Selján Péter[1]

A jelen kiberbiztonsági fenyegetései és a jövő kihívásai – A nemzetállami aktorok tevékenysége és a dezinformációk terjedése

A technológiai fejlődés rendkívüli gyorsasága miatt folyamatosan átalakulóban van a kiberbiztonsági környezet, amely ráadásul a kihasználható sérülékenységek számának, azaz a sebezhetőségek gyakoriságának, ezáltal pedig a „támadási felület" nagyságának növekedése nyomán egyre romló tendenciát mutat. A legkomolyabb kiberbiztonsági fenyegetést jelentő, államokhoz köthető aktorok viszont igyekeznek minél jobban kihasználni ezt a helyzetet. Jelen tanulmány vezető iparági és egyéb szakmai jelentések alapján kísérli meg összefoglalni 2021 és 2022 első felének legfontosabb kiberbiztonsági fejleményeit, elsősorban az állami szereplők jelentette fenyegetésekre koncentrálva. A teljesség igénye nélkül ismerteti a vezető rosszindulatú nemzetállami aktoroknak – köztük Oroszországnak és Kínának – tulajdonítható, a vizsgált időszakban megfigyelt kibertevékenységét. Mindemellett igyekszik felhívni a figyelmet napjaink kiberbiztonsági fenyegetéseire és a jövő várható kihívásaira – mint például a dezinformációk egyre gyorsabb terjedése –, mindezt azonban anélkül, hogy mélyebb elemzésbe bocsátkozna, szükségtelenül.

Kulcsszavak: *kiberbiztonság, kiberhadviselés, biztonságpolitika, Oroszország, Kína*

Current Cyber Security Threats and Future Challenges – Nation-State Threat Actors and Disinformation

The cybersecurity environment is constantly deteriorating partly due to the extraordinary speed of technological development, which increases the number and frequency of exploitable vulnerabilities i.e., the size of the "attack surface" in cyber space. However, nation-state threat actors that pose the most serious challenge are trying to make the most out of the deteriorating and unpredictable cyber security environment. Based on leading industry and cyber security reports, the present paper seeks to summarise the key developments of 2021 and the first half of 2022, focusing primarily on the leading nation-state threat actors. Without wishing to be exhaustive, this paper describes the cyber activities observed during the examined period which deemed attributable to the leading malicious nation-state actors – including hacker groups in Russia and China. In addition, it tries to draw attention to today's cyber security threats and the challenges ahead – such as the ever faster spread of disinformation – but all this without engaging in a deeper analysis, unnecessarily.

Keywords: *cybersecurity, cyberwarfare, security policy, Russia, China*

[1] Selján Péter okleveles biztonság- és védelempolitikai szakértő, a politikatudományok doktora. E-mail: peter@seljan.hu

1. Bevezetés

Az elmúlt néhány év rohamos technológiai fejlődésének következtében a forradalmi technológiák fejlesztése és alkalmazása vált a nagyhatalmak közötti versenyfutás egyik fő színterévé. Noha a technológiai rivalizálás elsősorban az Egyesült Államok és Kína között zajlik, közben egyre több szereplő kapcsolódik be a versenybe, amely már globális szinten megfigyelhető, és számos területen érzékelteti a hatását. Ennek a folyamatnak a következtében a digitális világ és a mindennapi életünk is jelentős átalakuláson megy keresztül, amelynek egyik lehetséges végeredménye a technológiai ellátási láncok szétkapcsolódása, vagy akár a globális internet széttöredezése *(splinternet)*[2] lehet.[3]

Az amerikai hírszerző szolgálatok vezetői már 2017 januárjában egy, a Szenátus fegyveres szolgálatokkal foglalkozó bizottságának küldött közös nyilatkozatukban felhívták a figyelmet arra, hogy az információs technológiák és a kommunikáció egyre nagyobb szerepet játszanak az Egyesült Államok biztonságában. A kibertér bár komoly lehetőségeket rejt magában, új fenyegetések forrása is egyben, amelyet az ellenséges szereplők kémkedésre, befolyásolásra és egyértelmű támadó szándékkal is felhasználnak. 2016 végén már több mint 30 ország fejlesztett offenzív kiberképességeket, a Belfer Center által összeállított *National Cyber Power Index 2020* megállapításai szerint pedig 27 ország már biztosan rendelkezik valamilyen offenzív jellegű képességgel.[4] A trend évek óta egyértelmű, és már mindenki számára világos, hogy a mai világban a kiberképességek elengedhetetlenek egy állam számára a biztonság és a hatalom garantálásához. A 21. század első évtizedeinek eseményei már előrevetítették ezeket a folyamatokat. A kiberfegyverek államokkal szembeni alkalmazására 2007 óta több alkalommal is fény derült (lásd Észtország,[5] Grúzia,[6] Irán[7] vagy Ukrajna esetét), miközben a hírszerzési képességek is gyakorlatilag forradalmi átalakuláson mentek keresztül az új digitális eszközöknek köszönhetően.[8] A digitális technológiák tehát az államok közötti rivalizálás új színterei,

---

[2] A *„splinternet"* kifejezés alatt azt értjük, hogy a nyílt globális internet kormányok vagy nagyvállalatok által ellenőrzött „kisebb darabokra" eshet szét, illetve fragmentálódhat a következő években és évtizedekben. Ez a valóságban azt jelentené, hogy mindenhol csak ahhoz lehetne hozzáférni, amit az adott országban a kormány és a szolgáltatók elérhetővé tesznek, lásd Kína vagy az ukrajnai háború kapcsán Oroszország esetét. Dan York: *What Is the Splinternet? And Why You Should Be Paying Attention*. [online], Internet Society, 2022. március 23. Forrás: internetsociety.org [2022. 05. 31.].

[3] Az amerikai, európai, afrikai, ázsiai és ausztrál politikai vezetők nyíltan ki szoktak állni a digitális szuverenitás és a technológiai autonómia mellett, miközben elemzők és nemzetközi megfigyelők rendszeresen felhívják a figyelmet a digitális világ „blokkosodásának", elsősorban egymással szemben álló amerikai és kínai blokkok kialakulásának a reális kockázatára. Michał Rekowski et al.: *Geopolitics of Emerging and Disruptive Technologies*. [online]. Krakow, The Kosciuszko Institute, 2020. 8. Forrás: ik. org.pl [2022. 05. 29.].

[4] James R. Clapper – Marcel Lettre – Michael S. Rogers: *Joint Statement for the Record to the Senate Armed Services Committee, Foreign Cyber Threats to the United States*. [online], Senate Armed Services Committee, 2017. január 5. Forrás: armed-services.senate.gov [2022. 05. 29.]; Julia Voo et al.: *National Cyber Power Index 2020. Methodology and Analytical Considerations*. [online], Belfer Center, 2020. szeptember. 43. Forrás: belfercenter.org [2022. 08. 06.].

[5] *Cyber Attacks against Estonia (2007)*. [online], Cyber Law Toolkit, 2007. április 27. Forrás: cyberlaw.ccdcoe.org [2022. 06. 04.].

[6] *Georgia–Russia Conflict (2008)*. [online], Cyber Law Toolkit, 2008. július–augusztus. Forrás: cyberlaw.ccdcoe.org [2022. 06. 04.].

