Rozmán Tímea Krisztina[1]

A JÖVŐ HÁBORÚI - MESTERSÉGES INTELLIGENCIA, DRÓNOK ÉS KIBERFEGYVEREK

Col SC Tyagi (2021): "Future wars: Artificial Intelligence, drones and cyber weapons" (Financial Express, 2021. július 8.)

Az elmúlt pár év történései alapján egyre sürgetőbbé válik az a kérdés, hogy merre tart a modern hadviselés. Ha az egyik legelterjedtebb példát hozzuk fel és megnézzük Izrael Hamász elleni „Guardian of the Walls" hadműveletét, az irány elég egyértelműnek tűnik.

A tavalyi örmény-azeri konfliktus kiemelkedő eseménye, a hegyi-karabahi háború, vagy a 2021-es májusi Izrael-Hamász konfliktus példájával élve nyilvánvalóvá válik, hogy a hadviselés igencsak hosszú utat tett meg a kezdetektől. Mindkét háborúban mesterséges intelligenciát (AI), drónokat és egyéb autonóm fegyverrendszereket vetettek be a harcoló felek, nevezetesen Örményország és Izrael. Az izraeli-Hamász konfliktus alatt végrehajtott „Guardian of the Walls" hadművelet, más néven az „Első AI háború" nem véletlen kapta ezt a nevet. Ez volt az első olyan konfliktus, ahol kiterjedten használtak szuperszámítógépeket, drónokat, rakétákat és önműködő harckocsikat. Ez a művelet már nem csupán humán tevékenységen alapult, hanem az csak kiegészítője lett a mesterséges intelligencián alapuló eszközöknek. Egy, a Jerusalem Postban megjelent IDF tiszttel készített interjú során elhangzik az is, hogy a szárazföldi hadsereg vagy akár a légierő alkalmazása helyett a mesterséges intelligencia volt a kulcskomponens és az erő multiplikátora az Izraeli Védelmi Erők (IDF) számára [Ahronheim, 2021]. Ezen két példa a legjobb szemléltetés arra, hogy a hagyományos hadviselés korának régóta vége szakadt, elavulttá vált és ez meghatározó lesz a jövő háborúinak megvívása során.

A jövőt nem lehet soha pontosan megjósolni, de meg kell tenni a lehető legtöbbet annak érdekében, hogy fel tudjunk készülni a lehetséges kihívásokra. Ha elképzeljük, hogy mik lehetnek az összetevők, az biztos, hogy a mesterséges intelligencia lesz az egyik legfontosabb. Mindemellett a következő világháborúban a meglévő fegyverplatformokon kívül a kiberfegyverek, a drónok, a készenléti lőszerek, a ballisztikus rakéták és az űrbe telepített műholdak is szerepelnek majd. A háború megvívásának módjában érzékelhető változás világosan látható a horizonton. Azért, hogy ezen változásokkal fel tudjuk venni a lépést, meg kell

[1] NKE, HHK, Nemzetközi Biztonság- és Védelempolitika szakos hallgató

vizsgálni és át kell alakítani a kulcsfontosságú stratégiákat minden szektorban, de legfőképp a katonaiban. Az új dimenziók - mint a kibertér és az űr -, az új technológia és az újonnan megjelenő, eddig ismeretlen szereplők radikálisan megváltoztatják a jövő hadviselésének módját.

Az izraeli gyártmányú Harop lőszer, amelyet Azerbajdzsán használt Örményországban 2020-ban, tökéletes példája annak, hogy hagyományos fegyverek használata nélkül is lehetséges a pontos megsemmisítés, valamint annak, hogy ezek - a fizikai hatások mellett - komoly pszichés hatással vannak az ellenfélre.

Az USA a "terrorizmus elleni háború" részeként széles körben alkalmazott dróncsapásokat célpontok ellen. A legtöbben láttuk az ilyen támadásokról készült, a közösségi médiában széles körben elterjedt videókat. Az amerikaiak különösen Afganisztánban és Irakban, valamint az IDF által a regionális háborúkban elért sikerei új dimenziót adtak a háború fogalmának, és hamarosan Oroszországban, Kínában, Törökországban, Pakisztánban és Indiában is megindult a kutatás és fejlesztés, valamint az ilyen fegyverek megszerzésének vagy birtoklásának folyamata. Ezen országok egyike sem akar lemaradni a hasonló képességekért folytatott versenyben. A közelmúltban Delhiben tartott Hadsereg Napja alkalmából rendezett felvonulás bizonyította India hajlandóságát és képességeit is [Col SC Tyagi, 2021].

De ez jelentheti-e azt, hogy a hagyományos háború napjainak vége? Egyértelműen kijelenthető, hogy még nem. A harckocsik, gépesített hadosztályok és a tüzérség továbbra is nagy szerepet fog játszani, de bevetésük és szerepük különbözni fog a már megszokottól. Az ellenség háborús potenciáljának megsemmisítéséhez többféle eszközre lesz szükség, beleértve a légierőt, a haditengerészetet és az űrbe telepített rendszereket, az AI-al az élen, de mindennek fontos kelléke (továbbra is) a hírszerzés marad.

Ahogy John Naisbitt is mondta, „Az irányzatokat és a trendeket, akár csak a lovakat, könnyebb abba az irányba lovagolni, amerre maguk is haladnak". A jelenlegi trendeket látva úgy gondolják a hadtudósok és szakértők, hogy az előttünk álló háborúk kulcsfontosságú trendjei az AI, a drónok, a kiberfegyverek és a gyilkos alkalmazások (killer apps) széles körű használata, a megfigyelés világűrből történő irányítása és egy támadó képességekkel rendelkező védelmi ernyő létrehozása (Iron Dome-szerű képességek) és a halálos, autonóm robotok használata [Col SC Tyagi, 2021].

A világ gyorsan mozog, és vannak más aggasztó tendenciák is, mint például a kriptovaluta használata, ami lehetővé teszi a terroristák számára, hogy úgy utaljanak át pénzeszközöket vagy fizessenek fegyverek beszerzéséért, hogy ne legyen nyoma annak, hogy ki kinek fizetett, anélkül, hogy a jól bevált pénzügyi intézményeket, például a bankokat használnák. A világűrbe telepített műholdak és

navigációs berendezések egyszerre hasznosak és sebezhetők, és fontos szerepet fognak játszani a jövőbeli háborúban. A technológia ma már nem egyik változatról a másikra fejlődik, hanem ugrásszerűen halad előre, ahogyan azt Peter Warren Singer, egy kibernetikai szakértő nemrégiben kifejtette. A diszruptív technológiák gyorsan változtatják meg a világot. Nincs már nagyon messze az a nap, amikor egy újfajta háborús felhő borul ránk. A folyamat már elkezdődött, csak a jövő fogja megmutatni, hogy ezek közül a trendek közül melyik, és milyen mértékben fogja tovább változtatni a jövő háborúinak alakját.

