatok fontosságát a kibertéri események kapcsán. Ez az incidens ugyanis olyan kritikus pontokra mutatott rá a külkapcsolatok területén, amelyek a gyakorlatban is megmutatták, a Tallinni Kézikönyv létrehozása vagy a Digitális Genfi Egyezmény (később Párizsi Felhívás) megalkotására tett javaslat valóban szükséges volt egyes országok nemzetközi normákat szabadon értelmező gyakorlata miatt.

A Wired magazin összefoglalója alapján a NotPetya kampány 2017. június 27-én, késő délután tört ki, az ukrán alkotmány ünnepe előtti munkanap utolsó munkaóráiban. Már az első fertőzések időpontjai találgatásra adtak okot, ugyanis az ukrán köztársaság jeles ünnepét megválasztani a támadás kezdetének jelzésértű üzenet. Igaz, ekkor még valószínűsíthető volt, hogy az időzítésnél szempont volt az is, hogy az informatikai üzemeltetők nagy része szabadságon lesz, tehát a védelem alacsonyabb erőforrásokkal fog működni. Bár a fertőzések más országokban is hamar megjelentek, a legtöbb fertőzött gépet Ukrajnából jelentették, így gyaníthatóan a célpont Ukrajna, mint állam volt, nem pedig egyes vállalatok. A többi országban, így többek között Németországban, Franciaországban, Olaszországban, Lengyelországban és az Egyesült Államokban csak járulékos áldozatok voltak. Tovább erősíti ezt a teóriát az is, hogy ugyanaznap egy gépjárműbe rejtett robbanóeszköz ölt meg egy különleges erőknél szolgáló munkatársat Kijevben.[58]

---

[57] TIIRMAA-KLAAR, Heli: Cyber Diplomacy: Agenda, Challenges and Mission. In: ZIOLKOWSKI, Katharina (Ed.): Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. NATO CCD COE Publication, Tallinn, 2013. pp. 509-532.

[58] GREENBERG, Andy: Petya Ransomware Epidemic May Be Spillover From Cyberwar. Wired, 2017. június 28. https://www.wired.com/story/petya-ransomware-ukraine/

A kártékony kód a zsarolóvírusok jellegzetességeit viselte magán, így a fertőzés után titkosította a merevlemezt, a gép elindulása után pedig 300 dollárnyi bitcoint kért a feloldásért cserébe. Hamar kiderült azonban, hogy a kapcsolattartásra megadott e-mail-cím nem él, tehát esély sincsen az elvesztett adatok visszaszerzésére. Amennyiben anyagi motivációjú lett volna a támadás, mint a NotPetyát egy hónappal megelőző WannaCry esetén, akkor a támadó elérhető marad és biztosítja a váltságdíjért cserébe az adatok visszaszolgáltatását, hiszen a hasonló bűncselekmények tanulsága alapján az áldozat csak akkor fizet, ha van esélye a dekódoló kulcs megszerzésére, tehát a bűnelkövetőnek érdeke az áldozat megfelelő kiszolgálása. A zsarolóvírus-jelleget erősítette az első órákban az is, hogy a kód hasonlóságot mutatott a jól ismert Petya zsarolóvírussal, de hamar kiderítették, hogy ez szándékos maszkírozás volt, így terjedt el a NotPetya, azaz a Nem Petya elnevezés a szakmában.

Hatásmechanizmusát tekintve a kártékony kód a számítógép master boot recordját, tehát az operációs rendszer betöltéséért felelős merevlemezszegmenst fertőzte meg, a gép indítását követően pedig elkezdte titkosítani a fájlrendszert. Ha ez sikerült neki, a képernyőn feltüntette a zsarolóvírusok által használatos szöveget, jelezte, hogy mennyi pénzt kér és mi a kommunikáció módja. Mielőtt a gépet használhatatlanná tette volna, megpróbált elterjedni azon a hálózaton, amin a fertőzött gép volt. Ehhez egyrészt használta az EternalBlue sebezhetőséget, azaz a WannaCry-nál megismert módon féregjelleggel terjedt a korábban nem frissített gépekre, de a fertőzött gép memóriájából is összegyűjtötte az ott levő adminisztrátori jelszavakat, amelyek szintén hozzáférést adhattak neki más hálózati gépekhez. Az első fertőzések a feltételezések szerint az M.E. Doc nevű szoftver frissítési mechanizmusán keresztül érkeztek. Ez a szoftver az egyik hivatalosan jóváhagyott adóbevallási program, így az ukrán vállalatok jelentős részénél megtalálható volt. Ez a program jelezte, hogy frissíteni kell, majd miután a felhasználó engedélyezte a javítások telepítését, elkezdődött a fertőzés. Arról nincsen információ, hogyan tudták a M.E. Doc frissítési eljárását befolyásolni. A távoli feltöréstől kezdve a frissítőszerverhez való közvetlen, fizikai hozzáférésig számos lehetséges megoldás szóba kerülhet. Az biztosnak tűnik, hogy a támadó adminisztrátori jogosultságot szerzett a M.E.Doc vállalat egyik szerverén, ez tette lehetővé számára azt, hogy a frissítési mechanizmusba is beavatkozzon. A Talos kiberbiztonsági cég nyomozása szerint már 2017. április 24-én olyan frissítés ment a felhasználókhoz, ami hátsókaput tartalmazott, tehát elvileg lehetővé tette a támadás kivitelezését. A támadók tehát hónapokkal korábban elkezdtek felkészülni az akcióra. Szemben a WannaCry-jal, itt nem találtak olyan kapcsolót, úgynevezett „kill switch”-et, mely lehetővé tette volna a fertőzés gyors leállítását. A támadó célja egyértelműen a minél nagyobb, földrajzilag a lehető legjobban lokalizált pusztítás volt.[59,60]

[59] MAYNOR, David et. al.: The MeDoc Connection. Talos Intelligence, 2017. július 5. https://blog.talosintelligence.com/the-medoc-connection/

[60] Érdemes megfigyelni a hasonlóságot a Solarwinds támadással, illetve az orosz–ukrán háború első hónapjában felfedezett, wiper típusú kiberfegyverekkel! Az orosz műveleti képességek evolúcióját követve látható jól, hogy a kibertéri hadviselés sem a semmiből jön, hosszú évek fejlesztése szükséges hozzá, amelynek gyakorlótere Ukrajna volt. A háború után célszerű kielemezni, mennyire volt jó döntés előre felfedni ezeket a kiberműveleti képességeket orosz részről.

Végül több ezer ukrán vállalatot érintett az incidens. Az áldozatok között megtalálhatók bizonyos ukrán kritikus infrastruktúrák, így többek között helyi bankok, a kijevi Borispol repülőtér, az energetikai cégek közül pedig a Kyivenergo és az Ukrenergo. De több külföldi cég is jelentett fertőzést, így az amerikai gyógyászati vállalat, a Merck, az orosz Rosznyeft, illetve a magyar OTP Bank ukrajnai pénzkiadó automatáiról is elterjedtek olyan képek a világhálón, amelyek NotPetya fertőzést mutattak. A legnagyobb publicitást az A.P. Moller – Maersk cégnél történt pusztítás kapta. A cég a világ egyik legnagyobb logisztikai vállalata, a Forbes Global 2000 céglistája szerint a világ 558. legnagyobb konglomerátuma. A NotPetya fertőzés a beszámolók szerint két napra ellehetetlenítette a cég működését, a teherszállító hajók berakodását világszerte manuálisan kellett irányítani, számítógép helyett a papírra és a ceruzára voltak kénytelenek hagyatkozni. Ez meg is látszódott a dán vállalat bevételén, negyedéves beszámolójukban azt becsülték, hogy 200–300 millió dollár közötti kárt okozott nekik ez a kétnapos leállás.[61]

A NotPetya kártékony kód az első olyan kibertéri incidens, amely békeidőben történő koordinált támadásnak tűnik egy szuverén állam ellen, támadva annak kritikus infrastruktúráit, civil létesítményeit, járulékos kárt okozva más országokban működő civil vállalatoknak is. Célja egyértelműen a pusztítás volt. A kártékony kód által felhasznált eszközök korábban ismertek voltak, hiszen sem a hálózaton belüli terjedéshez kihasznált sebezhetőség, sem a kiemelt jogosultságú felhasználók hitelesítési adataihoz való hozzáférést megvalósító szoftver nem okozott meglepetést a szakembereknek. A támadási taktika azonban merőben új volt, érezhetően alapos műveleti tervezés előzte meg, hiszen a terjesztéshez választott M.E.Doc szoftver Ukrajna határain túl ismeretlen, csak megfelelő hírszerzési háttérrel lehetett biztosan tudni, hogy ez a terjedési vektor ennyire hatékony lehet egy földrajzilag fókuszált kibercsapás végrehajtására. A határon túlnyúló hatás elsősorban amiatt történt, hogy az Ukrajna területén működő multinacionális vállalatok belső hálózatain nem mindenki tudta földrajzi értelemben lokalizálni a kártékony kód hatásait. Külön ki kell emelni azt a lélektani csavart a támadásban, amivel az áldozatokkal elhitették, hogy a kártékony kód számára hátsókaput nyitó M.E.Doc-verziót fel kell telepíteni. Mind a végfelhasználók, mind az informatikai üzemeltetők számára ugyanis évtizedek óta tudatosítják a kiberbiztonsági szakemberek, hogy a szoftverekből a legfrissebb változatot kell használni, tehát ha egy szoftverfrissítés rendelkezésre áll, akkor azt a lehető leghamarabb telepíteni kell. A támadó tehát erre az alapvetésre építette fel a terjesztést, bízva abban, hogy a felhasználók külön kérdés nélkül, a lehető leghamarabb telepítenek bármit, ami frissítésnek tűnik, így a frissítőszerver megtámadása és terjesztési pontnak való használata briliáns választás volt a támadó részéről.

Az államok szempontjából az eldöntendő kérdés az, hogy ha adott egy kiberbiztonsági incidens, ami katonai kiberműveletnek látszódik, amelynek során egy fejlett kiberfegyvert vetettek be egy olyan országban, amely már korábban is szenvedett ilyen célzott támadásoktól, akkor vajon ki lehet-e mondani, hogy ez az incidens ténylegesen fegyveres támadásnak minősíthető a szó nemzetközi jogi értelmében, illetve élhetnek-e az attribúció eszközével, megnevezhetnek-e egy

[61] MOLLER, A. P.– MAERSK: A.P. Moller - Maersk improves underlying profit and grows revenue in first half of the year. 2017. augusztus 16. https://www.maersk.com/press/press-release-archive/20170816-a-p-moller-maersk-improves-underlying-profit-and-grows-revenue-in-first-half-of-the-year

országot támadóként? Másrészt kérdés az is, hogy a nemzetközi diplomácia felkészült-e arra, hogy egy ilyen nyilatkozat után a hagyományos diplomáciai eszközökkel kezelni tudják a megnevezett ország válaszlépéseit? Végül kérdés az is, hogy a megnevezett támadó országra lehet-e olyan nyomást gyakorolni, amelynek eredményeképpen az csökkenti vagy beszünteti a kibertérben történő ellenséges cselekményeit?

Schmitt és Biller a NotPetya támadás után pár héttel megvizsgálta, hogy az incidens hogyan viszonyul a nemzetközi jog előírásaihoz. Első megjegyzésük az volt, hogy a beszámolók szerint a kártékony kód nem okozott sérülést vagy halált a beszámolók szerint. Jelen tanulmány szerzője ehhez annyit tesz hozzá, hogy bár közvetlen halálesetekről sem a NotPetya, sem a WannaCry esetén nem olvashattunk, nem kizárt, hogy egyes egészségügyi létesítmények nem működő elektronikus információs rendszerei, különösen a WannaCry esetén a brit egészségügyi rendszert érő befolyás miatt, közvetve hozzájárulhattak olyan halálesetekhez, amelyek megelőzhetők lehettek volna, ha a beteget időben tudják a megfelelő ellátáshoz juttatni. Schmitt és Biller a nemzetközi jog alapján a számonkérhetőséget az attribúcióhoz köti, azaz a fő kérdés az, hogy a támadás mögött egy ország fegyveres erői, hírszerző ügynökségei vagy állami alkalmazottai álltak, vagy nem állami szereplő esetén az utasításokat állami szereplő adta-e, és kontrollt gyakorolt-e a tevékenység felett? Feltételezve, hogy ez történt, három állami kötelezettség megsértését lehet feltételezni. Ezek a szuverenitás tiszteletben tartása, a beavatkozás tilalmának elve és az erőszak alkalmazásának tilalma.

A szuverenitás a szakértők szerint sérült a NotPetya támadás alatt, ennek ugyanis két feltétele van. Egyrészt a területi integritás megsértése, amely a kibertérben úgy képzelhető el, hogy egy támadás fizikai károkat vagy személyi sérülést, esetleg halálesetet okoz. Kiterjesztő értelmezésben, amennyiben egy kiberinfrastruktúra hosszabb időre elérhetetlenné válik, a szerzők véleménye szerint szintén megfogalmazható a területi integritás megsértése. Mivel a NotPetya túlmutatott egy átlagos elosztott túlterheléses támadás hatásain, konkrétan kulcsfontosságú adatok elvesztésével járt, illetve kritikus számítógépes rendszerek helyett kellett új gépeket üzembe állítani, ez felfogható a fizikai létesítmények sérüléseként. A másik feltétel az alapvető kormányzati tevékenységek megzavarása lenne, ez azonban a NotPetya esetében nem történt meg. Habár a pénzintézeti tevékenységeket lehetővé tevő informatikai rendszerek sérültek, ezek nem alapvető kormányzati funkcionalitást támogatnak, tehát a szuverenitás megsértésének ez a feltétele nem állt fenn.