[7] Andrew Hanna: *The Invisible U.S.–Iran Cyber War*. [online], The Iran Primer, 2019. október 25. Forrás: iranprimer.usip.org [2022. 06. 04.].

[8] *Edward Snowden: Leaks that Exposed US Spy Programme*. [online], BBC, 2014. január 17. Forrás: bbc.com [2022. 06. 04.].

és minden bizonnyal meghatározó szerepet fognak játszani a globális vezető szerepért folytatott verseny alakulásában.[9]

Jelen tanulmány a 2021 ősze óta kiadott nemzetközi elemzések, jelentések és sajtóbeszámolók alapján igyekszik ismertetni az elmúlt egy-két év kiberbiztonsági fejleményeit, illetve egyfajta helyzetjelentéssel szeretne szolgálni a nemzetállami szereplők jelentette kiberbiztonsági fenyegetéseket és kockázatokat illetően. E cél elérése érdekében először a kiberbiztonsági környezet alakulását tárgyalja általánosságban, megemlítve a fontosabb trendeket és eseményeket. Ezt követően a legfontosabb vezető állami fenyegetéseket ismerteti, kezdve Oroszország kibertevékenységével, amelynek kiemelt figyelmet szán, ugyanakkor – bár a teljesség igénye nélkül, de – beszámol Kína, Irán és röviden Észak-Korea releváns kiberműveleteiről is. A nemzetállamokhoz köthető, kiemelt fenyegetést jelentő szereplőket egy táblázatban is összefoglalom (lásd 1. táblázat). A dolgozat végén szó esik a dezinformáció egyre gyorsabb terjedésének problematikájáról is, amely bár nem igazán tekinthető újdonságnak, a technológiai háttér drasztikus sebességű fejlődése miatt azonban várhatóan egyre komolyabb kihívást jelent majd, ezért mindenképp érdemes kitérni rá. A tanulmányt végül rövid összefoglalás zárja.

2. Romló kiberbiztonsági környezet

A Microsoft évente megjelenő, legutóbb 2021 októberében kiadott jelentése[10] szerint a kiberbűnözés új szintet lépett az elmúlt években: a bűnözők aktívabbá, míg a támadások kifinomultabbá váltak. Ahogy azt a jelentést készítő szakértők már a bevezetőben megjegyzik, az ellátási láncok elleni kibertámadások és a zsarolóprogramok okozta legutóbbi incidensek[11] emlékeztetőül szolgáltak arra, hogy a kiberbiztonság szavatolása érdekében valamennyi releváns szereplőnek együtt kell működnie. A kiberbűnözők taktikaváltásával megnövekedett azon típusú támadások száma, amelyek során az éppen valamilyen aktuális esemény vagy válság (járvány, fegyveres konfliktus) nyomán már amúgy is veszélyeztetett célpontokat támadnak új csatornákon keresztül. A 2021-es év tapasztalatai alapján az amerikai szoftveróriás szerint a kiberbűnözés, a nemzetállami fenyegetések, az ellátási láncok, a dolgok internete (*Internet of Things,* IoT), az üzembiztonság (*operational technology security,* OTS), a hibrid munkavégzés és a dezinformáció kerültek leginkább előtérbe.[12]

A Microsoft jelentése hangsúlyozza, hogy a kiberbűnözés nemzetbiztonsági fenyegetést jelent, függetlenül attól, hogy államilag finanszírozott vagy engedélyezett tevékenységről

[9] Rekowski et al. (2020): i. m. 7.

[10] Microsoft: *Microsoft Digital Defense Report.* [online], Microsoft, 2021. október. Forrás: microsoft.com [2022. 04. 29.]

[11] 2021 legfontosabb zsarolóprogramokkal végrehajtott kibertámadásai például: Microsoft Exchange, Colonial Pipeline, City of Tulsa, JBS Meat Company, Fujifilm. *Recent Ransomware Attacks.* [online], Checkpoint Research, é. n. Forrás: checkpoint.com [2022. 06. 04.]. De más amerikai vállalatokat és szervezeteket is ért komoly zsarolótámadás: Steamship Authority of Massachusetts, Washington DC Metropolitan Police Department. *The 10 Biggest Ransomware Attacks of 2021.* [online], Touro College Illinois, 2021. november 12. Forrás: illinois.touro.edu [2022. 05. 05.]; A JBS elleni zsarolótámadásról bővebben lásd Nicole Perlroth – Noam Scheiber – Julie Creswell: *Russian Cybercriminal Group Was Behind Meat Plant Attack, F.B.I. Says.* [online], The New York Times, 2021. június 2. Forrás: nytimes.com [2022. 05. 28.].

[12] Microsoft (2021): i. m. 5.

van-e szó, vagy esetleg egyénekről, akik úgymond a saját szakállukra törnek fel informatikai rendszereket. A kiberbűnözők a kritikus infrastruktúrák egy elemét sem kímélik, így kórházakat és más egészségügyi intézményeket, információs rendszereket, pénzügyi szolgáltatókat és az energiaszektor szereplőit is támadják. Ráadásul a zsarolóprogramok egyre elterjedtebbek, igen komoly károkat képesek okozni kormányzatok és üzleti vállalkozások számára egyaránt, miközben az ezt a módszert alkalmazó kiberbűnözők egyre nagyobb bevételre tesznek szert. Mindemellett megjegyzendő, hogy a kiberbűnözők folyamatosan bővülő és egyre kifinomultabb szolgáltatásait már szinte bárki megvásárolhatja,[13] noha a legfelkészültebbek jellemzően továbbra is állami megrendelésre végeznek többek között például hírszerzési, illetve információszerzési tevékenységet. Mára már folyamatosan bővülő globális iparággá szerveződött a kiberbűnözés, ami részben annak is köszönhető, hogy az elkövetők az automatizációban rejlő lehetőségeket kihasználva képesek egyszerre csökkenteni a kiadásaikat és fokozni tevékenységüket. Ebben a tekintetben mindössze annyi pozitív fejlemény történt, hogy egyre több esetben tesznek bejelentést kibertámadásnak áldozatul esett kormányzati szereplők és vállalatok, a növekvő átláthatóság pedig felhívja a figyelmet a kiberbiztonság fontosságára, és védekezésre ösztönzi a kormányokat.[14]

Az egyik legjobb megtérülési rátája a zsarolóprogramokkal végzett támadásoknak van,[15] amelyek komoly károkat képesek okozni a célba vett rendszerekben, legyen az akár nemzetbiztonsági szolgálaté, nagyvállalaté, egészségügyi vagy közegészségügyi intézményé. A zsarolóprogrammal végrehajtott támadások ma már olyan szintre fejlődtek, hogy valamennyi típusú számítógépes hálózatot veszélyeztetik világszerte. A bűnelkövetői taktikák, technikák és eljárások[16] kifinomultsága a támadások hatását maximalizálva rendkívül jövedelmezővé tette a zsarolóprogramok alkalmazását. A Microsoft szerint már csupán a nyilvánosságra került zsarolótámadások során kifizetett váltságdíjak összege is vetekszik a nemzetállamok által működtetett támadó szervezetek költségvetésének nagyságával. A zsarolóprogramokkal végzett kibertámadások visszaszorításához pedig a magánszektor, a bűnüldöző szervek és a kormányzatok globális szintű, szorosabb együttműködésére volna szükség.[17]

Az elmúlt években a bejelentések számát tekintve az Egyesült Államokban messze az adathalász-támadások voltak a leggyakoribbak, ami már évek óta jellemző trendnek tekinthető. Az FBI adatai szerint 2020-ra egy év alatt gyakorlatilag megduplázódott, az elmúlt öt évben (2017–2022 között) pedig több mint a tizenkétszeresére növekedett az adathalász-bűncselekmények száma.[18] A kibertámadásoknak ez a típusa pedig

[13] Lásd például a zsarolóprogramok esetében a *ransomware as a service* (RaaS) lehetőségét: a bűnözők pénzért megvásárolhatják a hackerektől az ártalmas kódot, amellyel utána képesek zsarolótámadást indítani, mindezt anélkül, hogy akár csak alapszinten is értenének a kódoláshoz.