1. ábra: Harop akcióban

https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3Ds1Z75jy5TGM&psig=AOvVaw0CKxN_HsaF7H7PqEv3aEJ2&ust=1632483654393000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCODmtN6FlfMCFQAAAAAdAAAAABAD

2. ábra: Iron Dome rakétaelhárítók (balra) a Gázai övezetből Izraelbe tartó Hamász-rakétákat (jobbra) lőnek ki

FELHASZNÁLT IRODALOM:

AHRONHEIM, A. (2021). *Israel's operation against Hamas was the world's first AI war*. The Jerusalem Post | JPost.com. https://www.jpost.com/arab-israeli-conflict/gaza-news/guardian-of-the-walls-the-first-ai-war-669371

Col ST Tyagi (2021). *Future wars: Artificial Intelligence, drones and cyber weapons*. The Financial Express. https://www.financialexpress.com/defence/future-wars-artificial-intelligence-drones-and-cyber-weapons/2286333/?fbclid=IwAR2mgE5FkgaQ77NAH2rPkVL_GSrIIlojQx1ZxXaGVBOjGgmirjYNoAwExNA

KATZ, Y. (2021). *Israel's Gaza war is like no other military operation in history*. The Jerusalem Post | JPost.com. https://www.jpost.com/opinion/israels-gaza-operation-is-like-no-other-military-op-in-history-opinion-668709

Málits Tamás[2]

KIBERFEGYVEREK: AZ EGYRE ÉGETŐBB VIRTUÁLIS HADSZÍNTÉR

Sanger, David E. (2021): „Once, superpower summits were about nukes; now, it's cyberweapons". (The New York Times, 2021. június 16.)

A második világháború óta, azaz immár több mint hét évtizede az amerikai elnökök és a szovjet, majd később az orosz vezetők közötti, változó rendszerességű csúcstalálkozókon egyetlen állandó téma folyamatosan napirendre került. A két szuperhatalom nukleáris arzenálja folyamatosan magában hordozta az elrettentés szükségességét, illetve a kölcsönös megsemmisítés (MAD – mutually assured destruction) veszélyét, ami az államfők számára is folyamatos beszédtémát jelentett.

Bár a nukleáris fegyverek jelentősége a 21. században sem elhanyagolható, az elmúlt évtizedben – javarészt az egyre gyakoribb alkalmazásuk miatt – a kiberfegyverek kérdése is a napirend legfontosabb elemei közé került. A téma Joe Biden amerikai elnök és Vlagyimir Putyin orosz elnök 2021. júniusi, genfi csúcstalálkozóján is kiemelt szerepet játszott, nem kis részben az egy hónappal korábbi, a Colonial Pipeline csővezetéket érintő támadás miatt [Helmore & Greve, 2021].

David E. Sanger összefoglalója, amely a *New York Times* hasábjain jelent meg a genfi Biden-Putyin csúcstalálkozó előestéjén, kontextusba helyezi azt a három fontos különbséget, amelyek miatt a kiberhadszíntér még a nukleáris veszéllyel hosszú ideje együtt élő amerikai politikai és katonai vezetés számára is újfajta kihívásokat jelent – ezek pedig új megközelítéseket is igényelnek.

Ezen különbségek közül az első, hogy a virtuális hadszíntér szereplői jóval sokszínűbbek: a nemzetállamok mellett hacker- és egyéb csoportok, valamint terrorista szervezetek is képesek bármikor támadást indítani egy állam létfontosságú infrastruktúrája ellen. A szereplők közötti elmosódó határok azt is jelentik, hogy manapság nem lehet tudni, ki indítja a támadást, és kinek a parancsára. A Colonial Pipeline elleni támadásért az amerikai hatóságok az orosz hátterű DarkSide csoport zsarolóvírusát tették felelőssé. A 2020 végén nyilvánosságra került, a többek között a SolarWinds ellátási láncát megbénító, illetve amerikai kormányzati szerverekbe is beférkőző kibertámadást szintén orosz csoportok hajthatták végre, melyeket a Biden-adminisztráció szerint az orosz

[2] Hallgató, KU Leuven, Gyakorlati Diplomácia Szakkollégiuma

kormány is támogat, de legalábbis szabad működést engedélyez nekik. Az orosz elnök mindeközben tagadja, hogy kiberfegyvereket használna az Egyesült Államok ellen, és amerikai dezinformációs kampányt emleget.

A második fontos különbség, hogy a kiberfegyverek – a rakétákkal és a robbanófejekkel ellentétben – nem számszerűsíthetők, és nem jelentenek látványos fenyegetést, amíg nem alkalmazzák őket. A Reagan elnök által a nukleáris leszerelési szerződések kapcsán megfogalmazott *„trust but verify"* elve emiatt nem alkalmazható a kiberfegyverekkel összefüggésben – bármilyen „leszerelési" kísérlet a kibertérben nem lenne ellenőrizhető.

A Sanger által azonosított harmadik jelentős különbség a következményekben rejlik. A már említett MAD-doktrína értelmében a nukleáris hadszíntéren mindenki számára egyértelmű, mi történik azzal az országgal, mely atomfegyvert vetne be az USA ellen. A kibertérben az eddigi tapasztalatok mást mutatnak. A Sony Entertainment filmstúdió ellen elkövetett észak-koreai kibertámadás a cég számítógépeinek jelentős részét megsemmisítette, mégis jelentős amerikai válaszcsapás nélkül maradt; a 2016-os amerikai elnökválasztásba történő orosz beavatkozás is viszonylag enyhe szankciókat, néhány diplomata kiutasítását vonta maga után. A SolarWinds-támadást követően Biden arányos választ ígért, amely főként gazdasági szankciókat jelentett – kérdés, hogy ezek milyen mértékben ösztönzik az orosz kormányt arra, hogy belföldön fellépjen a támadásokat feltételezhetően elkövető hackercsoportok ellen. A cikkben megszólaló Eric Rosenbach, a védelmi minisztérium korábbi kiberpolitikai vezetője szerint van esély arra, hogy a gazdasági szankciók egy apró lépést jelentenek a jó irányba.

Ahogyan Sanger írása előrevetítette, a genfi csúcstalálkozón a két elnök valóban mélységében érintette a kiberbiztonság témáját. Biden a találkozó utáni sajtótájékoztatón elmondta, egy 16 kritikus infrastrukturális elemből álló listát nyújtott át orosz kollégájának, melyek bármilyen módon történő megtámadása átlépne egy határt [White House, 2021]. Emellett kilátásba helyezte, hogy az említett létesítmények elleni kibertámadásra az Egyesült Államok is a kibertérben válaszolna.

