HADMÉRNÖK
VÉDELMI INFORMATIKA

14. évfolyam (2019) 4. szám 197–212.
DOI: 10.32567/hm.2019.4.13

Kralovánszky Kristóf[1]

A kibertér fejlődése

The Evolution of Cyberspace

A kibertér fogalmi meghatározása alapvető fontosságú az abban mint (hadviselési) tartományban zajló események helyes leírásához és megértéséhez. Az állami szerepvállalás növekedése mind a támadó, mind a védekező műveletekben tovább hangsúlyozza a kibertér jelentőségét, a kapcsolódó gazdasági és politikai kockázatok miatt is. A létfontosságú rendszerelemeken (kritikus infrastruktúrákon), infokommunikációs eszközeinken, illetve a rohamosan terjedő mesterséges intelligencián alapuló technológiákon keresztül pedig mindennapjaink meghatározó részévé vált. A kibertér szerepe a technológiai haladással tovább fog változni, ezért is fontos az eddigi fejlődés áttekintése.

Kulcsszavak: **kibertér, kiberhadviselés, kiberművelet, bizonyíthatóság**

It is essential to have a proper definition of cyberspace as it is the foundation of the proper understanding operations being performed therein. The increasing role of state actors both on the defensive and on the offensive side together with the economic and political risks and interconnections further emphasise the importance of cyberspace. Through critical infrastructures, infocommunication systems and artificial intelligence, cyberspace became an integral part of our day-to-day lives. Cyberspace will keep changing its role due to future technological advancements – that is why we should understand its evolution curve.

Keywords: **cyberspace, cyber warfare, cyber operations, attribution**

Bevezetés

A kibertér és az abban zajló műveletek és tevékenységek egyre szélesebb skálán és egyre szerteágazóbb tartalommal és végrehajtói körrel jelennek meg. Mindennapjaink meghatározó részévé vált, ám kockázatai és összefüggései sokszor még mindig jelentősen

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: kralovanszky.kristof@d-systems.hu, ORCID: https://orcid.org/0000-0002-5560-3525

alábecsültek világszerte, ami többek között tapasztalható az ebben feladatokkal rendelkező vállalatok, szervezetek és intézmények megnyilatkozásaiból, megismert képességeiből, az ezek nyomán bekövetkező sikeres támadásokból és az azok következményeként elszenvedett károkból.

Az információs társadalom egyik meghatározó alapja a kibertér, így annak labilis (nem biztonságos) működése jelentős társadalmi funkcionális megingásokhoz vezethet. Többek között ezért is kiemelkedően fontos alapvető kapcsolatainak és fogalmainak vizsgálata. Publikációnknak nem célja a kibertérrel kapcsolatos főbb fogalmakra egyedül helyes meghatározást adni, sokkal lényegesebbnek tartjuk az ezzel kapcsolatos bizonyos logikai összefüggések áttekintését, illetve annak a hipotézisnek a vizsgálatát, hogy a kibertér integráltabb részévé válik-e életünknek.

Számos esetben merül fel kérdésként egy adott sikeres kibertámadást követően, hogy a megtámadottak kibertérrel kapcsolatos tudatossága megfelelő volt-e. Sajnos a válaszok nagyobb részében általában megállapítható, hogy e tudatosság jelentősen elmaradt a megkívánt mértéktől és nagyban ennek köszönhető az elszenvedett kár.

Tanulmányunk első része a kibertér fogalmát, az ott zajló támadás, hadviselés és védekezés tartalmi jellemzőit és szereplőit vizsgálja különböző példákon keresztül, így keresve választ a növekvő kockázatok felismerhetőségére és ezen keresztül kezelhetőségük megteremthetőségére.

A leendő második rész a hadtudomány oldaláról vizsgálja a stratégiai jellegű kibertámadásokat és azok szélesebb összefüggéseit.

A kibertér fogalma

Számos olyan összetett szavunk van, amelyeknek első tagja a „kiber" szó. Ilyenek például a kiberhadviselés, a kibervédelem, a kiberfenyegetettség stb. Ezek mind a kibertérben értelmezett folyamatokat vagy eseményeket jelentenek, vagyis a kibertérben végzett műveleteket, ott történő védelmi feladatokat, intézkedéseket, illetve a kibertérben megjelenő fenyegetettségeket. Annak érdekében tehát, hogy bármelyik fenti összetett fogalmat helyesen tudjuk értelmezni, először a kibertér fogalmát kell megvizsgálnunk.

A kibertér – mint kifejezés – első megjelenéséről és kezdeti tartalmáról több hazai kutatás is született már, amelyek egyik konklúziója magának a fogalomnak a meghatározása volt [1]. Szintén komoly tudományos eredményekhez vezetett a kibertér különböző definícióinak Munk Sándor által végzett összehasonlítása is [2], aminek alapján (többek között) a fogalom értelmezésének különbségei az alkalmazási terület függvényében állapíthatók meg. Ezeken felül, a nemzetközi szakirodalomban és jogalkotásban is több tucat meghatározás jelent meg [3], amelyek ugyanezen fogalmat definiálják különböző módokon.

Jelen publikáció Haig Zsolt fogalmi meghatározását tekinti irányadónak és az abban foglalt kibertéri tulajdonságok szerint folytatja az elemzést. E főbb tulajdonságok a következők:

1. ember által mesterségesen létrehozott;
2. dinamikusan változó;
3. tartomány;

4. benne az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző folyamatok vannak jelen;
5. egymással hálózatba kapcsolt, az elektromágneses spektrumot is felhasználó – átvivőközeget alkalmaz;
6. benne infokommunikációs eszközök és rendszerek működnek;
7. emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot (nem helyhez kötött) biztosít.

A terület két meghatározó magyar kutatójának, Haig Zsoltnak és Kovács Lászlónak a civil tartalmú meghatározása 2008-ból a következő volt: „a cybertér az elektronikus kommunikációs eszközök és rendszerek (számítógép-hálózatok, internet, telefonvonalak, műholdas rendszerek stb.) és a rajtuk található szolgáltatások, információk alkotta virtuális tér vagy világ" [4].

Látható, hogy ma már alapvetőnek tartott minőségek, vagyis a dinamikus változás, a tartományjelleg, az információ gyűjtése, tárolása, feldolgozása, továbbítása és felhasználása még nem jelentek meg.

A két meghatározás között 10 év telt el. A változások legfőbb oka a technológiai fejlődésben keresendő: 10-20 éve nem álltak rendelkezésre széles körben olyan kereskedelmi adatátviteli lehetőségek (sebességek), technológiák és számítási kapacitások (ezzel párhuzamosan automatizáltsági állapotok), mint napjainkban. Ugyanígy, 10 év múlva, a kvantum-számítástechnika képességének (kapacitásának) várható növekedése [5], az emberekbe ültetett és vezérelhető eszközök[2] elterjedése, agyhullámok manipulálhatósága stb.[6], egészen más kibertér-definíciót fog eredményezni,[3] vagyis helyes tartalom meghatározása jellemzően az idő függvényében lehetséges csak.