A be nem avatkozás elvének megsértéséhez kényszerítő erejű tevékenységek társulnak, amelyet egy állam fejt ki egy másik állammal szemben a politikai, gazdasági, társadalmi és kulturális berendezkedés megváltoztatása, illetve a külpolitika befolyásolása céljából. Schmitt és Biller nem látta bizonyítottnak, hogy a NotPetya kártékony kód alkalmas lett volna ezen célok megvalósítására, tekintettel arra, hogy célja a pusztítás és nem a befolyásolás vagy az anyagi haszonszerzés volt. Amennyiben a kiberfegyver valóban zsarolóvírus lett volna, aminek az első pillantásra látszódott, elvileg meg lett volna a lehetőség a kényszerítésre, hiszen a zsarolás lényege valamilyen döntés kicsikarása vagy anyagi haszonszerzés a másik féltől.

Az erőszak alkalmazásának elve békeidőben azt jelenti, hogy egy állam ENSZ-felhatalmazás vagy mandátum nélkül hajt végre olyan erőszakos tevékenységet, amely nem minősül önvédelemnek vagy kollektív védelemnek. A kibertevékenységek jellemzően kis hatással vannak a fizikai környezetre, így nehéz olyan támadást elképzelni, amely eléri az erőszak alkalmazásának jogosulatlan szintjét. A kiberinfrastruktúra hosszú távú kiesése azért, mert az azt alkotó számítógépek vagy hálózati eszközök elérhetetlenné váltak egy NotPetyához hasonló kártékony kód miatt, viszont már minősíthető lenne jogosulatlan erőszak alkalmazásaként. A szerzők véleménye szerint a gazdasági destabilizáció is ebbe a körbe tartozhat. Az ukrán kormány véleménye szerint a kibertámadás elérte ezt a szintet, a nemzetközi gyakorlat azonban 2017 közepén még nem adott egyértelmű választ arra, hol a határ.

A nemzetközi humanitárius jog akkor tekinthető érvényesnek ebben az esetben, ha két állam, azaz Ukrajna, és tegyük fel, Oroszország között egyveres konfliktus állt volna fenn az érintett időszakban. Ennek feltétele, hogy egy ország megszállás alatt tartja egy másik ország területét vagy egy nem állami csoportot támogat, amely ellenséges tevékenységet fejt ki a másik ország ellen. Mivel a Krím-félsziget és a kelet-ukrajnai felkelőcsoportok támogatása miatt a szerzők meglátása szerint joggal feltételezhető, hogy a két állam között fegyveres konfliktus állt fenn, a NotPetya használatát a nemzetközi humanitárius jog alapján is vizsgálni kell, dacára annak, hogy az ENSZ GGE-ben erről nincsen teljes körű egyetértés. Ennek a kártékony kódnak a minősítését a Tallinni Kézikönyv alapján érdemes megvizsgálni, amely alapján támadásnak minősül az ilyen kiberfegyverek használata még akkor is, ha közvetlen kárt nem okoznak a kiberinfrastruktúrában, csak közvetve fejtik ki hatásukat, illetve egyes szakértők szerint az infrastruktúra elérhetetlenségének előidézése is a támadás körébe tartozik.

A NotPetya célpontjai között szerepelt a kijevi repülőtér, a csernobili erőmű és az ukrán egészségügyi rendszer is. Amennyiben feltételezhető, hogy ez a támadó szándékával megegyezően történt, akkor nem a kártékony kód koordinálhatatlan terjedése miatt valósult meg a fertőzés, tehát ez támadásnak minősíthető a szerzők álláspontja szerint. Habár egyes megtámadott létesítmények minősíthetők lennének kettős felhasználásúnak is, például a repülőtér, a legtöbb kiberinfrastruktúra-elem egyértelműen civil jellegű, nem szolgál katonai célokat, így akár a háborús bűncselekmény kategóriájába is tartozhatna a cselekmény. Ráadásul a kiberfegyver hatása túlmutatott Ukrajnán, harmadik országokban is éreztette hatását, így azok semlegességét is megsértette a támadó.[62]

Mindez természetesen csak a kutatók tudományos gondolatmenete, egy kibertámadás kapcsán háborús bűncselekményeket emlegetni komoly diplomáciai hatásokkal járhat, ha azt egy hivatalban levő politikus teszi. A NotPetya viszont különleges abban a tekintetben, hogy a kutatói álláspontok mellett megjelentek az olyan kommentárok, majd politikai állásfoglalások, amelyeket az elméleti gondolatmenetnél komolyabban kellett venni. Először a NATO Egyesített Kibervédelmi Kiválósági Központjának kutatói elemezték a kialakult helyzetet. Az idézett Michael Schmitt is ehhez a tudományos körhöz tartozik, a korábban idézett

[62] SCHMITT, Michael N.– BILLER, Jeffrey: The NotPetya Cyber Operation as a Case Study of International Law. EJIL: Talk!, 2017. július 11. https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/

elemzése azonban nem a szervezet honlapján jelent meg, így Blumbergs, Minárik, van der Meij és Lindström cikkét a világsajtó már mint a NATO álláspontját tette közzé, ezzel alakítva a nyugati narratívát a támadással kapcsolatban. Annak ellenére, hogy a CCD COE nem NATO szervezet, hanem „csak" egy tudományos központ, a közvélekedésben különös súlya lett annak, amit Minárik mondott: *„Amennyiben a művelet összefügg egy nemzetközi fegyveres konfliktussal, akkor a fegyveres konfliktusokra vonatkozó jogszabályok vonatkoznak rá"*. Korábban a NATO CCDCOE kommentárjai nem járták be a világsajtót ilyen kényes ügyben, így érzékelni lehetett, hogy a NotPetya súlya lényegesen nagyobb, mint bármilyen másik korábbi esetnek, hiszen ennyire egyértelműen korábban nem sugalmazták Oroszország felelősségét a sajtóban, felhasználva egy, a nevében a NATO-hoz tartozó, de valójában a katonai szervezet döntéshozatalában nem meghatározó intézményt.[63]

Az igazán nagy áttörést 2018 februárjában érte el az ügy, amikor 7 ország, az Egyesült Államok, Nagy-Britannia, Dánia, Litvánia, Észtország, Kanada és Ausztrália közösen ítélték el Oroszországot a NotPetya támadás miatt, ezt pedig hivatalosan is támogatta Új-Zéland, Norvégia, Lettország, Svédország és Finnország. Korábban soha nem történt meg, hogy több ország közösen élt volna az attribúció eszközével, azaz egyöntetűen mutattak volna rá a támadóra. A támadás mögött álló ország nevesítése mindig politikai döntés, amelyet támogathat műszaki vagy hírszerzési bizonyíték, de politikai akarat nélkül ezek nem sokat érnek. Tobias Feakin, Ausztrália kiberügyekben felelős nagykövete foglalta össze kiválóan, miért volt fontos lépés ez a közös kiállás és mit jelent ez a támadókra nézve: *„Amit teszünk, az az, hogy tovább érleljük hozzáállásunkat annak érdekében, hogy a következmények még jobban érezhetők legyenek a jövőben. Tehát az elrettentés egyik kulcsfontosságú jele más országok számára az, hogy tiszta, egyértelmű és hiteles üzenetet küldünk a támadóknak arról, hogy következményei lesznek viselkedésüknek."*[64]

[63] BLUMBERGS, Bernhards et. al.: NotPetya and WannaCry Call for a Joint Response from International Community. CCDCOE, 2017. július https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html

[64] STILGHERRIAN: Blaming Russia for NotPetya was coordinated diplomatic action. ZDNet, 2018. április 12. https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/

Felhasznált irodalom:

- 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- BÁNYÁSZ Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. Nemzetbiztonsági Szemle, 2015/2. pp. 21-36.
- BARRINHA, André– RENARD, Thomas: Cyber-diplomacy: the making of an international society in the digital age. Global Affairs, 2017/4-5. pp. 353-356.
- BLUMBERGS, Bernhards et. al.: NotPetya and WannaCry Call for a Joint Response from International Community. CCDCOE, 2017. július https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html
- BÓDI Stefánia – KÁDÁR Pál – PETRUSKA Ferenc: Jogi alapismeretek honvéd tisztjelölteknek. Nemzeti Közszolgálati Egyetem, Budapest, 2014.
- BUCHAN, Russell: The International Legal Regulation of State-Sponsored Cyber Espionage. In: OSULA, Anna-Maria – Henry RÕIGAS (Eds.): International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn, 2016. pp. 65-86.
- BUCHAN, Russell: The International Legal Regulation of State-Sponsored Cyber Espionage. In: OSULA, Anna-Maria – RÕIGAS, Henry (Eds.): International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn, 2016. pp. 65-86.
- CALATAYUD, Jose Miguel: Locked Shields: The world's largest cyber-war game. Al Jazeera, 2017. június 18. https://www.aljazeera.com/features/2017/6/18/locked-shields-the-worlds-largest-cyber-war-game
- CSERNY Ákos – TÉGLÁSI András: Jogforrástan: nemzetközi és uniós jog. Nemzeti Közszolgálati Egyetem, Budapest, 2014.
- DÁN Károly: Promoting confidence in Cyberspace: The workings of the OSCE. Elhangzott: Nemzeti Közszolgálati Egyetem, 2018. 03. 12.
- DEÁK Veronika (Szerk.): Az IBTV. gyakorlata. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára. Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, Budapest, 2020. pp. 6–36., 31 p.
- Elaine Korzak: UN GGE on Cybersecurity: The End of an Era? The Diplomat, 2017. július 31. https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/
- ENSZ: Az Egyesült Nemzetek Alapokmánya. 1945. június 26. http://www.grotius.hu/doc/pub/HBJFWJ/az%20ensz%20alapokm%C3%A1nya.pdf
- FERENCZY Gábor Zoltán: Internet alapú nyílt információszerzés elvi rendszertechnikai megvalósítása. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007.

- GOODIN, Dan: Suspicious" event routes traffic for big-name sites through Russia. Ars Technica, 2017. december 13. https://arstechnica.com/information-technology/2017/12/suspicious-event-routes-traffic-for-big-name-sites-through-russia/
- GREENBERG, Andy: Petya Ransomware Epidemic May Be Spillover From Cyberwar. Wired, 2017. június 28. https://www.wired.com/story/petya-ransomware-ukraine/
- https://www.nato.int/cps/en/natohq/official_texts_207156.htm
- https://www.theverge.com/2019/5/5/18530412/israel-defense-force-hamas-cyber-attack-air-strike
- ITU: ITU Cybersecurity Activities. 2018. július 5. https://www.itu.int/en/action/cybersecurity/Pages/default.aspx
- ITU: On the road to implement the Connect 2020 Agenda. 2014. https://studylib.net/doc/12920596/on-the-road-to-implement-the-connect-2020-agenda
- ITU: Report of the Working Group on Internet Governance. 2005. http://www.wgig.org/docs/WGIGREPORT.pdf
- IZSA Jenő: A hírszerzés céljáról és rendszeréről. Hadtudomány. 2009/1-2, pp. 72-83.
- KAJTÁR Gábor: Az önvédelem jogával kapcsolatos dilemmák a terrorizmus elleni háború korában. In: NAGY Marianna (Szerk.): Ünnepi konferencia az ELTE megalakulásának 375. évfordulója alkalmából. Jogi Tanulmányok, II. kötet, 2010. pp. 293-308.
- KOVÁCS Péter: A nemzetközi jog fejlesztésének lehetőségei és korlátai a nemzetközi bíróságok joggyakorlatában. Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar, Budapest, 2010.
- LATTMANN Tamás: A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén. In: CSAPÓ Zsuzsanna (Szerk.): Emlékkötet Herczegh Géza születésének 85. évfordulójára: A ius in bello fejlődése és mai problémái. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2013. pp. 209-220.
- LATTMANN Tamás: Nemzetközi jogi szabályozás célzott kibertámadások esetén. In: DEÁK Veronika (Szerk.): Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, Nemzeti Közszolgálati Egyetem, 2018.
- LIBICKI, Martin C.: Drawing Inferences from Cyber Espionage. In: MINÁRIK, T.– JAKSCHIS, R.– LINDSTRÖM, L. (Eds.): 2018 10th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinn, 2018. pp. 109-122.
- MANOR, Ilan: The Digitalization of Diplomacy: Toward Clarification of a Fractured Terminology. Exploring Digital Diplomacy, 2017. augusztus https://digdipblog.files.wordpress.com/2017/08/the-digitalization-of-diplomacy-working-paper-number-1.pdf

- MARTIN, Alexander J.: Russian hackers targeted Ukraine's water supply, security service claims. Sky News, 2018. július 11. https://news.sky.com/story/russian-hackers-targeted-ukraines-water-supply-security-service-claims-11432826
- MAURER, Tim: Cyber Norm Emergence at the United Nations – An Analysis of the UN‘s Activities Regarding Cyber-security. Belfer Center for Science and International Affairs, 2011.
- MAYNOR, David et. al.: The MeDoc Connection. Talos Intelligence, 2017. július 5. https://blog.talosintelligence.com/the-medoc-connection/
- Microsoft: A Digital Geneva Convention to protect cyberspace. 2017. április 13. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH
- MOLLER, A. P.– MAERSK: A.P. Moller - Maersk improves underlying profit and grows revenue in first half of the year. 2017. augusztus 16. https://www.maersk.com/press/press-release-archive/20170816-a-p-moller-maersk-improves-underlying-profit-and-grows-revenue-in-first-half-of-the-year
- Munich Security Conference: MSC 2011 Summary. 2011. február https://securityconference.org/en/ (Letöltés ideje:)
- MUNK Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. Hadtudomány, 2018/1. pp. 113-131.
- NATO: Az Észak-Atlanti Szerződés. 1949. április 4. https://www.nato.int/cps/ic/natohq/official_texts_17120.htm?selectedLocale=hu
- NATO: Brussels Summit Declaration. 2018. augusztus 30. https://www.nato.int/cps/en/natohq/official_texts_207156.htm
- NATO: Wales Summit Declaration. 2018. augusztus 30. https://www.nato.int/cps/ic/natohq/official_texts_112964.htm
- Nuclear Threat Initiative: The UN Groups of Governmental Experts (GGE). 2016. január. https://www.nti.org/education-center/treaties-and-regimes/united-nations-groups-governmental-experts/
- OSULA, Anna-Maria – RÕIGAS, Henry: Introduction. In: OSULA, Anna-Maria – RÕIGAS, Henry (Eds.): International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn, 2016. pp. 11-22.
- RÁCZ Lajos: Diplomácia – Katonadiplomácia. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2010.
- SCHMITT, Michael N. (Ed.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge, 2017.
- SCHMITT, Michael N.– BILLER, Jeffrey: The NotPetya Cyber Operation as a Case Study of International Law. EJIL: Talk!, 2017. július 11. https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/