[14] Microsoft (2021): i. m. 8.

[15] Zsarolóprogrammal végzett támadás során a támadók egy rosszindulatú, kártékony szoftver alkalmazásával általában először kivonják az érzékeny adatokat, majd titkosítják az áldozat rendszerét, a titkosítás feloldásáért és az adatok visszaszolgáltatásáért cserébe pedig váltságdíjat követelnek, jellemzően kriptovaluta formájában. Microsoft (2021): i. m. 10.

[16] *Tactics, techniques, and procedures* (TTPs). Bővebben lásd a MITRE ATT&CK nevű, a kibertámadások során alkalmazott taktikák és technikák globálisan elérhető, valós megfigyeléseken alapuló online tudásbázisát: https://attack.mitre.org

[17] Microsoft (2021): i. m. 10.

[18] Federal Bureau of Investigation: *Internet Crime Report 2021.* [online]. FBI, 2021. Forrás: ic3.gov [2022. 05. 05.].

a vállalkozásokra és a magánszemélyekre nézve is komoly veszélyt jelent. A legsúlyosabb kibertámadások során jellemzően „adathalászattal" *(phishing)* megszerzett tanúsítványokat használnak fel, ráadásul ezekhez egyre változatosabb módokon jutnak hozzá, majd hitelesítik és alkalmazzák is őket, miközben a támadók az automatizációban rejlő lehetőségek kiaknázásával és eszköztáruk bővítésével képesek bűnelkövetői tevékenységük jövedelmezőségét növelni.[19]

Az elmúlt években a rosszindulatú programok alkalmazása és a kiberbűnözők infrastruktúrája is sokat fejlődött. A *malware-ek* magatartását illetően a Windows PowerShell gyanús parancsokkal és kódokkal való rosszindulatú futtatása volt a leggyakoribb, amelyet az amerikai szoftveróriás az utóbbi években megfigyelt. Emellett említésre méltó még a „fájl nélküli" *malware,* amelynek komponensei a megtámadott eszközön futó rendszerfolyamatokból és eszközökből állnak össze, ami hátráltatja a detektálásukat és eltávolításukat, mivel nem csupán egy fájlt kell megtalálni és letörölni. Számos esetben a rosszindulatú programokkal végzett támadásokat legitim oldalak felhasználásával végzik.[20]

A népszerű felhőszolgáltatásokat (Google Drive, Microsoft OneDrive, Adobe Spark, Dropbox stb.) például gyakran veszik igénybe malware célba juttatására, míg a tartalommegosztó oldalakat (mint a Pastebin.com, Archive.org, Stikked.ch) egyre gyakrabban használják fel rejtett módon a több részből álló és a fájl nélküli rosszindulatú programok esetében. Utóbbinál a malware kódját közvetlenül a beillesztő oldalról másolják le, amely azonnal le is fut a memóriában, anélkül, hogy akár egyetlen rosszindulatú fájlt is le kellett volna töltenie az áldozatnak. Mindemellett a botnetek alkalmazása is fejlődött. Bár 2021 januárjában a hatóságoknak sikerült felszámolni az Emotet névre keresztelt rosszindulatú programcsaládot, más botnetek, mint például a Phorpiex, fokozatosan növelték megfertőzött állomásaik számát és több zsarolótámadás végrehajtásában is közreműködtek (például az Avaddon). A Lemon Duck, Purple Fox és Sysrv-Hello nevű botnetek tevékenysége szintén fokozódott, új programozási nyelvek használatát, új infrastruktúra kiépítését és új fertőzési módok alkalmazását is beleértve, habár a legtöbb támadási módszer továbbra is a nem frissített alkalmazások sebezhetőségét, a fájlmegosztásokon keresztüli hálózati terjedést és a gyenge tanúsítványokat használja ki. Emellett egyre többször alkalmazzák rosszindulatú programok célba juttatására az internetböngészőket és a keresőmotorokat, illetve a keresőtalálatokat, valamint az online hirdetéseket is, akár böngészőkiegészítők segítségével is.[21]

A rosszindulatú programok alkalmazása már kiterjed az eredendően nem ártó szándékkal kifejlesztett eszközök, az úgynevezett *toolok* felhasználására is. Jó példa erre a külső behatolásokkal szembeni sebezhetőség tesztelésére használatos, kereskedelmi forgalomban is elérhető Cobalt Strike nevű szoftver, amelyet már egyre több kibertámadás alkalmával használnak a támadók. Ezt az alkalmazást úgy tervezték, hogy

[19] Microsoft (2021): i. m. 20.

[20] Microsoft (2021): i. m. 34.

[21] Internetböngészőket és keresőmotorokat használtak ki, illetve keresési találatokat manipuláltak például a 2020-as Adrozek, Gootkit, Jupyter és a SolarMarker malware-ek. Microsoft (2021): i. m. 35.

a hagyományos módszerekkel ne lehessen detektálni, ráadásul több hasznos funkcióval is segíti a támadót.[22]

A *web shell scriptek* továbbra is népszerűek a magyarul fejlett vagy előrehaladott állandó fenyegetésként emlegetett (angolul *advanced persistent threat,* APT) csoportok körében.[23] A Microsoft kutatói az elmúlt években rendre a web shell alkalmazások számának növekedését mutatták ki az államokhoz köthető csoportok és a bűnszervezetek esetében is. A web shell gyakorlatilag egy rövid, általában valamelyik elterjedt webfejlesztői programozási nyelven (ASP, PHP, JSP) megírt rosszindulatú kód, amelyet a támadók webszervereken szoktak elhelyezni, hogy majd később ezen keresztül gyakorlatilag bármikor távoli hozzáférést és kódfuttatási jogosultságot tudjanak szerezni. Amennyiben egy ilyen web shell észrevétlen marad az áldozat szerverén, azzal a támadó szinte folyamatos hozzáférést kap az ott elérhető adatokhoz, ráadásul a jellemzően nagymértékű hálózati forgalom miatt ezeket a támadásokat nem könnyű detektálni.[24]