Hadviselés: támadás és védelem

A kibertérben eddig nem volt kölcsönös támadások és ellentámadások eseményegyüttesként végrehajtott műveletsor – a legnagyobb kiberműveletek (Észtország ellen 2007-ben,[4] Grúzia ellen 2008-ban,[5] Irán ellen 2010-ben[6] vagy Ukrajna ellen

[2] Olyan beültetett szem, amelyhez számítógép csatlakoztatható, vagy hálózati kapcsolattal rendelkezik; egyéb kívülről vezérelhető eszközök (szívritmus-szabályozás, defibrillátor, inzulinpumpa stb.)

[3] Nehéz egyedül helyes definíciót létrehozni a kibertér fogalmára – ezért is fontos lehatárolni, hogy egy adott értekezés tárgyában mi az alkalmazott tartalom.

[4] A támadások Észtország ellen 2007. április 27. és május 18. között folyamatosak voltak és Észtországon kívülről érkeztek. Számos orosz honlapon volt leírás arról, hogy a különböző támadásokat hogyan kell végrehajtani. Oroszország minden fórumon tagadta, hogy állami részvétellel történtek volna a támadások [7].

[5] 2008. július végétől (hetekkel Grúzia orosz fegyveres erők általi megtámadását megelőzően) számos kibertámadás ért grúz kormányzati honlapokat, médiumok online felületeit, elérhetetlenné téve azokat, vagy tartalmukat megváltoztatva. Ez volt az első olyan kombinált csapásmérés-sorozat, amelynek során kinetikus és kiberfegyvereket egyidejűleg használtak [8]. Oroszország minden fórumon tagadta, hogy állami részvétellel történtek volna a kibertámadások.

[6] Az Irán elleni támadás az ország urándúsítással foglalkozó intézményét célozta „csak". Ez volt a Stuxnet néven megismert kártevő.

2017-ben[7]) mind „csak" támadó műveletek voltak, vagyis a támadáshoz mérhető ellentámadás a megtámadott fél részéről nem történt. Ez természetesen nem azt jelenti, hogy a megtámadott fél védekező műveleteket ne hajtott volna végre: a kiberműveletek ugyanúgy lehetnek támadó és védekező műveletek.

A hadviselés hadtudományi értelemben „a hadban álló felek fegyveres erejének háborús katonai műveleti, illetve háborús küszöb körüli válságreagáló katonai műveleti alkalmazása a hadművészet elméletének és gyakorlatának elvei szerint" [10]. A hadviselés fogalmi feltétele tehát, hogy az érintett felek országok (államok) legyenek, hiszen csak azok esetében beszélhetünk fegyveres erőről. Így szorosan vett értelemben kiberhadviselésről is csak akkor beszélhetünk, ha az fegyveres erő által végrehajtott.[8]

Védekező műveletek során is szükséges lehet a támadási képesség és a támadás – akár válaszlépésként, akár megelőzésként. Ugyanúgy lehetséges, hogy kibertámadásra kinetikus válaszcsapás szülessen, ami sokáig teoretikus lehetőség volt csupán, ám 2019. május 5-én válaszlépésként, az izraeli hadsereg megtámadta és megsemmisítette a Hamász[9] egyik kiberműveleti központját, amelyet Izrael elleni kibertámadásokra használtak [11]. Izrael kinetikus válaszcsapása abban is új volt, hogy egy valós idejű (folyamatban lévő) kibertámadást állított meg, vagyis közvetlen és azonnali volt – több hetes vagy hónapos előkészítés nélkül. Amennyiben a konkrét példában szereplők személyétől eltekintünk, még nem hadviselésről van szó, hiszen egy támadásra egy válasz született.[10]

Bizonyíthatóság

Sem az Amerikai Egyesült Államok (a továbbiakban: Egyesült Államok), sem Izrael, sem Oroszország, sem Kína, sem Észak-Korea nem ismerte el soha az érintettségét kibertámadások elkövetőjeként, és mivel nincs kétséget kizáró, nyilvánosságra hozható bizonyíték, az érintettség tagadható marad(t). Így azt jelenthetjük csak ki, hogy több olyan ország van, amelyek esetében nagy bizonyossággal[11] feltételezhető, hogy számos kibertámadást támogattak, vagy azokban aktívan részt vettek.[12] Amennyiben csak minősített titkosszolgálati információk alapján, de biztosan megállapítható az elkövető személye, akkor kockázatot jelenthet az egyértelmű vád megfogalmazása a forrás felfedése nélkül. Ilyen formában tehát a válaszlépés is problémát jelenthet, hiszen megfelelő környezetben

[7] A támadáshoz a NoPetya kártevőt és annak variánsait használták, célja elsősorban Ukrajna volt, de számos más ország (Franciaország, Németország, Lengyelország, Amerikai Egyesült Államok, Egyesült Királyság) számítógépes rendszerei is elszenvedői voltak – bár kisebb arányban [9]. A források egy része a kártevőt „NoPetya" néven, míg egy másik része „NotPetya" néven említi.

[8] A hadtudományi és jogi kérdésekkel e tanulmány második része foglalkozik részletesebben.

[9] Hamász – arab kifejezés mozaikszava, jelentése: Iszlám Ellenállási Mozgalom. E palesztin szunnita mozgalom központja a Gázai övezetben található.

[10] Más kérdés, hogy Izrael és a Hamász összefüggésében a kettejük közötti hadviselésről van szó, függetlenül a konkrét példában bemutatott két cselekménytől.

[11] Ami messze nem jelent egyértelműséget.

[12] A bizonyíthatóság és az elkövető megnevezésének (attribúció) nehézsége lehet technikai eredetű (sokszor a forrás IP-cím maszkolhatóságának lehetőségeiből), vagy fakadhat politikai okokból – adott esetben e kettőből együttesen. Az attribúció kérdése rendkívül összetett és meghaladja jelen publikáció kereteit.

az eredeti agresszor a (jogos) válaszlépést a nyilvánosság felé eredő és megalapozottság nélküli agresszióként tudja bemutatni.[13]

A kibertéri műveleteknél a legritkábban áll rendelkezésre olyan konvencionális, térben és időben rögzíthető felvétel, amelyet audiovizuális eszközökkel közérthetően biztosítani lehet. Ha pedig rendelkezésre is állna, az elkövető legegyszerűbb védekezése, hogy a felvételek hamisítványok.[14]

A kibertérben sokkal inkább digitális nyomokat vagy közvetett bizonyítékokat kell keresni[15] és azok alapján azonosítani: például, hogy kinek állhatott érdekében egy adott cselekmény (művelet) elkövetése, illetve milyen motiváció lehetett az elkövetés mögött.

Ugyanennyire fontos a nemzetközi jog alkalmazhatósága a kibertérben, illetve a kibertér sajátosságai miatt a jogfogalmi meghatározások is komoly kihívást jelentenek. Többek között ennek rendezését célozza a NATO Kibervédelmi Együttműködési Kiválósági Központja[16] által, kiváló szaktekintélyek közreműködésével létrehozott Tallinn Manual első és második része [13], [14].