- SCHMITT, Michael N.– VIHUL, Liis: The Nature of International Law Cyber Norms. In: OSULA, Anna-Maria, RÕIGAS, Henry (Eds.): International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn, 2016. pp. 23-48.
- STILGHERRIAN: Blaming Russia for NotPetya was coordinated diplomatic action. ZDNet, 2018. április 12. https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/
- SUBA Ferenc: Nemzeti Kiberbiztonsági Stratégia. In: DOBÁK Imre (Szerk.): A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem, Budapest, 2014. pp. 110-115.
- TÁLAS Péter: A varsói NATO-csúcs legfontosabb döntéseiről. Nemzet és Biztonság. 2016/2. pp. 97-101.
- TIIRMAA-KLAAR, Heli: Cyber Diplomacy: Agenda, Challenges and Mission. In: ZIOLKOWSKI, Katharina (Ed.): Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. NATO CCD COE Publication, Tallinn, 2013. pp. 509-532.
- VEENENDAAL, Matthijs– KASKA, Kadri– BRANGETTO, Pascal: Is NATO Ready to Cross the Rubicon on Cyber Defence? NATO CCDCOE, 2016. június. https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf

5. FEJEZET

KIBERBIZTONSÁGI INNOVÁCIÓ AZ EURÓPAI SZABÁLYOZÁSOK TÜKRÉBEN[1]

Az elektronikusan kezelt információ biztonsága, általánosabban véve a kiberbiztonság az egyik legnagyobb kihívás a XXI. században. Folyamatosan jelennek meg újabb és újabb fenyegetések, amelyekre innovatív és újszerű válaszokat kell adni. Ezek az innovatív megoldások mindenképpen magukkal hozzák az olyan új típusú technológiák használatát az információbiztonságban, mint például a Nagy Adatokból (Big Data) való építkezést, és az ezen alapuló mesterséges intelligencia használatát. Ezeknek az innovációknak a támogatását az Európai Unió a 2021 és 2027 közötti időszakban kiemelt fontosságúnak tartja. A tanulmány bemutatja a kiberbiztonsági kompetenciahálózatok tervezetét, illetve ismerteti, hogy milyen kutatási fejlesztési és innovációs lehetőségek lesznek a következő évtizedben Európában.

1. BEVEZETÉS

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

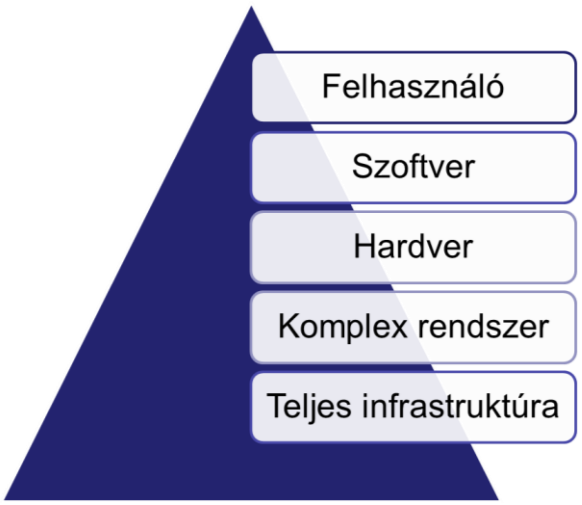
Az információbiztonsági szakértők körében az IoT rövidítés közkeletű feloldása az Internet of Threats, azaz a Fenyegetések Internete, utalva arra, hogy a szakértői közösségnek komoly aggályai vannak mind az egyes eszközök, mind pedig az ezekből felépülő ökoszisztéma védelmi szintjével kapcsolatban. Továbbmenve, a szakértők viccesen azt is megjegyzik, hogy az IoT betűszóban az S betű jelöli a Securityt, azaz a biztonságot. Az elmúlt évek kibertámadásainak köszönhetően ebben a félelemben ma már a stratégiai védelemmel foglalkozó szakemberek is osztoznak, így egyre több ország nemzeti biztonsági és kiberbiztonsági stratégiája kiemelt nemzetbiztonsági problémaként foglalkozik a

[1] Eredetileg megjelent: TÖRÖK Bernát (Szerk.): Információ- és kiberbiztonság: Fenntartható biztonság és társadalmi környezet tanulmányok V. Ludovika Egyetemi Kiadó, Budapest, 2020. pp. 83-97. Paper: 2, 15 p.

kibertéri fenyegetésekkel kiemelt nemzetbiztonsági problémaként. A kockázatok enyhítése céljából folyamatosan dolgozzák ki azokat a szabályozókat, amelyek kötelezik az okos infrastruktúrák építőit és üzemeltetőit bizonyos informatikai védelmi intézkedések megtételére.

2. AZ INFORMÁCIÓS RENDSZEREKET ÉRINTŐ FENYEGETÉSEK

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



1. ábra: Támadási felületek az okos infrastruktúrákban
(saját szerkesztés)

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

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

Nem szabad figyelmen kívül hagyni az emberi tényező fontosságát sem. Bányász Péter az ellátási láncok kiberbiztonságáról szóló munkájában a következőket említi az emberi hiszékenységet kihasználó (ún. social engineering) támadásokkal kapcsolatban:
„Tegyük fel, a külső támadás lehetetlenné vált, olyan mértékű védelmet valósítottak meg. Ilyen esetben van szerepe a social engineeringnek, hiszen, maradva a hipotetikus példánál, a kikötő takarítószemélyzetéből egy dolgozó megzsarolásával/megtévesztésével a támadók elérhetik, hogy a takarító az informatikai eszközökhöz hozzáférést biztosítson egy pendrive a számítógépbe történő helyezésével, amivel a támadók olyan hátsó kapukat nyithatnak, amellyel átvehetik az irányítást az eszköz felett.”[2]

A napvilágra került, kritikus infrastruktúrákat érintő támadások során szinte minden esetben sejthető, hogy szándékos vagy gondatlan emberi tevékenység nélkül a támadás kivitelezése lényegesen nehezebb vagy egyenesen lehetetlen lett volna.

A támadási felületek közül nem véletlenül nem került említésre a hardver, a komplex rendszer és a teljes infrastruktúra. Nem véletlenül. Ezek esetében ugyanis hiányoznak azok a megbízható statisztikák, adatforrások, amelyekkel szemléltetni lehet a kitettségüket. A hardverek esetében például tudjuk, hogy számos CPU[3] a tervezési sajátosságaik miatt elméletileg lehetőséget biztosít a számítógépen feldolgozott bizalmas adatokhoz való hozzáféréshez (lásd a Spectre és Meltdown hibákat)[4], de csak elképzeléseink lehetnek arról, hogy ezek valójában mekkora kockázatot jelentenek. A kínai távközlési gyártók angolszász országokból való távoltartásának szándéka is mutatja, milyen nemzetbiztonsági kihívást érzékelnek a stratégiai védelemért felelős vezetők abban, ha az 5G távközlési rendszerek infrastruktúráját ellenérdekelt országok gyártói szállítják.

A védelem komplexitását tovább fokozza az a tény, hogy az elmúlt 10–15 évben jelentősen átalakultak azok az alaptechnológiák, amelyek információtechnológiai értelemben védelemre szorulnak. Ezek között felsorolhatjuk a kétezres években tömegessé vált közösségi hálózatokat, a hordozható

---

2 BÁNYÁSZ Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In: CSENGERI J. – KRAJNC Z. (Szerk.): Humánvédelem - békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése. Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Budapest, 2016. p. 918.

3 Central Processing Unit, központi feldolgozóegység

4 Graz University of Technology: Meltdown and Spectre - Vulnerabilities in modern computers leak passwords and sensitive data. 2018. január https://meltdownattack.com/

infokommunikációs eszközöket, vagy éppen a felhő-számítástechnikát, de a 2010-es évek közepétől kezdve elterjedtek azok az ezekre épülő megoldások is, amelyek új szemléletű, új típusú kibervédelmet igényelnek.

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

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

3. AZ ÚJ TECHNOLÓGIÁK KIBERVÉDELMI SZABÁLYOZÁSA

Belátható, hogy a támadási felületek csökkentése, pusztán a mérnökök eszköztárával csak rendkívül lassan és körülményesen lenne megvalósítható, a veszély viszont reális, ezért azonnali, széles körű cselekvést kíván. Be kell tehát vonni azokat a közpolitikai és diplomáciai eszközöket, amelyek egyrészt a támadók motivációját törik le, másrészt rendszerszinten várnak el cselekvést a negyedik ipari forradalom szereplőitől. Fogalmi szinten ez azt jelenti, hogy az egyes rendszerelemeket érintő információbiztonság mellett az ennél szélesebb körű kiberbiztonság megvalósítása is kívánatos. A negyedik ipari forradalom és az elmúlt években megjelenő kibertéri fenyegetések miatt tehát új típusú kibervédelmet, új típusú kibervédelmi mentalitást kell megvalósítani, miközben az alapvető információbiztonsági alapelvek változatlanok maradnak.

A kiberbiztonság és az információbiztonság közötti fogalmi különbség egyértelműen megfogalmazott a magyar jogszabályokban. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény preambuluma így fogalmaz:
„Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei

sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme."

Az Értelmező rendelkezések szerint az elektronikus információs rendszer biztonsága *„az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos"*, míg a kiberbiztonság *„a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez"* [5]

Hasonló megközelítést mutat a 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról is, amelynek *„célja, hogy az Alaptörvény elveivel összhangban, az értékek és érdekek számbavétele, valamint a kibertér biztonsági környezetének elemzése alapján meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is."*[6]

Így tehát közel sem csak a mérnöki feladatokra koncentrál.

Az információbiztonságról, azaz a pusztán mérnöki megközelítésről a kiberbiztonságra, azaz az állami szervek általi intézkedésekre való áttérést mutatja egy másik trend is. E trend nyomán egyre több iparágban jelenik meg valamilyen kibervédelmi szabályozás, mely például hatósági eszközökkel kényszeríti ki az állami és piaci szereplők közötti együttműködést. A pénzintézeteknél és a kormányzati szektorban régóta léteznek olyan szabályozók és jogszabályok, melyeknek meg kell felelniük az oda tartozóknak, viszont az Európai Unió egy három pillérből álló kiberbiztonsági szabályozással jelentősen kiterjesztette a megfelelőségi kényszert. Ez a három pillér a személyes adatok védelmét, a kritikus információs infrastruktúrák biztonságát és a negyedik ipari forradalom eszközeivel kapcsolatos kockázatcsökkentést hivatott elősegíteni.

Az első pillér Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA[7]-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet (Kiberbiztonsági Jogszabály) hatályon kívül helyezéséről, azaz a Kiberbiztonsági Jogszabály. Ennek legfontosabb üzenete, hogy szükséges az információbiztonság erősítése mind termék-, mind szervezeti szinten,

[5] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[6] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

[7] European Union Agency for Cybersecurity. A rövidítés a szervezet korábbi nevéből, az European Network and Information Security Agency-ből (Európai Uniós Hálózat- és Információbiztonsági Ügynökség) származik.

de támogatni kell a kiberbiztonsággal kapcsolatos lépéseket is. Az Európai Unió kiberbiztonsági reformról szóló összefoglalójában a Kiberbiztonsági Jogszabály, azaz a Cybersecurity Act által lefedett területeket így foglalják össze:

„Kiberbiztonsági tanúsítási rendszer: Az Európai Bizottság a 2017. szeptemberi reformcsomagban javaslatot tett az ikt-termékekre, -szolgáltatásokra és -folyamatokra vonatkozó uniós tanúsítási rendszerek bevezetésére. A kezdeményezés célja az uniós kiberbiztonsági piac növekedésének elősegítése. E tanúsítási rendszerek szabályok, műszaki követelmények és eljárások formájában valósulnának meg. Szerepük az lenne, hogy csökkentsék a piac széttagoltságát és felszámolják a szabályozási akadályokat, továbbá, hogy segítsék a bizalomépítést is. A rendszereket valamennyi tagállam elismerné, ami megkönnyítené a vállalkozások számára a határokon átnyúló kereskedelmet.

- *Az uniós kiberbiztonsági ügynökség megerősítése: A Bizottság javasolta továbbá azt is, hogy a meglévő Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) struktúráját felhasználva jöjjön létre egy erősebb uniós kiberbiztonsági ügynökség. Az új ügynökségnek az lenne a feladata, hogy segítséget nyújtson a tagállamok, az uniós intézmények és a vállalkozások számára a kibertámadások kezelésében.*
- *A kompetenciatámogatástól a csalás elleni küzdelemig: Az Európai Bizottságnak az uniós kiberbiztonság megerősítését célzó javaslata további kezdeményezéseket is tartalmaz:*
  - *a nagy kiterjedésű kibertámadásokra adandó válaszlépéseket meghatározó terv*
  - *az Európai Kiberbiztonsági Kutatási és Kompetenciaközpont, kiegészülve a hasonló központok tagállami szintű hálózatával*
  - *hatékonyabb büntetőjogi fellépés a kiberbűnözéssel szemben a készpénz-helyettesítő fizetési eszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló új irányelv révén*
  - *a globális stabilitás erősítése nemzetközi együttműködés útján."*[8]

Fontosak tehát mind az információbiztonsági, mind a kiberbiztonsági szempontú tevékenységek. Az Európai Unió még két olyan pillért, szabályozást alkotott, amelyek komoly hatással vannak a nemzeti jogrendre, és a negyedik ipari forradalom szereplőinek is érdemben figyelembe kell ezeket venniük. Ezek egyrészt az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, közkeletű nevén a GDPR), másrészt az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, azaz a NIS Direktíva. Míg a GDPR célja nem elsősorban kiberbiztonsági jellegű, hiszen a személyes adatok védelmének biztosításáról szól, olyan környezetben is érvényes, ahol nagy mennyiségű adat keletkezik, tehát

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

tipikusan egy IoT-rendszerekből álló okoskörnyezetben, addig a NIS Direktíva kijelöli azokat az alapvető szolgáltatást nyújtó kritikus fontosságú információs infrastruktúrákat, amelyek védelme európai szinten kiemelten fontos, így például az olyan digitális infrastruktúra-szolgáltatók, mint az Internet Exchange Pointok, DNS-szolgáltatók vagy a legfelső szintű doménnév-nyilvántartó (TLD).