2017 nyarán Ukrajna tapasztalta meg a világ eddigi talán legnagyobb, nemzetállam ellen elkövetett kibertámadását; elsötétültek a képernyők, leálltak az internetes rendszerek, nem működtek az ATM-ek. Az okozott károk – melyeket mintegy 10 milliárd dollárra becsülnek – azonban sokkal nagyobbak is lehettek volna [Perlroth, 2021]. Afelől nem lehet kétségünk, hogy a kiberfegyverek jelentős pusztítást képesek okozni. A kérdés, hogy sikerül-e megegyezni használatuk korlátozásáról, akár egy „digitális genfi egyezmény" létrehozásával. Sanger szerint ez azonban nem reális – Putyin számára ugyanis jelenleg az egyetlen szuperfegyver a zavarkeltés demokratikus riválisainak rendszereiben.

FELHASZNÁLT IRODALOM

Helmore, E. & Greve, J. E. (2021): Biden says 'no evidence' Russia involved in US pipeline hack but Putin should act. *The Guardian*, 2021. május 10. Elérhető: https://www.theguardian.com/us-news/2021/may/10/colonial-pipeline-shutdown-us-darkside-message (Letöltés dátuma: 2021. 09. 20.)

Perlroth, N. (2021): *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race.* New York: Bloomsbury Publishing.

White House (2021): *Remarks by President Biden in Press Conference*, 2021. június 16. Elérhető: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/06/16/remarks-by-president-biden-in-press-conference-4/ (Letöltés dátuma: 2021. 09. 20.)

Hordós Alex[3]

NINCS MÉG A KÜSZÖBÖN A NEMZETKÖZI KIBERVÉDELMI MEGÁLLAPODÁS

Scott Neuman – Greg Myre: Hacks Are Prompting Calls For A Cyber Agreement, But Reaching One Would Be Tough)

2021 nyarán két zsarolóvírusos támadás érte az Amerikai Egyesült Államokat: májusban a Colonial nevű kőolajvezetéket, míg júliusban a JBS húsipari vállalat gyárát támadták meg ismeretlen hátterű hackerek. Az esetek a biztonságpolitikai megfontolásokkal összhangban egy nagyon is aktuális kérdést vetettek fel: miként lehetne szabályozni a nemzetközi kibertechnológia felhasználását?

A jelenleg hatályos nemzetközi jogi instrumentumok közül az Európa Tanács keretében tető alá hozott Budapesti Egyezmény (Egyezmény a Számítástechnikai Bűnözésről) az, ami a kibervédelem és a kiberbűnözés elleni küzdelem nemzetközi rezsimjének elsődleges (és a mai napig egyetlen) multilaterális normája. A szerződésnek tagja az Egyesült Államok, az európai kontinens zöme, valamint néhány másik állam különböző kontinensekről. Hátránya viszont a szerződésnek, hogy a kiberhadviselésben aktív nemzetközi szereplők, így Kína, Irán, Észak-Korea vagy éppen Oroszország nem tagja a megállapodásnak.

Oroszország pedig éppen az az állam, amelyet a nyári támadásokkal összefüggésbe hoztak: a Nemzetbiztonsági Ügynökség (*National Secuity Agency*, *NSA*) állítása szerint Moszkva több ízben támadja kormányzati és magánszemélyek eszközeit. Június közepén Genfben találkozott az év elején beiktatott Joe Biden Vladimir Putin orosz elnökkel, ahol kiemelte, hogy az Egyesült Államok nem fogja válasz nélkül hagyni a kibertámadásokat, különösen akkor, ha azok kritikusan fontos infrastruktúrát érintenek.

Az elsődleges probléma egy tényleg átfogó, nemzetközi kiberbűnözést szankcionáló szerződéssel kapcsolatosan a felek tárgyalóasztalhoz ültetése lesz. Ennek egyik oka, hogy a kibertámadások tipikus „*low-cost*, *high reward*" cselekmények, vagyis alacsony kockázat mellett lehet jelentős eredményt elérni velük. A nemzetközi politikában a geopolitikai-hatalmi pozíciókat javíthatják ezek a kibertámadások, mivel a katonai, hírszerzési és egyéb, az állam védelme szempontjából fontos apparátusok digitális szegmensének meggyengítésére alkalmasak. Az NSA korábbi munkatársa, April Falcon Doss szerint a szerződés betartásának monitorozása is kihívásokat jelentene: míg a nukleáris

[3] Jogászhallgató, ELTE ÁJK, 2020-ban nemzetközi tanulmányok alapszakon végzett a BCE-n.

fegyverzetkorlátozó szerződéseknél a kapacitáscsökkentést, a töltetek megsemmisítését és a gyártási folyamatokat jól lehet ellenőrizni, addig a számítógépes kódok előállítását „nem lehet látható módon ellenőrizni".

Klasszikus problémája a 21. századnak az is, hogy a nem állami szereplők megállítása akkor is próbatétel marad, ha az államok meg tudnak állapodni a kiberbiztonsági rezsim játékszabályaiban. A bevezetőben említett támadásokat is oroszországi bűnszervezetekre fogták, nem pedig az orosz kormányzatra. Ebben az összefüggésben is megjelenik a nemzetközi jog problematikája, nevezetesen a betudhatóság (*attributability*), vagyis az, hogy mennyiben felelős az állam a saját állampolgárai által, saját területén elkövetett nemzetközi jogi jogsértésekért (valamint, hogy az államnak volt-e effektív befolyása az adott tevékenységre). Glenn Altschulter professzor szerint ezen faktorok beazonosítása is hatványozottan nehezebb, mivel a támadók el tudják fedni lokációjukat a valós IP-cím elrejtésével. Altschulter és Robert G. Papp, a Center for Cyber Intelligence at the Central Intelligence Agency volt igazgatója is azon az álláspontón van, hogy legalább bilaterális szinten meg kell próbálni megállapodni Oroszországgal a kiberbűnözés területén.

A kibertérben végzett káros tevékenységek, bár nem kézzelfoghatók, megfelelő mértékben nagyon is valós, fizikai károkat tudnak okozni. A helyzet kezelése ezért is egyre égetőbb, mivel a globalizált, internet-dependens világunkban a digitális hálózatok elleni rosszindulatú támadások emberéletekbe is kerülhetnek. A genfi Biden-Putyin csúcson, bár szerződéses megállapodásról nem esett szó, a két fél ígéretet tett a párbeszédre, amely kapcsán megindulhat azon alapvető normák formálódása, amely keretek közt tartja a (virtuális térben egyébként nehezen értelmezhető) határokon átívelő kiberbűnözést.

Szekeres-Kovács Veronika[4]

AZ AMERIKAI HADSEREG KIBERPARANCSNOKSÁGÁNAK KAPACITÁSAIRÓL ÉS PARTNERI KAPCSOLATÁRÓL

Roche, William (2021): Army Cyber Command Leaders Discuss Capabilities, Partnership with Commander of U.S. Cyber Command. cybercom.mil, U.S. Army Cyber Command.

https://www.cybercom.mil/Media/News/Article/2695966/army-cyber-command-leaders-discuss-capabilities-partnership-with-commander-of-u/ (Letöltés ideje: 2021. 09. 30.)