Állami szereplők

Kibertéri műveleteknél elengedhetetlenül fontos (lenne) a támadó egyértelmű azonosíthatósága, ami állami szereplők (elkövetők) esetében szinte kizárható, ugyanis az elkövető államnak mindennél erősebb érdeke fűződik az elkövetés tagadhatóságához, így mindent meg fog tenni a bizonyosságot jelentő nyomok eltüntetéséért.

Vannak ugyanakkor olyan részletek, amelyek motívumokként megjelenő összessége mégis szinte egyértelművé teszi az állami érintettséget:

- az anyagi haszonszerzés céljának hiánya;
- az elkövetés módja és eszközei – részben titkosszolgálatokra jellemző eszközökkel;
- különösen óvatos előkészítés – részben titkosszolgálati módszerekkel.

Amennyiben az állami elkövetés így megállapítható, még mindig nyitott kérdés marad, hogy melyik állam áll valójában mögötte, hiszen elképzelhető, hogy egy A jelű állam egy másik, B jelű államot kíván elkövetőként megjeleníteni, úgy, hogy B is elkövethette volna az adott cselekményt, ám nem ő volt a valódi elkövető. Visszatértünk tehát a kétséget kizáró és nyilvánosan is védhető bizonyíthatóság kérdéséhez, amit pont a fentiek miatt a nagy horderejű támadások esetében gyakorlatilag lehetetlen (lesz) elérni.

A kibertérben ugyanúgy értelmezhető a proxyművelet.[17] Ennek lényege, hogy a valódi agresszor egy a támadás céljával egyetértő végrehajtón keresztül érvényesíti

[13] Ehhez kínál kiváló eszköztárat az információs hadviselés. A kibertéri műveletek és az információs hadviselés kapcsolatának összetettsége nem teszi lehetővé, hogy jelen tanulmány keretei között azokat érdemben elemezzük.

[14] Ilyen videók hamisítására alkalmas például a deepfake-technológia, amit e publikáció később részletesebben leír.

[15] Az infokommunikációs digitális nyomkeresés angol megnevezéssel: IT Forensics. Az ilyen tárgyú kriminalisztikai vizsgálatok egyre fontosabbá válnak a bűnelkövetés módjainak jelentős változása miatt, és így egyre több különböző ága létezik [12].

[16] NATO Cooperative Cyber Defense Center of Excellence.

[17] Tartalmilag a proxyhadviseléssel egyezik meg, de a hadviselés kétirányúságot feltételez, ezért jelen esetben egyirányú műveletre értelmezzük a proxy jelzőt.

támadási szándékát, amihez közvetett, vagy közvetlen műveleti támogatást is biztosíthat a végrehajtónak.[18] A támogatás természetesen indirekt is lehet, például: tudásátadás (sérülékenységi információ, konkrét támadási pont meghatározása és a kivitelezés részletes leírása), mögöttes irányítás, „menekülési út" biztosítása. Megkülönböztethetünk belföldi és külföldi proxykapcsolatokat. Belföldi esetekben az állami szereplő egy gazdasági társaságot/csoportot támogat,[19] [16] míg külföldi esetben egy másik államot, vagy egy másik állam gazdasági szereplőjét/csoportját [17].

A proxyműveleti elkövetés megvalósulhat állami szereplővel, tisztán gazdasági haszonszerzés céljából is – ezek a zsarolóvírusok bizonyos fajtái [18], [19]. Mellékesen károkozás is megvalósul (ami az elkövetőnek járulékos, de számára kedvező célja), hiszen mindazok a károsultak, ahol nem fizetik ki a váltságdíjat, az esetek nagyobb részében komoly adatvesztést szenvednek el, ami üzleti folyamataik korlátozódásához és ebből fakadóan anyagi veszteséghez vezet.

Szinte minden komolyabb erőforrást igénylő támadás mögött valamilyen (érdek-) csoport vagy közösség áll, hiszen maga a támadás kivitelezése egyéni elkövető által – főként az erőforrások nagysága és a szükséges eltérő területeket lefedő speciális szaktudás miatt – szinte lehetetlen. Amennyiben viszont mind a tudás, mind az erőforrások rendelkezésre állnak, logikusan célszerű, hogy az minél hatékonyabban hasznosuljon. Így jöttek létre a támadói csoportok, amelyek közül viszonylag sokat azonosítottak, róluk adatbázist készítettek és azt folyamatosan karbantartják [20]. Az így összegyűjtött adatokból jól látszik, hogy a csoportok nagyobb részénél vélelmezhető az állami kötődés és ugyanígy feltételezhető, hogy bizonyos országokban állami támogatás nélkül egyáltalán nem működhetnének. Az állami szerepvállalás célja itt is változó lehet, hiszen egy ilyen csoport kiválóan használható hírszerzési feladatokra is, támadó képességei mellett.[20]

Kritikus infrastruktúrák[21] kitettsége

A kritikus infrastruktúrák célponttá válása éppen a kritikusságuk miatt történik és célponti értékük egyenesen arányos a kritikusságukkal.[22] E minőségük nemcsak gazdasági, hanem politikai célokat is szolgálhat a támadó számára, így egyre inkább célja lehet állami támogatású támadásoknak. Az Egyesült Államok és Izrael különböző kritikusinfrastruktúra-rendszerei szinte folyamatos támadásoknak vannak kitéve:

[18] A szerző saját meghatározása. Léteznek olyan vélemények, hogy Irán és Észak-Korea kiberműveletei mögött részben kínai és/vagy orosz szándék feltételezhető. Ezeket a koncepciókat Kína és Oroszország egyrészt tagadja, másrészt nyílt forrásból nem áll rendelkezésre információ az ilyen állítások alátámasztására [15].

[19] Kína és Oroszország vélelmezhetően alkalmaz ilyen megoldásokat – ahogy adott esetben az Amerikai Egyesült Államok is megteszi ugyanezt, főként az állami szerepvállalás tagadhatósága miatt.

[20] Sikeres támadás egy jól védett infrastruktúra vagy állami intézmény ellen rendkívül nagy dicsőséget jelent az elkövetőnek (csoportnak), amivel saját piaci értéke, illetve politikai ereje is jelentősen növekszik.

[21] Hatályos honi jogi szabályozás szerint (2012. évi CLXVI. törvény) a hivatalos megnevezés létfontosságú rendszerelem, ami nemzetközileg elfogadott elnevezés szerint: kritikus infrastruktúra. Írásunkban a két kifejezést egymás szinonimáiként használjuk.