A három pillért figyelembe véve egyértelműen kirajzolódik az Európai Unió törekvése. Olyan termékek és szolgáltatások kialakítását szeretnék ösztönözni innovációs és regulációs eszközökkel az európai piacon – különösen az alapvető szolgáltatást nyújtó, kritikus információs infrastruktúrát alkotó kiberfizikai rendszerek esetében –, amelyek egyszerre veszik figyelembe az adatvédelmi és kiberbiztonsági szempontokat. Tekintettel arra, hogy a negyedik ipari forradalom infrastruktúrája és szolgáltatásai éppen kialakulófélben vannak, az európai okosinfrastruktúrában érintett szereplőknek ezt a politikai szándékot mindenképpen érdemes figyelembe venni.

4. INNOVÁCIÓS IGÉNYEK A KIBERBIZTONSÁGBAN

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

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

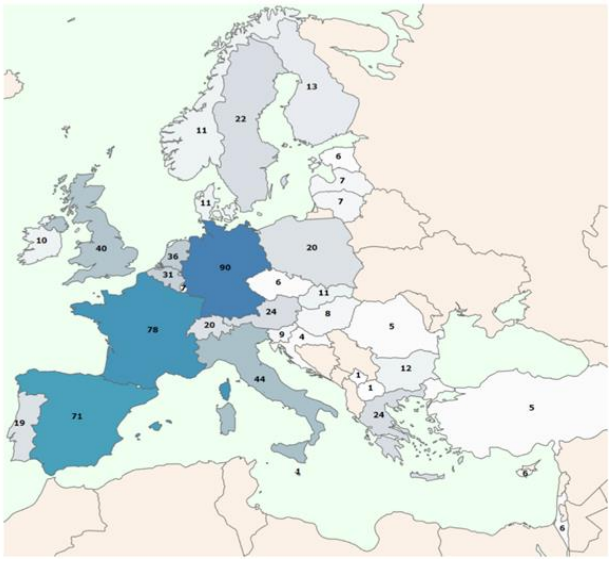
Különös figyelmet kell fordítani a magánszemélyekre is, hiszen jelenleg több mint 4,5 milliárd ember[9] használja az internetet, és a legtöbben olyan eszközökkel kapcsolódnak a világhálóhoz, amelyek információbiztonsági felkészültsége hiányos. A magánszemélyek túlnyomó többsége nem ismeri a kiberhigiénia, azaz a minimálisan elvárt információbiztonsági tevékenységek alapvető fogalmait, így egyrészt potenciálisan saját magukat veszélyeztetik, másrészt pedig ezekkel a nem megfelelően felkészített eszközökkel és elégtelen tudással veszélyt jelentenek a többi internetezőre, az internet teljes struktúrájára vonatkozóan.

9 2022-ben már 4,9 milliárd ember.

Elmondható tehát, hogy a negyedik ipari forradalom minden szereplője számára létfontosságú az új típusú kiberbiztonsági kihívásokat kezelni képes termékek és szolgáltatások megalkotása. Számos iparági elemzés témája a kiberbiztonsági piac növekedési üteme. Eltérő számokat látunk, de abban nagyjából minden elemzés egyetért, hogy éves szinten százmilliárd dolláros iparágról beszélünk. A Fortune elemzése szerint 2019-ben 112,01 milliárdos forgalmat bonyolítottak az iparági szereplők, mely éves 12,6%-os növekedési ráta mellett 2027-re 281,74 milliárd dollárra fog nőni. Az európai piac mérete 2019-ben 36,02 milliárd dollár volt.[10]

5. KIBERBIZTONSÁGI K+F+I EURÓPÁBAN ÉS A VILÁGBAN

2018-ban az Európai Unió – készülve a kiberbiztonsági szabályozásainak bevezetésére és a 2021-től induló költségvetés megtervezésére – felmérte azon kutatás-fejlesztéssel foglalkozó intézmények számát az Európai Unió tagállamaiban, amelyek kimondottan kiberbiztonsággal foglalkoznak.[11] Azt lehetett látni a válaszadásból, hogy míg például Németországban, Franciaországban vagy éppen Spanyolországban meglehetősen sok olyan intézmény van, ahol kiberbiztonsági kutatás-fejlesztés-innovációval foglalkoznak, addig Kelet-Közép-Európában, így Magyarországon is ezen intézmények száma alacsony, ahogy az a 2. ábrán is megjelenik. Ez azt is jelenti, hogy a globális versenyben, ahol hatalmas országokkal és tudástőkével kell versenyeznie az európai iparnak, nem igazán van meg az az alap, amire föl lehet építeni a saját információbiztonsági piacot, illetve tudásbázist.



2. ábra Európai kiberbiztonsági kutatóközpontok száma országonként[12]

[10] Fortune: Cyber security market analysis 2020-2027. 2020. április 22. https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

[11] NAI-FOVINO, Igor et. al.: European Cybersecurity Centre of Expertise - Cybersecurity Competence Survey. Publications Office of the European Union, Luxembourg, 2018. ISBN 978-92-79-92954-0, doi:10.2760/42369, JRC111211.

[12] Forrás: NAI-FOVINO et al. (2018): i. m.

Ez azért lenne fontos, mert a negyedik ipari forradalom kirobbanásával Európa egyre inkább ki lesz téve azoknak a gyártóknak, amelyek nem európaiak. A hardvereszközöket jellemzően Kínában gyártják, a szoftverek jellemzően amerikai forrásból érkeznek. Éppen ezért az európai államok és az európai vállalkozások gyakorlatilag szinte védtelenül állnak az egyes államok által indított kibertámadások előtt, tekintettel arra, hogy az európai kibervédelem jelenleg nem, vagy nagyon kis számban tud olyan saját gyártású eszközöket használni, amelyek felhasználhatók a külső, akár kiberbűnözésből, akár pedig állami forrásból származó támadások ellen.[13]

Az Európai Unió ezt felismerte és stratégiai célkitűzése változtatni ezen. Mivel azonban a kutatás-fejlesztéssel foglalkozó intézmények száma meglehetősen alacsony Európában, először is összpontosítani kell az erőfeszítéseket. A felmérés azt is bemutatta, hogy a válaszadók túlnyomó többségében az állami szférából jöttek, tehát valamilyen közintézmény formájában működnek, a magánkézben lévő, piaci alapon működő kutatás-fejlesztéssel foglalkozó intézmények száma lényegesen alacsonyabb, nagyjából harmada a közfinanszírozású intézményekének, és ennél még alacsonyabb azoknak a PPP[14] konstrukcióban működő intézményeknek a száma, akik mind a magán, mind pedig a köz tudását és tőkéjét felhasználják.

A tervek alapján a következő kutatási érában – a korábbiakhoz hasonlóan – három pillérre épül a kutatás-fejlesztés-innováció támogatása, ebből az első pillér a kiváló tudomány, a második pillér a globális kihívások és az európai ipar versenyképessége, míg a harmadik pillér az innovatív Európáról fog szólni.[15] Ez látható a 3. ábrán. A második pillérben „A társadalmat szolgáló polgári biztonság" nevű klaszterben a kiberbiztonság nevesítve szerepel, ez pedig meglehetősen pozitív jövőképet fest azoknak a kutatás-fejlesztés-innovációval foglalkozó intézményeknek és szakembereknek, akik szeretnék az európai kiberbiztonsági ipart megteremteni. Az Európai Bizottság tervei alapján a 2021-2027 közötti szakaszban 100 milliárd euró nagyságrendű összeg áll majd rendelkezésre a kutatás-fejlesztés-innovációra, ezen belül a Globális kihívások és az európai ipar versenyképessége pillér 52,7 milliárd euróra számíthat. A kiberbiztonság a jelenlegi tudásunk szerint körülbelül 2 milliárd euróval fog részesülni ebből a hatalmas összegből.[16,17]

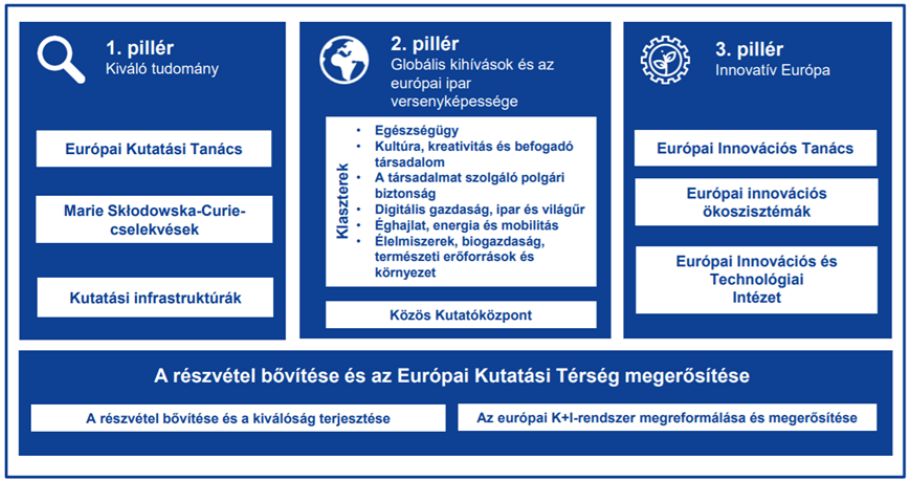
[13] Emiatt érthető, hogy miért az európai digitális szuverenitás megteremtése az Európai Bizottság egyik legfontosabb programpontja a 2020-as években.

[14] Public-Private Partnership, az állami és a magánszféra partnersége

[15] Európai Bizottság: EU-finanszírozás a kutatás és az innováció területén (2021–2027). 2018. május. https://ec.europa.eu/info/

[16] Digital Single Market: New Digital Europe Programme brings €9.2 billion investment between 2021-2027. 2018. június 11. https://ec.europa.eu/isa2/news/european-commission-has-announced-investment-%E2%82%AC92-billion-align-next-long-term-eubudget-2021_en

[17] A végleges döntés alapján a 2021-2027 közötti szakaszban 96,899 milliárd euró összeg áll rendelkezésre a kutatás-fejlesztés-innovációra. A Globális kihívások és az európai ipar versenyképessége pillérre 53,516 milliárd euró jut. A társadalmat szolgáló polgári biztonság klaszter, ezen belül a kiberbiztonság 1,596 milliárd euróval tervezhet.



3. ábra: EU-finanszírozás a kutatás és az innováció területén (2021–2027)[18]

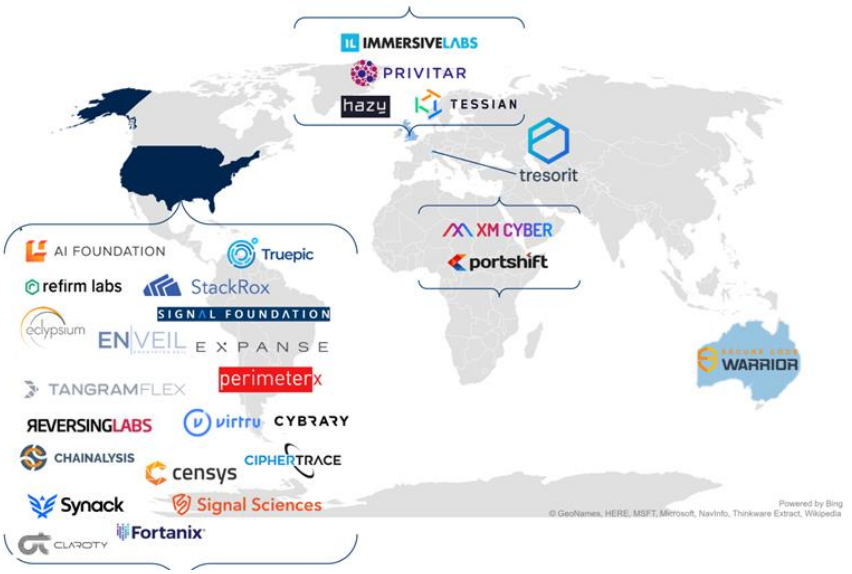
Magyarország természetesen aktívan követi az Európai Unió innovációs törekvéseit, és bár a következő időszakra vonatkozó tervek még nem ismertek, a kiberbiztonság biztosan része lesz a magyar kutatásfejlesztési és innovációs stratégiának. Ezt támasztja alá, hogy a 2020-ban érvényes stratégiai dokumentumok is kivétel nélkül foglalkoznak ezzel a szakterülettel. A 1414/2013. (VII. 4.) Korm. határozat a Nemzeti Kutatás-fejlesztési és Innovációs Stratégia (2013-2020) elfogadásáról már kiemeli, hogy az egyik cél az adaptív innovációs megoldások – elsősorban informatikai és kommunikációs technológiákra alapozott – terjedésének gyorsítása. A részleteket az 1640/2014. (XI. 14.) Korm. határozat a Nemzeti Intelligens Szakosodási Stratégia (S3) elfogadásáról és a Kutatási Infrastruktúrák Európai Stratégiai Fóruma Útitervében szereplő kutatási infrastruktúra nagyprojektekben való magyar részvételről mentén kiadott Nemzeti Intelligens Szakosodási Stratégia (S3) – 2014–2020 segít megérteni. Ebben az IKT terület céljait az alábbiak szerint fogalmazzák meg: *„Az infokommunikációs technológiák széleskörűen fogják át és segítik elő az ágazati prioritásokat, úgy is, mint az egészségiparban a bioinformatika, vagy a diagnosztikai képalkotás, a járműiparban az intelligens közlekedési rendszerek, az energetikában a «smart city». Az ágazati prioritásokhoz nem, vagy nem egyértelműen, vagy akár több ágazathoz is sorolható IKT megoldások alatt olyan technológiák érthetőek (példálózó jelleggel, nem kizárólagosan), mint: (…) információbiztonság, biztonságtechnika."* A kiberbiztonság, mint fejlesztés terület emiatt az összes releváns kormányzati stratégiából visszaköszön, így a 2020-ban elfogadott Mesterséges Intelligencia Stratégia is kitér erre a szempontra.[19]

[18] Az ábra a jelenleg futó, 7 évre szóló Horizon Europe (a tanulmányban korábban: Európai horizont) keretproram elvi felépítését mutatja. Forrás: Európai Bizottság, 2018.