Érdemes röviden kitérni még a rosszindulatú tartománynevek *(domainek)* témakörére, már csupán azért is, mert az utóbbi években jelentős mértékben megnőtt a számuk. Ezek lehetnek feltört weboldalak, amelyeken a kiberbűnözők kártékony tartalmat tárolnak *subdomainek* alatt, vagy lehetnek teljes mértékben csalás céljából létrehozott tartománynevek. A Microsoft elemzői szerint a kiberbűnözők elsősorban információk továbbítására, lokáció elfedésére és ellenálló képesség növelésére használják a rosszindulatú tartománynéveket. A top-level domainnevek és a regiszterek növekvő száma pedig jelentős mértékben megnehezíti a rosszindulatú tartománynevek felől érkező kiberfenyegetésekkel szembeni védekezést és ártalomcsökkentést. Mindemellett az elemzők már 2021-ben felhívták a figyelmet arra, hogy a következő komoly fenyegetést a blokklánc-technológia gyors terjedése miatt a teljesen szabályozatlanul működő blokkláncalapú tartománynevek *(blockchain domains)* jelentik majd.[25]

A gépi tanulás módszereit alkalmazó kiberbiztonsági rendszerek is támadások célpontjai lehetnek, sőt, rendszerszinten sebezhetők a gépi tanulás folyamatában jelen lévő új sérülékenységi osztály, az ellenséges gépi tanulás *(adversarial machine learning)* miatt. Az ellenfelek e sérülékenységek kihasználásával manipulálhatják a mesterséges intelligenciával működő rendszerek működését és módosíthatják annak viselkedését egy rosszindulatú cél elérése érdekében. Ez a jelenség azért is aggasztó, mert maga a mesterséges intelligencia és a gépi tanulás módszerei egyre inkább integrálódnak mindenféle rendszerekbe, beleértve a kritikus infrastruktúrákat és a biztonsági rendszereket is, ez pedig

[22] Microsoft (2021): i. m. 36.

[23] Fejlett, folyamatos fenyegetést (*advanced persistent threat,* APT) jelent az a rejtőzködő állami vagy nem állami bűnözői csoport, amely magas szintű szervezettség mellett képes rendkívül kifinomult módszerekkel hozzáférést szerezni informatikai rendszerekhez, és ott hosszabb időtartamon keresztül észrevétlen maradni. A kutatók az elemzett incidensek hasonlósága alapján különítik el egymástól az egyes csoportokat, amelyeket általában egy APTx elnevezéssel (ahol x a csoport sorszáma) vagy valamilyen fantázianévvel jelölnek meg a szakemberek. Ilyen APT-csoport például a Nobelium vagy a Hafnium. Selján Péter – Selján Gábor: Kiberbiztonsági kitekintés. *Nemzet és Biztonság,* 14. (2021), 1. 29.

[24] Microsoft (2021): i. m. 36.

[25] Microsoft (2021): i. m. 38–40.

a mesterségesintelligencia-alapú rendszerekre specifikus új biztonsági fenyegetéseket hoz magával, valamint még kellemetlenebbé teszi egy kibertámadás esetleges következményeit.[26]

Az elmúlt években számos olyan esemény történt, amely jelentős geopolitikai változásokat indukált, és egyúttal váratlan kihívások jelentkezésével is együtt járt, ami kihatott a kibertérben zajló tevékenységekre is. A Microsoft megállapítása szerint az állami szereplők ezekben az években is szinten tartották műveleti tevékenységüket, de közben új taktikákat és technikákat is kifejlesztettek, hogy észrevétlenek tudjanak maradni, illetve növelhessék támadásaik volumenét. Az ellátási láncok és a számítógépes rendszerek védelmének fontosságára az elmúlt években például a Nobelium nevű APT-csoporthoz köthető SolarWinds[27] vagy a Hafnium számlájára írható Exchange Server-támadások és még számos más szereplőhöz köthető támadás is világszerte felhívta a kiberbiztonság szavatolásában érintett valamennyi szereplő figyelmét.[28]

3. A nemzetállami fenyegetések

Az állami szereplők kibertevékenysége[29] és számos kiberbűncselekmény is a sérülékenységek kihasználására vagy a nem frissített (rosszul karbantartott), ugyanakkor az üzletfolytonosság fenntartásához nélkülözhetetlen rendszerek felderítésére koncentrál, amelyek működésére ráadásul a szervezetek még jobban rá lettek utalva a világjárvány hatásai miatt. Az elmúlt években megfigyelt kibertámadások is megmutatták, hogy egyre fontosabb a biztonsági frissítések telepítése és naprakészen tartása valamennyi működő informatikai rendszer esetében, hiszen talán ez a legegyszerűbb és leghatékonyabb módja a rohamtempóban fejlődő fenyegetések elleni védekezésnek.

A Microsoft kiberbiztonsági fenyegetések felderítésével foglalkozó központjának (*Microsoft Threat Intelligence Center,* MSTIC)[30] és a digitális biztonsággal foglalkozó osztályának (*Digital Security Unit,* DSU) megfigyelései szerint a legtöbb nemzetállam továbbra is elsősorban állami intézmények és kormányzati szervek, kormányközi szervezetek, nem kormányzati szervezetek és kutatóintézetek ellen hajt végre kiberműveleteket és kibertámadásokat, hagyományosan elsősorban hírszerzési és felderítési céllal. Ezekben az esetekben nyilvánvalóan az áll a támadások hátterében, hogy a célpontok a támadó

---

[26] Microsoft (2021): i. m. 42–46.

[27] A SolarWinds esete a szakértők szerint mérföldkő volt a kiberbiztonság történetében, hiszen egy állami szereplő hajtott végre kifinomult és összetett kibertámadást az Egyesült Államok ellen, amelynek eredményeként kormányzati informatikai rendszerekhez sikerült hozzáférést szereznie. Nem véletlen, hogy ezt az incidenst követően a Biden-adminisztráció számára prioritás lett a kiberbiztonság. Selján Gábor: The Remarkable 10th Anniversary of Stuxnet. *AARMS,* 19. (2020), 3. 85–98.

[28] Microsoft (2021): i. m. 48.

[29] Bár az előzőekben már utaltunk rá, érdemes hangsúlyozni, hogy az állami szereplőkhöz köthető kibertámadások jelentik általában a legkomolyabb fenyegetést a kiberbiztonsági szakértők szerint, mivel általában stratégiai célokat szolgálnak. Ebben a tekintetben a legelszántabb szereplőkről van szó, akik időt és anyagi erőforrásokat sem spórolva igyekeznek elérni műveleti céljaikat. Támadó tevékenységüket többnyire a képességeiket folyamatosan fejlesztő, az adott feladatra létrehozott csoportokkal *(advanced persistent threat groups)* hajtják végre, amelyek képesek új eljárásokat, technikákat kifejleszteni és alkalmazni. Selján–Selján (2021): i. m. 27–28.