[22] Kiváló példája, hogy egy adott kritikus infrastruktúra mennyire értékes, a szaudi Aramco Abqaiq-i finomítója elleni támadás 2019. szeptember 15-én: a támadással a világ napi felhasználásának 5%-át meghaladó finomítói kapacitás esett ki, vélhetően hónapokra [21].

mindkét országban különösen a villamosenergia-rendszer a célpont, hiszen ott lehet az egyik leglátványosabb módon kárt okozni. Hivatalosan publikált adatok nem állnak rendelkezésre, de különböző szakmai fórumok szakértői több tízezres nagyságrendű és folyamatosan, dinamikusan emelkedő számú éves támadásról beszélnek. Ezeknek csak egészen kis töredéke tud átjutni az elsődleges védelmi vonalakon (határvédelmi rendszereken [22]) és azokból is csak néhány az, ami valós kárt tud okozni – amelyek elsősorban a nem termelő rendszereket érintik. Vannak azonban olyan kártevők, amelyek a rendszerbe bejutva nagyon komoly fennakadást tudnak okozni. Erre volt példa a 2016. januári, az Israel Electric Corporation elleni támadás, ami a villamosenergia-rendszerben ismert ellátási kiesést ugyan nem okozott,[23] de rendkívüli nehézséget jelentett a szolgáltatónak, mivel a hideg időjárás miatt rekordméretű villamosenergia-ellátási igény lépett fel [23]. Feltételezhető, hogy nem volt véletlen a támadás időzítése sem.

Amikor egy ország valamilyen kormányzati rendszerét vagy kritikus infrastruktúráját meghatározott küszöbértéket[24] el nem érő kibertámadás éri, a megtámadott fél (kormányzati szerv) megpróbálhatja jelentéktelenné tenni a támadást (és az okozott kárt), hiszen hatalmas erkölcsi veszteséget szenved el a saját állampolgáraival szemben: nem tudta önmagát otthon megvédeni. Mindez tovább fokozható, ha a lakosság is kárt szenvedett ebből, hiszen akkor már nem csupán önmagát, hanem saját állampolgárait sem tudta megvédeni – otthon.[25] Ezért van az, hogy nagyon sok esetben minimális információ áll csak rendelkezésre egy támadásról és szinte csak a kötelező tájékoztatás teljesül.[26] A következő példában egy néhány szavas, a negyedéves energetikai üzemzavarokat összefoglaló táblázatból lehetett értesülni: 2019. március elején az Egyesült Államok nyugati partvidékét ellátó egyik villamosenergia-szolgáltatót érte támadás, ami közel 10 órás üzemi fennakadást okozott, de végfelhasználói szolgáltatási kiesés nem következett be [25], [26].

Kiberműveleti képességek

Képességekben is meg kell különböztetni egy ország egészének kiberműveleti képességeit a fegyveres erejének hasonló képességeitől. A kibervédelemben számos más kormányzati szereplő vesz részt a fegyveres erő szakcsapatai mellett és ezek összessége adja az adott ország kibervédelmi képességét.

[23] Vélelmezhetően pont ettől vált küszöbérték alatti műveletté.

[24] A konkrét küszöbérték meghatározása többek között ágazattól is függő, rendkívül összetett feladat, ezért meghatározása nem tárgya jelen tanulmánynak. A tárgyban több hazai kutatás született, amelyek küszöbérték fogalmával és tágabb értelemben a kritikus infrastruktúrák meghatározásának módszertanával részletesen foglalkoznak [24].

[25] Ez az egyik motívum, amitől szinte biztosan küszöbérték felettivé válik egy elszenvedett kibertámadás.

[26] A konkrét küszöbérték pont ezen okokból nagyon nagyban politikai kérdés is. Tehát ugyanazon esemény két eltérő belpolitikai környezetben jelentősen eltérő küszöbértéket jelenthet.

Amerikai Egyesült Államok

Az Egyesült Államok működteti az egyik legnagyobb kiberképességekkel felruházott komplex rendszert,[27] ami katonai és civil fő részekre oszlik. A katonai rész a Védelmi Minisztérium (Department of Defense, DoD) hatáskörébe tartozik, ahol a haderőnemek saját kibervédelmi parancsnokságokat működtetnek,[28] amelyeket a Kiberparancsnokság (U.S. Cyber Command), mint egyesített parancsnokság (EPK) fog össze. A Kiberparancsnokság a 11 EPK egyike.[29] A haderőnemi kiberparancsnokságok pedig támogatást nyújtanak a többi EPK-nak:

- Tengerészgyalogság – különleges műveleti EPK-nak.
- Szárazföldi erők – központi, afrikai és északi EPK-nak.
- Haditengerészet – csendes-óceáni, déli EPK-nak.
- Légierő – európai, stratégiai és szállítási EPK-nak.

A kiber EPK parancsnoka egyben a Nemzetbiztonsági Ügynökség (National Security Agency – NSA) főigazgatója is.

A kiber EPK kialakulása és fejlődése [27] kiválóan mutatja a kibertér és a kiberműveletek egyre növekvő fontosságát és hangsúlyait:

- 1998-ban megalakul a Védelmi Minisztérium számítógép-hálózatok védelmét ellátó munkacsoportja (Joint Task Force – Computer Network Defense).
- 2000-ben a csoport neve megváltozik és már számítógéphálózati műveletek munkacsoport néven működik tovább, jól mutatva, hogy tevékenységük már messze nem csak védelemről szól (Joint Task Force – Computer Network Operations, JTF-CNO).
- 2002-ben az Űr EPK számítógépes támadási képességei beolvadnak a Stratégiai EPK-ba, de a JFT-CNO továbbra is megmarad.
- 2002–2004 között a Stratégiai EPK-n belül szétválasztják a számítógéphálózat támadási és védelmi képességeket. Az előbbi az NSA-hez, míg az utóbbi a Védelmi Információs Rendszerek Ügynökséghez (Defense Information Systems Agency – DISA) kerül.
- 2004-ben a JTF-CNO nevet vált és Globális Hálózati Műveletek Munkacsoport (Joint Task Force – Global Network Operations, JTF-GNO) néven működik

[27] Nyílt forrásból pontos összehasonlítás nem végezhető Kína és Oroszország hasonló képességeiről. Megállapítható azonban, hogy e három ország (Amerikai Egyesült Államok, Kína, Oroszország) rendelkezik a legkomolyabb ilyen szervezeti rendszerrel és erőforrásokkal. Nem szabad azonban figyelmen kívül hagyni Izrael hasonló képességeit sem, de meg kell jegyezni, hogy azok változó arányban, de akár jelentősen is támaszkodhatnak az Amerikai Egyesült Államok támogatására.

[28] Szárazföldi erők (U.S Army – Army Cyber Command), Haditengerészet (U.S. Navy – U.S. Fleet Cyber Command 10th Fleet), Tengerészgyalogság (U.S. Marine Corps – U.S. Marine Corps Forces Cyberspace), Légierő (U.S. Air Force – 24th Air Force)
Az Amerikai Egyesült Államok Parti Őrsége (U.S. Coast Guard) békeidőben a Belbiztonsági Minisztérium alárendeltségébe, míg háborúban a Haditengerészet parancsnoksága alá tartozik. A Parti Őrség rendelkezik saját kiberparancsnoksággal, Coast Guard Cyber Command néven.
A Nemzeti Gárda szintén rendelkezik kiberműveleteket végző egységekkel, ezek azonban jellemzően támogató, illetve önálló regionális védelmi feladatokat látnak el. Természetesen ugyanúgy a Kiber EPK részeként.