[19] A terület új szabályozói 2021-ben jelentek meg. A fő stratégiai dokumentum a Magyarország kutatási, fejlesztési és innovációs stratégiájának (2021-2030) elfogadásáról szóló 145/2021. (VII. 13.) Korm. határozat alapján létrehozott stratégia. A részleteket az 1428/2021. (VII. 2.) Korm. határozat a 2021–2027. évekre vonatkozó Nemzeti Intelligens Szakosodási Stratégia (S3) elfogadásáról alapján megalkotott S3 stratégia segít megérteni. Ebben a kiberbiztonsággal is foglalkozó Gazdaság digitalizációja prioritás céljait az

6. STARTUP ÖKOSZISZTÉMA A KIBERBIZTONSÁGBAN

A forrás tehát kétségtelenül rendelkezésre fog állni ahhoz, hogy az európai kutatás-fejlesztés-innováció a kiberbiztonsági területen fejlődjön. A kérdés az, hogy hogyan lehet mindezt megtenni. A CB Insight nevű kutatócég 2019-es felmérése alapján ugyanis jelen pillanatban a kontinentális Európában, tehát az Európai Unió jelenlegi országai között nagyon kevés olyan startup van, amelynek terméke megfelel a globális igényeknek, illetve a piaci potenciálja olyan, hogy ezekkel hosszú távon lehessen vele számolni. A felmérés alapján a legígéretesebb kiberbiztonsági startupok jelen pillanatban elsősorban az Egyesült Államok területén találhatók elsősorban, emellett Nagy-Britannia és Izrael a két másik olyan szereplő, akikre érdemes odafigyelni, ahogy azt a 4. ábra is mutatja. Európában egyedül egy svájci bejegyzésű cég, a Trezorit szerepel a listán, mint ígéretes startup. A Trezorit egyébként magyarországi alapítású, a termék eredetileg a Budapesti Műszaki és Gazdaságtudományi Egyetem hallgatóinak projektjeként indult, de jelen pillanatban ők is az Európai Unió területén kívüli jogi entitásnak számítanak.[20,21]



4. ábra: 2019 legígéretesebb kiberbiztonsági startupjai[22]

alábbiak szerint fogalmazzák meg: *„A XXI. századra fokozottan jellemző digitalizáció és robotizáció korában a kiber- és egyéb biztonsági kihívásokra tekintettel, az S3-hoz kapcsolódóan megvalósított fejlesztések során a hazai szellemi tulajdon védelmi, adatvédelmi és nemzetbiztonsági követelményeket, illetve a nemzeti ellenállóképesség és a (védelmi ipar esetén) a kettős hasznosíthatóság egységes szempontjait az érintetteknek maradéktalanul érvényre kell juttatni."*

20 CB Insight: 2019 Cyber Defenders. CB Insight. 2019. április 10. https://www.cbinsights.com/research/report/cyber-defenders-2019/

21 A Trezoritot időközben felvásárolta a Swiss Post. A 2021-es felmérésben sincsen egyetlen európai szereplő sem.

22 Forrás: CB Insight, 2019

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

Még aggasztóbb a kép, hogyha megnézzük a CB Insight azon elemzését, amely 2014 és 2019 között mutatja be, hogy melyik országokban mekkora beruházások történtek a kiberbiztonsági kutatás-fejlesztés-innovációba. Ebből látszódik, hogy a kiberbiztonsági K+F+I-re elköltött összegek túlnyomó többsége (kétharmada) az Egyesült Államokban jelent meg, mögötte pedig egy kis ország, Izrael áll, ahol nagyon jól működik a gyakorlatilag az iskolától a piacig tartó kutatás-fejlesztési és innovációs támogatás. Izrael a globális kiberbiztonsági innovációra fordított befektetésekből 6,7%-kal részesül, utánuk következik az Egyesült Királyság 6,5%-os aránnyal, majd Kína jön 5,6%-kal. 14,4%-kal részesül az említetteken kívül minden más ország a világon a beruházásokból, beleérve az Európai Unió tagállamait is.[23]

7. LEHETŐSÉGEK KELET-KÖZÉP-EURÓPÁBAN

Magyarországon, illetve kicsit tágabb értelemben véve a kelet-közép-európai régióban hatalmas innovációs potenciál rejtőzik. Tehetségeket, jó ötleteket a környező országokban, így elsősorban Romániában, Ukrajnában,[24] Lengyelországban, Csehországban, valamint Észtországban is lehet látni. A régió első számú komoly kihívása az, hogy bár a kelet-közép-európai gondolkodásmód nagyon sokban és nagyon jól támogatja a mérnöki gondolkodást, ezek nem konvertálódnak üzleti sikerré. Azt lehet tapasztalni, hogy a nyugati nagyvállalatoknál mérnöki pozícióban számos esetben Kelet-Közép-Európából származó szakembereket alkalmaznak, de a vállalati hierarchiában a régiós szakemberek ritkán jutnak el vezető testületi pozíciókba.

A régióban a tehetséges mérnökök számát tekintve jól állunk. A kérdés csak az, hogy ezeket a tehetségeket hogyan lehet bátorítani. Ennek lehet az egyik alapköve az, hogy egy olyan ökoszisztéma épül ki ezekben az országokban, amely már akár középiskolában, vagy legkésőbb az egyetemeken segíti a tehetségek fejlesztését, és a mérnöki tudás mellé egy jól meghatározott üzleti, vállalkozásfejlesztési tudást is ad a mérnököknek. Éppen ezért bátorítani kell az iskolai, akár egyetemi szinten történő innovációs képességek fejlesztését. (Magyarországon egyébként 2020 szeptemberétől indul több egyetemen is olyan innovációs képzés, amely segítheti

[23] A 2021-es felmérésben 53% szerepel az USA mellett, 12% Kína befektetése, 10% pedig Izraelé, Nagy-Britannia 5%-ra csúszott vissza.

[24] A kelet-közép-európai régióban Ukrajna, valamint Fehéroroszország és Oroszország is jelentős IT-fejlesztési bázissal rendelkezik. Az orosz–ukrán háború egyelőre beláthatatlan változásokat fog hozni a régiós fejlesztési képességekben.

ezeknek a tehetségeknek a piacra jutását, illetve cégalapítását.) Emellett segíteni kell azt, hogy a különböző diszciplínákban, különböző tudományterületeken dolgozó szakértők egymással tudjanak dolgozni.[25]

Fontos állami fejlesztéspolitikai lépés lehet az, hogy létrejönnek azok az úgynevezett Science Parkok, melyekben több egyetem együttesen tudja fölépíteni a saját innovációs ökoszisztémáját, beleértve ebbe a kiberbiztonságot is. A Nemzeti Közszolgálati Egyetem például a Semmelweis Egyetem által vezetett Science Park részese, és ezen Science Park-fejlesztés, innovációs központ egyik eleme a kiberbiztonság az orvosi technológiákban, amely potenciálisan piacképes ötleteket tud majd eredményezni.[26]

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

További kérdés a finanszírozás rendelkezésre állása. Startupokra rengeteg pénz van, a tőke alapvetően keresi a jó ötleteket. Ez Európában is így van, de nagy aránytalanságokat lehet észrevenni a startup-finanszírozásban. Míg Magyarországon például 1 millió forint kockázati tőkét aránylag könnyen lehet szerezni egy izgalmas startup ötletre, ez az összeg Nyugat-Európában már 10 millió forint, míg az Egyesült Államokban akár a 100 millió forintos nagyságrendet is elérheti a bevonható kockázati tőke az izgalmas ötletekhez. Ez a különbség mindenképpen azt szüli, hogy az ötleteket inkább az Egyesült Államokban célszerű megvalósítani, nem pedig itt, Kelet-Közép-Európában.

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

Sokat segíthet, ha Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról,

[25] NKFIH: Szeptemberben startol a Hungarian Startup University Program. 2020. február 17. https://nkfih.gov.hu/hivatalrol/online-sajto/szeptemberben-startol

[26] DOBOZI Pálma: Bemutatták a Science Park tervezett szakmai tartalmát. Nemzeti Közszolgálati Egyetem, 2019. október 24. https://www.uni-nke.hu/hirek/2019/10/24/bemutattak-a-science-park-tervezett-szakmai-tartalmat

valamint az 526/2013/EU rendelet hatályon kívül helyezéséről, azaz a Kiberbiztonsági Jogszabályból egyelőre még hiányzó kutatás-fejlesztés-innovációs terület végre elfogadásra kerülne az Európai Unióban. A tervek szerint a Tanács kiberbiztonsági hálózatokat hoz létre, amelyek három szinten épülnének ki. Elsősorban létrejönne valamelyik európai uniós tagországban egy olyan központ, amelynek feladata a kutatás-fejlesztéssel és innovációval kapcsolatos források koordinálása, annak érdekében, hogy a Horizont Európa keretprogramban rendelkezésre álló összeg jól kerüljön elköltésre. Ez az Európai Kiberbiztonsági Ipari Technológiai és Kutatási Központ nevet viseli, és a tanulmány írásának pillanatában tagországi tárgyalás folyik arról, hogy pontosan milyen felhatalmazással működjön ez a központ.[27] Figyelembe véve, hogy az ENISA-val, az Európai Hálózatbiztonsági Ügynökséggel párhuzamosan kellene ennek működnie, gondoskodni kell arról, hogy ne legyenek olyan átfedések a hatáskörökkel kapcsolatban, amelyek nehezítenék a központ működését. Ennek a központnak a székhelye egyelőre nem ismert, több európai ország is bejelentkezett annak érdekében, hogy a központot vendégül láthassa.[28]

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

8. ÖSSZEFOGLALÁS

A negyedik ipari forradalom elengedhetetlen előfeltétele a (kiber)biztonságosan működő digitális infrastruktúra létrehozása. Ez azonban nem csupán műszaki feladat, a digitális ökoszisztéma minden szereplőjének, így az államoknak is komoly feladatai és felelősségei vannak a kibertéri fenyegetések kezelésében. Mivel az amerikai és kínai vállalatok jelentős előnyre tettek szert az európai versenytársakkal szemben a modern ipari fejlesztésekben, nem utolsósorban a célzott állami beavatkozásnak köszönhetően, az Európai Unió elemi érdeke olyan környezet létrehozása, mellyel az európai vállalkozások is versenyben tudnak maradni innovatív megoldásaikkal és szolgáltatásaikkal, és az európai gazdaságok

[27] A Központ létrehozásáról időközben megszületett a döntés, az Bukarestben kezdi meg működését.

[28] EU Tanácsa: Az EU összefogja és hálózatba szervezi kiberbiztonsági szakértelmét – a Tanács megállapodott a kiberbiztonsági központokkal kapcsolatos álláspontjáról. 2019. március 13. https://www.consilium.europa.eu/hu/press/press-releases/2019/03/13/eu-to-pool-and-network-its-cybersecurity-expertise-council-agrees-its-position-on-cybersecurity-centres/

képesek lehetnek csökkenteni a tengerentúli és ázsiai digitális megoldásoktól való függőségüket, ezzel pedig az államilag támogatott kibertámadásokkal szembeni kitettségüket is.

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

Az előíró szabályozás mellett azonban fontos a támogató szabályokat is megemlíteni, amelyek segítségével az európai kiberbiztonsági innováció olyan eredményeket érhet el, amelyeket a szolgáltatók külön előírás nélkül is célszerűnek tarthatnak bevezetni. A kiberbiztonsági kiválósági központok hálózata egyfajta keltetője lehet a világszínvonalú ötleteknek, amelyek érdemi eredményekhez vezethetnek. Ennek az elképzelésnek a pilotolására, kipróbálására az Európai Bizottság 2019-től kezdve négy kiemelt projektet indított el. Ezek a Concordia, a Cyber Security for Europe, az ECHO, illetve a Sparta nevű kezdeményezések, amelyek számos Európai Uniós tagországot egyesítenek és fognak össze, és próbálják kialakítani, hogyan tud majd működni ez a háromszintű felosztás, hogyan valósítható meg az, hogy az európai kutatási pénzek a leghatékonyabban jussanak el az innovációval foglalkozó magán- és közfinanszírozású szereplőkhöz.[29]

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

[29] Európai Bizottság: Four EU pilot projects launched to prepare the European Cybersecurity Competence Network. 2019. február 26. https://wayback.archive-it.org/12090/*/https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

Felhasznált irodalom:

- 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- A 2021-es felmérésben 53% szerepel az USA mellett, 12% Kína befektetése, 10% pedig Izraelé, Nagy-Britannia 5%-ra csúszott vissza.
- A kelet-közép-európai régióban Ukrajna, valamint Fehéroroszország és Oroszország is jelentős IT-fejlesztési bázissal rendelkezik. Az orosz–ukrán háború egyelőre beláthatatlan változásokat fog hozni a régiós fejlesztési képességekben.
- Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről
- BÁNYÁSZ Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In: CSENGERI J. – KRAJNC Z. (Szerk.): Humánvédelem - békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése. Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Budapest, 2016. p. 918.
- CB Insight: 2019 Cyber Defenders. CB Insight. 2019. április 10. https://www.cbinsights.com/research/report/cyber-defenders-2019/
- Digital Single Market: New Digital Europe Programme brings €9.2 billion investment between 2021-2027. 2018. június 11. https://ec.europa.eu/isa2/news/european-commission-has-announced-investment-%E2%82%AC92-billion-align-next-long-term-eubudget-2021_en
- DOBOZI Pálma: Bemutatták a Science Park tervezett szakmai tartalmát. Nemzeti Közszolgálati Egyetem, 2019. október 24. https://www.uni-nke.hu/hirek/2019/10/24/bemutattak-a-science-park-tervezett-szakmai-tartalmat
- EU Tanácsa: Az EU összefogja és hálózatba szervezi kiberbiztonsági szakértelmét – a Tanács megállapodott a kiberbiztonsági központokkal kapcsolatos álláspontjáról. 2019. március 13. https://www.consilium.europa.eu/hu/press/press-releases/2019/03/13/eu-to-pool-and-network-its-cybersecurity-expertise-council-agrees-its-position-on-cybersecurity-centres/
- Európai Bizottság: EU-finanszírozás a kutatás és az innováció területén (2021–2027). 2018. május. https://ec.europa.eu/info/
- Európai Bizottság: Four EU pilot projects launched to prepare the European Cybersecurity Competence Network. 2019. február 26. https://wayback.archive-it.org/12090/*/https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

- European Union Agency for Cybersecurity. A rövidítés a szervezet korábbi nevéből, az European Network and Information Security Agency-ből (Európai Uniós Hálózat- és Információbiztonsági Ügynökség) származik.
- Fortune: Cyber security market analysis 2020-2027. 2020. április 22. https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165
- Graz University of Technology: Meltdown and Spectre - Vulnerabilities in modern computers leak passwords and sensitive data. 2018. január https://meltdownattack.com/
- NAI-FOVINO, Igor et. al.: European Cybersecurity Centre of Expertise - Cybersecurity Competence Survey. Publications Office of the European Union, Luxembourg, 2018. ISBN 978-92-79-92954-0, doi:10.2760/42369, JRC111211.
- NKFIH: Szeptemberben startol a Hungarian Startup University Program. 2020. február 17. https://nkfih.gov.hu/hivatalrol/online-sajto/szeptemberben-startol
- TÖRÖK Bernát (Szerk.): Információ- és kiberbiztonság: Fenntartható biztonság és társadalmi környezet tanulmányok V. Ludovika Egyetemi Kiadó, Budapest, 2020. pp. 83-97. Paper: 2, 15 p.

6. FEJEZET

NEM HAGYOMÁNYOS HATALMI KÉPESSÉGEK – A DIGITÁLIS VILÁGRAND ÁTALAKULÁSA A 2020-AS ÉVEKBEN

A II. világháborút követő geopolitikai környezet végérvényesen megváltozni látszik. A hatalmi egyensúly újraalakításában a digitális technológiáknak kiemelten fontos szerepe van. Ebben a környezetben kellene Európának és ezen belül Magyarországnak is megtalálnia a helyét oly módon, hogy értékei és érdekei is képviselve legyenek, függetlenül a többi nagyhatalomtól. Autonómnak lenni tehát annyit jelent, hogy kulcsfontosságú stratégiai céljainkat külső felek befolyásától és függőségeitől mentesen tudjuk elérni. Az Európai Unió digitális autonómiájának elérése attól függ, mennyire lehet megteremteni azt a környezetet, amelyben a szükséges és elégséges mértékben ki lehet zárni a globális versenytársaktól, elsősorban az Amerikai Egyesült Államokból (USA) és Kínából származó technológiákat, és mennyire lehet ellensúlyozni az olyan klasszikus geopolitikai hatásokat, mint az orosz–ukrán háború. A technológiai függésnek azonban számos dimenziója van, amellyekkel számolni kell a digitális szuverenitás kivívásának érdekében, hiszen a műszaki kérdések mellett gazdasági, jogi, politikai vagy éppen katonai befolyásolás is akadálya lehet az önálló és versenyképes európai digitális piac megteremtésének, a két nagyhatalomnak pedig nem érdeke támogatni az EU digitális autonómiatörekvéseit.

A digitális függés kialakulásának egyik legjobb történelmi példája a geopolitikai küzdelmek egyik legaktuálisabb helyszíne, a kibertér. Míg az olyan hagyományos fizikai dimenziókban, mint a világtengerek, a sarkvidékek vagy éppen a világűr, a történelem során már többször élesedett ki a nagyhatalmak közötti versengés, a digitális technológiák és az általuk alkotott hálózatok csak az elmúlt 30 évben jelentek meg széles körben, és alakították át gyökeresen a világunkat. Ráadásul – szemben a fizikai térrel, amelyet leginkább a természet alakított – a kibertér egy teljesen az emberiség által megalkotott virtuális tér, amely a kiváló tudósok és elsősorban az amerikai kormányzati finanszírozás nélkül nem is létezne. A kibertérben emellett nem is azonosíthatóak könnyen olyan klasszikus erőforrások, amelyek indokolhatnák azt a megkülönböztetett figyelmet, amit a világpolitika színterén kap ez a nem kézzelfogható helyszín.

A kibertér kiemelt fontosságát a XXI. század társadalmi és gazdasági fejlődésében kell keresni. A számítógépek az 1980-as években kezdtek elterjedni, az internet az 1990-es évek terméke. Egészen pontosan a ma ismert internetet (World Wide Web) 1989-ben alkotta meg a brit Tim Berners-Lee, a svájci CERN kutatóintézetben. Ezt azért fontos kiemelni, mert ez a világot átalakító felfedezés ugyan egy európai projekt égisze alatt jött létre, de egy jelenleg nem EU-tagállam tudósa egy nem EU-tagállamban hozta létre, ráadásul nem Európa profitált belőle a legjobban. Ekkoriban az internet még csak néhány millió nyugati tudós és mérnök játszótere volt elsősorban, míg ma már világszerte közel 5 milliárd internetfelhasználó van. Bár a számítógépek fontossága egyértelmű volt már a kezdetekkor is, hiszen mind a kormányzati, mind a versenyszférában folyamatosan terjedt a használatuk, a kommunista rezsimek bukása után, a Pax Americana globális

kiterjesztésének hajnalán kevesen gondoltak arra, hogy a digitális tér egyszer a világpolitika meghatározó kérdése lesz. Az USA korabeli kormányzati politikája azonban előrevetítette, hogy az internetet a globális dominancia egyik eszközének tekinti.

Bill Clinton első elnöki periódusának egyik korai, de talán leglényegesebb stratégiája volt a The National Information Infrastructure: Agenda For Action (NII) című kiadvány. Ebben szerepel a következő célkitűzés:
„Az NII előnyei a nemzet számára óriásiak. A fejlett információs infrastruktúra lehetővé teszi az amerikai cégek számára, hogy versenyezzenek és győzedelmeskedjenek a globális gazdaságban, jó munkahelyeket teremtve az amerikaiak számára és gazdasági növekedést a nemzet számára. Ugyanilyen fontos, hogy az NII átalakíthatja az amerikai emberek életét – enyhítve a földrajzi, fogyatékossági és gazdasági helyzetből adódó korlátokat –, és minden amerikainak tisztességes lehetőséget adva arra, hogy tehetségük és ambícióik szerint olyan messzire jussanak, amilyen messzire csak akarnak. [...] Az információ a nemzet egyik legkritikusabb gazdasági erőforrása, a szolgáltatóipar és a feldolgozóipar, a gazdaság és a nemzetbiztonság szempontjából egyaránt. Egy becslés szerint az amerikai munkavállalók kétharmada az információval kapcsolatos munkakörökben dolgozik, a többiek pedig olyan iparágakban, amelyek nagymértékben támaszkodnak az információra. A globális piacok és a globális verseny korában az információ létrehozására, manipulálására, kezelésére és felhasználására szolgáló technológiák stratégiai jelentőségűek az Egyesült Államok számára. Ezek a technológiák segítik az amerikai vállalkozásokat abban, hogy versenyképesek maradjanak, és kihívást jelentő, jól fizető munkahelyeket teremtsenek. Emellett a gazdasági növekedést is táplálják, ami viszont minden amerikai számára folyamatosan növekvő életszínvonalat teremt.”[1]

Az Európai Unióban a digitális fejlődést, az információs társadalom felé történő legelső lépést megalapozó dokumentumnak a Bangemann-jelentést szokták tartani. Ez 1994 májusában jelent meg, kijelölve azt az utat, amelyet az Európai Bizottság a következő évtizedekben – kisebb korrekciókkal – követett. Három évtizeddel később érdekes megállapítani azokat a filozófiai különbségeket, amelyek az amerikai és az európai vízióban rejlenek, és amelyek hosszú távon Európa digitális függőségéhez vezettek. A jelentés vezetői összefoglalója így kezdődik:
„Ez a jelentés sürgeti az Európai Uniót, hogy bízzon a piaci mechanizmusokban, mint az információs korszakba való átmenet motorjában. Ez azt jelenti, hogy európai szinten és a tagállamok részéről is lépéseket kell tenni az Európát versenyhátrányba hozó berögzült álláspontok felszámolása érdekében:

- *ez a vállalkozói mentalitás előmozdítását jelenti, hogy lehetővé váljon a gazdaság új, dinamikus ágazatainak megjelenése,*
- *ez a közös szabályozási megközelítés kidolgozását jelenti az információs szolgáltatások versenyképes, egész Európára kiterjedő piacának megteremtése érdekében,*

[1] BROWN, Ronald Harmon: The national information infrastructure: agenda for action. Executive Office of the President Information Infrastructure Task Force, 2003. p. 2.

- *ez NEM jelent több közpénzt, pénzügyi támogatást, szubvenciókat, dirigizmust vagy protekcionizmust."*[2]

Míg az NII-ben megfogalmazott gondolatok előrevetítették azt, hogy az USA-val versengő hatalmaknak képesnek kell lenniük az információtechnológiai területen is alternatívát nyújtani, és saját képességeiket fejleszteni – és ez a Bangemann-jelentés idejében már ismert volt –, az európai politika nem ismerte fel, hogy pusztán szabályozással és a piaci liberalizálással hosszú távon a régió nem lesz versenyképes az amerikai versenytársakkal. Bár szinte minden pontban kiemelik Európa relatív lemaradását az USA-val szemben, a technológiai területen a következő megállapítást tették a Bangemann-csoport tagjai:
„A jelenlegi európai technológiai bázis elegendő az e jelentésben javasolt alkalmazások késedelem nélküli bevezetéséhez. Elég nagy léptékű, reális rendszerekre kell összpontosítani annak érdekében, hogy azok feltárják a felhasználók számára kínált szolgáltatások értékét, és hogy értékeljék az új információs rendszerek gazdasági megvalósíthatóságát.

Az új technológiákat azonban még ki kell fejleszteni ahhoz, hogy bemutatásukat követően teljeskörűen bevezethetők legyenek. Különösen a rendszerek használhatóságát és költséghatékonyságát kell javítani, és a tömeges használat következményeit tovább kell vizsgálni.

Az Unió és a tagállamok kutatási programjait, különösen a Negyedik Keretprogramot úgy kell végrehajtani, hogy figyelembe vegyék a piaci követelményeket. A technikai célokat és a projektek időzítését a felhasználók megfelelő bevonásával kell meghatározni."[3]

Érdekesség, hogy az 1990-es évek elején Japán tűnt ezen a területen a leginkább kompetitív vetélytársnak mind az USA, mind az EU számára, ám a 2020-as évtizedre egyértelműen Kína az az ország, amely a második, néhány területen pedig az első a technológiai területen. Ahhoz képest, hogy Kína az 1990-es évek elején gazdaságilag jelentéktelen ország volt, egészen rendkívüli, ahogy felépítették azt a fejlett digitális gazdaságot, amelyet akár Európa is megtehetett volna. Paradox módon ebben sokat segített a Pax Americana jelentette globális nyitás. Kínai diákok tűntek fel tömegesen az USA legjobb egyetemein, eközben pedig amerikai és európai gyártók nyitottak gyártóegységeket Kínában az olcsó munkaerő reményében. Látszólag minden az USA gazdasági előnyéről szólt, hiszen az agyelszívás az amerikai tudásintentív gazdaságot erősítette, miközben az ennek eredményeképp létrejött termékeket a lehető legolcsóbban lehetett létrehozni Ázsiában. A 2000-es években viszont a kínai mérnökök és tudósok elkezdtek hazatérni, és tudásukat a kínai egyetemeken és vállalatoknál kamatoztatni. A gyártás során Kínába került szellemi tulajdont a helyiek meglehetősen lazán kezelték, akár az ipari kémkedést is kimerítő módon másolták le a nyugati megoldásokat. Nem

[2] European Commission: Europe and the Global Information Society: Recommendations to the European Council: Conference G7 – Raport BANGEMANN. Publications Office, 1995. p. 3.
[3] European Commission (1993): i. m. p. 22.

csoda, hogy a 2010-es évekre létrejött a digitális képességeket létrehozni képes szellemi tőke és gyártási kapacitás.[4]

Ezzel szemben az európai diákok amerikai tanulmányaik után ott is maradtak, az európai egyetemeken végzett fiatal mérnököket tömegesen csábították el amerikai vállalatok, a legjobb európai egyetemi oktatók pedig jelentős ösztöndíjakat kaptak azért, hogy kutatásaikat az USA-ban folytassák. 2022-ben a QS World University Rankings egyetemi rangsorban a mérnöki és technológiai területen mindösszesen egy európai egyetem szerepel a Top10-ben és kilenc a Top50-ben. Ugyanebben a rangsorban három Top10-es és 14 Top50-es amerikai, valamint két Top10-es és 13 Top50-es ázsiai egyetem található. A Brexit jelentette veszteséget és Svájc EU-n kívüliségének problémáját mi sem mutatja jobban, hogy Svájc és Nagy-Britannia egyetemei a rangsorban négy Top10-es és hat Top50-es egyetemet tudhatnak magukénak.[5]

A direkt állami támogatással kapcsolatos hibás európai megközelítést, amelyet egyébként a 2021-ben elfogadott Európa digitális évtizede: a 2030-ra kitűzött célok program felülírni látszik. Kínában viszont eközben már egy évtizede erőltetik a digitális iparba történő állami befektetéseket. A 2012-ben elfogadott 12. Ötéves Terv például már kimondottan támogatja a feltörekvő technológiák gyártási képességeinek megerősítését, a 2017-es 13. Ötéves Terv pedig komoly hangsúlyt helyez az olyan technológiák elterjesztésére, mind a mobiltechnológia, a cloud computing vagy az Internet of Things. A China 2025 stratégiából pedig egyértelműen kiderül, hogy Kína célja a legerősebb „kiberhatalommá" válni.[6] Ugyanezeket az irányokat csak évekkel később lehetett megtalálni az EU stratégiai dokumentumaiban. Az Európai Parlament és a Tanács határozata „A digitális évtizedhez vezető út" elnevezésű, 2030-ig szóló szakpolitikai program létrehozásáról így fogalmaz: *„Az EU arra törekszik, hogy digitálisan szuverén legyen egy nyílt és összekapcsolt világban, és olyan digitális politikákat folytasson, amelyek lehetővé teszik az emberek és a vállalkozások számára, hogy emberközpontú, fenntartható és virágzó digitális jövőt valósítsanak meg. Ez magában foglalja a sebezhetőségek és függőségek kezelését, valamint a beruházások felgyorsítását."*[7] Ez jelentős előrelépés a korábbi évtizedek megközelítéséhez képest, és elismeri, szükség van a stratégiai európai beruházásokra a digitális technológiák területén. A program a következő beavatkozási területeket és célokat azonosította:

4 Yingying Zhang – Yu Zhou: The Source of Innovation in China. Palgrave Macmillan London, 2015. XIV-XIX.

5 QS Top Universites: QS World University Rankings by Subject 2022: Engineering & Technology https://www.topuniversities.com/university-rankings/university-subject-rankings/2022/engineering-technology

6 Francois Godement et al.: The China dream goes digital: Technology in the age of Xi. European Council on Foreign Relations, 2018.