[30] Microsoft Security Intelligence Twitter handle: https://twitter.com/MsftSecIntel

számára fontos és releváns információk birtokában lehetnek, amelyekről az adott ellenséges állami szereplő szeretne tudomást szerezni. Mindazonáltal a világjárvány éveiben a magánszektor is kiemelt célponttá vált, elsősorban az informatikai rendszerek támogatásával megvalósuló otthoni és távoli munkavégzés elterjedése miatt, de előkelő helyen szerepelnek már a támadók célpontjai között az egészségügyi szolgáltatók, a vakcinakutatásban részt vevő intézetek és központok, és a Covid–19-oltóanyagokat kiszállító szervezetek is, amelyeket – a Microsoft kiberfenyegetésekkel foglalkozó szakemberei szerint – szintén információszerzési céllal érnek kormányoktól eredeztethető kibertámadások nemzetbiztonsági és hírszerzési megfontolásokból.[31]

A legnagyobb állami szereplők kibertevékenységeinek célja továbbra is jellemzően a kémkedés, a zavarkeltés vagy károkozás, az alkalmazott technikák között pedig jelenleg is megtalálható a felderítés, a hitelesítő adatok/tanúsítványok begyűjtése, a malware, vagy éppen a virtuális privát hálózatok (*virtual private network*, VPN) kihasználása. Emellett a hackerek eszköztárában még mindig előkelő helyen szerepel a jól bevált célzott adathalászat is. A támadók azonban jellemzően folyamatosan kutatnak a célpontjaik után, hogy továbbfejlesszék technikáikat, vagy éppen valamilyen bűnözői magatartást utánozva álcázzák valódi szándékukat és céljaikat.[32]

A Microsoft adatai szerint 2020. július és 2021. június között a célországok közül az első az Egyesült Államok (46%), a második Ukrajna (19%), a harmadik pedig az Egyesült Királyság (9%) volt. Ami pedig a legtöbb támadásnak kitett szektorokat illeti, a fő célpontok kormányzati intézmények (48%) és nem kormányzati szervezetek, valamint kutatóintézetek (31%) voltak. Érdekességként megjegyzendő, hogy a támadások túlnyomó többsége a nem kritikus infrastruktúrákat érte. A legnagyobb arányban Kínához köthető támadók vettek célba kritikus infrastruktúrákat (13%), míg a legkisebb arányban az orosz támadók (2%). Az orosz Nobelium eddigi tevékenysége jól mutatja, hogy Oroszország a kritikus infrastruktúrákban való károkozás helyett elsősorban inkább hírszerzési céllal folytatott kiberműveleteket. Mindazonáltal az állami szereplők között éppen Oroszország volt a legaktívabb a kibertérben, méghozzá elsősorban pont az orosz támadások túlnyomó többségéért (92%) felelős Nobelium tevékenységének köszönhetően. A támadások 58%-áért felelős oroszokat Észak-Korea követte a második helyen (23%), a harmadik Irán (11%), a negyedik „helyezett" pedig Kína lett (8%).[33]

A nemzetállamok többnyire ugyanazokat az eszközöket[34] alkalmazzák a célpontjaik informatikai rendszerének támadására, mint más ártó szándékú szereplők, ugyanakkor magasabb fejlettségi szintjük révén képesek előzetes felderítést is végezni, hogy ki tudják választani a számukra legcélravezetőbb támadási módot. Ezzel kapcsolatban azonban érdemes megjegyezni, hogy azok az általános biztonsági intézkedések és informatikai higiéniai megoldások, amelyek megvédhetnek minket az általános fenyegetésekkel szemben (erős jelszavak használata, kétlépcsős azonosítás bekapcsolása, frissítések rendszeres

[31] Microsoft (2021): i. m. 48.
[32] Microsoft (2021): i. m. 52.
[33] Microsoft (2021): i. m. 52–55.
[34] A rosszindulatú aktorok által alkalmazott eszközök és támadói vektorok angol szakkifejezésekkel: *password spray, social engineering, phishing, identify spoofing, malware, supply chain insertion, man-in-the-middle, denial of service.*

telepítése stb.), segíthetnek a nemzetállamokhoz köthető kibertámadásokkal szembeni védekezésben is.

3.1. Orosz kibertámadások

Az elmúlt években az oroszországi csoportok alkalmazkodóképességük, kitartásuk és ártó szándékaik demonstrálásával megszilárdították pozícióikat mint a globális digitális ökoszisztéma elleni akut fenyegetést jelentő aktorok, miközben a nyílt forráskódú eszközök és az anonimizálás segítségével támadásaik egyre nehezebben detektálhatók, illetve azonosíthatók. A már említett oroszországi Nobelium APT-csoport a SolarWinds Orion frissítésének feltörésével jól demonstrálta, milyen komoly hatással lehetnek a szoftverellátási láncok elleni támadások. A csoport műveleti technikái között ugyanakkor a rosszindulatú „hátsó ajtó" *(backdoor)* mellett megtalálható volt a „jelszópermetezés" *(password spraying)* és az adathalászat is. Mint ismeretes, 2021 májusában a Nobelium feltörte egy amerikai kormányzati intézmény (USAID) felhasználói fiókját egy népszerű e-mail-marketingszolgáltatónál (Constant Contact), ahonnan tömegesen küldött szét adathalász-e-maileket. Az elektronikus levelek bár első ránézésre autentikusnak tűntek, egy linket is elhelyeztek bennük, amely kattintásra beillesztett egy rosszindulatú fájlt, ami egy hátsó ajtó létrehozását eredményezte *(NativeZone backdoor)*.[35]

A Microsoft megfigyelései szerint egyértelmű taktikai váltás volt látható a „SolarWinds hack" felfedezését követő első hónapok és a 2021 júniusáig terjedő időszak között a Nobelium célpontjait illetően. Az oroszországi eredetű APT-csoport mindkét időszak alatt gyakorlatilag folyamatosan támadott kormányzati intézményeket,[36] nem kormányzati szervezeteket, informatikai szolgáltatókat és más szolgáltatószektorokat, de a támadások, illetve kísérletek száma változó volt, a taktikai váltásnak megfelelően. 2020. december és 2021. január között a legtöbb támadás az informatikai szolgáltatókat érte (45%), amelyet a nem kormányzati szervezetek és a kutatóintézetek (20%), majd a kormányzati célpontok követtek. Ezzel szemben 2021. január és június között a támadások többsége már a kormányzati intézményeket érte (53%),[37] az informatikai szolgáltatók ellen már a támadásoknak csupán 1%-a irányult, míg a nem kormányzati szervezetek és a kutatóintézetek a támadások 38%-ának voltak célpontjai.[38]

Az orosz aktorok valamennyi támadás alkalmával tudatosan jártak el, és bizonyos szintű alkalmazkodási képességet is fel tudtak mutatni, ami segített nekik a hálózati védelmet megkerülni és csökkenteni a lebukás veszélyét. A Nobelium bizonyította, hogy nagyon

---

[35] Tom Burt: *Another Nobelium Cyberattack*. [online], Microsoft blog, 2021. május 27. Forrás: blogs.microsoft.com [2022. 05. 14.].

[36] A kormányzati szervezetek elleni kibertámadásoknak jellemzően külügyi, biztonsági vagy védelmi szférához tartozó intézmények a célpontjai, noha előfordul az is, hogy önkormányzatokat, légiforgalmi célpontot vagy kikötői hatóságot ér támadás (lásd például a Bromine névre keresztelt APT-csoport tevékenységét). A harmadik legtöbbet támadott szektor az elmúlt években az egészségügy, illetve a Covid–19-vakcinakutatásban és kezelések kidolgozásában érintett szervezetek voltak (lásd a Strontium által végrehajtott adathalász-támadásokat).

[37] Sergiu Gatlan: *Microsoft: Russian State Hackers Behind 53% of Attacks on US Govt Agencies*. [online], Bleeping Computer, 2021. október 8. Forrás: bleepingcomputer.com [2022. 05. 15.].