[29] A többi 10 egyesített parancsnokság: Afrika, központi, európai, Indo-csendes-óceáni, északi, déli, űr, különleges műveletek, stratégiai, szállítási.

tovább. Ugyanebben az évben a Nemzeti Katonai Stratégia a kiberteret önálló tartománnyá nyilvánítja.[30]

- 2005 elején a Stratégiai EPK-n belül megalakul a Hálózati Hadviselési Parancsnokság (Joint Functional Component Command – Network Warfare, JFCC-NW), de megmarad a JTF-GNO is – jól jelezve a műveleti képességek deklarált kiterjesztését.
- 2008-ban a JTF-GNO egyesül a Hálózati Hadviselési Parancsnoksággal.
- 2008-ban megalakul a Kiberparancsokság, de akkor még nem egyesített parancsnokságként, hanem a Stratégiai EPK alárendelt parancsnokságaként. A Kibervédelmi Parancsnokság 2010. májusában éri el teljes műveleti képességét. A 2008–2010 közötti időszakban a két elődszervezet (JTF-GNO és JFCC-NW) szervezetileg beolvad a kialakuló Kiberparancsnokságba.
- 2017 augusztusában a Kiberparancsnokság önálló EPK lesz.

Az Egyesült Államok civil kiberműveleti felügyeletét és működtetését a Belbiztonsági Minisztérium (Department of Homeland Security – DoHS) látja el [30], [31], [32]. A tevékenységek jogszerűségét, valamint a kiberbiztonsággal kapcsolatos jogszabályok betartatását az Igazságügyi Minisztérium (Department of Justice – DoJ) végzi, más egyéb, a kibertérrel kapcsolatos információgyűjtés, nemzetbiztonsági fenyegetettség értékelése, nyomozás stb. mellett, aminek egyik ügynöksége a Szövetségi Nyomozóiroda (Federal Bureau of Investigations – FBI) [33], [34].

A DoHS alárendeltségében működik a 2018-ban megalakított Kiberbiztonsági és Isnfrastruktúra Biztonsági Ügynökség (Cybersecurity and Infrastructure Security Agency – CISA) [35]. Jellemzően ez az ügynökség támogatja és védi az Egyesült Államok fizikai és kiber-infrastruktúráinak biztonságát. Jogelődjük a DoHS egy igazgatósága, amelynek egy hivatala volt a Nemzeti Kibervédelmi és Kommunikációs Integrációs Központ (National Cybersecurity and Communications Integration Center, NCCIC).

A szervezet létrehozása jól mutatja, hogy az infrastruktúrák védelmének fontossága magasabb szintre lépett, illetve ezzel egyidőben a kibertérből való támadhatóság kockázatai ugyanakkora problémát jelentenek, mint a fizikai támadások lehetőségei.

Katonai szervezetek és gazdasági társaságok kapcsolatai

Különböző gazdasági társaságok, amelyek a DoD szerződött partnerei és a védelmi ipar fontos szereplői, a kiber EPK védelmét élvezik, vagyis e társaságokat érő kibertámadás esetén a kiber EPK megfelelő szervezeti egységei támogatást és adott esetben teljes védelmet is fognak biztosítani számukra – igénybe véve akár a Nemzeti Gárda illetékes kiberszakcsapatait.

[30] Ugyanezt a NATO hivatalosan csak 12 (!) évvel később, 2016-ban tette meg. Igaz ugyanakkor, hogy a NATO 2008-ban alkotta meg az első kibervédelmi alapszabályzatát [28], majd 2014-ben a kollektív védelem alapvető részévé nyilvánította kibervédelmet (ezzel a NATO alapszerződés V. cikkelyének aktiválását tette lehetővé kibertámadás esetére) [29].

Az NSA az Egyesült Államok kormányzati ügynökségeinek és szervezeteinek fő kriptográfiai szolgáltatója is. Ellátja a TEMPEST[31]-eszközök gyártóinak és bevizsgálóinak felügyeletét. Számos saját fejlesztésű szoftvereszközt biztosít, amelyek különböző infokommunikációs rendszerek biztonsági ellenőrzését vagy biztonságának növelését segítik elő [36], így értékes támogatást nyújtva a legkülönbözőbb méretű gazdasági szereplőknek. Katonai szervezetként számos ponton kapcsolódik tehát a civil vállalatokhoz, illetve a kormányzat nem katonai intézményeihez.

A civil részen a másodlagos feladatokat egy sor intézmény és szervezet látja el, a különböző CERT-ek[32] vagy CSIRT-ek[33] formájában,[34] amik működhetnek önálló gazdasági társaságként, vagy egy adott kritikus infrastruktúra saját védelmi elemeként.[35]

Az Egyesült Államok védelmi szerkezeti berendezkedése különösen jól mutatja a kibertéri fenyegetettségek és lehetséges támadások elleni védekezés komplexitását, illetve hogy a kibertérnek egyaránt részei a katonai és civil rendszerek is, amelyek összekapcsolt és összehangolt védelmet igényelnek.

Fontos megállapítani továbbá (nem minősítési céllal), hogy az Egyesült Államokban jelentős túlsúllyal bírnak a kibertér katonai szereplői, aminek legfőbb oka, hogy az NSA katonai szervezet. Ettől az európai berendezkedések eltérnek és a polgári szervek nagyobb arányt képviselnek az adott ország kibervédelmi és kiberműveleti képességeiben. A polgári szervek sikeres küldetéséhez azonban Európában is elengedhetetlenek a fegyveres erő(k) készségei és erőforrásai.

Magyarország

Hazánk sem méretében, sem fenyegetettségében, sem védelmi doktrínájának számos részében nem összehasonlítható az Egyesült Államokkal.[36]

A honi elsődleges kibervédelmi és kiberbiztonsági feladatokat az alábbi szervezetek látják el:

- Nemzeti Kibervédelmi Intézet (a Nemzetbiztonsági Szakszolgálat szervezetén belül);[37]
- Katonai Nemzetbiztonsági Szolgálat Kiberbiztonsági Központ;

[31] TEMPEST – Elektromágneses kisugárzástól nagymértékben védett infokommunikációs eszközök gyűjtőneve, amely eszközök a védettségük miatt alkalmasak különböző szintű minősített adatok feldolgozására. A TEMPEST-nek több védettségi fokozata létezik. A szabványt az NSA dolgozta ki, egy része ma is minősített. A szabvány a NATO-n és az EU-n belül egyaránt használatos.

[32] CERT – Computer Emergency Response Team, magyarul számítógép biztonsági incidens kezelő csapat. MilCERT: Military (katonai) CERT.

[33] CSIRT – Computer Security Incident Response Team, magyarul számítógépbiztonsági incidenskezelő csapat.