7 Európai Bizottság: Javaslat AZ EURÓPAI PARLAMENT ÉS A TANÁCS HATÁROZATA „A digitális évtizedhez vezető út" elnevezésű, 2030-ig szóló szakpolitikai program létrehozásáról. COM(2021) 574 (2021. szeptember 15.) https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52021PC0574

- Szakértelem:
  - IKT-szakemberek: 20 millió, továbbá a nemek közötti kiegyensúlyozottság megteremtése;
  - Digitális alapkészségek: a népesség legalább 80%-a.

- Biztonságos és fenntartható digitális infrastruktúrák:
  - Konnektivitás: gigabit mindenkinek, 5G mindenütt;
  - A csúcstechnológiát képviselő félvezetők: az EU részesedésének megkétszerezése a világ össztermeléséből;
  - Adatok – peremhálózat és felhő: 10 000 klímasemleges, rendkívül biztonságos peremcsomópont;
  - Számítástechnika: az első számítógép, amely kvantumgyorsulással rendelkezik.

- A vállalkozások digitális transzformációja:
  - Technológiafejlesztés: az uniós vállalkozások 75%-a használja a felhőszolgáltatásokat, a mesterséges intelligenciát és a nagy adathalmazokat;
  - Innovátorok: a növekvő innovatív vállalkozások erősítése és az EU-beli unikornisok finanszírozása;
  - Kései csatlakozók: a kkv-k több mint 90%-a használja intenzíven a digitális eszközöket, legalább alapszinten.

- A közszolgáltatások digitalizálása:
  - Kulcsfontosságú közszolgáltatások: 100%-ban online;
  - E-egészségügy: minden európai polgárnak hozzáférése van az egészségügyi adataihoz;
  - Digitális személyazonosság: a polgárok 80%-a használ digitális azonosítót.[8]

Kérdéses viszont, hogy ez elérhető-e. Amellett, hogy a minimum évtizedes lemaradás ledolgozása nagyságrendileg több költségvetési forrást igényel az európai tagállamoktól – amely a háborús időszakban nem feltétlenül fog a legfontosabb feladatok közé tartozni –, számolni kell a politikai akadályokkal is. Erre kiváló példa az, ahogy az USA már Obama elnöksége alatt felismerte a technológiai területen megjelenő kínai fenyegetést, és elkezdte blokkolni Kína ezirányú tevékenységét. Trump elnöksége alatt például kemény szankciókkal igyekezett visszavetni a kínai technológiai cégek piaci megjelenését, gondoljunk csak az 5G technológiák kitiltására, egyes kínai mobilgyártók amerikai szoftverektől való elzárásán át az egyik legnépszerűbb, kínai tulajdonú közösségi hálózat felvásárlására tett kísérletig. Biden elnöksége alatt ez a trend tudatosan folytatódik, az USA számára Kína az elsődleges stratégiai ellenfél, és mindent megtesz azért, hogy globális pozícióját tartani tudja és letörje Kína (kiber)hatalommá válását. Az Európai Unió tagállamai ezekben a kérdésekben meglehetősen megosztottak, a kínai 5G technológia kitiltását például csak a leghűségesebb USA-szövetséges országokban sikerült elérni, annak ellenére, hogy jelentős európai 5G gyártók vannak, és ez a lépés a potenciális nemzetbiztonsági fenyegetés csökkentése mellett az európai digitális ipar

[8] Európai Bizottság: Európa digitális évtizede: a 2030-ra kitűzött célok https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_hu

fejlődéséhez is hozzájárulhatna. Az egységes európai politikai válasz helyett azonban ebben az esetben is csak egy szabályozási lépés, az 5G Kiberbiztonságára irányuló Uniós eszköztár létrehozása történt meg, amellyel évekre el lehetett tolni a probléma megoldását.

A két nagyhatalom, az USA és Kína közötti viszonyban eközben viszont számos olyan pont van, amely a következő évtizedekben nyitottá teszi a kibertér feletti dominancia kérdését, és amely masszívan befolyásolja az EU digitális autonómia irányába tett lépéseit. Ezek közül talán a legfontosabb kérdés az, hogyan alakul át a II. világháború után kialakult, multilaterális kapcsolatokra és nemzetközi szervezetekre épülő világpolitika. Oroszország Ukrajna elleni katonai agressziója és a szuverén ukrán területek annektálása az ENSZ Biztonsági Tanácsának egyik tagja által egyértelműen megrengeti a nemzetközi rendet, felborítja a status quo-t és erősítheti Kína szándékait a XXI. századi erőviszonyoknak megfelelő nemzetközi rend kialakításában, beleértve ebbe a globális (amerikai dominanciájú) kibertér nemzeti irányú elmozdítását, segítve ezzel a nemzeti hálózatok hálózatának (splinternet) kialakítását. Európa ebben nem érdekelt, minden nemzetközi fórumon támogatja a jelenlegi kibertér fenntartását, ezzel viszont kialakulni látszik egy olyan Kelet–Nyugat szembenállás a digitális technológiákat érintő kérdésekben is, amelynek keretében az európai érdekek képviselete igen nehéznek ígérkezik.

További fontos kérdés Kína szándéka Oroszországgal és Tajvannal kapcsolatban. Oroszország háborús agresszióját a nyugati világ erőteljes technológiai szankciókkal bünteti, így amennyiben Oroszország „bent kívánja tartani a gazdaságát a XXI. században", egyedül Kínára támaszkodhat. A kiberteret tekintve Oroszország évtizedek óta küzd az USA dominanciája ellen, és használja ki a technológia jelentette befolyásolási lehetőségeket saját céljai elérése érdekében, ám ezektől a lehetőségektől a háborús cselekedetei miatt hosszabb időre el fogják vágni úgy diplomáciai, mint műszaki értelemben. A kiberdiplomáciában azonban jellemzően együtt mozgott Kínával, így valószínűsíthető, hogy a szándékok nem fognak változni, de azokat Kína fogja a jövőben artikulálni, elsősorban saját érdekeinek megfelelően. Így Oroszország minden valószínűség szerint függővé fog válni Kínától, viszont az egységes európai kiállás, például a technológiai szankciók területén prognosztizálhatóan ellenlépéseket fog szülni orosz részről. Nem elég tehát, hogy az EU digitális ipara jelentős piacot veszít, de kibertámadások formájában még ellenséges lépésekre is számíthat orosz részről.

Tajvan esete a digitális függetlenség szempontjából azért különösen fontos, mert jelenleg a világ chipjeinek nagyjából 2/3-át a szigeten gyártják, és bár komoly törekvések vannak arra, hogy ezen gyártási kapacitás egy része visszakerüljön az USA-ba, és az EU is megteremtse saját félvezető iparát, ez csak évtizedes távlatban és elképesztő anyagi ráfordítással képzelhető el. Amennyiben tehát Kína akár blokáddal, akár direkt katonai csapással avatkozik be a tajvani kereskedelembe, annak minden bizonnyal hosszabb távú hatása lesz az USA, Európa és a teljes világ digitális gazdaságára, tekintettel arra, hogy a kibertér alapvető infrastruktúraelemeinek, a számítógépeknek, mobileszközöknek vagy éppen hálózati megoldásoknak a gyártása és szállítása válik kérdésessé, nem is beszélve az európai

ipar számára számottevő gépjárműiparról. A digitális autonómia szempontjából éppen ezért a legsürgetőbb lépés a félvezetőipar (újra)építése Európában.[9]

Jelenleg az USA és Kína tehát az a két szereplő, aki érdemben bele tud szólni az európai digitális autonómia alakításának kérdésébe. Az Európai Unió is aktívan próbálja alakítani a kibertér szabályait, de a jól érzékelhetően kialakult kelet–nyugati szembenállás jelentősen csökkenti az önálló stratégiai célok elérése sikerességének lehetőségét. A Covid19 miatt digitális transzformáció, a globális felmelegedés elleni küzdelem és az orosz–ukrán háború azonban olyan társadalmi és gazdasági változásokat hozott, amelyek egyben lehetőséget is jelentenek Európa digitális szuverenitásának kivívására. A globális ellátási láncok ellehetetlenülése, az alapvető erőforrásoktól való elzáródás, az olcsó ázsiai munkaerőre épülő gyártás megnehezülése, az európai perifériaországok integrációs törekvéseinek felgyorsulása, vagy éppen a csúcstechnológiás hadiipari gyártás széles körű beindítása mind abba az irányba mutatnak, hogy az európai iparnak sebességet kell váltania, és néhány éven belül meg kell teremtenie saját képességeit, különben függősége hosszú évtizedekre megmarad. Függetlenül attól, hogy az európai politika milyen irányba halad előre, hogy az európai állampolgárok a föderalista, a nemzetállami vagy a kétsebességes Európa mellett döntenek, a digitális autonómia megteremtése az összehangolt tagállami lépések nélkül nem kivívható. A digitális szuverenitás elvesztése pedig azzal jár, hogy Európa kiesik a XXI. század hatalmi központjai közül, és bizonytalan időre befolyásolási övezetté válik. Kína példája azonban azt mutatja, hogy 2-3 évtized elég lehet egy európai digitális reneszánsz eléréséhez.

Fontos azonban megemlíteni a kiberbiztonságra vonatkozó közvetlen változásokat is. Jelen kötet írása közben már hónapok óta tart Oroszország fegyveres agressziója Ukrajna ellen, amely egyben világossá is tette számunkra, mit jelent a kiberháború a valóságban. Mindaz, ami az korábbi években még csak elméleti lehetőség volt, 2022-ben gyakorlattá vált. Ez az első olyan háború ugyanis, amely az ötödik műveleti tér, azaz a kibertér lehetőségeit is kihasználja a többi négy, azaz a föld, a víz, a levegő és a világűr mellett. Bár a szakértők számára az eddig nyilvánosságra került kibertéri események komoly meglepetéseket nem okoztak, sőt, az egyes háborús műveletek egyenesen következnek az előző fejezetekben leírtakból, a laikus tömegek most először szembesülnek azzal, miért kongatják a vészharangot a kiberbiztonsággal foglalkozók évtizedek óta. A „háború köde” ugyan még elég sűrű, a nyílt forrásból elérhető információk között pedig bőségesen vannak dezinformációk, de mégis érdemes megvizsgálni néhány olyan szempontot, amellyel a sajtó és az internet közönsége eddig kevésbé foglalkozott, de hosszú távon komoly hatással lesz a mindennapi életünkre! Az orosz–ukrán kiberfront nyolc olyan új szempontra világított rá, amelyek hosszú távon is hatással lehetnek a kibertér hétköznapjaira.

[9] Ryan Hass – Jude Blanchette: Central Questions in U.S.-China Relations amid Global Turbulence. Center for Strategic & International Studies, 2022. július 21. https://www.csis.org/analysis/central-questions-us-china-relations-amid-global-turbulence

1. Kiberhadviselés, ahogy az a valóságban történik: A kibertér esetében a kiberfölény kivívása a cél. A háború eddigi legnagyobb tanulsága az, hogy az orosz hadsereg nem tudta kivívni a kiberfölényt, hiszen az ukrán információs rendszerek működnek, az információs teret egyértelműen az ukrán narratíva uralja, eközben folyamatosan esnek el kulcsfontosságú orosz információs szolgáltatások. Ennek a háborúnak a kimenetele nagyban fog függni a kibertér uralásától, így a XXI. század fegyverei, például a közösségi média jól mutatják hatékonyságukat a XX. század fegyverei ellen. A kibertéri műveleteket négy területen vívják: az információs térben, a hagyományos informatikai rendszerek ellen, a kritikus információs infrastruktúrákkal szemben és a katonai IT-rendszerek ellenében. Mind a defenzív, mind az offenzív kiberműveletek csak összehangoltan valósíthatók meg, amelynek során a védelmi és a belbiztonsági szervezetek mellett a privát szektor is bevonásra kerül, illetve a belföldi kooperációt kiegészítik a szövetségesi rendszerben történő együttműködések, beleértve ebbe a nagy technológiai cégeket is. Kiemelten fontos tehát az előbb említett felek közötti bizalom kiépítése és folyamatos fejlesztése minden együttműködő irányába.