Az Amerikai Egyesült Államok hadseregének Kiberparancsnoksága (ARCYBER[5]) Paul Nakasone tábornokot, a Védelmi Minisztérium (Pentagon) Kiberparancsnokságának (USCYBERCOM[6]) vezetőjét, a Nemzetbiztonsági Ügynökség főigazgatóját és a Központi Biztonsági Szolgálat vezetőjét fogadta július 14-én Fort Gordonban, a hadsereg Georgia állambeli főhadiszállásán.

Nakasone megtekintette az ARCBYER létesítményeit, illetve a parancsnokság kapacitásairól szóló eligazításokon vett részt. A megbeszélések egyik tárgya az volt, hogy miként segítik ezek az egységek és a USCYBERCOM-mal való partneri kapcsolatuk az amerikai fegyveres erők hadműveleteit, gyakorlatait.

Az ARCYBER parancsnoka, Stephen Fogarty hadnagy kiemelte, hogy a parancsnokság beépíti ezeket a törekvéseket küldetései prioritásai közé a hálózatok adatainak és fegyverrendszereinek működtetése és védelme érdekében, továbbá a kiberhatások bevetésére, illetve az információs hadműveletek vezénylésére. Az integrálásnak köszönhetően az ARCYBER képes érzékelni, érteni és folyamatosan felmérni a kiberteret, emellett az információs dimenziót is, ami lehetővé teszi a műveleti parancsnokok számára az információfölény és a döntési dominancia fenntartását.

Az ARCYBER kiberhaderőt is biztosít az Egyesült Államok Központi Parancsnokságának, ezzel hozzásegítve a fegyveres erőket ahhoz, hogy teljesítsék működési és stratégiai céljaikat a kibertérben.

---

[4] Gyakorlati Diplomácia Szakkollégiuma, a Budapesti Corvinus Egyetem nemzetközi tanulmányok szakos hallgatója

[5] Army Cyber Command

[6] A 2010-ben megalakított U.S. Cyber Command „központosította a védelmi és támadó kibertéri műveletek vezetését és irányítását, valamint a végrehajtó szervezeteket." [Haig, 2018:281]

A Nakasone által látogatott eligazításokon az ARCYBER központjának, illetve főbb alárendelt egységeinek[7] magas rangú vezetői és szakértői vettek részt, ami szintén jelezte az ARCYBER támogatását a USCYBERCOM és a fegyveres erők parancsnokai felé.

A megbeszélések fő fókusza azokon az ARCYBER egységek által biztosított kapacitásokon és szakértelmen volt, amelyekkel a parancsnok indiai-csendes-óceáni hadszíntéren jelenleg zajló, „Defender Pacific" gyakorlatra kidolgozott műveleti tervét támogatták. A rendelkezésre bocsátott kapacitások magukba foglalják

- a hírszerzési források áramlását és támogatását,
- a hálózati és adatokkal való műveleteket,
- a kibervédelmi egységeket és offenzív kiberhadműveletek végrehajtását,
- a kiber-elektromágneses aktivitást vizsgáló expedíciós erők kivezénylését ellenintézkedésekhez és a gyors mozgósításhoz,
- tájékoztató és befolyásoló tevékenységek megszervezését a nemzetközi közönségnek,
- illetve ezen kapacitások egységesítésében a korábbi tapasztalatokat felhasználva a műveleti támogatás lehetővé tételét és erősítését.

FELHASZNÁLT IRODALOM:

Haig, Zsolt (2018): *Információs műveletek a kibertérben*. Dialóg Campus Kiadó, Budapest.

[7] Joint Force Headquarters-Cyber, the Network Enterprise Technology Command, 1st Information Operations Command, the 915th Cyberspace Warfare Battalion, the Army Cyber Protection Brigade

Rimóczi Martin[8]

DÉL-KOREA A VIRTUÁLIS VALÓSÁGOT ÁLLÍTJA A NÖVEKEDÉSI POTENCIÁLOK KÖZÉPPONTJÁBA

Arirang News (2016): Korean startup releases VR simulators for military training https://www.youtube.com/watch?app=desktop&v=Et5BsV0U1Lw

Míg a virtuális valóság különböző formái gyorsan barátságos fogalmakká válnak a hétköznapi emberek számára – többek között ilyenek a legmodernebb szórakoztatóeszközök -, addig a többi területen dolgozók is felismerik e technológia nagy lehetőségeit és alkalmazási potenciáljait. Többek között ilyen terület a katonai kiképzés is.

A harci gyakorlatok sokszor kockázatosak és veszélyesek, de a virtuális valóság korában nem kell, hogy azok legyenek. Erre példa a "virtual shooting combat", ami egy katonai kiképzés VR-szimulációja egy túszmentési helyzetben. Ez az egyik legélethűbb szimuláció, amelynek prototípusát várhatóan katonák is használni fogják. A készüléket robot futópaddal és mozgásrögzítő érzékelőkkel szerelték fel, amelyek a felhasználók cipőibe ágyaztak, valamint egy 2.7 kilogramm súlyú M4-es modellel.

Ez a hagyományos képernyőalapú szimulátorok továbbfejlesztett változata, annyiban különbözik tőlük, hogy kiváló minőségű VR-headseteket vagy fejre szerelt kijelzőket használ. A "küldetés" végén a felhasználók teljesítményét értékelik a leadott lövések száma, az időzítés, a csapattársakkal való koordináció és a célpontok eltalálása alapján.

A "virtual shooting combat" eszközhöz hasonlóan a vállalat "virtual parachuting" szimulációja 360 fokos videokijelzőkkel és mozgásérzékelőkkel van felszerelve, lehetővé téve a katonák számára, hogy átéljék a szabadesés érzetét, valamint ejtőernyős meghibásodás esetén kezeljék felszerelésüket – mind olyan helyzetek, amelyeket eddig nehéz volt utánozni a kockázatok miatt.

Az Optimus System nevű vállalat 3D robotszimulátorokat biztosít neves cégeknek, köztük a Hyundai Engineering and Constructionnek, továbbá a koreai technológiai óriás Samsung Electronicsnak és olyan autógyártóknak, mint a Ford és a Chrysler.

Katonai célok tekintetében a cég azt állítja, hogy a Közel-Keletre, Oroszországba, Vietnamba és a Fülöp-szigetekre kíván exportálni, miközben a szórakoztatóiparnak, többek között vidámparkoknak is biztosít technológiát Koreában és Kínában. Ennek

[8] Gyakorlati Diplomácia Szakkollégiuma, NKE-HHK, Nemzetközi Biztonság és Védelempolitika mesterszakos hallgató

érdekében reméli, hogy 2030-ig akár 3.5 milliárd dollárt is biztosíthat állami és magánberuházásokból szimulátorainak tömeggyártására.