[34] A CERT és a CSIRT tartalmilag nagyjából megegyező fogalmak, így akár szinonimaként is használhatók. Megjegyzendő, hogy a CERT rövidítés intézmény nevében történő használata engedélyhez kötött, mivel az a Carnegie Mellon Egyetem bejegyzett védjegye 1997 óta. Az engedélyezéshez a szervezet megfelelőségét (is) kell igazolni.

[35] Kritikus infrastruktúrák védelmében számos egyéb szervezet vesz részt, amelyeket egy következő tanulmányunkban fogunk bemutatni.

[36] Ilyen például a világméretű erőegyensúly fenntartása, világűr mint hadviselési színtér, rakétavédelem – műveleti képesség szinten is.

[37] A magyarországi állami CERT-feladatait (GovCERT) is a Nemzeti Kibervédelmi Intézet mint eseménykezelő központ látja el.

- Magyar Honvédség Parancsnoksága Kibervédelmi Szemlélőség;
- Polgári és katonai nemzetbiztonsági szolgálatok,[38] hírszerzési és elhárítási kapacitásukban.

Legalább ennyire fontosak az akkreditált kiberbiztonsági oktatásokat biztosító felsőfokú tanintézmények, valamint a 2019-ben megalakult Magyar Honvédség Parancsnoksága Kiber Képzési Központja [37].

Léteznek még a Belügyminisztérium alárendeltségében működő további szervezetek,[39] amelyek Magyarország kibertéri tevékenységében részt vállalnak, ám ilyen tárgyú pontos tevékenységi körükről nyílt információ gyakorlatilag nem áll rendelkezésre.

Természetesen Magyarországon is működnek különböző, nem állami CERT-ek, ilyen például a hazai internetszolgáltatók megbízásából és támogatásával létrejött HU-CERT-ISZT, amit a Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutatóintézete (MTA-SZTAKI) működtet.

Ugyanígy találunk hazánkban gazdasági társaság által üzemeltetett biztonsági műveleti központokat (Security Operations Center – SOC), amelyek szolgáltatásait bármilyen gazdasági szereplő igénybe veheti. Magyar gazdasági társaság természetesen külföldi magán SOC/CERT/CSIRT-et is használhat – és fordítva.[40]

Bizonyos önálló szervezetek létrehozása (amelyek az Egyesült Államokban léteznek) Magyarországon indokolatlan lehetne, de összeurópai kérdésként vizsgálva a szervezetek létjogosultságát más eredményre jutunk. Az európai országok rendkívül sok szálon való összekapcsoltsága alapvetően indokolna olyan integrált mechanizmusokat, amelyek például a kritikus infrastruktúrák védelmét látnák el. Különösen igaz ez a villamosenergia-ellátásra, amiben az európai országok hálózatai a gyakorlatban is, fizikailag összekapcsoltak, így egymásra utaltságuk rendkívül magas.[41]

Kibertér és a mesterséges intelligencia kapcsolata

A kibertér meghatározó jellemzői (ember által mesterségesen létrehozott adatok feldolgozását, továbbítását végzi, hálózatba kapcsolat eszközökkel működik) alapján a mesterséges intelligencia (MI) értelmezési (üzemi) tartománya a kibertér.[42] Vagyis az MI fogalma csak a kibertér összefüggéseiben értelmezhető. Ugyanígy, ma a kibertér nincs MI nélkül. Ezért ezekben a kapcsolatokban is kezelni kell a kibertér összes kockázatát, ám léteznek olyan kiemelt kockázatok is, amelyek az MI-re különösen érvényesek.

[38] Alkotmányvédelmi Hivatal, Információs Hivatal, Katonai Nemzetbiztonsági Szolgálat, Nemzetbiztonsági Szakszolgálat, Terrorelhárítási Információs és Bűnügyi Elemző Központ.

[39] Ilyen szervezet többek között a Terrorelhárítási Központ (TEK).

[40] A CERT/CSIRT/SOC feladatrendszerek rendkívül összetettek és szerteágazók, amelyek bemutatása – terjedelmi korlátok miatt – jelen tanulmányban nem lehetséges.

[41] A felvetett problémák részletes vizsgálatát a szerző egy következő tanulmányában végezte, ami egyelőre kéziratként elérhető csak.

[42] Ugyanez igaz fordítva is, ma már nem lehet a kibertérről úgy beszélni, hogy annak kapcsán a mesterséges intelligenciáról ne essen szó.

A gépi tanulási folyamatokban kritikus, hogy a források manipulálhatósága megakadályozható legyen – másként fogalmazva e források hitelesek (és kiegyensúlyozottak) maradjanak. Ugyanennyire fontos, hogy a döntési mechanizmusok (algoritmusok) felügyelhetők legyenek, és különösen védettek maradjanak illetéktelen módosításoktól.

Jó példája volt e problémának 2016-ban, a Microsoft által fejlesztett, Tay nevű MI-alapú csevegőalkalmazás (chat-bot), amely a készítői általi (egyébként szórakoztatónak szánt) szociológiai kísérletnek indult [38]. Az alkalmazás egy 19 éves fiatal stílusát kellett volna felvegye, ám ennek keretében nagyon hamar rendkívül rasszista és uszító üzeneteket kezdett küldeni. A Tayjel kommunikálók hamar rájöttek, hogy miként lehetséges a tanítása és elirányították olyan internetes tartalmakra, amelyekből e kirívóan szélsőséges ismereteket szerezte. A gyártó – komoly közösségi felháborodást követően – az indulástól számított kevesebb mint 24 órát követően lekapcsolta Tayt [39].

Ugyanígy rendkívül magas lehet egy hangfelismerő és diktáló rendszer manipulálhatóságának kockázata is. Maga a szoftver az adott (beléptetett) felhasználó hangját ismeri fel és írja le egy alkalmazás szövegmezőjébe. Amennyiben nem a szokásos felhasználó diktál az alkalmazásnak, a felismerés elkezd torzulni és néhány óra múlva az eredeti felhasználó hangfelismerése elkezd hibázni. Kritikus esetben annyira torzulhat az eredeti felhasználó adaptációja, hogy annak törlése válik szükségessé.[43] Ugyanezen rendszer hangadaptáció fájlja, ami a felismerési szótárat tartalmazza, támadható, vagyis benne például „bal" szó „jobb"-ra módosítható, ami egy orvosi alkalmazásnál rendkívül komoly problémát jelenthet. Ilyenkor a rendszer a „bal" szót felismeri, majd a szótárnak megfelelően leírja, hogy „jobb".

Az előbbi példa nagyon elgondolkodtató, ha figyelembe vesszük, hogy a személyi asszisztens funkciót betöltő alkalmazást futtató eszközök 2021-re várható száma eléri majd a 7,5 milliárdot, vagyis átlagban a föld minden lakosára fog jutni egy ilyen eszköz [40]. További kockázatot jelent, hogy leszámítva a csak a kínai belföldi piacon elérhető hasonló alkalmazásokat, e fenti értéken öt gyártó osztozik: Apple Siri, Google Assistant, Microsoft Cortana, Amazon Alexa, Samsung Bixby.[44]

Az MI terjedése szinte exponenciális, mivel az egyre alapvetőbb infokommunikációs eszközöknek is része lett, már hardveres szinten. Térfigyelő kamerák esetében például az MI elsődleges feldolgozás a kamerában megtörténik, ami néhány évvel ezelőtt még csak a szerveroldalon tudott megvalósulni a magas processzorteljesítmény-igény miatt. Többek között ez a technológiai lépés teszi lehetővé az arcfelismerő technológiák (rendszerek) tömeges terjedését is.