[38] Microsoft (2021): i. m. 57–58.

jól ismeri az elterjedt szoftvereszközöket, a hálózati biztonsági rendszereket, a felhőalapú technológiákat, valamint az incidenskezelő teamek által használt kármentesítési módszereket is, és ennek megfelelően változtattak a műveleteiken a folytonosság megőrzése érdekében.[39] Az elmúlt években az oroszországi APT-csoportok egyre hatékonyabbak lettek, és jellemzően már egyre többször vesznek célba kormányzati intézményt, ami arra enged következtetni, hogy a következő években is egyre több és egyre komolyabb ilyen kibertámadásra lehet majd számítani Oroszország részéről. A Microsoft adatai szerint az orosz hackerek gyakorlatilag minden kontinensen támadtak célpontokat, ugyanakkor elsősorban amerikai, ukrán és brit szervezeteket, valamint NATO-szövetségeseket és európai tagállamokat vettek célba.[40]

2021 májusában az orosz kormány hivatalosan „barátságtalan" országnak minősítette az Egyesült Államokat és Csehországot, és egy kiszivárgott lista szerint már ekkor arra készült, hogy Lengyelországot, Észtországot, Lettországot, Litvániát, az Egyesült Királyságot, Kanadát, Ukrajnát és Ausztráliát is ebbe a kategóriába sorolja.[41] A Microsoft a 2021. őszi jelentésében megjegyezte, hogy megfigyelései szerint az orosz kibertevékenység elsősorban hírszerzési és információgyűjtési célokat szolgált, amire az enged következtetni, hogy az általa nyomon követett APT-csoportok elsősorban adatokhoz igyekeztek hozzáférést szerezni, és nem bocsátkoztak destruktív akciókba. Az amerikai kormány ezeket a támadásokat jellemzően az orosz hírszerzéshez köti, amely számára tulajdonképpen rutinfeladat az ellenfélnek tekintett országok szándékairól és terveiről információkat gyűjteni.[42] 2021 áprilisában az amerikai Nemzetbiztonsági Ügynökség (National Security Agency, NSA), a Kiberbiztonsági és Infrastruktúra-biztonsági Ügynökség (Cybersecurity and Infrastructure Security Agency, CISA) és a Szövetségi Nyomozó Iroda (Federal Bureau of Investigation, FBI) közös nyilatkozatban hívta fel a figyelmet arra, hogy az orosz hírszerzéshez köthető csoportok (APT29, Cozy Bear, The Dukes) gyakran használnak ki nyilvánosan ismert sérülékenységeket, hogy széleskörűen feltérképezzék és feltörjék a sérülékeny rendszereket a hitelesítési tanúsítványok, illetve további hozzáférés megszerzése céljából. A célpontok között pedig jellemzően amerikai és szövetséges informatikai hálózatok is szerepelnek, köztük nemzetbiztonsági és kormányzati rendszerek.[43]

A Nobelium tevékenysége kapcsán megjegyzendő, hogy az amerikai kormány és az európai szövetségesek továbbra sem tudták eldönteni, hol húzzák meg azt a bizonyos vörös vonalat a kibertámadások tekintetében, aminek a túllépése elfogadhatatlan, azaz már a kiberhadviselés keretében értelmezhető ellenséges fegyveres támadással lenne egyenlő. Ezt jelezte, amikor 2021 márciusában egy korábbi brit főtanácsadó arra sürgette a Biden-adminisztrációt, hogy ne reagáljon „túl szigorúan" Oroszország „sebészi pontosságú"

---

[39] Ramin Nafisi – Andrea Lelli: *GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM's Layered Persistence.* [online], Microsoft, 2021. március 4. Forrás: microsoft.com [2022. 05. 14.].

[40] Microsoft (2021): i. m. 58.

[41] Brendan Cole: *Russia Puts U.S. Top of 'Unfriendly Countries' List.* [online], Newsweek, 2021. április 27. Forrás: newsweek.com [2022. 05. 15.].

[42] Microsoft (2021): i. m. 59.

[43] *Russian SVR Targets U.S. and Allied Networks.* [online], NSA, CISA & FBI, Cybersecurity Advisory, 2021. április 5. Forrás: media.defense.gov [2022. 05. 15.].

hírszerzési kampányára.[44] Ezt a politikai kétértelműséget az orosz aktorok előszeretettel használták ki az elmúlt években, és ez várhatóan a következő években is így lesz, hacsak nem lesz valamilyen előrelépés ezen a téren. A Microsoft szerint ráadásul a SolarWinds esetéből tanulva a jövőben a Nobelium és más APT-csoportok a következő kibertámadásnál egy kvázi figyelemelterelő akcióval leköthetik a fontosabb kiberbiztonsági teamek figyelmét abban a reményben, hogy ezáltal hátráltatva a beazonosításukat és a kármentési tevékenységet, időt nyerhetnek a fontosabb támadásaik kivitelezéséhez.[45]

Érdemes megjegyezni, hogy 2022 márciusában az Egyesült Államok azzal vádolt meg összesen négy orosz állampolgárt (köztük három FSZB-ügynököt), hogy 2012 és 2018 között kibertámadásokat hajtottak végre amerikai kritikus infrastruktúrák ellen (elsősorban az energiaszektor ellen), többek között egy kansasi atomerőmű és egy szaúd-arábiai petrolkémiai létesítmény ellen is. A bejelentéssel egyidejűleg az állami főügyészhelyettes megjegyezte, hogy bár a vádemelés a múltban történt támadásokra vonatkozik, annak mégis egyértelmű üzenetértéke van az amerikai cégek és vállalkozások számára, hogy meg kell erősíteniük kibervédelmüket, és résen kell lenniük, hiszen az Oroszország által támogatott hackerek komoly fenyegetést jelentenek a kritikus infrastruktúrákra nézve az Egyesült Államokban és világszerte.[46] A Biden-adminisztráció és biztonsági szakértők pedig arra kérték az amerikai cégeket, hogy jelentsék az FBI-nak és más illetékes ügynökségeknek, ha valami gyanús tevékenységet észlelnek – vagy esetleg kibertámadás áldozataivá válnának[47] –, és egy tájékoztatót[48] is kiadtak a hackerek által alkalmazott technikákról. Az egyik vádiratban megnevezett három FSZB-ügynök állítólag engedély nélküli hozzáférést szerzett több olajipari, gázipari, energetikai cég és atomerőmű informatikai rendszereihez, amelyeket folyamatosan megfigyeltek, az irányítórendszerek feletti ellenőrzés megszerzésével pedig megvolt a képességük a számítógépes rendszerek megzavarására és megrongálására.[49]

Nem sokkal később, 2022 áprilisában az Egyesült Államok bejelentette, hogy titokban felszámolt egy nemzetközi robothálózat *(botnet)* kiépítését szolgáló rosszindulatú programot a nemzetközi informatikai rendszerekben, hogy megelőzze a további orosz kibertámadásokat. Erre azt követően került sor, hogy amerikai tisztségviselők arra hívták fel a figyelmet, hogy válaszként az Ukrajna orosz inváziója miatt Moszkvával szemben

---

[44] Jenna McLaughlin: Top Biden Cyber Official: SolarWinds Breach Could Turn from Spying to Destruction 'in a Moment'. [online], Yahoo News, 2021. április 8. Forrás: news.yahoo.com [2022. 05. 15.].

[45] Microsoft (2021): i. m. 59.