Bár nagy a kereslet a VR-alapú eszközök iránt, a VR-vállalatok együttműködési és fejlődési hálózata és ökoszisztémája Koreában még korai, mert a vállalatok nem szívesen teszik közzé üzleti ötleteiket és fejlett technológiáikat, elsősorban a különböző technológiai fejlesztések kiszivárgásával kapcsolatos aggodalmak miatt. A kormány általi helyes irányelvek bevezetése nagy segítséget jelentene.

Az ipar ilyen igényeire válaszul a Tudományos Minisztérium, az IKT és a Future Planning a hónap elején bejelentette a fenntartható ökoszisztéma létrehozásának terveit, ahol a VR platformjai számos ágazatban alkalmazhatóak, beleértve a számítógépes játékokat, a sportot és a turizmust. Emellett remélik, hogy több mint 35 millió dollárt fektethetnek be a kezdeményezés finanszírozására.

A minisztérium 2017-től azt mondja, hogy elősegíti a VR-tartalmak alkalmazását az oktatás, az építőipar, az orvosi szolgáltatások és a kereskedelem területén. Emellett kijelölte a Digital Media City-t, a legmodernebb szórakoztatásra irányuló területet Szöul nyugati részén a VR-technológiai cégek infrastrukturális központjaként. A létesítmény egy VR vidámparknak is otthont adott és az adott év októberében tervezett első szöuli VR fesztivál helyszínéül is szolgált.

Tóth Eszter[1]

AZ USA KIBERBIZTONSÁGI FEJLESZTÉSEI VISSZAFELÉ SÜLHETNEK EL

Néhány hónappal ezelőtt az Egyesült Államok legnagyobb üzemanyagszállító vezetéke leállásra kényszerült. A Colonial Pipelinet, mely a keleti államokat látja el benzinnel, gázolajjal és repülőgépüzemanyaggal, egy zsarolóvírus támadta meg. Amennyiben ez az állapot sokáig állt volna fent, az hatalmas károkat okozott volna az USA több iparágának. A történelem során először az Egyesült Államokban egy kibertámadás következtében kellett szükségállapotot elrendelni.

Vagy hogy egy másik esetet említsek, még egy év sem telt el egy rendkívül jelentős az USA ellen irányuló kibertámadás óta. Hackerek feltörték a SolarWinds amerikai szoftvercég által kifejlesztett rendszerek kiskapuit és ezt arra használták fel, hogy megtámadjanak főbb amerikai kormányzati intézményeket; érintettek volt többek között a belbiztonság, védelmi és kereskedelmi területek.

Mindezek az események arra mutatnak rá számunkra, hogy még az Egyesült Államok, az az ország, amely a világ legkiterjedtebb és leginkább kidolgozott kiberbiztonsági rendszerével rendelkezik, sem immunis a kibertámadásokra. Mindez pedig arra enged következtetni, hogy globális szinten is hagy még kívánnivalót maga után ez a terület.

Az Egyesült Államok egyértelmű fölénnyel rendelkezik a kibertérben, ennek következtében effektív kiberbiztonsági stratégiák kidolgozása, illetve további támadó kiberfegyverek fejlesztése központi kérdés számára. Azt azonban alábecsülte, hogy mennyire nehéz ezeket az eszközöket kontrollálni, illetve a fejlesztéseket ténylegesen titokban végezni. Míg az USA célja ezekkel elsősorban az, hogy erőteljesebben tudjon fellépni többek között Kína vagy Oroszország ellen, addig nem fordított elég figyelmet a nem állami szereplőkre. Felülbecsülte a nagyon komplex támadó kiberfegyverek kifejlesztésének számára releváns előnyeit, de nem foglalkozott azzal, hogy egyidejűleg mekkora káoszt okozhatnak a globális kibertérben, amennyiben ezen fejlesztések rossz kezekbe kerülnek.

A nyitottság jegyében az amerikaiak, miután létrehozták az internetet, globálisan is elterjesztették azt. Azonban a 21. századra az internethasználatra és a kibertérre is átterjedt az éppen aktuális geopolitikai gondolkodás, az Egyesült Államok részéről a világ még a hidegháborús viszonyokhoz hasonló megosztása. 2017 májusában a WannaCry zsarolóvírus egyszerre a világ közel 100 országában

[1] Budapesti Corvinus Egyetem nemzetközi tanulmányok szakos hallgatója

okozott problémákat. Az EternalBlue, az eszköz, amit a hackerek ehhez használtak, mint kiderült, az USA Nemzetbiztonsági Ügynökségének kiberfegyverekkel foglalkozó osztályáról szivárgott ki. Ez is egy bizonyíték a sok közül, hogy az USA támadó kiberbiztonsági stratégiája gyakorlatilag bármely országot veszélybe sodorhatja. Egy felmérés alapján 2020-ban világszerte a szervezetek 61%-át érte támadás valamilyen zsarolóvírus által.

A Colonial Pipelinet ért kibertámadás esete, ami kapcsán szükségállapot állt be az Egyesült Államokban, nagy port kavart. Egyre több aggodalom merült fel annak kapcsán, hogy a kibertér további fejlesztése mennyire kockázatossá és veszélyessé vált. Egyre inkább realitássá válik, hogy nemzetgazdaságokat és átlagos emberek mindennapjait érintő területet ér kibertámadás. A hagyományos kiberbiztonsági rendszerek és technológiák is egyre inkább elavulnak, sőt még az Egyesült Államok kiberbiztonsági támadó és védekező modellje is nehézségekkel néz szembe. Mióta az internetet használók száma meghaladta az 5 milliárdot, egy sokkal inkább összekapcsolt és hatékonyabb globális kiberbiztonsági kormányzás kidolgozása sürgető kérdés.

A kibertérben jelen pillanatban is uralkodó káosz sokak szerinti elsődleges felelőse az Egyesült Államok támadóstratégiája. Az USA továbbra is riválisaiként festi le többek között Kínát és Oroszországot, ezáltal megosztottságot kreál a kibertérben is. Ez azért probléma, mert azáltal, hogy egyre jelentősebbé válnak nemzetközi nem állami aktorok, mint például internetes szuperplatformok vagy nemzetközi hacker szervezetek, a globális kiberbiztonságot már nem tudja az USA önmagában fenntartani.

Emellett a közhatalom és a közjavak birtokában a kormányoknak feladatuk lenne őrködni a hálózatbiztonság felett. Ennek ellenére azonban az Egyesült Államok olyannyira dominálja a kiberteret, hogy számos állam labdába se rúghat mellette, olyankor sem, amikor saját kiberbiztonságukról van szó. Ezen felül az ENSZ globális szinten kormányzó és koordináló szerepvállalását is visszautasítja ezen a területen. Ez, párosulva azzal, hogy számos a hackerek által alkalmazott eszköz is az amerikai fejlesztések révén szivárgott ki, összességében elmondható, hogy az USA több aspektusból is inkább ront, mint segít a globális kiberbiztonság helyzetén.