2. Kiberreziliencia a valóságban: Oroszország jól láthatóan küzd az ukrán kiberfölény ellen, leginkább azzal, hogy megpróbálja az internetelérést ellehetetleníteni, vagy legalábbis a forgalmat saját maga felé terelni a megszállt területeken. Ehhez egyrészt folyamatosan veszik át az ukrán internetinfrastruktúrát, másrészt elérhetetlenné teszi a nyugati közösségi médiaszolgáltatókat. Sőt, felmerült annak a lehetősége is, hogy az oroszok leválasztják magukat a globális internetről, de ez kivitelezhetetlennek látszódik. Az elsődleges tapasztalat az, hogy egy Ukrajna méretű államban az internet lekapcsolása legfeljebb lokálisan valósítható meg, akkor is csak ideiglenesen. Az internet tehát pont olyan jó ellenállóképességgel rendelkezik, ahogy azt az 1960-as években eredetileg megálmodták. Eközben viszont más ukrán kritikus infrastruktúrát sem sikerült kibertámadás útján lekapcsolni, helyette a hagyományos, kinetikus, azaz fegyveres megoldásokkal pusztít az agresszor. Ennek nyilván pszichológiai hatása is van, de érdemes végiggondolni a jövőre nézve, hogy egy valódi fegyveres konfliktusban mekkora szerepe lehet a kibertéri műveleteknek a hagyományos, fegyveres pusztítással szemben. Úgy tűnik, hogy a tiszta kiberműveletek elsősorban a hibrid műveletek során, tehát a „se nem béke, se nem háború" állapotában hasznosak, hiszen egy kritikus információs infrastruktúra megbénítása hosszú hónapok előkészületét igényli, amelyre a háború során egyszerűen nincsen idő. Viszont ahogy a háború véget ér, és visszatér a hibrid műveletek kora, komolyan kell számolni azzal, hogy az állami hátterű célzott kibertámadások megsokasodnak.

3. Hacktivista csoportok a jövőben: Jelentős hacker aktivitás mutatkozik mindkét oldal támogatása érdekében. Az elmúlt évtized minden fegyveres konfliktusát kísérték ugyan hacktivista megmozdulások, de soha korábban nem volt ennyi ember, aki billentyűzetet ragadott volna az általa támogatott fél érdekében. A hackercsoportokban ugyanúgy megtalálhatók kiberbűnözők, mint lelkes amatőrök, vagy éppen a főállású, de fedésben dolgozó titkosszolgák. Az ilyen proxycsoportok alkalmazása nem új taktika, de erősen kérdéses, mennyire lehet majd kontroll alatt tartani a háború után a függetlenebb csoportokat, és mi fog történni az általuk felfedezett, de nem publikált találatokkal. Mivel a hacktivista csoportok nehezen kontrollálhatók, a háborús időszakban nem feltétlenül érdeke a hadban álló országoknak ilyen proxyk alkalmazása, célszerűbb inkább az erre nyitott embereket becsatornázni a nemzeti kibererőkbe. Feltételezhető, hogy az ukrán IT Army és az

orosz csoportok esetében is ez történik, de a nem bevonódó országokban is célszerű aktív toborzást tartani. Akik viszont nem állnak állami szolgálatba, azok idővel vagy abbahagyják ezirányú tevékenységüket, vagy át/visszatérnek a kiberbűnözéshez. Komolyan kell tehát számolni olyan kiberbűnözői csoportok feltűnésével, amelyeket „harctéri" tapasztalattal rendelkező emberek alkotnak, új szintre emelve ezzel a csoportok műveleti képességeit.

4. Nagy adatmennyiség a szabadban: Több terabájtnyi digitális adat került már ki az internetre oroszországi célpontok feltörése után. A korábbi években több terabájtnyi adatot loptak el Oroszországhoz köthető kiberbűnözői csoportok, például a zsarolóvírus-támadások során. Ezeknek az adatoknak a feldolgozása évekig tarthat, hacsak a felek nem kezdik el a mesterséges intelligenciát felhasználni az adatelemzésben. Félő, hogy olyan információkhoz jutnak az elemzést végző felek, amelyek a következő években lehetetlenné teszik a megfelelő szervezeti védekezést. Nem véletlen, hogy a következő évek stratégiai küzdelme a mesterséges intelligencia körül fog csúcsosodni. A rengeteg kiszivárgott adat miatt pedig abból kell kiindulni, hogy legyen szó akár piaci cégekről, akár állami szervezetekről, nincsenek többé igazi titkok. Ez egészen újszerű védelmi stratégiákat fog igényelni, illetve a műszaki védekezést is arra kell építeni, hogy az ellenfél tudja, hol vannak a gyenge láncszemek. Az egyre jobban terjedő „zero trust", azaz zéró bizalom tervezési elve kell, hogy megjelenjen mindenhol, széles körben.

5. Az űr és a kibertér konvergenciája: Talán ez az első olyan háború, ahol az űreszközök biztonsága kiberbiztonsági szempontból kerül megkérdőjelezésre, illetve a kibertér fenntarthatósága űreszközöktől függ. A háború megkezdése előtt állítólag az ukrán katonai kommunikációt biztosító Viasat műholdat hackelték meg, amely egyébként számos nyugati kritikus infrastruktúra esetében is fennakadást okozott, majd az orosz űrügynökség, a Roszkozmosz szenvedett el kibertámadást. Eközben Ukrajnában az amerikai Starlink bevonásával is biztosítják a zavartalan internet-elérést. A tengerészeti rendszerek és a légiközlekedés kiberfüggősége már évek óta vizsgált terület, azonban ennek a két műveleti térnek a konvergenciájára aránylag kevés figyelmet fordítottak eddig erre a kutatók és a műveleti tervezők. Ha hozzátesszük ehhez azt, hogy mind a Viasat, mind a Starlink magánvállalkozás, egyértelműen látszik az eddig feltáratlan állami beavatkozási terület is. Összességében a kritikus információs infrastruktúrák interdependenciájára mutat rá ez az eset is. Egyelőre nincsenek jó modellek arra, hogy az összetett kiberfüggőségeket akár nemzeti, akár európai szinten felmérjük, de mindenképpen el kell kezdeni ezt a munkát is.

6. A technológiáktól való leválasztás hatása: A XXI. század iparának alapját az okoseszközök jelentik. Nincsen ez másképp a harctéren sem, a Harcászati Dolgok Internete (Internet of Military Things – IoMT) egyre inkább elterjedőben van a fejlett hadseregeknél. Ezek komoly információs fölényt tudnak biztosítani, akár harcoló katona szinten is. A nyugati szankciók azonban Oroszországot elvágták a fejlett technológia beszerzésének lehetőségétől. Mivel nem képes a fejlett félvezetőgyártásra és hardver-összeszerelésre, biztosan nem tudja tartani a lépést a NATO-hadseregekkel, de valószínűsíthetően a már elhasznált, saját fejlesztésű csúcseszközöket sem tudja majd nagy mennyiségben gyártani. Hadserege így megragad az 1970-es évek fejlettségi szintjén. Oroszország digitális gazdaságát pedig az olyan lépések fogják visszavetni, mint az okoseszközöktől és felhőtechnológiáktól való elzárás. Okoseszköz nélkül nincs adat, felhő nélkül nincs

tömeges adattárolás és feldolgozás, adattárolás és feldolgozás nélkül nincs mesterséges intelligencia, MI nélkül pedig nincs automatizálás. A digitális autonómia ezért elemi érdek, ha a hazai és európai digitális gazdaságot fenn kívánjuk tartani, függetlenedni kell az amerikai és kínai megoldásoktól.

7. A szoftverfejlesztés biztonsága: Ukrajna, Oroszország és Fehéroroszország rendkívül fejlett szoftverfejlesztői iparral rendelkezik – bár a háború és a fejlesztők elvándorlása miatt ezt talán múlt időbe is lehet tenni. A többszázezer „felszabaduló", menekülő programozó már most is a nyugati „agyelszívás" elsődleges célpontja, igaz, az orosz és fehérorosz állampolgárok kivándorlását egyelőre akadályozzák a nyugati kormányok. Idővel azonban tömegesen fognak megjelenni szinte az összes szoftvercégnél olyanok, akiknek a háttere, esetleges nemzetbiztonsági kockázata kevéssé lesz ismert a munkaadók számára. A személybiztonsági átvizsgálások kiemelt fontosságúak lesznek az ilyen jellegű tapasztalattal egyáltalán nem rendelkező szoftvercégeknél is. Ennek hiányában számos, Solarwinds támadáshoz hasonló „állami backdoor"-ra kell felkészülni, amelyet akár a beszervezett programozó is elhelyezhet a forráskódban. A kulcsfontosságú szoftvervállalatoknak emiatt szorosabb együttműködést kell kialakítania a nemzeti elhárító szervezetekkel, amelyre nincsenek felkészülve, sem folyamataikat tekintve, sem kulturálisan. A titkosszolgálatok és a piaci cégek közötti bizalomépítés mindkét oldal számára kiemelt fontosságú, de ezt egyelőre nem ismerték fel a felek.

8. Változó kockázati modell a vállalatoknál: Jelenleg vihar előtti csend honol a nemzetközi kibertérben. Nem dördültek el a rettegett orosz csoda-kiberfegyverek (mert jó eséllyel ilyenek nem is léteznek), és egyáltalán nem lettek felvillantva a nyugati kiberképességek sem. Amit látunk orosz részről, azt láttuk már korábban is – és már ezek is nagyon fájtak, például a 2017-es NotPetya támadás. De ne ringassuk magunkat abban a hitben, hogy ez a csend sokáig fenn fog maradni! Amíg a háború kiberfrontja Ukrajnában és Oroszországban van, a felek egymásra fordítják minden energiájukat. Azonban, ha a háború nyugvópontra jut, évekig tartó megtorlásra kell felkészülni orosz részről, nyugati célpontok ellen. Amit eddig kiberbűnözésként ismertünk, félő, hogy inkább a kiberhadviselés irányába fog elmozdulni. A vállalatoknak ezért újra kell gondolniuk a kockázati modelljeiket, és meg kell érteniük, egyedül nem képesek megvédeni saját magukat. Az elektronikus információbiztonság, azaz a szervezetek belső védelme és a kiberbiztonság, azaz az állami eszközökkel történő kibertérvédelem együttműködése minden korábbinál fontosabbá válik. Ehhez elengedhetetlenül fontos az információmegosztás nemzeti és európai szinten is, amelyet csak a mindenkire érvényes szabályozás tud kikényszeríteni. Erre vonatkozóan készülnek az európai szabályozások, de kölcsönös bizalom nélkül nehéz lesz a gyakorlati megvalósítás.

A kibertér biztonsága tehát egyik napról a másikra változott meg, ami alapjaiban más megközelítésre kényszeríti a kormányzatokat. Magyarország 2020-ban elfogadott Nemzeti Biztonsági Stratégiája helyesen ismeri fel a kiberbiztonság fontosságát, így többek között a következő megfogalmazást is használja: *„A kibertérben jelentkező kihívások, kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelmi feladatok ellátására, a nemzeti létfontosságú információs infrastruktúra zavartalan működésének biztosítására Magyarországnak készen kell állnia. Elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális kihívások, kockázatok és fenyegetések azonosítása és nyomon követése, a kormányzati koordináció erősítése, a kibertér jogi*

szabályozásának fejlesztése, a felhasználók biztonságtudatos viselkedésének elősegítése, a kormányzati infokommunikációs rendszerek, a nemzeti létfontosságú információs infrastruktúra, a minősített információk és a nemzeti adatvagyon védelmének erősítése, valamint a kiberbiztonsággal kapcsolatos nemzetközi együttműködés bővítése. A katonai kibervédelmet növekvő mértékben alkalmassá kell tenni a haderő kinetikus műveleteinek kibertérbeli támogatására, ki kell alakítani a kiberműveletekben alkalmazható offenzív képességeket. Ennek érdekében fejleszteni kell a Magyar Honvédség kibervédelmi és kiberműveleti erőit." Megjegyzi tovább, hogy: *„A forradalmi technológiák fejlesztése stratégiai fontosságú kérdés. Hazánk biztonsága megkívánja, hogy a kulcsfontosságú területeken - mint például a kibervédelem, a mesterséges intelligencia, az autonóm rendszerek, a biotechnológia - kiemelt figyelmet fordítsunk a kutatás-fejlesztésre és annak védelmi összetevőjére."* Stratégiai szinten tehát hazánk készen áll az újtípusú fenyegetések kezelésére. Megfelelő anyagi és humán erőforrások nélkül azonban ezeket a fenyegetéseket nem leszünk képesek kezelni. A kihívás hatalmas, de nem megoldhatatlan. Winston Churchill mondása azonban itt is igaz: *„Nem ígérhetek mást, csak vért, erőfeszítést, verítéket és könnyeket."*

Felhasznált irodalom:

- BROWN, Ronald Harmon: The national information infrastructure: agenda for action. Executive Office of the President Information Infrastructure Task Force, 2003. p. 2.
- Európai Bizottság: Európa digitális évtizede: a 2030-ra kitűzött célok https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_hu
- Európai Bizottság: Javaslat AZ EURÓPAI PARLAMENT ÉS A TANÁCS HATÁROZATA „A digitális évtizedhez vezető út" elnevezésű, 2030-ig szóló szakpolitikai program létrehozásáról. COM(2021) 574 (2021. szeptember 15.) https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52021PC0574
- European Commission: Europe and the Global Information Society: Recommendations to the European Council: Conference G7 – Raport BANGEMANN. Publications Office, 1995. p. 3.
- Francois Godement et al.: The China dream goes digital: Technology in the age of Xi. European Council on Foreign Relations, 2018.
- HASS, Ryan– BLANCHETTE, Jude: Central Questions in U.S.-China Relations amid Global Turbulence. Center for Strategic & International Studies, 2022. július 21. https://www.csis.org/analysis/central
- QS Top Universites: QS World University Rankings by Subject 2022: Engineering & Technology https://www.topuniversities.com/university-rankings/university-subject-rankings/2022/engineering-technology
- ZHANG, Yingying– ZHOU, Yu: The Source of Innovation in China. Palgrave Macmillan London, 2015. XIV-XIX.