Selján Péter[1] – Selján Gábor[2]

Kiberbiztonsági kitekintés[3]

Az információs technológiák dinamikus fejlődésével a kibertér önálló hadszíntérré vált, ahol már évek óta zajlanak az összecsapások a világ nagyhatalmai, elsősorban az Amerikai Egyesült Államok, Oroszország és Kína között. Ugyanakkor a vezető regionális hatalmi és nukleáris ambíciókkal rendelkező Irán, valamint a hozzá hasonlóan a nemzetközi közösség aggodalmát kiváltó, vitatott atomprogramot folytató és ballisztikus rakétatechnológiát fejlesztő Észak-Korea is figyelemre méltó szereplők a kibertérben. Ezen országok már évekkel ezelőtt felismerték a kiberhadviselésben rejlő lehetőségeket és várhatóan egyre több ország kezd majd ilyen irányú fejlesztésekbe, mert a lemaradásnak komoly következményei lehetnek.

Kulcsszavak: *kiberbiztonság, kiberhadviselés, információs hadviselés, információbiztonság, IT-biztonság*

Cyber Security Review

With the dynamic development of information technology, cyberspace has become an independent domain, where clashes have taken place for years between the world's great powers, primarily the United States, Russia and China. At the same time, Iran along with North Korea, which are similarly a concern for the international community with pursuing their controversial nuclear program and developing ballistic missile technology, are also notable players in cyberspace. These countries recognised the potential of cyber warfare years ago and it is expected that more and more countries will begin to develop cyber capabilities, as any delay could have serious consequences.

Keywords: *cybersecurity, cyberwarfare, information warfare, information security, IT security*

Bevezetés

Az első, 1988-ban egy amerikai egyetemi hallgató, Robert Tappan Morris által gyakorlatilag egy óvatlan tervezői hiba folytán világhírűvé vált számítógépes féreg *(computer worm)* óta egyre több állam biztonságpolitikájának lesz fontos prioritása a kiberbiztonság. Ma már a kibertér külön hadszíntérnek tekinthető, a nagyhatalmak pedig az utóbbi évtized folyamán külön a kiberbiztonság témájának szentelt stratégiai dokumentumokkal is előáll-

[1] Selján Péter a Budapesti Corvinus Egyetem Nemzetközi Kapcsolatok és Politikatudományi Doktori Iskola doktorjelöltje, okleveles biztonságpolitikai szakértő. E-mail: peter@seljan.hu

[2] Selján Gábor a Budapesti Corvinus Egyetem Közgazdasági és Gazdaságinformatikai Doktori Iskola doktori hallgatója, okleveles gazdaságinformatikus, mérnökinformatikus. E-mail: gabor@seljan.hu

[3] Jelen publikáció az Európai Unió, Magyarország és az Európai Szociális Alap társfinanszírozása által biztosított forrásból az EFOP-3.6.3-VEKOP-16-2017-00007 azonosítószámú „Tehetségből fiatal kutató – A kutatói életpályát támogató tevékenységek a felsőoktatásban" című projekt keretében jött létre.

tak. A kiberbiztonság területén a legkiemelkedőbb szereplők – az Egyesült Államok, Kína és Oroszország – folyamatosan igyekeznek megerősíteni kibervédelmüket, miközben egy már évek óta zajló fegyverkezési versenyben szakadatlanul fejlesztik támadó képességeiket, és olykor tesztelik is más országok védelmi rendszereit.[4]

Az amerikai, a kínai és az orosz kiberbiztonsággal kapcsolatos stratégiai dokumentumok és egyéb információk alapján kijelenthető, hogy e hatalmak számára járhat az egyik legnagyobb haszonnal a kiberhadviselés folytatása. Egyes országok esetében rendelkezésre álló stratégiai dokumentumok betekintést nyújtanak az adott államok biztonsági percepcióiba, és jelzik, hogy milyen hozzáállásra számíthatunk tőlük a kiberhadviselés terén. Az USA, Kína és Oroszország azért is tekinthetők a legfontosabb szereplőknek a kibertérben, mert ezen országok rendelkeznek a legszélesebb körű és legkifinomultabb képességekkel, és minden bizonnyal ők szolgálnak majd követendő példaként azok számára, akik szintén ki szeretnék majd terjeszteni tevékenységüket a kibertérre.[5]

A NATO a folyamatosan változó, összetett biztonsági környezetre tekintettel 2016 júliusában ismerte el a kiberteret mint olyan műveleti tér, ahol a Szövetségnek képesnek kell lennie megvédeni magát, éppen úgy, ahogy földön, vízen vagy levegőben.[6] Ebben a fejleményben az is közrejátszott, hogy Washington korábban jelezte, Peking és Moszkva elrettentéséhez sokkal erősebb kibervédelemre lesz szükség, ennek érdekében pedig az USA kész a Szövetség számára biztosítani aktív kibervédelmi képességeit. Az Egyesült Királyság is határozottabb kibervédelmi politikát hirdetett, kijelentve, hogy London nem hagyna válaszcsapás nélkül egy külföldi kormányokhoz köthető, az ország kritikus infrastruktúrája elleni kibertámadást.[7] Az USA és az Egyesült Királyság mellett még Németország és Franciaország is megerősítette elkötelezettségét az offenzív kiberképességek kifejlesztése mellett. E négy, hasonló értékeket és érdekeket képviselő ország a NATO-szövetségen belül is egyfajta kiberbiztonsági közösséget alkot, mindazonáltal ezen a téren is egyértelműen az Egyesült Államoké a vezető szerep. Az USA adott ki először kiberbiztonsági stratégiát még 2003-ban, majd hat évvel később, 2009-ben követte Washington példáját az Egyesült Királyság, Németország és Franciaország pedig csak 2011-ben adták ki saját kiberbiztonsági stratégiai dokumentumaikat. Ennek fényében tehát nem beszélhetünk összehangolt stratégiaalkotási folyamatról. Ez a négy NATO-tagállam hasonló értékeket és érdekeket képvisel, a kiberbiztonsági fenyegetések értékelésével kapcsolatban azonban van némi eltérés közöttük. Az USA, az Egyesült Királyság és Németország ugyanis a „lator államokat" látja a fő kiberfenyegetéseknek, míg Franciaország elsősorban a nem állami szereplőket, például a kiberterroristákat. Az ellenfél egységes megítélésének hiányában viszont a négy ország kiberbiztonsági közössége is éretlen marad.[8]

---

[4] Sanjay Goel: National cyber security strategy and the emergence of strong digital borders. *Connections,* 19. (2020), 1. 74–76.

[5] Brian M. Mazanec: Constraining norms for cyber warfare are unlikely. *Georgetown Journal of International Affairs,* 17. (2016), 3. 103.

[6] NATO: *NATO cyber defence fact sheet.* [online], July 2016. Forrás: nato.int [2020. 11. 23.]

[7] Sinan Ülgen: *A lack of cybernorms threatens Western democracies.* [online], 2016. 12. 14. Forrás: carnegieeurope.eu [2020. 11. 23.]

[8] A. Tumkevič: Uncertain security community: Building Western cyber-security order. *Journal of Information Warfare,* 17. (2018), 1. 74–86.

A 21. század egyik legnagyobb kihívása az egyének és az államok számára is az információk és az adatok védelme. Az informatikai biztonság szerepe tíz évvel ezelőtt talán még nem volt olyan jelentős, mint napjainkban, az azonban már 2012-ben is látható volt, hogy egy olyan „kiberprobléma" van kibontakozóban, amelynek lényege, hogy technikai, politikai és társadalmi dimenziók összefonódásával egy olyan, folyamatosan fejlődő, összetett adaptív informatikai rendszer (*Complex Adaptive System* – CAS) jött létre, amelyre nincs egyszerű megoldás, csupán evolúciójának alakítására és befolyásolására van lehetőségünk.[9] Az internet mára gyakorlatilag a világ digitális idegrendszerévé fejlődött, azonban még mindig megvannak a maga gyermekbetegségei. A kiberbiztonság egyik legfőbb kihívását pedig éppen az az adottsága jelenti, hogy egy gyorsuló fejlődési folyamatban minden védekezési stratégiát egy a körülményekhez alkalmazkodott támadási technika követ, és fordítva.[10] A támadók tehát egyre kifinomultabb módszereket alkalmaznak, és ezért nagy kihívás velük lépést tartani.[11]

Jelen tanulmány célja egy rövid, de átfogó globális kiberbiztonsági kitekintést adva felhívni a figyelmet a téma aktualitására és jelentőségére, majd ismertetni a kibertér főszereplőinek kibertevékenységét jellemző sajátosságokat. A környezeti értékeléshez és a fenyegetések felméréséhez vállalati jelentések, kormányzati dokumentumok és médiabeszámolók szolgáltatnak forrást. Az Egyesült Államok vezető szerepéből fakadóan nagyobb számban állnak rendelkezésre amerikai források a téma iránt érdeklődők számára, míg Oroszország és Kína esetében számottevően kevesebb nyilvánosan elérhető információra támaszkodhatunk. A nagyhatalmak stratégiai célkitűzéseinek, kiberképességeinek és tevékenységének bemutatását követően Irán és a világ legtöbb kiberkatonájával rendelkező Észak-Korea is sorra kerül. A tanulmány végül következtetések levonásával zárul.

A globális kiberbiztonsági környezet értékelése és a fő fenyegetések

A Microsoft 2005 óta a minden ősszel megjelenő digitális védelmi jelentésében *(Digital Defense Report)* foglalja össze az aktuális kiberbiztonsági trendeket. A legfrissebb, 2020 szeptemberében kiadott jelentésében az amerikai technológiai óriás a kiberbiztonsági fenyegetések egyre fokozódó kifinomultságára figyelmeztetett, kiemelve, hogy a támadók egyre nehezebben azonosítható és felderíthető technikákat alkalmaznak, amelyekkel még a legfelkészültebb célpontokat is képesek sikerrel támadni. A felmérésük eredményeit összefoglaló blogbejegyzésében Tom Burt, a Microsoft ügyfélbiztonságért felelős alelnöke külön kiemelte az új felderítési technikákat alkalmazó állami szereplőket, akik így már kiemelt fontosságú célpontokat is veszélyeztetnek. Mindemellett azzal is számolnunk kell,

[9] A Komplex Adaptív Rendszer (CAS) definíciója John Holland szerint olyan rendszerek, amelyeknek nagyszámú komponense vagy szereplője van, amelyek egymással interakcióban vannak és adaptálódnak vagy tanulnak. John H. Holland: Studying complex adaptive systems. *Journal of Systems Science and Complexity,* 19. (2006), 1. 1.