Már az eddigiekből is következik, hogy bármely, akár hivatalos szervek által végzett kiberbiztonsági fejlesztés globális szinten fokozza kibertámadások valószínűségét. Ezt csak akkor tudjuk meggátolni, ha kevésbé átpolitizált és megosztott a kibertér. Ha az egyes államok elköteleződnek a kibertér biztosítása mellett, akkor alakulhat csak ki egy olyan keret, ami globális szinten hatékonyabbá teszi a kiberbűnözés elleni fellépést. Ennek pedig első lépése lehet az Egyesült Államok attitűdjének megváltozása, ugyanis csak kooperációval lehet globális eredményeket elérni.

Kovács Borbála[1]

HOGYAN LEHET HATÉKONY A SZEMÉLYAZONOSÍTÁS ARCFELISMERŐ RENDSZEREKKEL, OPENCV PYTHON ÉS RASPBERRY PI ÁLTAL?

Basyal, Lochan–Karki, Bishal–Adhikari, Gaurav–Singh, Jagdeep (2018): Efficient human identification through facedetection using raspberry PI based on Python-openCV. Proceedings of WRFER International Conference, 24th June, 2018, New Delhi, India.

Az OpenCV Python alapú képfeldolgozás fogalma már korábban is elterjedt volt az arcfelismerés általi személyazonosításban. A személyazonosítás azt jelenti, hogy bizonyos személyeket az egyedi jellemzőik (ujjlenyomat, tenyér, írisz vagy arcfelépítés) alapján ismernek fel. Lochan Basyal, Bishal Karki, Gaurav Adhikari és Jagdeep Singh tanulmánya az arcfelismerő rendszerek adatbázisokba való integrálásával foglalkozik. A technológia tesztelése laptopon és Raspberry PI eszközökön történt.

Ez a folyamat három lépésből áll: elsőként egy nagyjából húsz mintából álló adatbázist kell készíteni az egyes egyénekről, amelyben OpenCV alapú arcfelismerő (face.xml) algoritmust használunk. A személyazonosítás második lépése a trainer, ami az adatbázis .YML fájlformátumúvá konvertálását jelenti. Ezt a YML fájlt lefuttatják egy detektáló parancsállományon, amely felismeri a megfelelő felhasználó arcát, amikor valós időben használjuk a fájlt. Ez alapján valós idejű képet kaphatunk a megfelelő, adatbázisba csatolt információval együtt, illetve egy ismeretlen személy esetében a rendszer illetéktelen személyről ad visszajelzést. Ez a folyamat hatékonyan alkalmazható biztonsági és védelmi projekteknél, melyekbe beépíthető egy arcfelismerő rendszer és ajtózár mechanizmus. Az alábbiakban az ehhez felhasznált technológia rövid ismertetése következik.

A **Raspberry PI** egy kisméretű számítógép, amelyet arra használtak, hogy egy olyan beágyazott rendszert fejlesszenek ki, ami adott, specifikus feladat végrehajtására képes. Ez az elektronikus modul raspbian operációs rendszerrel működik, Linux felületen.

A **PI kamera** egy olyan speciális kamera, amelyet arra terveztek, hogy Raspberry PI-hoz csatlakozzon. Általában 5 megapixeles. Ezzel a kamerával készül egy

[1] Nemzetközi tanulmányok szakos hallgató, Budapesti Corvinus Egyetem

mintakép a felhasználóról, amely egy adathalmaz-generáló mappába kerül. A Detektor.PY parancsállomány lefuttatása után megnyílik a PI kamera, hogy valós idejű képet készítsen, majd egy képmegjelenítő ablak is a releváns információval, ami az adatbázison keresztül elérhető.

Az **OpenCV** (Open Source Computer Vision) egy nyílt forráskódú könyvtár (gépi látás), amely minden programozási nyelvbe importálható, például Python, C, Java stb. Optimalizált képfeldolgozó eszközöket tartalmaz. Az OpenCV Pythonban való használata lehetővé teszi a numpy (Numerikus Python) beépítését a rendszerbe, ezáltal fokozva annak képességeit. A képeket nagy, 3D-s tömbökként dolgozza fel, és a numpy a numerikus tömbök számításának eszközeként működik. Az OpenCV, Matplot könyvtár és numpy Raspberry PI-ba való telepítéséhez használt parancsok: "sudo apt-get install python-opencv", "sudo apt-get install python matplotlib", "sudo apt-get install python-numpy". A Matplot könyvtár Pythonban való használata teszi lehetővé a grafikus ábrázolást.

Az **SQLite Studio** egy adatbázis, amelyet arra használnak, hogy egyedi sorrendben tároljanak adatokat. Az arcfelismerési folyamat során a felhasználó személyes adatainak tárolására szolgál, és azoknak a detektálási folyamat alatti előállítására. Ismeretlen személy esetén a detektáló rendszer köteles jelentést tenni. Minden újonnan regisztrált felhasználó esetében a rá vonatkozó információkat is csatolni kell az adatbázisba. Ez az adatbázis a laptoppal végzett arcfelismerés alapú személyazonosítás során volt használatban.

A **PhpMyAdmin** egy ingyenes, PHP-ban írt szoftvereszköz, ami a MySQL webes adminisztrációjáért felelős. Jelen esetben az arcfelismerés alapú személyazonosítás Raspberry PI rendszerekbe való implementálása során alkalmazták. A PhpMyAdmin Raspberry PI-ba való telepítéséhez egy két lépéses folyamatot kell követni: elsőként be kell írni a "sudo bash" parancsot, hogy megváltoztassuk a Raspberry PI-t a root felhasználón. Másodszor be kell írni az "apt-get install phpmyadmin" parancsot a PhpMyAdmin telepítéséhez és ki kell választani az „Apache2" webkiszolgálót.

Összefoglalva: a személyazonosítás arcfelismerés által, hatékony módon, PHPmyadmin használatával valósult meg, és SQLiteStudio adatbázist használtak a releváns információ tárolására. A rendszer teljesítménye három lépésen alapszik, ezek az adatbázis, trainer és a detektáló Python parancsállomány. A képfeldolgozásra használt algoritmus az OpenCV, és specifikusan az arcfelismerés esetében "Haarcascade frontal face".

A jövőben ez a projekt úgy fog módosulni, hogy alkalmas legyen magas szintű biztonsági és arcfelismerésen alapuló jelenléti rendszerekbe való implementálásra, illetve képfeldolgozáson, neurális hálózaton és mesterséges intelligencián alapuló technológiák kifejlesztésére.

Oláh Tamás Gergő[1]

A KIBERHÁBORÚ, MINT A VALÓS XXI. SZÁZADI FENYEGETÉS

Powers, John (2021): „Nuclear warfare or cyber warfare: which is the bigger threat?" (The Strategist—The Australian Strategic Policy Institute, 2021. február 24.)