Ugyanígy megjelenik az MI a legújabb prémium okostelefonokban, ahol például a fényképezést végzi úgy, hogy akár 8 képet készít gyors egymásutánban a valós exponálás előtt és azokból vágja össze a végleges, legjobbnak ítélt verziót – ami adott esetben a valóságban soha nem létezett, hiszen montázsról van szó [41].

Az MI leginkább látványos és szinte bárki által elérhető megjelenése az úgynevezett „deepfake"-technológia, ami egy létező személy néhány fényképfelvételéből képes egy a felhasználó által elmondott szöveget az adott személyre montírozni, aminek

[43] A szerző saját tapasztalatából származó üzemeltetési példa.
[44] Forrás ugyanott.

eredményeként egy szabadon választott személlyel elmondatható bármilyen szöveg. E szoftvereknek létezik amatőr verziója, ami egy okostelefonra letölthető, korlátozott karakterekkel és alap videókkal működik, így viszonylag észrevehető a hamissága [42]. Megtalálható ennek a professzionális megoldása is még 2017-ből, a Washington Állami Egyetem tudományos kutatásából és fejlesztéséből [43]. Az ilyen minőségű videók hitelességét sokszor már csak másodlagos eszközökkel vagy indirekt módon lehet megállapítani.[45]

A fenti példák jól mutatják, hogy az MI-képességek rendkívül komoly és új kockázatokat hoztak a kibertéri műveleti lehetőségekben, amely veszélyek kezelésére jelenleg csak nagyon korlátozottan vagyunk képesek.

Összefoglalás, következtetések

A fejlett információs társadalmakban egy ország vagy szövetségi rendszer mára egyik legfontosabb pillére a kibertér mint tartomány. E pillér jelentős sérülése automatikusan és szinte azonnal hozza magával az adott ország vagy rendszer gazdaságának sérülését is, aminek késedelem nélkül, a gazdasági kárral arányos politikai következményei is lesznek.

Ahogy az állami rendszerek és kritikus infrastruktúrák támadása indirekt módon hat a lakosságra, úgy az MI alkalmazásának növekedése ugyanerre direkt hatással lehet, hiszen olyan rendkívüli manipulációs képességet ad eszközként, ami széles elérhetőségben néhány éve még nem létezett. Ez az elérhetőség jelenti a valós kockázatot, hiszen olyan csoportoknak is hozzáférést biztosít, akik az elérhető nyereséghez képest, azt csekély befektetéssel és célzott eszközként tudják használni. Amikor mindez a technológia állami támogatással (is) bíró szervezetek alkalmazási tárházába kerül, akkor a kibertéri kockázatok magasabb dimenzióba lépnek.

A kibertér – az eddigi tapasztalatok alapján – vélhetően ugyanazt az evolúciós vonalat fogja bejárni, mint az összes többi katonai tartomány (szárazföld, tenger/víz, levegő, űr) hiszen az aktuálisan rendelkezésre álló legfejlettebb technológiát fogja alkalmazni a saját területén. Amiben szinte biztosan el fog térni, az a fejlődés üteme és a jelentős állomások között eltelt idő exponenciális csökkenése lesz.

Akár az MI különböző szolgáltatásai kapcsán, akár a kritikus infrastruktúráktól (különösen a villamosenergia-szolgáltatást végző infrastruktúráktól), különösen az adatátvitelt és az online tartalmat biztosító kritikus információs infrastruktúráktól való függésünk miatt, az ezeken keresztül igénybe vett szolgáltatások növekedésével a kibertéri eseményekkel szembeni kitettségünk ugyanúgy növekszik.

Csak rövid pillanatokra lehetséges párhuzamos világok létrehozása, ahol az egyik világban a kibertér részei vagyunk, de egy másikban ugyanaz nincs ránk hatással. A következő pillanatban ugyanis a sok-sok szálból néhány azonnal megjelenik ismét és emlékeztet arra, hogy a társadalom részeként e kapcsolatunk a kibertérrel erősebb, mint korábban volt – sokszor akaratunk ellenére is.

[45] Például egyéb bizonyítékokkal kizárható, hogy az adott személy a kérdéses időpontban a videón láthatókat elmondta, mert ugyanakkor máshol volt és mást csinált.

Hivatkozások

[1] Zs. Haig, *Információs műveletek a kibertérben*. Budapest: Dialóg Campus Kiadó, 2018.

[2] S. Munk, „A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései", *Hadtudomány,* 28. évf. 1. sz., pp. 113–131, 2018. DOI: https://doi.org/10.17047/HADTUD.2018.28.1.113

[3] T. Maurer and R. Morgus, "Compilation of Existing Cybersecurity and Information Security Related Definitions," New America, Report, Oct. 2014.

[4] Zs. Haig és L. Kovács, „Fenyegetések a cybertérből," *Nemzet és Biztonság,* 1. évf. 5. sz., pp. 61–69, 2008.

[5] J. Hruska, "IBM Preps 53-Qubit Quantum Computer for Launch in October – ExtremeTech," 20 Sept. 2019. [Online]. Elérhető: www.extremetech.com/computing/298719-ibm-preps-53-qubit-quantum-computer-for-launch-in-october (Letöltve: 2019. 09. 22.)

[6] G. Guglielmi, "Brain signals translated into speech using artificial intelligence," Nature.com, 24 Apr. 2019. [Online]. DOI: https://doi.org/10.1038/d41586-019-01328-x

[7] R. Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," NATO CCD CoE, [Online]. Elérhető: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (Letöltve: 2019. 09. 22.)

[8] P. Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review,* no. 6, pp. 63–68, 2011.

[9] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", wired.com, 2018. [Online]. Elérhető: www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (Letöltve: 2018. 11. 20.)

[10] I. Szendy, „A hadviselés, mint tudományelméleti és tudomány-rendszertani kategória," *Hadtudomány*, 27. évf. 3–4. sz., pp. 106–129, 2017.

[11] Israeli Defense Forces, "CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work," 2019. [Online]. Elérhető: https://twitter.com/IDF/status/1125066395010699264 (Letöltve: 2019. 09. 13.)

[12] S. L. Garfinkel, "Digital forensics research: The next 10 years," Digital Investigation, vol. 7, pp. S64–S73, 2010. DOI: https://doi.org/10.1016/j.diin.2010.05.009

[13] M. N. Schmitt ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press, 2013. DOI: https://doi.org/10.1017/CBO9781139169288

[14] M. N. Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press, 2017. DOI: https://doi.org/10.1017/9781316822524

[15] C. DeVore, "The problem with North Korea is China," *Washington Examiner,* 14 Aug. 2017. [Online]. Elérhető: www.washingtonexaminer.com/the-problem-with-north-korea-is-china (Letöltve: 2019. 09. 18.)