[10] A kibertérben megjelenő fenyegetésekről és a védelem kérdésköréről – beleértve az EU, a NATO és a nemzetek, köztük Magyarország stratégiai és jogszabályi erőfeszítéseit – bővebben lásd Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

[11] Oliver Wyman Forum Team: *Why is cybersecurity so hard – and getting harder? What can be done?.* [online], 2019. 09. 18. Forrás: oliverwymanforum.com [2021. 05. 30.]

hogy a vállalatokat támadó bűnözői csoportok az infrastruktúrájukat a virtuális felhőbe költöztetve igyekeznek elrejtőzni a hétköznapi szolgáltatók és szereplők között, és új módszereket fejlesztettek ki a zsarolóvírusokkal szemben sérülékeny rendszerek felkutatására. Az elkövetők láthatóan jobban preferálnak egyes technikákat, mint például a felhasználónevek és jelszavak megszerzését takaró *credential harvesting* és a gyakorlatilag váltságdíj megfizetését követelő zsarolóvírusok, azaz *ransomware* alkalmazását. Mindeközben egyre inkább középpontba kerülnek a támadásoknak leginkább kiszolgáltatott és igen sebezhető *IoT*- (*Internet of Things*) eszközök is, amelyeket 2020-ban 35%-kal nagyobb arányban ért támadás a megelőző évhez képest.[12]

A Microsoft jelentése azt is megállapította, hogy 2020 márciusában jelentősen megugrott a Covid-19-járvánnyal kapcsolatos adathalász támadásoknak a száma, ami jól mutatja, hogy a kibertér ártó szándékú szereplői igyekeznek kihasználni a világjárvány kapcsán fokozódott információéhséget, az otthoni munkavégzésre való tömeges áttérés és a távoktatás bevezetése miatt nagymértékben megnövekedett online eszközhasználatban rejlő lehetőséget. Mindemellett az amerikai vállalat szakemberei 16 állami szereplőhöz köthető, a koronavírus-járvány elleni védekezésben érintett felhasználókkal szembeni adathalász kísérletet, illetve támadást azonosítottak. A pandémiához köthető támadások főleg állami egészségügyi intézményeket, valamint a vakcinakutatásban közreműködő tudományos szervezeteket és kereskedelmi szereplőket vettek célba a munkavállalóik és informatikai infrastruktúrájuk feltérképezése céljából.[13]

Az adatok és a tapasztalatok alapján a Microsoft három területet határozott meg a kiberbiztonságon belül, amelyek a biztonsági környezet értékeléséhez is alkalmazhatók számunkra. Ez a három terület pedig a kiberbűnözés, az állami szereplők és a távmunka. A kiberbűnözők a sikerességük érdekében folyamatos innovációra kényszerülnek, motivációjuk lehet gazdasági vagy politikai hátterű is, tevékenységük pedig akár globális szintű.[14] A kiberbűnözőkre is jellemző az opportunizmus, így a világjárvány által az emberekben kiváltott félelem és a járványkezelés során jelentkezett zavarok kitűnő alkalmat kínáltak számukra többek között olyan adathalász-támadások végrehajtására, mint például az Egészségügyi Világszervezet nevében küldött elektronikus levelek, amelyekben ártalmas linkeket és csatolmányokat helyeztek el adatlopás és kártékony programok futtatása céljából.[15]

Az állami szereplők esetében olyan kibertámadásokról beszélünk, amelyek egy adott országhoz és annak nemzeti érdekeihez köthetők, így ezek általában a legkomolyabb fenyegetést jelentik a kiberbiztonsági közösség szerint, már csak azért is, mert általában stratégiai célt szeretnének elérni. Ennek értelmében gyakorlatilag a legelszántabb szereplőkről van szó, akik akár igen jelentős időt, továbbá komoly mértékű anyagi és egyéb erőforrásokat is készek felhasználni műveleti céljaik elérése érdekében. Támadó tevékenységüket

[12] Tom Burt: *Microsoft report shows increasing sophistication of cyber threats.* [online], 2020b. 09. 29. Forrás: blog.microsoft.com [2020. 11. 08.]

[13] Tom Burt: *Protecting healthcare and human rights organizations from cyberattacks.* [online], 2020a. 04. 14. Forrás: blogs.microsoft.com [2020. 11. 08.]

[14] Micorsoft: *Microsoft Digital Defense Report.* [online], 2020. 09. 5. Forrás: microsoft.com [2020. 11. 08.]

[15] Sergiu Gatlan: *World Health Organization warns of coronavirus phishing attacks.* [online], 2020. 02. 17. Forrás: bleepingcomputer.com [2020. 11. 08.]

többnyire a képességeiket folyamatosan fejlesztő, az adott feladatra létrehozott csoportokkal hajtják végre, amelyek képesek új eljárásokat, technikákat kifejleszteni és alkalmazni. Ezeknek az állami szereplőknek a támadótevékenységét beazonosítani, nyomon követni és kivédeni az egyik legnehezebb kihívás a szakértők számára.[16] A Microsoft jelentése szerint az államokhoz köthető kibertámadások 52%-a oroszországi, 25%-a iráni, 12% kínai, 11% észak-koreai vagy egyéb eredetű. A célországok között pedig 69%-kal az első helyen az Egyesült Államok, 19%-kal a másodikként az Egyesült Királyság, harmadik helyen 5%-kal Kanada, majd 5%-kal Dél-Korea és 3%-kal Szaúd-Arábia szerepel.[17] Oroszország tevékenysége elsősorban újságírókat, egyetemeket, politikai és kormányzati szerveket érint, de a célpontok között megtalálhatók külügyminisztériumok, nagykövetségek, telekommunikációs cégek, internetszolgáltatók, katonai szervezetek, kutatóintézetek és más szélsőséges csoportok is. Az iráni eredetű kibertámadások az energiaszektort, a védelmi ipart, a nem kormányzati szervezeteket, kormányokat, segély- és jogvédő szervezeteket, illetve a magánlevelezést is támadják.[18] Az államokhoz köthető kibertámadások 2019 júliusa és 2020 júniusa között 90%-ban nem a kritikus infrastruktúrák ellen irányultak, hanem elsősorban nem kormányzati szervezetek (32%), szakmai szolgáltatások (31%), kormányzati szervek (13%), nemzetközi szervezetek (10%), információtechnológiai cégek (7%) és felsőoktatási intézmények (7%) ellen. Ugyanakkor megjegyzendő, hogy ugyanebben az időszakban a kritikus infrastruktúrákat ért támadásoknak a 60%-a volt állami szereplőkhöz köthető. A tapasztalatok szerint az államok által végrehajtott kibertámadásoknak rendszeresen kerülnek a célkeresztjébe fontos események, például választási kampányok, olimpiai játékok, illetve az állami szereplők is igyekeznek előnyt kovácsolni a Covid-19-világjárvány által kiváltott zűrzavarból. A stratégiai céltól eltekintve, az államokhoz köthető kibertámadások műveleti célja többnyire az információszerzés (kémkedés), de előfordul a működészavar kiváltása, illetve a károkozás is.[19]

Támadási technikák, fogalommagyarázat

A különböző közbeékelődéses támadásokkal, adathalászattal és egyéb módszerekkel a támadók gyakori célja minél több *felhasználói fiókot összegyűjteni* (credential harvesting) a hozzájuk tartozó azonosító-jelszó párosokkal későbbi újrafelhasználás céljából.

Rosszindulatú szoftver (malware) bármely program, amit szándékos károkozás céljával hoztak létre. Számos különböző fajtája ismert, mint például a számítógépes vírusok, férgek, trójai programok, zsarolóvírusok, kémprogramok, reklámprogramok és ijesztőprogramok.

A *zsarolóvírus (ransomware)* olyan kártékony szoftver, amely titkosítja a fertőzött eszközön tárolt adatokat annak érdekében, hogy a személyes vagy éppen üzleti adatokért cserébe pénzt csaljon ki a tulajdonostól.

A *dolgok internete (Internet of Things, IoT)* kifejezés alatt olyan dolgok hálózatát értjük, amelyek különböző beágyazott érzékelőkkel, szoftverekkel és egyéb technológiákkal vannak felszerelve abból a célból, hogy az interneten keresztül kapcsolatba lépjenek és adatot cseréljenek más eszközökkel.

A *jelszószórás (password spray)* olyan támadás, amely során az elkövetők több felhasználói fiókhoz igyekeznek hozzáférni mindössze néhány gyakran használt jelszó kipróbálásával. Ezzel szemben a hagyományos „nyers erő" (brute force) avagy „teljes kipróbálás módszerével" a támadók egyetlen felhasználói fiókhoz szándékoznak hozzáférést szerezni sok lehetséges jelszó kipróbálásával.

[16] Az államokhoz köthető kiberfenyegetések jelentőségéről bővebben lásd Gregory Conti – Robert Fanelli: How could they not: Thinking like a state cyber threat actor. *The Cyber Defense Review,* 4. (2019), 2. 50–58.

[17] Microsoft (2020) i. m. 41–42.

[18] Microsoft (2020) i. m. 44.

[19] Microsoft (2020) i. m. 46–49.

A *célzott adathalászat (spear phishing)* során a támadók nem véletlenszerűen választják ki a lehetséges áldozatokat, hanem ismert csoportokat céloznak és specifikus, akár személyre szabott üzenetekkel próbálkoznak. Az adathalász támadások leggyakoribb célja az adatlopás, azonban szervezett bűnözői csoportoknak szándékában állhat akár kártékony szoftverek telepítése is az áldozat számítógépére.
A *DDoS támadás* célja, hogy a célszolgáltatás elérhetetlenné váljon a több forrásból, azonos időben érkező hálózati forgalom által túlterhelődő eszközök miatt.
Fejlett, folyamatos fenyegetés (Advanced Persistent Threat – APT) alatt olyan rejtőzködő állami vagy nem állami bűnözői csoportokat értünk, amelyek magas szintű szervezettség mellett, rendkívül kifinomult módszerekkel szereznek hozzáférést informatikai rendszerekhez, és képesek hosszabb időtartamon keresztül észrevétlenek maradni.[20]
A hátsó ajtó (backdoor) olyan, szándékosan akár előre beépített jelszó, esetleg programhiba vagy utólag elhelyezett önálló program, amely a szokásos azonosítást és engedélyezést megkerülve korlátlan és ellenőrizetlen hozzáférést biztosít az adott rendszerhez.

Az utóbbi évek egyik legjelentősebb munkaerőpiaci változása, hogy az infokommunikációs technológiák fejlődésével egyre több olyan munkalehetőség jelenik meg, amelyet a munkavállaló gyakorlatilag a világon bárhonnan végezhet. A távoli munkavégzés növekvő trendje az utóbbi években folyamatos volt, azonban 2020-ban a Covid-19-világjárvány jelentős mértékben felgyorsította ezt a folyamatot azáltal, hogy számos vállalatot kényszerített az otthoni munkavégzés azonnali elrendelésére.[21] A *„home office"* tömeges mértékű és sürgős bevezetése azonban érthető módon újabb kiberbiztonsági kihívásokat is hozott magával, hiszen ideális esetben a távoli munkavégzés feltételeinek biztosítása a Microsoft úgynevezett *Zero Trust* kezdeményezéshez hasonló, vagy annak megfelelő felkészülést igényel, amelynek lényege, hogy az adott cég hálózatának üzemeltetői minden hozzáférési kísérletet potenciálisan támadó jellegűnek tekintenek, így a hálózatot az óvatosságból feltétlenül szükséges bizalmatlanságra alapozva működtetik.[22]

Napjainkban már az asztali és a hordozható számítógépek is visszaszorulóban vannak, helyüket fokozatosan átveszik az okostelefonok és a táblagépek. A GSM Szövetség (*Global System for Mobile Communication Association* – GSMA) idén kiadott mobilpiaci jelentése *(The Mobile Economy 2020)* szerint számos mérföldkövet ért el az iparág 2019–2020 folyamán. Felmérésük szerint a világ népességének kétharmada rendelkezik mobiltelefon-előfizetéssel és 65% az okostelefonok aránya. Jelenleg még a 4G technológia az uralkodó, azonban a GSMA előrejelzése szerint az 5G kapcsolatok száma gyors iramban és jelentősen fog növekedni a következő években. Az új 5G technológia nyújtotta előnyök, különösképpen a rendkívül alacsony jelkésleltetés és megnövekedett sávszélesség jelentős mértékben segítheti eddig elképzelhetetlennek tűnő termékek és szolgáltatások létrejöttét. Mindez egyben azt is jelenti, hogy az iparágnak számos új kihívással kell szembenéznie. A GSMA felmérésben részt vevő vállalatok 46%-a szerint a biztonsági követelmények és az adatvédelmi elvárások jelentős kihívást támasztanak a cégekkel szemben, és hátráltathatják az IoT-eszközök

[20] A kutatók által elemzett incidensek hasonlósága alapján elkülöníthető csoportokat jelölik a szakemberek egy APTx elnevezéssel, ahol x a csoport sorszáma. Emellett gyakran adnak a kutatók fantázianeveket a vizsgált csoportoknak. Így fordulhat elő, hogy a nyilvánosság akár több különböző néven is találkozhat ugyanazzal a csoporttal, mint például az APT31 csoport egyik fantázianeve a ZIRCONIUM.

[21] Radmilla Suleymanova: *As new wave of COVID-19 cases hits, remote work becomes the norm.* [online], 2020. 10. 18. Forrás: aljazeera.com [2020. 11. 09.]