A XXI. századi technológiai innovációnak köszönhetően új kihívásokkal néznek szemben a világgazdaság és a világpolitika aktorai, amelyekhez szükséges alkalmazkodniuk. A műszaki tudomány területén jelenleg is zajló folyamatos változások során olyan fogalmak nyertek új értelmet, mint a biztonság, a védelem vagy a fenyegetés. Ugyan ezek a fogalmak pár évtizeddel is jelen voltak, de a hozzájuk kapcsolódó jelentés átalakult vagy kibővült az utóbbi időben.

A második világháborút követően az Egyesült Államok és a Szovjetunió által birtokolt nukleáris fegyverarzenál jelentette a világ számára a legpusztítóbb fenyegetést. A hidegháború során a két szuperhatalom közötti konfliktus globális méretű eszkalálódását a kölcsönösen biztosított megsemmisítés (MAD) elve hiúsította meg, mivel egyik fél sem kívánta a katasztrofális hatással járó nukleáris fegyvert éles helyzetben felhasználni. Habár a bipoláris világrend végével nem tűnt el nyomtalanul az atombombák felhasználásától való félelem, a számítástechnika korának beköszöntével újfajta fenyegetéssel szembesülnek a nemzetközi közösség tagjai. Azáltal, hogy ma már a technológia, az internet és a digitalizáció az élet minden területén jelen van, egyre nagyobb kockázatnak vannak kitéve nemcsak az állami, hanem a nem állami aktorok is.

John Powers [2021] az összefoglaló cikkében arra próbál rámutatni, hogy napjainkban sokkal reálisabb veszély egy a kibertérben történő hadviselés, mint egy nukleáris háború. Annak ellenére, hogy az atomfegyverek továbbra is a valaha feltalált legpusztítóbb háborús eszközök közé tartoznak, a MAD-nek köszönhetően stabilizáló hatással is rendelkeznek, mivel a konfliktus eszkalációját túl költségessé teszik. Ezzel szemben számos olyan jelenleg is zajló konfliktus van a Földön, ahol a hadszíntér csak részben vagy egyáltalán nem konvencionális módon a harcmezőkre, hanem a kibertérre tevődött át. Manapság ahelyett, hogy az atombombák telepítésére törekednének a szereplők, a nemzeti hatalom egyéb összetevőinek, úgymint a diplomáciának, a kultúrának vagy akár a gazdaságnak a fegyverré való tétele kerül előtérbe [Lupovici, 2011]. Ezeket megtámadva kívánják

[1] Mesterszakos nemzetközi tanulmányok hallgató az Andrássy Egyetemen, 2021-ben nemzetközi tanulmányok alapszakon végzett a Budapesti Corvinus Egyetemen, Gyakorlati Diplomácia Szakkollégiumanak a tagja

destabilizálni a fennálló hatalmi rendszert és befolyásolni a társadalmat úgy, hogy az állami intézményekbe vetett bizalom meggyengüljön.

Powers Ausztrália példáján keresztül mutatja be, hogy a biztonság definiálása során egyre hangsúlyosabbá válnak az úgynevezett nem hagyományos elemek, ezek közül is kiemelkedik a kiberbiztonság. A tavalyi évben a koronavírus által okozott leállás mutatott rá arra, hogy az állami és nem állami szereplők egyre nagyobb mértékben szorulnak az internetre, valamint a számítástechnikai eszközökre. Az ausztrál kormány éppen emiatt új kiberbiztonsági stratégiát dolgozott ki, amely különválasztja a kormányt, a gazdaságot és a társadalom szereplőit érintő kibernetikai fenyegetéseket és egyesével próbál rájuk megoldást találni [Australian Government, 2020]. Ezen felül az óceániai állam Kanadával, Új-Zélanddal, az Egyesült Királysággal és az Egyesült Államokkal kiegészülve tagja az Öt Szem (*Five Eyes*) névre hallgató hírszerzési partnerségnek, amelynek keretein belül a részes országok hírszerző szervei megosztják egymással az információkat és szorosan együttműködnek egyéb biztonsági, hírszerzői és rendőri szolgálatok terén. Az ausztrál nemzetközi kiberstratégia összhangban van a másik négy angolszász országéval és egymással kooperálva készek globális válaszlépéseket megtenni a kibertámadásokkal szembeni küzdelem, elrettentés és visszatartás érdekében [Gold, 2020].

2021-ben elmondható, hogy a potenciális veszélyek közül az atomtámadás valószínűsége rendkívül alacsony, míg az információs hadviselésé magas. Ebből kifolyólag a döntéshozóknak alkalmazkodniuk kell és a mai kornak megfelelő választ kell adniuk az újfajta kihívásokkal és fenyegetettségekkel teli világban.

FELHASZNÁLT IRODALOM:

Australian Government (2020): "Australia's Cyber Security Strategy 2020". *Departement of Home Affairs*, 2020. 08. 06. Online. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf (Hozzáférés: 2021. 09. 29.)

Lupovici, Amir (2011): " Cyber Warfare and Deterrence: Trends and Challenges in Research". *Military and Strategic Affairs*, Vol. 3, No. 3, pp. 49–62.

Gold, Josh (2020): „The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'". *NATO Cooperative Cyber Defence Centre of Excellence,* 2021.02.24. Online. https://www.ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf (Hozzáférés: 2021. 09. 29.)

Powers, John (2021): "Nuclear warfare or cyber warfare: which is the bigger threat?" *The Strategist-The Australian Strategic Policy Institute*, 2021.02.24.

Online. https://www.aspistrategist.org.au/nuclear-warfare-or-cyber-warfare-which-is-the-bigger-threat/?fbclid=IwAR0MnvKvWJ95D-fZcTMGTmkbrOI8D5tBuFTSHcqpbzmoF3ot9Ye0fNiVdg8 (Hozzáférés: 2021. 09. 28.)

Szabó Ádám Zoltán[2]

BEPILLANTÁS A KIBER-FEGYVERKEZÉSI VERSENY KULISSZATITKAIBA[3]

A XXI. század digitalizációs fejlődése – felváltva a hidegháború nukleáris fegyverkezési versenyének bő négyévtizedes hagyományait – új versengési távlatokat nyitott a nemzetközi arénában. Nicole Perlothnak, a New York Times kiberbiztonsággal foglalkozó munkatársának nemrég megjelenő, „*This is How They Tell Me The World Ends*" című könyve[4] ezt az új hadszínteret, valamint az Amerikai Egyesült Államoknak ebben betöltött szerepét igyekszik bemutatni. A hidegháborút követő időszak legnagyobb befolyású nemzeti szereplőjeként – bár a mai multipolaritásban kétségtelenül mérséklődött globális befolyása – az USA megkerülhetetlen aktor a nemzetközi színtéren nemcsak katonai, de gazdasági, politikai, valamint kulturális tekintetben is. Érdekes kérdés azonban, hogy kiberbiztonság területén rendelkezik-e dominanciával, és ha igen, milyen mértékű ez a monopóliuma.