[46] 2022 áprilisában az Egyesült Államok, Ausztrália, Kanada és Új-Zéland közös tájékoztatót adtak ki, amelyben arra hívták fel a figyelmet, hogy az Oroszországhoz köthető szereplők az ukrajnai háború miatt elrendelt szankciók miatt célba vehetik a nyugati vállalatokat. *Alert (AA22-110A). Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.* [online], Cybersecurity and Infrastructure Security Agency, 2022. április 20. Forrás: cisa.gov [2022. 05. 28.].

[47] Kate Conger: *With Eye to Russia, Biden Administration Asks Companies to Report Cyberattacks.* [online], The New York Times, 2022. március 23. Forrás: nytimes.com [2022. 05. 26.]

[48] *Alert (AA22-083A). Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector.* [online], Cybersecurity and Infrastructure Security Agency, 2022. március 24. Forrás: cisa.gov [2022. 05. 24.].

[49] Katie Benner – Kate Conger: *U.S. Accuses 4 Russians of Hacking Infrastructure, Including Nuclear Plant.* [online], The New York Times, 2022. március 24. Forrás: nytimes.com [2022. 05. 24.].

bevezetett szankciókra Oroszország támadásokat hajthat végre a kibertérben a kritikus infrastruktúrák ellen.[50]

3.2. Az Ukrajna elleni orosz kiberműveletekről

Oroszország a kiberműveleteket a tágabb értelemben vett információs hadviselés részének tekinti, beleértve az elektronikai hadviselést és a pszichológiai vagy információs műveleteket is. A Kreml hagyományos katonai műveletek elősegítésére is alkalmaz kibertámadásokat, és előszeretettel működik együtt kiberbűnözői csoportokkal, mivel azok könnyen letagadhatók.[51] 2022 áprilisában a Microsoft kiadott egy jelentést[52] az Oroszország ukrajnai inváziójával összefüggésben megfigyelt orosz kiberműveletekről, hogy betekintést nyújtson az orosz kiberképességeknek az ukrajnai „hibrid háború", illetve az információs hadviselés[53] keretében megvalósuló alkalmazásába.[54] Az amerikai szoftverfejlesztő cég szerint a fegyveres konfliktus eszkalálódásával legalább hat APT-csoport és számos más eddig beazonosítatlan aktor hajtott végre pusztító jellegű támadásokat és hírszerző műveleteket, miközben az orosz fegyveres erők szárazföldön, vízen és levegőben is támadást indítottak Ukrajna ellen. Bár nem világos, hogy mennyire volt szoros a koordináció a kiberműveleteket végrehajtók és a konvencionális fegyveres erők alakulatai között – vagy akár inkább egymástól függetlenül, de párhuzamosan tevékenykedtek egy közös cél elérése érdekében –, az ugyanakkor kijelenthető, hogy a kiber- és a kinetikus műveletek együtt gyakorlatilag egymást kiegészítve szolgálják az ukrán kormány és a fegyveres erők működésének meggyengítését, továbbá a lakosság kormányzati intézményekbe és az ukrán hadseregbe vetett bizalmának aláásását.

A Microsoft szakértőinek megfigyelései szerint az orosz katonai invázió megindulása (2022. február 24.) előtt[55] egy nappal a katonai hírszerzéshez, azaz a vezérkar hírszerzési főigazgatóságához (*Glavnoje Razvedivatyelnoje Upravlenyije,* GRU) köthető elkövetők

---

[50] Kate Conger – David E. Sanger: *U.S. Says It Secretly Removed Malware Worldwide, Pre-empting Russian Cyberattacks.* [online], The New York Times, 2022. április 6. Forrás: nytimes.com [2022. 05. 25.].

[51] Michael Connell – Sarah Vogler: *Russia's Approach to Cyber Warfare.* [online], CNA, 2017. március. Forrás: cna.org [2022. 05. 28.].

[52] *Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine.* [online], Microsoft Digital Security Unit, 2022. április 27. Forrás: microsoft.com [2022. 04. 28.]

[53] Az orosz katonai megközelítés szerint az információs hadviselés „az információs térben történő konfrontációt jelenti, melynek célja a kritikus fontosságú információs rendszerekben való károkozás, a politikai, gazdasági és szociális rendszerek aláásása, a lakosság manipulálása az állam destabilizálása érdekében, hogy a vezetést rákényszerítse az ellenfél hasznára váló döntések meghozatalára". Az ellenség moráljának gyengítése, a vezetés lejáratása és a katonai, valamint gazdasági teljesítmény aláásása az információs hadviselés eszközeivel az orosz elképzelések szerint néha akár még hatékonyabb is lehet a hagyományos fegyverek alkalmazásánál. Erre utalt 2017 februárjában Jurij Balujevszkij korábbi vezérkari főnök is, amikor a RIA Novosznyi hírügynökségnek nyilatkozott egy hír kapcsán. *Conceptual Views On The Activity Of The Armed Forces Of The Russian Federation In Information Space.* [online], Ministerstvo Oborony Rossiyskoy Federatsii, 2011. Forrás: pircenter.org [2022. 05. 24.]; *Шойгу рассказал о задачах войск информационных операций.* [online], РИА Новости, 2017. február 22. Forrás: ria.ru [2022. 05. 24.].

[54] Kate Conger – David E. Sanger: *Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds.* [online], The New York Times, 2022. április 27. Forrás: nytimes.com [2022. 05. 25.].

[55] Jelentések szerint az orosz invázió indulásának megelőző óráiban kibertámadás érte az ukrán kormány által is igénybe vett kaliforniai cég, a Viasat műholdas kommunikációs rendszerét, amit amerikai tisztségviselők az orosz katonai felderítés, a GRU munkájának tulajdonítottak. David E. Sanger – Kate Conger: *Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds.* [online], The New York Times, 2022. május 10. Forrás: nytimes.com [2022. 05. 28.].

pusztító adattörlő támadásokat indítottak több száz ukrán kormányzati, informatikai, energetikai és pénzügyi célpont, illetve szervezet ellen. Ezt követően április elejéig számos támadást és támadási kísérletet figyeltek meg, amely a kritikus infrastruktúrák ellen irányult,[56] amelyeket esetenként szárazföldi erők is célba vettek és olykor rakétatalálat is ért. A támadók ugyanakkor a kritikus infrastruktúrák mellett az állampolgárokat is célba vették, hogy megakadályozzák a lakosság megbízható információkhoz és létfontosságú szolgáltatásokhoz való hozzáférését, ezáltal is megingatva az embereknek az ukrán vezetésbe vetett bizalmát.[57] A feltételezett orosz katonai célokat figyelembe véve valószínűsíthető, hogy az orosz kiberműveletek is azt a célt szolgálták, hogy aláássák Ukrajna ellenálló képességét, miközben hírszerző tevékenységet, illetve felderítést is végeztek.