[22] Mark Simos: *Zero Trust strategy – what good looks like.* [online], 2019. 11. 11. Forrás: microsoft.com [2020. 11. 09.]

terjedését, ezért az 5G beruházások egyik legfontosabb prioritása a telekommunikációs hálózatok biztonságának fejlesztése.[23]

Az Amerikai Egyesült Államok kiberbiztonsági stratégiája és képességei

2007-ben Észtország egy hetekig tartó kibertámadásnak esett áldozatául, amelyet követően egyre többen szorgalmazták a kiberbiztonsági problémák kezelésére a katonai megoldások alkalmazását. Az észtországi támadások hatására a NATO 2008-ban elkezdte kidolgozni kibervédelmi politikáját és fejleszteni képességeit egy kibervédelmi kiválósági központ létrehozásával, amelynek 2010 óta Magyarország is teljes jogú tagja.[24] Majd ezt követően, a kilencnapos orosz–grúz háború során Grúzia vált az észtországihoz hasonló kibertámadások célpontjává.[25] Az Egyesült Államokban ekkor már több szakértő számára világossá vált, hogy valójában már évek óta kiberfegyverkezési verseny zajlik, amelyben az USA sem maradhat le, és 2009-ben létre is hozták a kiberhadviselésért felelős parancsnokságot (USCYBERCOM). Szintén 2009-ben vált ismertté a világ számára a Stuxnet létezése, amely gyakorlatilag az első, kormányokhoz (minden bizonnyal az USA-hoz és Izraelhez) köthető digitális fegyvernek tekinthető, amelyet az iráni atomprogram lelassítása érdekében hoztak létre.[26]

2013-tól az amerikai Nemzeti Hírszerzési Igazgató *(Director of National Intelligence),* James Clapper rendszeresen a kiberfenyegetést nevezte meg, mint első számú stratégiai szintű fenyegetést az Egyesült Államok számára, ezzel pedig 2001. szeptember 11. óta első alkalommal szorult vissza az első számú biztonsági fenyegetés helyéről a terrorizmus.[27] 2015-ben az amerikai hírszerző szervek az államokhoz köthető kibertámadásokat és a kiberbűnözők tevékenységét is az Egyesült Államokra leselkedő legnagyobb fenyegetésekként értékelték, az állami szereplők között nevesítve Oroszországot, Kínát, Iránt és Észak-Koreát, de az orosz fenyegetést jelölték meg a legnagyobbnak.[28] A kibertérben már évek óta folytatnak állami és nem állami szereplők kártékony kibertevékenységeket az Egyesült Államok ellen világszerte, részben azért, hogy próbára tegyék az USA és a nemzetközi közösség tűrőképességét. Ezek a kibertámadások lehetővé tehetik az ellenséges aktorok számára, hogy hozzáférést szerezzenek védett adatokhoz, fennakadásokat okozzanak egyes szervezetek működésében, de akár katonai műveleti célokat is szolgálhatnak. A nem állami szereplőket illetően megjegyzendő, hogy az Iszlám Állam is a kibertér adta lehetőségeket

[23] GSMA: *The Mobile Economy 2020.* [online], 2020. 03. 11. Forrás: gsma.com [2020. 11. 15.]
[24] Kovács (2018) i. m. 147.
[25] John Markoff: *Before the gunfire, cyberattacks.* [online], 2008. 08. 12. Forrás: nytimes.com [2020. 11. 22.]
[26] Mark Clayton: *The new cyber arms race.* [online], 2011. 03. 07. Forrás: csmonitor.com [2020. 11. 22.]
[27] Mark Hosenball – Patricia Zengerle: *Cyber attacks leading threat against U.S.: spy agencies.* [online], 2013. 03. 12. Forrás: reuters.com [2020. 11. 14.]
[28] Guy Taylor: *James Clapper, intel chief: Cyber ranks highest on worldwide threats to U.S.*. [online], 2015. 02. 26. Forrás: washingtontimes.com [2020. 11. 14.]; Aaron Boyd: *DNI Clapper: Cyber bigger threat than terrorism.* [online], 2016. 02. 04. Forrás: federaltimes.com [2020. 11. 14.]

használja ki harcosok toborzására és a propagandájának terjesztésére, miközben deklarált céljuk lett támadó jellegű kiberképességek megszerzése is.[29]

Koncepció, célok, lehetőségek, eszközök

Az amerikai Védelmi Minisztérium (*Department of Defense* – DoD) utoljára 2015 áprilisában adta ki a Kiberbiztonsági Startégiáját, amelynek előszavában Ashton Carter akkori védelmi miniszter emlékeztet rá, hogy az Egyesült Államokban számos kritikus fontosságú szolgáltatás biztosítása gyakorlatilag az internetes hálózatoktól és a kibertérben tárolt adatoktól függ, ez a fajta kiszolgáltatottság pedig valamennyiünk számára veszélyt jelent a valós kiberbiztonsági fenyegetések révén. Napjainkban már állami és nem állami szereplők egyaránt olyan kibertámadások végrehajtására készülnek, amelyek képesek az Egyesült Államok kritikus infrastruktúrájának működésében fennakadást vagy akár maradandó károkat is okozni, valamint amerikai szellemi tulajdont ellopni, ezzel is aláásva az USA technológiai és katonai fölényét. Mivel a DoD feladata az ország területének és érdekeinek a védelme, a kibertámadások elleni védekezés is elsősorban a Pentagonhoz tartozik. A kiberstratégia célja a kibererők és a kibervédelem fejlesztése a Védelmi Minisztérium számára meghatározott három területen, amelyek közül az első a hálózatok, rendszerek és információk védelme; a második az ország területének és az amerikai nemzeti érdekek védelme a jelentős kibertámadásokkal szemben; a harmadik pedig a műveletek támogatása. Az Egyesült Államok elkötelezett egy nyílt, biztonságos, interoperábilis és megbízható internet mellett, amely az amerikai értékekkel (véleménynyilvánítás szabadsága, magánélet, kreativitás, innováció) összhangban biztosítja a prosperitást, a közbiztonságot, a kereskedelmi kapcsolatok és az információáramlás szabadságát.[30]

Az amerikai kiberstratégia az államokhoz köthető kibertámadásra a legfőbb példaként említi azt az esetet, amikor 2014-ben Észak-Korea minden bizonnyal *Az Interjú* című vígjáték miatti megtorlásként – amelyben két amerikai újságírót Kim Dzsongun észak-koreai vezető meggyilkolásával bíz meg a Központi Hírszerző Ügynökség (CIA) – támadást hajtott végre a Sony Pictures Entertainment ellen, működésképtelenné téve több ezer számítógépet, és hozzáférést szerezve a Sony bizalmas üzleti információihoz, köztük még meg nem jelent filmek digitális másolataihoz, alkalmazottak és híresség adataihoz.[31] A stratégia megjegyzi, hogy a kibertámadások politikai célú alkalmazásának növekedése veszélyes trend a nemzetközi kapcsolatok terén, így az Egyesült Államoknak számolnia kell annak a folyamatosan fokozódó lehetőségével, hogy konfliktus esetén kibertámadások célpontja lehet az amerikai vagy a szövetséges országok kritikus infrastruktúrája, katonai hálózatok, ipari létesítmények vezérlőrendszerei. A stratégiai szintű támadások mellett a fejlett technológiával rendelkező támadók képesek lehetnek például akár egészségügyi intézmények adatbázisaihoz is hozzáférést szerezni, ott pedig dokumentációkat módosítani,

[29] International Telecommunication Union: *US Department of Defense Cyber Strategy.* [online], 2015. 04. 9. Forrás: itu.int [2020. 11. 13.]

[30] International Telecommunication Union (2015) i. m. előszó 1.

[31] Emily Van Der Werff – Timothy B. Lee: *The 2014 Sony hacks, explained.* [online], 2015. 06. 03. Forrás: vox.com [2020. 11. 13.]

hogy egy konkrét személy egészségét és biztonságát veszélyeztessék. Erre volt példa, amikor 2020 szeptemberében egy az Egyesült Államokban országszerte az egyik legtöbb kórházat üzemeltető cég informatikai rendszerét érte éppen egy hétvégén kibertámadás, ami több mint 400 helyszínen okozott fennakadásokat, ezért az egészségügyi személyzetnek papír és toll használatával kellett vezetnie az egészségügyi dokumentációt és végezni a gyógyszerelést.[32] Egy ilyen komoly kibertámadás pedig súlyos biztonsági fenyegetést jelenthet az Egyesült Államok számára, hiszen akár halálos áldozatokhoz is vezethet,[33] anyagi károkat okozhat, politikai célokat hiúsíthat meg vagy gazdasági érdekeket sérthet. Ennek a fenyegetésnek az elhárításában a kormányzatoknak, vállalatoknak és a szervezeteknek is meg van a felelőssége, amennyiben nem mérik fel helyesen a kockázatokat és nem invesztálnak megfelelő mértékben a kiberbiztonságba és a kibervédelmi képességek fejlesztésébe.[34]

A DoD a kollektív biztonság növelése és az amerikai érdekek védelme érdekében a digitális téren kívül is tevékenykedik, többek között például információmegosztási együttműködést és szoros koordinációt tart fenn valamennyi kormányzati szervvel, köztük például a Belbiztonsági Minisztériummal (DHS) és a Szövetségi Nyomozó Irodával (FBI). Ennek az együttműködésnek ma már szerves részét képezik a kongresszus által 2013-ban elfogadott *Cyber Warrior Act* keretében minden államban a Nemzeti Gárda szervezeti keretén belül létrehozott kiberbiztonsági és hálózati incidens kezelő csoportok *(Cyber and Network Incident Response Team).*[35] 2015 óta pedig a Nemzeti Gárda által létrehozott kibermissziós csoportok *(Cyber Mission Teams)* is részesei a katonai és a civil együttműködésnek a kritikus infrastruktúrák kibervédelme érdekében.[36] Megjegyzendő, hogy a kritikus infrastruktúrák védelméért felelős DHS a Kiberbiztonsági és Infrastruktúra Biztonsági Ügynökség (CISA) részeként működteti a kiberfenyegetésekkel kapcsolatos információk értékeléséért felelős Számítógépes Sürgősségi Készenléti Csoportot (US-CERT), amely egyben az informatikai incidensek figyelését, a sérülékenységek vizsgálatát, riasztások kiadását és az incidensek kezelésének koordinálását is végzi.[37]

A magánszektor főszereplői és a Pentagon között elengedhetetlen a szoros együttműködés, hiszen a Védelmi Minisztérium az informatikai hálózatának működtetése, a kiberbiztonsági szolgáltatások és a kutatás-fejlesztés terén is a magánvállalatokra van utalva. A kibertérben a védelem első vonala az informatikai hálózatok több mint 90%-át birtokló és üzemeltető magánszektor, ezért az érintett vállalatoknak prioritásokat kell felállítani és folyamatosan biztonsági fejlesztéseket kell végezniük a kritikus fontosságú hálózatok

---

[32] Kevin Collier: *Major hospital system hit with cyberattack, potentially largest in U.S. history.* [online], 2020. 09. 28. Forrás: nbcnews.com [2020. 11. 15.]

[33] 2020 szeptemberében egy düsseldorfi kórház informatikai rendszerét támadták meg kiberbűnözők egy zsarolóvírussal, az incidens során pedig egy a kórházban ápolt beteg életét vesztette, miután a számítógépek használhatatlansága miatt nem kaphatta meg időben a szükséges kezelést. Ez az eset volt az első, hogy kibertámadás vezetett egy ember halálához, noha a könnyű célpontoknak számító egészségügyi intézményeket gyakran éri támadás. Melissa Eddy – Nicole Perlroth: *Cyber attack suspected in German woman's death.* [online], 2020. 09. 18. Forrás: nytimes.com [2020. 11. 15.]

[34] International Telecommunication Union (2015) i. m. 2.

[35] H. R. 1640 – Cyber Warrior Act of 2013. 113th Congress (2013–2014). [online], 2013. 04. 18. Forrás: congress.gov [2020. 11. 15.]

[36] A Nemzeti Gárda kiberbiztonsági és kibervédelmi szerepéről bővebben lásd Brian Claus et alii: Using the oldest military force for the newest national defense. *Journal of Strategic Security,* 8. (2015), 4. 1–22.