Az ország, mely 2010-ben precedenst teremtve elsőként alkalmazott digitális kártevőt egy másik országgal szemben – amikor feltételezhetően Izraellel kooperálva ártalmatlanította Irán urándúsító centrifugáit a Stuxnet féreg segítségével –, majd pedig a Microsoft szoftverének hibáját kihasználva hosszú éveken át kémkedett világszerte a külföldi rendszerekbe történő illegális belépés útján, kétségtelenül a világ egyik legjelentősebb kiberhatalmának tekinthető. Figyelembe véve azonban a kibertér sajátos mivoltát, ahol az offenzív kapacitások kiépítése jóval költséghatékonyabb a defenzívnél, ahol komoly nehézséget jelent a fenyegetettségeknek és azok forrásainak konkrét azonosítása, ahol az államokon kívül még megannyi szereplő jelen van (magánvállalatok, magányos hackerek, szervezett bűnözői csoportok, nemzetközi szervezetek), valamint ahol a szuperszámítógépeken kívül a hétköznapi használati tárgyak (okoshűtőszekrény, babatelefon) is bármikor célpontokká válhatnak, még a legfejlettebb kiberhatalmakat is súlyos sebezhetőség jellemzi.

---

[2] Budapesti Corvinus Egyetem 2021-ben mesterdiplomát szerzett hallgatója

DOI: 10.14267/RETP2022.01.03

[3] Fresh Air: *Inside The Cyber Weapons Arms Race*, National Public Radio, via: https://www.npr.org/2021/02/10/966360714/inside-the-cyber-weapons-arms-race?t=1632818768437 (letöltve: 2021.09.10.)

[4] Nicole Perloth: *This is How They Tell Me The World Ends - The Cyberweapons Arms Race*, Bloomsbury Publishing, 2021

Ahogy azt Perloth is bizonyítja, az elmúlt években több intő jel is megmutatkozott, mely alátámasztani látszik az USA vulnerabilitását, vezető szerepének halványodását. 2019-ben egy orosz hackereknek tulajdonított támadás során 18.000 entitás informatikai rendszerébe sikerült bejutni egy SolarWinds nevű szoftveren keresztül. A támadás amerikai érintettjei között tartják számon a Pentagont, az NSA-t, az Energiaügyi-, Belbiztonsági- valamint a Pénzügyminisztériumot, de a támadók feltételezhetően hozzáfértek az országos energiarendszer vészhelyzeti leállást követő újraindítási protokolljához, az ún. Black Starthoz is. Bár a jelenlegi információk alapján nem értek el bizalmas adatokat, az esetlegesen hátrahagyott és a későbbi támadásokat – vagy akár szabotázsokat – megkönnyítő „hátsó ajtók" aggodalomra adnak okot. Szintén aggasztó hírek érkeztek 2021 elején, amikor a floridai Oldsmar település vízhálózatát érte kibertámadás, melynek során hackerek próbálták a város vízének nátrium-hidroxid tartalmát radikális mértékben megnövelni, ezáltal pedig a lakosságát megmérgezni. A kísérlet ugyan kudarcot vallott, ám a jelenség mindenképpen riasztónak mondható.

Köztudott tény, hogy a különböző szoftverek programozási soraiban vétett, illegális belépésre lehetőséget adó hibák, az ún. zero day-ek nagy népszerűségnek örvendő globális feketepiaccal rendelkeznek. Ám míg az 1990-es évek jelentette kezdeti időszakban elmondható volt, hogy az Amerikai Egyesült Államok rendelkezik bizonyos kontrollal az itt gazdát cserélő biztonsági rések fölött, Nicole Perloth kutatómunkája ennek az amerikai ellenőrzésnek napjainkra történő megszűnését látszik bizonyítani. Mára 2-3 millió dollárt is érhet egy-egy felfedezett zero day, melyek értékesítésekor a legjobb ajánlattal rendelkező vevő viheti haza a kibertámadási potenciált. A legtöbb pénz pedig napjainkban már a Perzsa-öböl környékéről, az Egyesült Arab Emirátusok és Szaúd-Arábia területéről áramlik a feketekereskedelembe.

Mindezek alapján megállapítható tehát, hogy az USA elveszítette monopóliumát, potens kihívókra akadt a kibertérben folyó fegyverkezési versenyben, akik már nem egyszer sikeres támadást is indítottak ellene. Nem meglepő módon a 2021 januárjában hivatalba lépő Biden-adminisztráció a főbb prioritások közé emelte az ország kiber-rezilienciájának fejlesztését. Attól függetlenül azonban, hogy 10 milliárd dollár pluszforrást allokált a területre, valamint új pozíciókat hozott létre annak fejlesztésére, mégis egy ambivalens amerikai cselekvésminta bontakozik ki előttünk. Ez az adminisztrációkon átívelő, pártállástól független, következetes hozzáállás azt jelenti, hogy az USA egyre nagyobb kiszolgáltatottsága ellenére sem hajlandó olyan nemzetközi kiberegyezménybe belépni, mely – valamennyi részes állammal egyetemben – korlátozná a máig a legfejlettebbek közé tartozó kiberkapacitásait.

A jelen nagy kérdése, hogy mikor érkezik el az a pont, amikor az Amerikai Egyesült Államok rászánja magát, hogy egy globális nemzetközi rezsimhez csatlakozva, vagy azt tevékenyen létrehozva korlátozza saját, és valamennyi részes állam kiberkapacitásait. Amikor a hidegháborút jellemző nukleáris fegyverkezési verseny Ronald Reagan kormányzása alatt elérte zenitjét, Carl Sagan egy érzékletes analógiát használva ekképp érvelt a fegyverkorlátozási rezsim implementálása mellett: „*Képzeljünk el egy szobát, ami benzinben úszik, benne két kérlelhetetlen ellenséggel. Az egyiküknek három gyufája van, a másiknak öt. Ha a kérdés az, hogyan teremtsünk biztonságot, akkor az a válasz, hogy elvesszük a gyufákat és feltakarítjuk a benzint.*”[5] Most digitális gyufák gyűlnek a kiberszereplők kezében, kiknél a non-proliferáció is jóval komplexebb kérdés, mint az atombombák esetében. Figyelembe véve, hogy a kortárs kibertámadások a konvencionális hadviselés válfajaihoz hasonlatosan mára közvetlen emberéleteket követelnek (pl. kórházak informatikai rendszerének megbénítása, vízmérgezés stb.), egyre elkerülhetetlenebbé válik egy a kiberteret szabályzó Genfi Egyezmény életre hívása.

[5] ABC News Viewpoint - "*The Day After*" in 1983, via: https://www.youtube.com/watch?v=PdYMLq7NY_M&ab_channel=sanitykey (letöltve: 2021.09.03.)