[16] J. Chin, "Cyber Sleuths Track Hacker to China's Military," *Wall Street Journal,* 23 Sept. 2015.
[17] F-P. van der Putten, M. Meijnders, S. van der Meer és T. van der Togt ed., "Hybrid Conflict: The Roles of Russia, North Korea and China," Report of Dutch National Network of Safety and Security Analysts, Clingendael Institute, 2018.
[18] C. Hopping és D. Walker, "NHS ransomware: UK government says it's North Korea's fault WannaCry happened," *ITPRO,* [Online]. Elérhető: www.itpro.co.uk/security/28648/nhs-ransomware-attack (Letöltve: 2019. 09. 18.)
[19] C. Cimpanu, "How US authorities tracked down the North Korean hacker behind WannaCry," *ZDNet,* 2018. [Online]. Elérhető: www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/ (Letöltve: 2019. 09. 18.)
[20] The Mitre Corporation, "Groups," *The Mitre Corporation,* 24 Sept. 2019. [Online]. Elérhető: https://attack.mitre.org/groups/ (Letöltve: 2019. 09. 18.)
[21] BBC News, " Saudi Arabia oil and gas production reduced by drone strikes," *BBC News,* 14 Sept. 2019. [Online]. Elérhető: www.bbc.com/news/world-middle-east-49703143 (Letöltve: 2019. 09. 18.)
[22] K. Kralovánszky, „Elektronikus határvédelmi rendszerek jellemző sebezhetőségei és védelmük lehetőségei," *Hadmérnök,* 14. évf. 1. sz., p. 12, 2019.
[23] S. Khandelwal, "Israeli Electrical Power Grid Suffers Massive Cyber Attack," 27 Jan. 2016. [Online]. Elérhető: http://thehackernews.com/2016/01/power-grid-cyberattack.html?m=1 (Letöltve: 2019. 09. 14.)
[24] Zs. Haig, B. Hajnal, L. Kovács, L. Muha és Z. Sík, *A kritikus információs infrastruktúrák meghatározásának módszertana.* Budapest: ENO Advisory Kft., 2009.
[25] B. Barrett, "An Unprecedented Cyberattack Hit US Power Utilities," Wired.com, 07 Sept. 2019. [Online]. Elérhető: www.wired.com/story/power-grid-cyberattack-facebook-phone-numbers-security-news/ (Letöltve: 2019. 09. 13.)
[26] United States Department of Energy, "Electric Disturbance Events," *United States Department of Energy.* [Online]. Elérhető: www.oe.netl.doe.gov/download.aspx?type=OE417PDF&ID=79 (Letöltve: 2019. 09. 15.)
[27] U.S. Cyber Command, "Command History," [Online]. Elérhető: www.cybercom.mil/About/History/ (Letöltve: 2019. 09. 15.)
[28] L. Brent, "NATO's role in cyberspace," *NATO Review,* 2019. [Online]. Elérhető: www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm (Letöltve: 2019. 09. 15.)
[29] NATO, "Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales," *NATO*, 05 Sept. 2014. [Online]. Elérhető: www.nato.int/cps/en/natohq/official_texts_112964.htm (Letöltve: 2019. 09. 15.)
[30] L. Kovács, *Kiberbiztonság és stratégia.* Budapest: Dialóg Campus Kiadó, 2018.
[31] D.B. Johnson, "DHS grapples with cyber enforcement," *FCW*, 12 Mar. 2019. [Online]. Elérhető: https://fcw.com/articles/2019/03/12/dhs-bod-conundrum-johnson.aspx (Letöltve: 2019. 09. 22.)

[32] S. Hazlegreaves, "Strengthening cybersecurity in the U.S.," *Open Access Government,* 10 Jul. 2019. [Online]. Elérhető: www.openaccessgovernment.org/strengthening-cybersecurity/68873/ (Letöltve: 2019. 09. 22.)
[33] C. Wray, "The Way Forward: Working Together to Tackle Cybercrime," *Federal Bureau of Investigation,* 25 Jul. 2019. [Online]. Elérhető: www.fbi.gov/news/speeches/the-way-forward-working-together-to-tackle-cybercrime (Letöltve: 2019. 09. 22.)
[34] B. Gaskew, "Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget – Third Way," Third Way. [Online]. Elérhető: www.thirdway.org/memo/readers-guide-to-understanding-the-us-cyber-enforcement-architecture-and-budget (Letöltve: 2019. 09. 22.)
[35] U. S. Department of Homeland Security, "Cybersecurity," *U. S. Department of Homeland Security,* 18 June 2012. [Online]. Elérhető: www.dhs.gov/topic/cybersecurity (Letöltve: 2019. 09. 22.)
[36] National Security Agency, "NSA-Developed Open Source Software," [Online]. Elérhető: https://code.nsa.gov/ (Letöltve: 2019. 09. 15.)
[37] Á. Draveczki-Ury, „Átadták a Magyar Honvédség Kiber Képzési Központját," Honvédelem.hu, 13. jún. 2019. [Online]. Elérhető: https://honvedelem.hu/galeriak/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat/ (Letöltve: 2019. 09. 18.)
[38] R. Metz, "Microsoft's neo-Nazi sexbot was a great lesson for makers of AI assistants," *MIT Technology Review,* 27 Mar. 2018. [Online]. Elérhető: www.technologyreview.com/s/610634/microsofts-neo-nazi-sexbot-was-a-great-lesson-for-makers-of-ai-assistants/ (Letöltve: 2019. 09. 17.)
[39] P. Mason, "The racist hijacking of Microsoft's chatbot shows how the internet teems with hate," *The Guardian,* 29 Mar. 2016.
[40] R. De Renesse, "Virtual digital assistants to overtake world population by 2021," *Ovum,* 17 May 2017. [Online]. Elérhető: https://ovum.informa.com/resources/product-content/virtual-digital-assistants-to-overtake-world-population-by-2021 (Letöltve: 2019. 09. 17.)
[41] D. Cooper, "Deep Fusion is the iPhone's take on AI photography," *Engadget,* 10 Sept. 2019. [Online]. Elérhető: www.engadget.com/2019/09/10/apple-iphone-deep-fusion/ (Letöltve: 2019. 09. 18.)
[42] J. Porter, "Another convincing deepfake app goes viral prompting immediate privacy backlash," *The Verge,* 2 Sept. 2019. [Online]. Elérhető: www.theverge.com/2019/9/2/20844338/zao-deepfake-app-movie-tv-show-face-replace-privacy-policy-concerns (Letöltve: 2019. 09. 18.)
[43] J. Langston, "Lip-syncing Obama: New tools turn audio clips into realistic video," *UW News*. 11 July. 2017. [Online]. Elérhető: www.washington.edu/news/2017/07/11/lip-syncing-obama-new-tools-turn-audio-clips-into-realistic-video/ (Letöltve: 2019. 09. 18.)