[37] Department of Homeland Security, CISA: *US-CERT, United States Computer Emergency Readiness Team.* [online], DHS Info Sheet. Forrás: us-cert.cisa.gov [2020. 11. 22.]

és adatok védelme érdekében. Ahogy maga az amerikai kiberstratégia is megjegyzi, a kibertámadások túlnyomó többsége viszonylag csekély mértékű anyagi és technikai ráfordítással is megoldható, ezek azonban gyakorlatilag nélkülözhetetlenek.[38]

Meg kell még jegyezni továbbá, hogy a DoD a kiberbiztonság növelése és a kibervédelmi műveletek kapacitásának fejlesztése érdekében külföldön is törekszik szövetségi és partnerségi kapcsolatokat kialakítani, koalíciókat létrehozni. A Pentagon igyekszik közreműködni abban, hogy az Egyesült Államok szövetségesei helyesen fel tudják mérni a digitális fenyegetések jelentőségét és ki tudják építeni a számítógép-hálózataik és adataik védelméhez szükséges képességeket. Mindemellett a partnerországok is rendelkezhetnek az USA számára is fontos, kiegészítő képességekkel. Az Egyesült Államok jelenleg az „Öt szem" szerződés partnerországaival, azaz a Nagy-Britannia, Kanada, Ausztrália és Új-Zéland hírszerzéseit tömörítő csoporttal van szoros együttműködésben, de az amerikai Védelmi Minisztérium közel-keleti, csendes-óceáni és európai országokkal is együttműködik a kiberbiztonsági környezet megértése és a védelmi képességek fejlesztése érdekében.[39]

Az amerikai haderő kibertérre utaltsága még 2011-ben kényszerítette rá a védelmi minisztert, hogy a kiberteret is műveleti térnek nyilvánítsa. Mivel a DoD feladatai közé tartozik, hogy a saját informatikai hálózatainak (*Department of Defense Information Network* – DoDIN) a védelmét biztosítsa az esetleges támadásokkal szemben – valamint, hogy felkészüljön azok helyreállítására, amennyiben a biztonsági óvintézkedések kudarcot vallanának –, ennek érdekében gyorsreagálású képességeket is kifejlesztett, amelyek segítségével a sérülékenységek kijavíthatók, a károk pedig mérsékelhetők. A hálózatok biztonságos működése mellett a Pentagonnak készen kell állnia az Egyesült Államok és érdekeinek a jelentős következményekkel járó kibertámadásokkal szembeni védelmére, szükség esetén kiberműveletek végrehajtására egy készülődő vagy már folyamatban lévő támadás elhárítása érdekében. Továbbá képesnek kell lennie katonai műveletek integrált kiberképességekkel történő támogatására is.[40] Utóbbit illetően a Védelmi Minisztérium kiberbiztonsággal foglalkozó állományából kiemelt szerepet élvez a 2012-ben megalapított, 2013-tól pedig az amerikai fegyveres erőkbe integrált,[41] 6200 főt számláló Kiber Missziós Erő (*Cyber Mission Force* – CMF), amelynek operátorait 133 csoportba szervezték. Ezek között van a hagyományos védelmi intézkedésekért felelős csoport, van a komoly következményekkel járó kibertámadásokkal szembeni védekezéssel foglalkozó, és van harcoló missziós erő is, amelyek képesek katonai műveletek támogatására.[42]

Állandó fenyegetettség és megújulási kényszer

A kibertérben a fő kockázatokat továbbra is az ártalmas szoftverek *(malware)* jelentik, amelyekkel kapcsolatban az amerikai kiberstratégia megjegyzi, hogy a potenciális támadónak nem szükséges hatalmas pénzösszegeket fordítani a támadó képesség kifejlesztésére.

[38] International Telecommunication Union (2015) i. m. 5.
[39] International Telecommunication Union (2015) i. m. 4.
[40] International Telecommunication Union (2015) i. m. 3–5.
[41] International Telecommunication Union (2015) i. m. 6–7.
[42] DoD Fact Sheet: *Cyber Mission Force.* [online], 2020. 02. 10. Forrás: arcyber.army.mil [2020. 11. 14.]

Egy állam, egy nem állami szereplő vagy akár egy magánszemély is bármikor vásárolhat komoly károkozásra alkalmas programokat a feketepiacon, ahogy más képességeket is. Mindemellett az államok és a nem állami szereplők esetében is jellemző gyakorlat, hogy jól fizetett információbiztonsági szakértőket bíznak meg új sérülékenységek felkutatásával és azok kihasználására képes eszközök *(exploit)* kifejlesztésével, ezzel pedig gyakorlatilag egy szabályozatlan nemzetközi piac jött létre, ahol a szereplők adják-veszik a sérülékenységeket és a kibertámadások végrehajtásához szükséges programokat. A Védelmi Minisztérium nem csupán a saját informatikai hálózatát, de az ország kritikus infrastruktúráit is képes kell legyen megvédeni a kibertámadásokkal szemben, amelyek nem csupán károkat okozhatnak, hanem adatszivárgást is eredményezhetnek. A védekezés egyik módja pedig az elrettentési képességek kifejlesztése.[43] A kiberképességek lehetővé tehetik egy államhoz köthető és egy nem állami szereplő számára is, hogy oly módon hajtson végre támadást az Egyesült Államok ellen, hogy az nem eredményez feltétlenül katonai válaszcsapást, ugyanakkor komoly fenyegetést jelenthet a nemzeti biztonsági érdekekre, így valamilyen nem katonai választ minden bizonnyal maga után vonhat, például diplomáciai vagy jogi lépéseket, esetleg gazdasági szankciók bevezetését.[44]

Az offenzív kiberműveleteket illetően az Egyesült Államokban számos korlátozás mérsékli az egyes képességek hatékony alkalmazhatóságának lehetőségeit. A támadó kiberműveletek többnyire elnöki vagy védelmi miniszteri jóváhagyást igényelnek, és ez vészhelyzetek esetére is vonatkozik, miközben ilyen beavatkozások szükségességének eldöntéséhez minden esetben nélkülözhetetlen az illetékes szervek és ügynökségek szoros koordinációja. Mindemellett a gyakorlatban sokszor nem célravezető offenzív jellegű kiberműveletet végrehajtani, mert bár gyorsan kivitelezhetők, az előkészítésük és a tervezésük általában időigényesebb a hagyományos katonai műveletek tervezésénél.[45] Ráadásul egy adott támadó kiberművelet többnyire csak egy alkalommal hajtható végre. Ugyanis többször már nem lehet újra ugyanazt az eljárást alkalmazni, mivel az ellenfél azt már megismerhette, így fel is készülhet a támadás kivédésére, akár be is foltozhatja a kihasznált sérülékenységet, és mérsékelheti a támadás hatását is. Mindez azt eredményezi, hogy a parancsnokok vonakodnak ezeknek az „egyszer használatos" támadó képességeknek az alkalmazásától, így viszont idővel használhatatlanná is válnak.[46]

A kiberfegyverekkel szembeni védelem tehát a mai napig elégtelennek tekinthető. Az amerikai Védelmi Minisztérium Védelemtudományi Tanácsának egy 2013-as jelentése már úgy fogalmazott, hogy az Egyesült Államok nem lehet biztos abban, hogy a kritikus fontosságú informatikai rendszereket meg lehet védeni egy jelentős anyagi erőforrásokkal rendelkező ellenfél támadásával szemben.[47] A kibertér titokzatossága és az úgynevezett nul-

[43] Az Egyesült Államok kiberelrettentési politikájának egyik fontos kérdése, hogy a „leghangosabb" úgynevezett zero-day típusú sérülékenységeket milyen céllal, milyen döntéshozatali folyamat után és melyik szervezet (hírszerző közösség vagy védelmi minisztérium) vetheti be. Az USA kiberelrettentési politikájának hatékonyságáról és a kiberfegyverek paradoxonjáról bővebben lásd Timothy M. Goines: Overcoming the cyber weapons paradox. *Strategic Studies Quarterly,* 11. (2017), 4. 86–111.

[44] International Telecommunication Union (2015) i. m. 9–12.

[45] James E. McGhee: Liberating cyber offense. *Strategic Studies Quarterly,* 10. (2016), 4. 47.

[46] McGhee (2016) i. m. 57.

[47] Department of Defense, Defense Science Board: *Resilient military systems and the advanced cyber threat.* [online], Task Force Report, January 2013. 1. Forrás: nsarchive2.gwu.edu [2020. 11. 18.]

ladik napi *(zero-day)* sérülékenységek létezése a védelmet nagymértékben megnehezítik, ezért más védekezési megoldásokat és stratégiákat tesznek szükségessé, köztük a nemzetközi kiberhadviselési normák esetleges jövőbeni szabályozását, amelyre a kiberfegyverek proliferációjának elkerülése érdekében is szükség lehet.[48]

Oroszország tevékenysége és információbiztonsági doktrínája

Oroszország, a nyugati országoktól eltérően, egész másként gondolkodik a kiberhadviselésről: a különböző kiberműveleteket a tágabb értelemben vett információs hadviselés részeként értelmezi, beleértve a számítógép-hálózatokat, az elektronikai hadviselést és a pszichológiai vagy információs műveleteket is. Az amerikai döntéshozókhoz képest a Kreml könnyebb szívvel engedélyezi kibertámadások végrehajtását, akár hagyományos katonai műveletek elősegítésére is, továbbá Moszkva előszeretettel működik együtt különböző kiberbűnözői csoportokkal, amelyek könnyen bevethetők és letagadhatók.[49]

Az orosz kibertevékenységben az észtországi események tekinthetők az első mérföldkőnek a szakértők szerint. 2007-ben egy szovjet emlékmű áthelyezése heves tiltakozásokat váltott ki a helyi orosz kisebbségből. A demonstrációkat egy hónapon át tartó túlterheléses *(DDOS)* támadás követte, amely eleinte csak az észt szervereket, kormányzati oldalakat és szolgáltatásokat érintette, majd később a pénzügyi intézeteket, híroldalakat sem kímélte, és előfordult, hogy a feltört webhelyeken a támadók saját üzeneteiket helyezték el *(deface)*.[50] Hasonló kibertámadásokat hajtott végre Oroszország a grúz kormányzati infokommunikációs infrastruktúra ellen a 2008-as orosz–grúz háború idején.[51]

Újabb fordulatot jelentettek az orosz kibertevékenységekben a dél-ukrajnai Krímfélsziget elcsatolását követő események. A 2013-tól kezdődő kisebb kellemetlenségeket okozó kibertámadások után 2015-ben több órás áramkimaradást idézett elő egy kifinomult kibertámadás az egyik áramszolgáltató három nyugat-ukrajnai elosztóközpontjában. Az események rekonstrukciója alapján a szakértők megállapították, hogy egy jól szervezett és összehangolt támadásról van szó, amelyet több hónapos felderítés előzött meg. A támadás kifinomultsága arra enged következtetni, hogy minden bizonnyal állami vagy katonai irányítás alatt zajlott.[52] A Kovács László és Krasznay Csaba által elemzett amerikai hírszerzési jelentések arra is rámutatnak, hogy Oroszországnak komoly érdeke és lehetősége is volt kibertámadásokkal és álhírekkel világszerte befolyást gyakorolni emberek tömegére a 2016-os amerikai elnökválasztás során.[53]

Oroszország eddigi kiberhadviselési tevékenysége alapján elmondható, hogy Moszkva is készen áll kiberfegyverek alkalmazására a konfliktusok széles körét illetően és számos célpont ellen. Ugyanakkor megjegyzendő, hogy az amerikai atomfegyverek elítéléséhez

---

[48] Mazanec (2016) i. m. 106.

[49] Michael Connell – Sarah Vogler: *Russia's approach to cyber warfare.* [online], 2017. 03. Forrás: cna.org [2020. 11. 28]

[50] Joshua Davis: *Hackers take down the most wired country in Europe.* [online], 2007. 08. 21. Forrás: wired.com [2020. 11. 28.]

[51] Markoff (2008) i. m.

[52] Pavel Polityuk: *Ukraine sees Russian hand in cyber attacks against power grid.* [online], 2016. 02. 12. Forrás: reuters.com [2020. 11. 28.]

[53] Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság,* 10. (2017), 3. 3–15.

hasonlóan Oroszország most a poszthidegháborús időszakban ezúttal a kiberfegyverek nemzetközi tiltásának szükségességét hangoztatja, miközben saját maga is ilyen képességek kifejlesztésén fáradozik. Bár a kiberbiztonság és a kiberhadviselés területein az Egyesült Államok rendelkezik a legkifinomultabb eszközrendszerrel, Kína kibertevékenysége a leghangosabb, Moszkva pedig talán a leginkább titkolózó.[54]

Oroszország utoljára 2016-ban adott ki információbiztonsági doktrínát, amelyben az internettel, a kommunikációs hálózatokkal, az információs technológiákkal, az információk generálásával és feldolgozásával, illetve az információbiztonsággal foglalkozó entitások kombinációjával azonosítja az információs szférát. Az orosz stratégiai dokumentum az információs fenyegetést különböző tevékenységek és tényezők kombinációjaként értékeli, amelyek kockázatot jelentenek az orosz nemzeti érdekekre nézve az információs szférában. Az információs biztonság pedig a személyek, a társadalom és az orosz állam védelmi állapota a külső és a belső információs fenyegetésekkel szemben, amelynek szavatolására kormányzati szervek hivatottak (információs biztonsági erők). A dokumentum az információs szférában öt nemzeti érdeket határoz meg, és ezek között elsőként említi az alkotmányos emberi és állampolgári jogok és szabadságok biztosítását és védelmét. Ezt követi a kritikus információs infrastruktúra és az integrált telekommunikációs hálózatok működtetése békeidőben és háború esetén egyaránt. Harmadikként szerepel az információs és elektronikus technológiákkal kapcsolatos kutatás-fejlesztés, negyedikként az orosz és a nemzetközi közösség megbízható információkkal történő ellátása Oroszország politikáját illetően, ötödikként pedig egy nemzetközi információs biztonsági rendszer kifejlesztésének elősegítése, a stratégiai partnerségek erősítése és Oroszország információs szuverenitásának védelme.[55]

Az információs fenyegetéseket illetően az orosz doktrína kiemeli, hogy az információs technológiák fejlődésével egyre csak nő az információs fenyegetések száma. Részben azért is, mert egyre több állam fejleszt önálló kiberképességeket, amelyek alkalmasak lehetnek katonai alkalmazásra is. Az orosz doktrína szerint mindemellett a hírszerző szervek is egyre gyakrabban folyamodnak információs és pszichológiai eszközök alkalmazásához, hogy politikai és társadalmi instabilitást idézzenek elő egyes államokban. A dokumentum kiemeli, hogy a külföldi média egyre gyakrabban publikál az orosz politikával kapcsolatosan elfogult megállapításokat tartalmazó anyagokat, az orosz média komoly diszkriminációval néz szembe külföldön, az orosz újságírókat pedig rendszeresen megakadályozzák szakmai kötelességeik teljesítésében. Mindemellett különböző terrorszervezetek és szélsőséges csoportok is igyekeznek kihasználni az információs technológiákban rejlő lehetőségeket, ahogy a számítógéppel elkövetett bűncselekmények száma is növekszik.[56]

Nemzetvédelmi területen az orosz védelempolitika öt kulcsfontosságú területet jelölt meg, ahol kiemelt fontosságú az információbiztonság. Elsőként említi a stratégiai elrettentést és a katonai konfliktusok megelőzését, másodikként az orosz fegyveres erők információs rendszereinek fejlesztését, harmadikként az információs fenyegetések felderítését

[54] Mazanec (2016) i. m. 103–104.

[55] The Ministry of Foreign Affairs of the Russian Federation: *Doctrine of Information Security of the Russian Federation.* [online], 2016. 12. 05. Forrás: mid.ru [2020. 11. 15.]

[56] The Ministry of Foreign Affairs of the Russian Federation (2016) i. m.

és értékelését, negyedikként az orosz érdekek képviseletét az információs térben, végül pedig az anyaország védelmével kapcsolatos információs és pszichológiai tevékenységeket. Stratégiai célként a dokumentum Oroszország szuverenitásának, politikai és szociális stabilitásának, területi integritásának a védelmét, az alapvető emberi jogok és szabadságjogok biztosítását és a kritikus infrastruktúrák védelmét jelölte meg.[57]

Általánosságban elmondható, hogy a jövőben egyre nagyobb hangsúlyt kaphat az offenzív kiberműveletek hagyományos katonai műveletekbe integrálásának szükségessége. Ennek sikerességéhez azonban elengedhetetlen, hogy a katonai vezetők megértsék a kiberhadviselésben rejlő lehetőségeket. Az Egyesült Államok esetében a kiberműveletek végrehajtását jelenleg merev szabályok korlátozzák, ezzel szemben azonban a kibertér más főszereplői, köztük Oroszország is, gyakorlatilag korlátlanul hajthat végre kibertámadásokat. Mindemellett Moszkva és Peking is gyakran sikerrel alkalmaz a kormányhoz közvetlenül nem kötődő, kilétüket elfedő, független civil hackereket, ezzel is növelve képességeiket, illetve biztosítva az „elfogadható tagadhatóságra" való hivatkozás lehetőségét.[58] Az Orosz Belbiztonsági Szolgálat (FSB) emberei a klasszikus politikai kémkedésükkel már képesek voltak bejutni az Amerikai Külügyminisztérium, a Védelmi Minisztérium és a Fehér Ház informatikai hálózataiba is.[59] Kijelenthető, hogy sok tekintetben az orosz kiberképességek megfelelnek az amerikai képességeknek, miközben az orosz tevékenységet gyakorlatilag semmi sem korlátozza, ezáltal viszont az Egyesült Államok állandó védekező szerepbe kényszerül, ahelyett, hogy proaktív szereplő lenne a kibertérben.[60]

A Kínai Népköztársaság kiberképességei

Kína évekig kitartóan tagadta, hogy támadásokat hajtana végre a kibertérben, azonban egy 2012-es incidenst követően elismerte, hogy vannak titkos kiberhadviselési egységei a katonai és a civil szférában egyaránt.[61] Peking kiberképességeit és törekvéseit tárgyaló 2019-es cikkében Lyu Jinghua mégis amellett érvel, hogy Kína az őt érő fenyegetések hatására kezdett a kiberképességei fejlesztésébe a katonai stratégiájával teljes összhangban. Szerinte a 2000-es években hírszerzésre és ipari kémkedésre korlátozódott a kibertér szerepe Kína nemzetbiztonsági stratégiájában, mert a katonai döntéshozók úgy látták, hogy az információs technológia kulcsfontosságú tényezővé vált a fegyveres erők harcképességének növelésében. Peking célkitűzéseit tekintve kiemeli, hogy a kínai katonai stratégia egyik alapvető célja a társadalmi stabilitás biztosítása. Az utóbbi években ugyanis számos esemény rávilágított a közösségi média szerepére a tömegeket megmozgató tüntetések és tiltakozó akciók megszervezésében, illetve végrehajtásában. Az internet ellenőrzésével

[57] The Ministry of Foreign Affairs of the Russian Federation (2016) i. m.
[58] Bill Gertz: *Report: Chinese spies stole Pentagon secrets.* [online], 2016. 10. 27. Forrás: freebeacon.com [2020. 11. 23.]
[59] Bill Gertz: *China continuing cyber attacks on U.S. networks.* [online], 2016. 03. 18. Forrás: freebeacon.com [2020. 11. 22.]
[60] McGhee (2016) i. m. 58–59.
[61] BBC News: *US accuses China government and military of cyber-spying.* [online], 2013. 05. 07. Forrás: bbc.com [2020. 11. 27.]

a kormány célja a világszerte tapasztaltakhoz hasonló társadalmi elégedetlenséget szülő információk terjedésének megakadályozása a kommunista országban.[62]

A „csak védekező" Kínáról árnyaltabb képet festett le Mikk Raud egy 2016-os tanulmányában.[63] Míg az USA és Oroszország is publikált hivatalos dokumentumokat a kibertérben kifejtett aktivitásáról, Peking nem adott ki ilyen jellegű dokumentumot. Mindazonáltal az információ mindig kulcsszerepet játszott a kínai katonai stratégiában és a kibertér szorosan kapcsolódik a hírszerzéshez, ezáltal fellelhetők erre vonatkozó utalások a különböző katonai útmutatásokban. Nyilvánosan elsőként a *The Science of Military Strategy* 2013-as kiadásában jelent meg a kiberhadviselés, majd azt követően a 2015-ben publikált *China's Military Strategy* tanulmányban fogalmazódott meg a kiberbiztonság mai szerepe. Előbbi nyíltan tárgyalja Kína hálózati hadviselésre specializálódott egységeit is, amelyek mind a civil mind a katonai szférában tevékenykednek.[64] Washington gyakran vádolja Pekinget kémkedéssel, például a Huawei eszközeibe épített hátsó ajtókon *(backdoors)* keresztül, és 2020-ban nemzetbiztonsági érdekekre hivatkozva szabott ki jelentős gazdasági szankciókat a ZTE és a Huawei vállalatokra is az amerikai kormány. Ugyanakkor az USA és Kína közötti kereskedelmi háború az infokommunikációs ágazatban nem Donald Trump amerikai elnök intézkedéseivel kezdődött. Az amerikai cégek 20 évvel ezelőtt még számottevően több pénzt kaptak az infokommunikációs technológiai szabadalmaik után, ez azonban az utóbbi években jelentősen megváltozott, méghozzá a kínai versenytársak javára. Tekintettel az amerikai infokommunikációs vállalatok, mint például a Cisco iparági vezető szerepére és az 5G technológia térnyerésével az abban élen járó kínai Huawei jelentette veszélyre, a szigorú amerikai fellépés könnyen tűnhet megkésett gazdaságpolitikai reakciónak, sem mint nemzetbiztonsági érdekeket szolgáló intézkedésnek.[65]

A szakemberek szerint számos különböző APT[66]-csoport tevékenysége köthető Kínához, amelyeken keresztül az ország kiaknázhatja mind a kormányzati, mind a civil szférában tevékenykedő szakemberek tehetségét, köztük akár egyetemistákét vagy magánszemélyekét is.[67] Bár a nyilvánosan fellelhető információk korlátozottak, a kínai szakemberek által publikált információbiztonsági kutatások eredményeiből is lehet arra következtetni, milyen támadó jellegű képességekkel rendelkezhet Peking. Például, a Microsoft által legutóbb 2020 augusztusában közzétett kimutatás alapján – amelyben a vállalat az egyes kutatókat rangsorolja az általuk azonosított nulladik napi *(zero-day)* sérülékenységek szerint – a kínai kutatók évről évre az élmezőnyben végeznek, nem kis előnnyel vezetve a tabellát.[68] Mindez azért is figyelemre méltó, mert Krekel Bryan már egy 2009-es átfogó

---

[62] Lyu Jinghua: *What are China's cyber capabilities and intentions?.* [online], 2019. 04. 01. Forrás: carnegieendowment.org [2020. 11. 19.]

[63] Mikk Raud: *China and cyber: Attitudes, strategies, organisation.* [online], 2016. 08. Forrás: ccdcoe.org [2020. 11. 19.]

[64] Shannon Tiezzi: *China (finally) admits to hacking.* [online], 2015. 03. 18. Forrás: thediplomat.com [2020. 11. 19.]

[65] Evgeny Morozov: *There's a war going on over 5G (and no, that's not a conspiracy theory).* [online], 2020. 11. 18. Forrás: thecorrespondent.com [2020. 11. 28.]

[66] Advanced Persistent Threat (APT) alatt olyan kiberbűnözői csoportokat értünk, amelyek szervezetten, kifinomult módszerekkel és hosszú távon fejtik ki tevékenységüket.

[67] Jeff Stone: *Foreign spies use front companies to disguise their hacking, borrowing an old camouflage tactic.* [online], 2020. 10. 05. Forrás: cyberscoop.com [2020. 11. 27.]

[68] Sylvie Liu: *Congratulations to the MSRC's 2020 most valuable security researchers.* [online], 2020. 08. 05. Forrás: msrc-blog.microsoft.com [2020. 11. 19.]

jelentésében hangsúlyozta a civil fekete kalapos hackerek és az állam közvetlen együttműködésének valószínűségét, illetve a kereskedelmi alapú fehér kalapos információbiztonsági szakemberek kiterjedt kormányzati ügyfélkörét.[69] A 2017-ben alapított és azóta évente megrendezett *Tianfu Cup* napjainkra a legfontosabb információbiztonsági rendezvénnyé vált Kínában, amely jelentős pénzjutalmakkal vonzza a térség legtehetségesebb szakembereit. A szervezők nem titkolt szándéka, hogy a rendezvény az amerikai *Pwn2Own* verseny kínai megfelelője legyen.[70] A végeredmények alapján akár nyílt erődemonstrációnak is értékelhető az esemény, ugyanis a versenyzőknek a legnagyobb amerikai gyártók (köztük a Google, Apple, Microsoft, Adobe, Mozilla) termékeit sikerült feltörni, olykor mindössze öt perc leforgása alatt.[71] 2020-ban a *Microsoft Most Valuable Researcher* (MVR) program és a Tianfu Cup esemény győztesei is a Qihoo 360 vállalat szakemberei voltak, amely az egyik legkiemelkedőbb biztonsági kutatóvállalat Kínában. A kínai szakemberek sikerei egyértelműen azt mutatják, hogy a kormány és az információbiztonsági közösség közti együttműködés lehetősége nem elhanyagolható tényező.[72]

Kína folyamatosan fejleszti kiberképességeit, és láthatóan ezt aszimmetrikusan és stratégiai érdekek mentén teszi, arra készülve, hogy képes legyen kiberfegyverekkel gazdasági károkat okozni, kritikus infrastruktúrákat megrongálni vagy fegyveres konfliktusok menetét befolyásolni. Kínához az elmúlt években már számos hírszerzési célokat szolgáló kiberművelet volt köthető, amelynek eredményeként 2012-ben az amerikai védelmi minisztérium Kínát a „világ legaktívabb és legkitartóbb ipari kémkedőjének" minősítette, hozzátéve, hogy egyúttal „kiberképességek támadó jellegű műveletekben történő alkalmazására is törekszik".[73] Mindennek fényében megállapítható, hogy Peking nem érdekelt abban, hogy kiberképességei alkalmazásának valamilyen határt szabjon, vagy akár nemzetközi normákhoz kösse információs technológiai fejlesztéseit.[74]

Az internet megjelenése és elterjedése Kínában a médiát jelentős mértékben átalakította, hiszen egy zárt és központosított rendszerből egy nyílt és decentralizált rendszer felé mozdult el, miközben a lakosság nagy része is aktív internethasználó lett. 2020 márciusában a kínai internetezők száma elérte a 900 milliót, amivel Kína lépett az első helyre az online lakosság számát tekintve, megelőzve Indiát (560 millió internetező) és az Egyesült Államokat (313 millió internethasználó).[75] Ezzel párhuzamosan Peking jelentős lépéseket tett annak érdekében, hogy valamilyen mértékben ellenőrzése alatt tudja tartani

---

[69] Bryan Krekel: *Capability of the People's Republic of China to conduct cyber warfare and computer network exploitation.* [online], 2009. 10. 09. Forrás: nsarchive2.gwu.edu [2020. 11. 19.]

[70] A Pwn2Own egy nemzetközi hackerverseny, amelynek lényege, hogy a versenyzők megtarthatják az általuk feltört eszközöket és persze pénzjutalomban is részesülnek. 2007-ben Vancouverben hirdették meg először, és azóta évente két alkalommal is megrendezik. Az esemény egyik fő támogatója a Trend Micro, aki a sérülékenységeket a *Zero Day Initiative (ZDI)* programja keretében továbbítja az érintett gyártóknak, hogy kijavíthassák azokat.

[71] Catalin Cimpanu: *Windows 10, iOS, Chrome, and many others fall at China's top hacking contest.* [online], 2020. 11. 08. Forrás: zdnet.com [2020. 11. 09.]

[72] Jake Doevan: *Tianfu Cup 2020: Chinese hacking contest shows flaws in Chrome, Windows.* [online], 2020. 11. 10. Forrás: 2-spyware.com [2020. 11. 19.]

[73] Anna Mulrine: *China is a lead cyberattacker of US military computers, Pentagon reports.* [online], 2012. 05. 18. Forrás: csmonitor.com [2020. 11. 18.]

[74] Mazanec (2016) i. m. 103.

[75] Wan Lin: *China's internet users reach 900 million, live-streaming ecommerce boosting consumption: report.* [online], 2020. 04. 28. Forrás: globaltimes.cn [2020. 11. 17.]

az interneten megjelenő tartalmakat, többek között például nagyszámú propagandistát alkalmaz (50 Cent Army), akik a Kínai Kommunista Párt védelme érdekében szólnak hozzá különböző tartalmakhoz az interneten.[76] Peking álláspontja szerint minden ország saját kormányának kellene eldöntenie, hogy milyen információkat hagy az interneten az országhatárokon túljutni, nem cégeknek vagy nem kormányzati szervezeteknek. Ezért a Kínai Kommunista Párt egyfajta „kiberszuverenitás" kialakítására törekszik, amelynek érdekében cenzúrázni is hajlandó az internetet, a kínai példát pedig úgy tűnik, Oroszország és Irán is kész követni. Az internet szabadságának korlátozása már egy több éve zajló trend volt, amikor 2019 és 2020 telén kitört a koronavírus-járvány és jelentősen felgyorsította ezt a folyamatot, hiszen számos ország politikai vezetése a járványkezelés ürügyén igyekezett az információhoz való hozzáférést korlátozni és az internetet szabályozni.[77]

A Covid-19-pandémia mellett azonban voltak további jelentős események a világban, amelyeket az állami szereplők gyakran igyekeznek kihasználni. Ilyen volt a 2020-as amerikai elnökválasztás is, amellyel kapcsolatban Kínából tevékenykedő csoportok is igyekeztek minél több információt szerezni. A Microsoft jelentése szerint az egyik ilyen bűnözői csoport több ezer támadást hajtott végre. A közel 150 sikeres adathalász kísérlet, illetve rosszindulatú szoftver telepítését eredményező támadás biztosítja Kínának a további támadások megtervezéséhez és sikeres végrehajtásához szükséges információkat.[78]

Irán és Észak-Korea kibertevékenysége

Az 1978–79-es iráni iszlám forradalom óta Teherán kapcsolatai a nyugati országokkal konfliktusokkal terhelt, az Egyesült Államokkal és Izraellel azonban leginkább ellenséges. Washington – különösen a 2017–2021 közötti Trump-adminisztráció – az utóbbi években számos módon igyekezett az iráni rezsim regionális befolyását csökkenteni, beleértve a diplomáciai és a jogi lépések mellett a gazdasági szankciókat. Irán vitatott atomprogramja csak fokozta a nemzetközi feszültséget, Teherán katonai ambíciói miatt pedig nagymértékben megnőtt a nyugati országok aggodalma egy lehetséges iráni kibertámadás miatt is. A perzsa állam kiberbiztonságát illetően a minden bizonnyal az Egyesült Államokhoz és a zsidó államhoz köthető Stuxnet 2010-es felfedezése jelentette az igazi fordulópontot. Teherán ugyanis erre a Natanzi erőművet ért kibertámadásra válaszul kezdett a kiberképességei fejlesztésébe. A nyugati országokhoz hasonló katonai és gazdasági erő hiányában Irán az aszimmetrikus hadviselés egy új hadszíntereként tekint a kibertérre. Bár az iráni kiberműveletek elmaradnak kifinomultságukban, az iráni vezetés elszántsága miatt komoly fenyegetést jelentenek a célpontok számára, ahogy azt a *Microsoft Security Intelligence* által 2020. október 5-én kiadott figyelmeztetés is megállapította, amely szerint a MERCURY

[76] Henry Farrell: *The Chinese government fakes nearly 450 million social media comments a year. This is why.* [online], 2016. 05. 19. Forrás: washingtonpost.com [2020. 11. 17.]

[77] Adrian Shahbaz – Allie Funk: *Freedom on the Net 2020, The pandemic's digital shadow.* [online], 2020. 10. 12. Forrás: freedomhouse.org [2020. 11. 17.]

[78] Microsoft (2020) i. m. 48.

néven ismert iráni APT-csoport egy a közelmúltban javított kritikus sebezhetőséget kihasználva hajt végre kibertámadásokat.[79]

Kínához hasonlóan Irán sem adott ki hivatalos dokumentumokat a kibertevékenységét illetően, azonban az iráni kibertámadások stratégiai céljait Adam Hlavek négy pontban foglalta össze egy 2020 őszén megjelent cikkében. Hlavek szerint Irán elsődleges célja a mély gazdasági visszaesést kiváltó nemzetközi szankciók megkerülése és a gazdaság modernizációja. A második stratégiai cél a közel-keleti ellenfelek legyőzése kormányzatok, vállalatok és civil szervezetek elleni kibertámadások végrehajtásával, jellemzően hírszerzési, de – kivételes esetekben – akár károkozási céllal is. Mindezek mellett Kínához hasonlóan stratégiai cél a társadalmi stabilitás fenntartása és a rezsim hatalmának megőrzése is, amelynek Iránban is szerves része a média cenzúrája és a lakosság megfigyelése.[80] Ez utóbbi célt egészíti ki az ideológiai ellenfelek büntetése és hitelrontása, amit a szaúdi és katari olajvállalatok ellen bevetett *Shamoon* (APT33) névre keresztelt kártékony szoftver is jól illusztrál.[81]

Észak-Korea az elsők között

A CSIS jelentése szerint Észak-Korea eddig is rendszeresen folyamodott aszimmetrikus és irreguláris eszközökhöz, hogy kijátssza a Koreai-félszigeten előállt hagyományos katonai patthelyzetet. Phenjan kiberképességeit is fejleszti, hogy egy esetleges háború kitörése esetén bevethetők legyenek. A kiberképességek addig is lehetővé teszik az Egyesült Államok és Dél-Korea sebezhetőségeinek kihasználását a megtorlás vagy eszkaláció kockázatának minimalizálásával.[82]

Hyeong-wook Boo, a Koreai Védelmi Elemző Intézet (KIDA) kutatója szerint Észak-Korea jelenti az egyik legnagyobb kihívást a hírszerző szolgálatok számára, egyrészt az ideológiája, másrészt gazdasági helyzete miatt. Mivel a legszegényebb országok közé tartozik, ezért informatikai infrastruktúrája kezdetlegesnek tekinthető.[83] Észak-Koreában nem jellemző, hogy nyilvános Wi-Fi-hálózatot vagy felhőszolgáltatást venne igénybe a lakosság. A Google vezérigazgatója, Eric Schmidt egy 2013-as észak-koreai látogatását követően arról számolt be, hogy a lakosságnak gyakorlatilag egyáltalán nincs internet-hozzáférése. Csupán egy kiváltságos kisebbség csatlakozhat a világhálóra, leginkább kormányzati tisztségviselők, propagandisták, vezető kutatók és néhány egyetemi hallgató, de nekik is valószínűleg csak korlátozott hozzáférésük van, és a hatóságok folyamatosan monitorozzák az internethasználatot.[84] Ehhez képest viszont a kiberbiztonsági szakemberek több, igen

[79] Twitter: *Microsoft Security Intelligence, Twitter Thread on MERCURY.* [online], 2020. 10. 06. Forrás: twitter.com [2020. 11. 06.]

[80] Adam Hlavek: *The 4 strategic goals behind recent Iranian cyber attacks.* [online], 2020. 10. 26. Forrás: securityboulevard.com [2020. 11. 24.]

[81] Charlie Osborne: *Shamoon data-wiping malware believed to be the work of Iranian hackers.* [online], 2018. 12. 20. Forrás: zdnet.com [2020. 11. 24.]

[82] Jenny Jun et alii: *North Korea's cyber operations: Strategy and responses.* [online], 2015. 11. 23. Forrás: csis.org [2021. 05. 30.]

[83] Hyeong-wook Boo: An Assessment of North Korean Cyber Threats. *The Journal of East Asian Affairs,* 31. (2017), 1. 98.

[84] Justin McCurry – Jonathan Kaiman: *Google's Eric Schmidt says North Korea must open up to internet as visit ends.* [online], 2013. 01. 10. Forrás: theguardian.com [2020. 11. 26.]

kifinomult észak-koreai eredetű kibertámadást is megfigyeltek Dél-Korea és az Egyesült Államok ellen, kezdve 2004-ben az egyszerűbb DDoS-támadásoktól a népszerű weboldalak és e-mail-fiókok feltörésén keresztül a fejlett APT-támadásokig. Mindazonáltal még a kiberbiztonsági szakemberek számára sem könnyű felmérni Észak-Korea kiberképességeit és szándékait.[85]

Talán az egyik leghíresebb Észak-Koreához köthető kibertámadás a *Lazarus Group* által az amerikai *Sony Pictures* ellen végrehajtott támadás volt 2004-ben, amelyben a *Destover* néven ismert rosszindulatú szoftver segítségével jelentős adatvesztést okoztak a vállalatnak. Ez az incidens komoly figyelemfelkeltő hatású volt, ám nem sokkal később egy újabb hasonló, észak-koreai kötődésű támadásra lettek figyelmesek a szakemberek, amelynek célpontja a dél-koreai *Korea Hydro* nevű, atomerőműveket üzemeltető vállalat volt. Ez a támadás valószínűleg arra szolgált, hogy Észak-Korea megmutassa, képes akár komoly fizikai károkat is okozni egy kibertámadással, és világszerte növelte az atomlétesítmények biztonságával és védelmével kapcsolatos aggodalmakat.[86]

Az észak-koreai kiberképességeket vizsgálva Boo szerint figyelemre méltó, ahogy az vált az általános támadási eljárássá, hogy a hagyományos biztonsági fenyegetéseket nem hagyományos fenyegetésekkel vegyítik, azaz összehangolják a kibertámadásokat az egyéb katonai műveletekkel, például nukleáris vagy rakétatesztekkel. Másrészt pedig az is figyelemre méltó, hogy a kiberműveleteiket ki tudták terjeszteni a mobileszközökre is, szöveges üzeneteket megszerezve, telefonbeszélgetéseket rögzítve és kontaktszemélyek információit ellopva. Emellett az észak-koreai kibertámadások eddigi egyik legkomolyabb ambíciója a dél-koreai tömegközlekedés megbénítása volt, amelyre több alkalommal is kísérletet tettek a szöuli metróhálózat irányító rendszerének támadásával. Az utóbbi időben pedig az észak-koreai kibertevékenység egyre inkább katonai motivációval és célokkal zajlik. Kijelenthető, hogy Észak-Korea számára az atomprogramja mellett a kiberfegyverek fejlesztése volt a másik lehetőség, amellyel a rezsim ellensúlyozhatja lemaradását Dél-Koreával szemben, hiszen a kibertevékenységével Észak-Korea könnyen káoszt idézhetne elő fejlett déli szomszédjánál, például a tömegközlekedés megbénításával.[87]

Disszidensektől származó információk szerint Kim Dzsongil 1998-ban hozta létre a Bureau 121 (vagy Unit 121) nevű kiberhadviselési ügynökségét, amely azóta 30 ezernél is több kibertámadást hajtott végre, elsősorban Dél-Korea ellen. Médiajelentések szerint akkoriban maga a „Nagy Vezető" hangsúlyozta a kiberháborús képességek fejlesztésének fontosságát, kijelentve, hogy „a 20. század háborúja az olaj és a golyók háborúja volt, de a 21. századé hírszerzési háború".[88] Szakértők szerint ennek az észak-koreai „hírszerzési háborúnak" a része a kiberháború, ezért a fegyveres erők az „elektronikai hírszerzés" keretében igyekeztek fejleszteni kiberhadviselési képességeiket, amelyekkel képesek lehetnek informatikai hálózati kapcsolatokat megszakítani, infrastruktúrát megrongálni és az ellenség vezetés-irányítási rendszereit megbénítani.[89]

---

[85] Boo (2017) i. m. 99.

[86] Justin McCurry: *South Korean nuclear operator hacked amid cyber-attack fears.* [online], 2014. 12. 23. Forrás: theguardian.com [2020. 11. 26.]

[87] Boo (2017) i. m. 103–104.

[88] Mok Yong Jae: *North Korea's powerful cyber warfare capabilities.* [online], 2011. 05. 04. Forrás: dailynk.com [2020. 11. 26.]

[89] Boo (2017) i. m. 107–108.

Megjegyzendő, hogy Észak-Korea kormánya a jövő szakembereinek kiképzése érdekében külön intézményrendszert – beleértve több felsőoktatási intézményt – hozott létre, és gyakorlatilag már az 1980-as évek közepe óta képzi a hivatásos kiberkatonákat, így érthető, hogyan sikerült figyelemre méltó támadó képességekre is szert tennie. Médiajelentések szerint a legjobb szakembereket képző főiskolák (Mirim College, Moranbong College) szoros kapcsolatban állnak a Koreai Néphadsereggel, és évente több száz hivatásos kiberkatonát képeznek.[90] Az amerikai hadsereg egy 2020 júliusában kiadott jelentése szerint Észak-Koreának már legalább 6000 informatikai és elektronikai hadviselési specialistája van, amelyek közül sokan külföldről tevékenykednek, például Beloruszból, Kínából, Indiából, Malajziából vagy Oroszországból.[91]

Következtetések

A szakértők rendszeresen felhívják a figyelmet arra, hogy a támadók képességeinek fejlődésével egyre fontosabbá válik a kibertér biztonsága érdekében új szabályokat alkotni és bizonyos óvintézkedéseket fokozott figyelemmel betartani. Legyen szó akár a vállalati szféráról, akár kormányzati hivatalokról és ügynökségekről, a támadások megelőzése és sikeres elhárítása érdekében nem megspórolható a szükséges emberi erőforrásba és technológiába történő befektetés. Továbbá kiemelt jelentősége van a felhasználók felkészítésének, különösképpen az olyan alapvető óvintézkedések betartására vonatkozó figyelemfelhívásnak, mint a biztonsági frissítések rendszeres telepítése, gyakori biztonsági mentések készítése, valamint a többlépcsős azonosítás *(multi-factor authentication)* alkalmazása, amellyel a Microsoft szerint a sikeres támadások többsége megakadályozható lett volna.[92]

Mindemellett megjegyzendő, hogy egyesek szerint bizonyos támadó jellegű kibereszközök tömegpusztító fegyvernek is minősülhetnek, az amerikai vezérkari főnökök egyesített bizottságának elnöke (JCS) pedig már 2004-ben hivatalosan elismerte a kiberfegyverek potenciális romboló erejét a fizikai hadszíntéren.[93] Médiajelentések és más nyilvánosan hozzáférhető beszámolók alapján arra lehet következtetni, hogy az Egyesült Államok rendelkezik olyan kiberfegyverekkel, amelyek a fizikai hadszíntéren is jelentős pusztítást végezhetnek. Például a Stuxnethez hasonló kártékony programmal, ami képes volt túlterhelni az iráni nukleáris dúsítócentrifugákat, vagy olyan vírusokkal, amelyekkel szabotálni lehet egy észak-koreai rakétakilövést.[94] Bár e támadások hatása nem ér fel egy tömegpusztító

[90] Bruce Harrison: *How North Korea recruits its army of young hackers.* [online], 2017. 12. 08. Forrás: nbcnews.com [2020. 11. 26.]

[91] Catalin Cimpanu: *US Army report says many North Korean hackers operate from abroad.* [online], 2020. 08. 18. Forrás: zdnet.com [2020. 11. 26]

[92] Burt (2020b) i. m.

[93] Benjamin B. Hatch: Defining a class of cyber weapons as WMD: An Examination of the Merits. *Journal of Strategic Security,* 11. (2018), 1. 44–47.

[94] David E. Sanger – Eric Schmitt: *U.S. cyberweapons, used against Iran and North Korea, are a disappointment against ISIS.* [online], 2017. 06. 12. Forrás: nytimes.com [2020. 11. 17.]

fegyver erejével, de jól jelzik a kiberfegyverek fejlesztésében rejlő lehetőségeket és azok potenciális romboló erejét.[95]

A kiberfenyegetések azonosítása és értékelése *(cyber threat intelligence)* továbbra is a már bekövetkezett támadásokkal kapcsolatos adatok összegyűjtésén alapszik, miközben egyre nyilvánvalóbbá válik, hogy ez a fajta reaktív megközelítés már ma sem elegendő biztonsági szempontból. Éppen ezért, a kiberbiztonsági területnek proaktívvá kell majd válnia, hálózati adatokat és a kibertéren kívüli, az ellenfelek képességeire, szándékaira és tevékenységeire vonatkozó hírszerzési információkat is magában foglaló kiberhírszerzési elemzések és értékelések által vezérelve. A kiberhírszerzésnek nem csupán a hálózati műveletek technikai aspektusaival kellene foglalkoznia, hanem az ellenfelek képességeivel és motivációival is. Amennyiben a kiberbiztonsági szakemberek számára több információ állna rendelkezésre, az jelentős mértékben segíthetné a kibervédelmi intézkedések mellett a műveleti és a stratégiai döntéshozatali irányba történő elmozdulást. A biztonsági környezet folyamatosan változik. A kibertér gyakorlatilag napról napra összetettebb és még nehezebben átlátható lesz, s ez továbbra is állandó kihívást jelent majd a szakemberek számára. Az elmúlt évtizedben a mobileszközök széles körű elterjedése tette még bonyolultabbá a kiberbiztonsági szakemberek dolgát, a következő években pedig az 5G technológia elterjedése és az IoT-eszközök számának gyors növekedése fog várhatóan komoly változásokat és kihívásokat hozni. Mindeközben a kibertér ártó szándékú szereplői igyekeznek majd a technológiai fejlődésben rejlő lehetőségeket saját céljaikra felhasználni, amelyre válaszul a információbiztonsági közösségnek folyamatosan fejlesztenie kell majd a biztonsági termékeket és szolgáltatásokat, a technológiai problémákra azonban nem jelenthet mindig megoldást egy következő technológiai újítás, ezért ezen a téren szemléletváltásra lesz szükség.[96]

A kiberfenyegetések egyre inkább összekapcsolódnak az aszimmetrikus fenyegetések kifejezéssel, hiszen a kiberhadviselés lehetőséget ad arra, hogy egy korlátozott anyagi erőforrásokkal rendelkező fejlődő ország károkat tudjon okozni akár egy nála jóval fejlettebb és gazdagabb ország információtechnológiai és kommunikációs rendszereiben, szinte minimális anyagi ráfordítással. Ebben a tekintetben pedig egy adott ország magasan fejlett technológiai színvonala hátrány is lehet, hiszen az egész országot lefedő informatikai hálózatok működésében okozott fennakadások vagy károk tovagyűrűző működészavart is eredményezhetnek.[97]

---

[95] Albert Mauroni, a tömegpusztító fegyverek egyik elismert szakértője szerint három feltételnek kell megfelelnie egy kiberfegyvernek ahhoz, hogy tömegpusztító fegyvernek lehessen azt minősíteni. Ebből az egyik az, hogy az adott rendszert fegyvernek kellett, hogy tervezzék. A második pedig az, hogy bevetésének legalább ezer halálos áldozattal és sebesülttel kell járnia. Az amerikai védelmi minisztérium három példát is megadott, amikor kiberfegyverek bevetése tömeges áldozatokkal járna: 1. atomerőmű leolvadásának előidézése; 2. egy duzzasztógát megnyitása lakott területek elárasztásával; 3. légiforgalom-irányító szolgálatok megbénítása, amely repülőgép-szerencsétlenségekhez vezetne. Az utolsó feltétel Mauroni szerint pedig az, hogy a tömegpusztító fegyverek definícióját nemzetközi megállapodásban a fegyverrendszerek speciális kategóriájaként kellene definiálni. Albert J. Mauroni: *Countering Weapons of Mass Destruction: Assessing the U.S. Government's Policy.* New York, Rowman & Littlefield, 2016. 36.

[96] E. J. Mandt: Integrating cyber-intelligence analysis and active cyber-defence operations. *Journal of Information Warfare,* 16. (2017), 1. 38. 45.

[97] Boo (2017) i. m. 104.

Felhasznált irodalom

BBC News: *US accuses China government and military of cyber-spying.* [online], 2013. 05. 07. Forrás: bbc.com [2020. 11. 27.]

Boo, Hyeong-wook. An Assessment of North Korean Cyber Threats. *The Journal of East Asian Affairs,* 31. (2017), 1. 97–117.

Boyd, Aaron: *DNI Clapper: Cyber bigger threat than terrorism*. [online], 2016. 02. 04. Forrás: federaltimes.com [2020. 11. 14.]

Burt, Tom: *Protecting healthcare and human rights organizations from cyberattacks.* [online], 2020a. 04. 14. Forrás: blogs.microsoft.com [2020. 11. 08.]

Burt, Tom: *Microsoft report shows increasing sophistication of cyber threats.* [online], 2020b. 09. 29. Forrás: blogs.microsoft.com [2020. 11. 08.]

Cimpanu, Catalin: *US Army report says many North Korean hackers operate from abroad.* [online], 2020. 08. 18. Forrás: zdnet.com [2020. 11. 26]

Cimpanu, Catalin: *Windows 10, iOS, Chrome, and many others fall at China's top hacking contest*. [online], 2020. 11. 08. Forrás: zdnet.com [2020. 11. 28.]

Claus, Brian – Robin A. Gandhi – Julia Rawnsley – John Crowe: Using the oldest military force for the newest national defense. *Journal of Strategic Security,* 8. (2015), 4. 1–22. Online: https://doi.org/10.5038/1944-0472.8.4.1441

Clayton, Mark: *The new cyber arms race.* [online], 2011. 03. 07. Forrás: csmonitor.com [2020. 11. 22.]

Collier, Kevin: *Major hospital system hit with cyberattack, potentially largest in U.S. history.* [online], 2020. 09. 28. Forrás: nbcnews.com [2020. 11. 15.]

Connell, Michael – Sarah Vogler: *Russia's approach to cyber warfare.* [online], 2017. 03. Forrás: cna.org [2020. 11. 28]

Conti, Gregory – Robert Fanelli: How could they not: Thinking like a state cyber threat actor. *The Cyber Defense Review,* 4. (2019), 2. 49–64.

Davis, Joshua: Hackers Take down the most wired country in Europe. [online], 2007. 08. 21. Forrás: wired.com [2020. 11. 28.]

Department of Defense, Defense Science Board: *Resilient military systems and the advanced cyber threat.* [online], Task Force Report, 01. 2013. Forrás: nsarchive2.gwu.edu [2020. 11. 18.]

Department of Homeland Security, CISA: *US-CERT, United States Computer Emergency Readiness Team.* [online], DHS Info Sheet. Forrás: us-cert.cisa.gov [2020. 11. 22.]

DoD Fact Sheet: *Cyber Mission Force.* [online], 2020. 02. 10. Forrás: arcyber.army.mil [2020. 11. 14.]

Doevan, Jake: *Tianfu Cup 2020: Chinese hacking contest shows flaws in Chrome, Windows.* [online], 2020. 11. 10. Forrás: 2-spyware.com [2020. 11. 19.]

Eddy, Melissa – Nicole Perlroth: *Cyber attack suspected in German woman's death.* [online], 2020. 09. 18. Forrás: nytimes.com [2020. 11. 15.]

Farrell, Henry: *The Chinese government fakes nearly 450 million social media comments a year. This is why.* [online], 2016. 05. 19. Forrás: washingtonpost.com [2020. 11. 17.]

Gatlan, Sergiu: *World Health Organization warns of coronavirus phishing attacks.* [online], 2020. 02. 17. Forrás: bleepingcomputer.com [2020. 11. 08.]

Gertz, Bill: *China continuing cyber attacks on U.S. networks.* [online], 2016. 03. 18. Forrás: freebeacon.com [2020. 11. 22.]

Gertz, Bill: *Report: Chinese spies stole Pentagon secrets.* [online], 2016. 10. 27. Forrás: freebeacon.com [2020. 11. 23.]

Goel, Sanjay: National cyber security strategy and the emergence of strong digital borders. *Connections,* 19. (2020), 1. 73–86. Online: https://doi.org/10.11610/Connections.19.1.07

Goines, Timothy M.: Overcoming the cyber weapons paradox. *Strategic Studies Quarterly,* 11. (2017), 4. 86–111.

GSMA: *The Mobile Economy 2020.* [online], 2020. 03. Forrás: gsma.com [2020. 11. 15.]

H. R. 1640 – Cyber Warrior Act of 2013, 113th Congress (2013–2014), [online], 2013. 04. 18. Forrás: congress.gov [2020. 11. 15.]

Harrison, Bruce: *How North Korea recruits its army of young hackers.* [online], 2017. 12. 08. Forrás: nbcnews.com [2020. 11. 26.]

Hatch, Benjamin B.: Defining a class of cyber weapons as WMD: An examination of the merits. *Journal of Strategic Security,* 11. (2018), 1. 43–61. Online: https://doi.org/10.5038/1944-0472.11.1.1657

Hlavek, Adam: *The 4 strategic goals behind recent Iranian cyber attacks.* [online], 2020. 10. 26. Forrás: security-boulevard.com [2020. 11. 24.]

Holland, John H.: Studying complex adaptive systems. *Journal of Systems Science and Complexity,* 19. (2006), 1. 1–8. Online: https://doi.org/10.1007/s11424-006-0001-z

Hosenball, Mark – Patricia Zengerle: *Cyber attacks leading threat against U.S.: spy agencies.* [online], 2013. 03. 12. Forrás: reuters.com [2020. 11. 14.]

International Telecommunication Union: *US Department of Defense Cyber Strategy.* [online], 2015. 04. Forrás: itu.int [2020. 11. 13.]

Jae, Mok Yong: *North Korea's powerful cyber warfare capabilities.* [online], 2011. 05. 04. Forrás: dailynk.com [2020. 11. 26.]

Jinghua, Lyu: *What are China's cyber capabilities and intentions?.* [online], 2019. 04. 01. Forrás: carnegieendowment.org [2020. 11. 19.]

Jun, Jenny – Victor Cha – James Andrew Lewis – Scott LaFoy – Ethan Sohn: North Korea's Cyber operations: Strategy and responses. [online], 2015. 11. 23. Forrás: csis.org [2021. 05. 30.]

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

Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság,* 10. (2017), 3. 3–15.

Krekel, Bryan: C*apability of the People's Republic of China to conduct cyber warfare and computer network exploitation.* [online], 2009. 10. 09. Forrás: nsarchive2.gwu.edu [2020. 11. 19.]

Lin, Wan: *China's internet users reach 900 million, live-streaming ecommerce boosting consumption: report.* [online], 2020. 04. 28. Forrás: globaltimes.cn [2020. 11. 17.]

Liu, Sylvie: *Congratulations to the MSRC's 2020 most valuable security researchers.* [online], 2020. 08. 05. Forrás: msrc-blog.microsoft.com [2020. 11. 19.]

Mandt, EJ.: Integrating Cyber-intelligence analysis and active cyber-defence operations. *Journal of Information Warfare,* 16. (2017), 1. 31–48.

Markoff, John: *Before the gunfire, cyberattacks.* [online], 2008. 08. 12. Forrás: nytimes.com [2020. 11. 22.]

Mauroni, Albert J.: *Countering Weapons of Mass Destruction: Assessing the U.S. Government's Policy*. New York, Rowman & Littlefield, 2016.

Mazanec, Brian M.: Constraining Norms for Cyber Warfare Are Unlikely. *Georgetown Journal of International Affairs,* 17. (2016), 3. 100–109. Online: https://doi.org/10.1353/gia.2016.0040

McCurry, Justin – Jonathan Kaiman: *Google's Eric Schmidt says North Korea must open up to internet as visit ends.* [online], 2013. 01. 10. Forrás: theguardian.com [2020. 11. 26.]

McCurry, Justin: *South Korean nuclear operator hacked amid cyber-attack fears.* [online], 2014. 12. 23. Forrás: theguardian.com [2020. 11. 26.]

McGhee, James E.: Liberating cyber offense. *Strategic Studies Quarterly,* 10. (2016), 4. 46–63.

Microsoft: *Microsoft Digital Defense Report.* [online], 2020. 09. Forrás: microsoft.com [2020. 11. 08.] Online: https://doi.org/10.1016/S1353-4858(20)30114-8

The Ministry of Foreign Affairs of the Russian Federation: *Doctrine of Information Security of the Russian Federation.* [online], 2016. 12. 05. Forrás: mid.ru [2020. 11. 15.]

Morozov, Evgeny: *There's a war going on over 5G (and no, that's not a conspiracy theory).* [online], 2020. 11. 18. Forrás: thecorrespondent.com [2020. 11. 28.]

Mulrine, Anna: *China is a lead cyberattacker of US military computers, Pentagon reports.* [online], 2012. 05. 18. Forrás: csmonitor.com [2020. 11. 18.]

NATO: *NATO cyber defence fact sheet.* [online], July 2016. Forrás: nato.int [2020. 11. 23.]

Oliver Wyman Forum Team: *Why is cybersecurity so hard – and getting harder? what can be done?.* [online], 2019. 09. 18. Forrás: oliverwymanforum.com [2021. 05. 30.]

Osborne, Charlie: *Shamoon data-wiping malware believed to be the work of Iranian hackers.* [online], 2018. 12. 20. Forrás: zdnet.com [2020. 11. 24.]

Polityuk, Pavel: *Ukraine sees Russian hand in cyber attacks against power grid.* [online], 2016. 02. 12. Forrás: reuters.com [2020. 11. 28.]
Raud, Mikk: *China and cyber: Attitudes, strategies, organisation.* [online], 2016. 08. Forrás: ccdcoe.org [2020. 11. 19.]
Sanger, David E. – Eric Schmitt: *U.S. cyberweapons, used against Iran and North Korea, are a disappointment against ISIS.* [online], 2017. 06. 12. Forrás: nytimes.com [2020. 11. 17.]
Shahbaz, Adrian – Allie Funk: *Freedom on the Net 2020, The pandemic's digital shadow.* [online], 2020. 10. 12. Forrás: freedomhouse.org [2020. 11. 17.]
Simos, Mark: *Zero Trust strategy – what good looks like.* [online], 2019. 11. 11. Forrás: microsoft.com [2020. 11. 09.]
Stone, Jeff: *Foreign spies use front companies to disguise their hacking, borrowing an old camouflage tactic.* [online], 2020. 10. 05. Forrás: cyberscoop.com [2020. 11. 27.]
Suleymanova, Radmilla: *As new wave of COVID-19 cases hits, remote work becomes the norm.* [online], 2020. 10. 18. Forrás: aljazeera.com [2020. 11. 09.]
Taylor, Guy: *James Clapper, intel chief: Cyber ranks highest on worldwide threats to U.S..* [online], 2015. 02. 26. Forrás: washingtontimes.com [2020. 11. 14.]
Tiezzi, Shannon: *China (finally) admits to hacking.* [online], 2015. 03. 18. Forrás: thediplomat.com [2020. 11. 19.]
Tumkevič, A.: Uncertain security community: Building Western cyber-security order. *Journal of Information Warfare,* 17. (2018), 1. 74–86.
Twitter: *Microsoft Security Intelligence, Twitter Thread on MERCURY.* [online], 2020. 10. 06. Forrás: twitter.com [2020. 11. 06.]
Ülgen, Sinan: *A lack of cybernorms threatens Western democracies.* [online], 2016. 12. 14. Forrás: carnegieeurope.eu [2020. 11. 23.]
Van Der Werff, Emily – Lee, Timothy B.: *The 2014 Sony hacks, explained.* [online], 2015. 06. 03. Forrás: vox.com [2020. 11. 13.]