A Microsoft a jelentésében megállapította, hogy az oroszországi aktorok már 2021 márciusában felsorakoztak Ukrajna ellen a kibertérben. Erre abból lehetett következtetni, hogy rövid időn belül megugrott a korábban elenyésző mértékű kibertámadások száma Ukrajna és szövetségesei ellen, noha az ukrán fegyveres erők és a kiberbiztonsági szakemberek gyakorlatilag ekkor már 2014 óta folyamatosan harcban álltak az orosz erőkkel. A megfigyelések szerint már a február 24-i inváziót megelőző időszakban aktivizálódtak a Strontium, Iridium, a DEV-0586, a Nobelium, az Actinium, a Bromine és a Krypton nevű APT-csoportok, amelyek az Orosz Föderáció katonai hírszerzéséhez, a külföldre irányuló polgári hírszerzéshez (Szluzsba Vnyesnyej Razvedki, SZVR) és a Szövetségi Biztonsági Szolgálathoz (Fegyeralnaja Szluzsba Bezopasznosztyi, FSZB) köthetők. 2022 elején, miután a konfliktus deeszkalálására tett összes diplomáciai kísérlet kudarcot vallott, az orosz APT-csoportok adattörlő támadásokat indítottak ukrán szervezetek ellen, ami előrevetítette a konfliktus további eszkalációjának lehetőségét. Ezt követően az invázió megindulásának hajnalán a kibertámadások ismét intenzívebbek lettek, miután az Iridium bevetette a FoxBlade (HermeticWiper) nevű rosszindulatú programját több mint egy tucat kormányzati, informatikai, energetikai, mezőgazdasági és pénzügyi szervezet ellen, hogy működésképtelenné tegyen nagyjából 300 informatikai hálózatot Ukrajnában.[58] Az orosz kibertámadások azóta is szinte folyamatosak Ukrajna ellen.[59] A fegyveres konfliktus elhúzódásával az orosz APT-csoportok várhatóan fokozni fogják tevékenységüket, amely Ukrajnán kívüli célpontokra is kiterjed. Ebből kifolyólag bármikor célkeresztbe kerülhetnek a balti államok, Törökország és azok a tagállamok a NATO

---

[56] 2022. április 12-én ukrán tisztségviselők bejelentették, hogy megakadályoztak egy, az ukrán elektromos hálózat ellen indított orosz kibertámadást, amely elmondásuk szerint az egyik legkifinomultabb támadás lehetett, amely, ha sikerrel jár, akár 2 millió ember áramellátását lett volna képes megzavarni. Az ukrajnai elektromos hálózatot eddig összesen kétszer, egyszer 2015-ben, majd pedig 2016-ban sikerült orosz kibertámadással átmenetileg működésképtelenné tenni, ami akkor jelentős áramkimaradásokat eredményezett. Kate Conger: *Ukraine Says It Thwarted a Sophisticated Russian Cyberattack on Its Power Grid.* [online], The New York Times, 2022. április 12. Forrás: nytimes.com [2022. 05. 25.].

[57] Ukrajna orosz inváziójának február 24-i kezdetét követően hekkerek több alkalommal is feltörték a megbízható és hiteles információkat szolgáltató ukrán hírszolgáltatók közösségi oldalait és műsorszóró rendszereit, hogy téves információkat terjesszenek, többek között például Ukrajna kapitulációjáról. Ezeket az állításaikat és üzeneteiket pedig olykor manipulált videókkal is igyekeztek megerősíteni. Kate Conger: *Hackers' Fake Claims of Ukrainian Surrender Aren't Fooling Anyone. So What's Their Goal?.* [online], The New York Times, 2022. április 5. Forrás: nytimes.com [2022. 05. 25.].

[58] Brad Smith: *Digital Technology and the War in Ukraine.* [online], Microsoft, 2022. február 28. Forrás: blogs.microsoft.com [2022. 05. 24.].

[59] A kézirat lezárásának idején: 2022. június 6.

keleti szárnyán, amelyek katonailag, politikailag, vagy akár csak humanitárius segítségnyújtással is, de aktívan támogatták Ukrajnát az orosz „különleges katonai művelettel" szemben.

Megjegyzendő, hogy az ukrán kormány és az Ukrajnát támogató amatőr hekkerközösség sem maradt tétlen a háború első hónapjaiban.[60] 2022 áprilisában például Ukrajna oldalán álló hekkerek arról számoltak be, hogy több tucat orosz intézmény, köztük a Kreml internetcenzorának és az egyik hírszerző szolgálatnak az informatikai rendszerét is feltörték, amelyekről adatokat loptak el és szivárogtattak ki az interneten, bár azok hitelességét a szakértők sem tudták megállapítani. Erre egyébként azt követően került sor, hogy maga az ukrán kormány elkezdte nyilvánosságra hozni azoknak az orosz katonáknak a nevét, akikről a hatóságok feltételezik, hogy részük lehetett a bucsai mészárlásként emlegetett háborús bűncselekmények elkövetésében.[61] Mindemellett 2022. június elején az amerikai kiberparancsnokság is megerősítette, hogy az Egyesült Államok is hajtott végre offenzív, defenzív és információs kiberműveleteket Ukrajna megsegítésére.[62]

3.3. A kínai kibertevékenységről

A Kínához köthető APT-csoportok a vizsgált időszakban elsősorban az amerikai külpolitikai döntéshozatalban illetékes kormányzati intézményeket támadták – valószínűleg információszerzési céllal –, a jelek szerint pedig ennek érdekében több kínai csoport több korábban ismeretlen sérülékenységet is kihasznált. A Microsoft először 2021 márciusában adott hírt a Hafnium névre keresztelt APT-csoportról, miután az több nulladik napi *(zero-day)* sérülékenységet is kihasznált a Microsoft Exchange Server feltörésére, hozzáférést szerezve e-mail-postafiókokhoz, valamint további rosszindulatú programokat telepítve, ezáltal pedig hosszú távú hozzáférést szerezve az áldozat rendszereihez.[63] A Microsoft a célpontok kiválasztása *(targeting)*, valamint az alkalmazott taktikák és eljárások alapján jutott arra, hogy minden bizonnyal egy kínai APT-csoportról van szó, amely elsősorban amerikai célpontokat támad valamennyi szektort érintve, ideértve a fertőző betegségekkel foglalkozó kutatóintézeteket, ügyvédi irodákat, felsőoktatási intézményeket, védelmi ipari cégeket, politikai kutatóintézeteket, nem kormányzati szervezeteket is. A Microsoft adatai szerint 2020 júliusa és 2021 júniusa között a kínai eredetű támadások többsége

[60] 2022. február végén alakult meg az „IT Army of Ukraine" önkéntes kiberhadviselési szervezet azzal a céllal, hogy visszaverje az orosz támadásokat a kibertérben, illetve offenzív kiberműveleteket hajtson végre orosz katonai célpontok ellen. Bővebben lásd Stefan Soesanto: *The IT Army of Ukraine*. [online], Center for Security Studies, 2022. június. Forrás: css.ethz.ch [2022. 09. 11.].

[61] Kate Conger – David E. Sanger: *Hackers Claim to Target Russian Institutions in Barrage of Cyberattacks and Leaks*. [online], The New York Times, 2022. április 22. Forrás: nytimes.com [2022. 05. 24.].

[62] Alexander Martin: *US Military Hackers Conducting Offensive Operations in Support of Ukraine, Says Head of Cyber Command*. [online], Sky News, 2022. június 1. Forrás: news.sky.com [2022. 06. 04.].

[63] *HAFNIUM Targeting Exchange Servers with 0-day Exploits*. [online], Microsoft Threat Intelligence Center (MSTIC), 2021. március 2. Forrás: microsoft.com [2022. 05. 16.].

(47%) a kormányzati intézményeket érte, míg 16%-a a nem kormányzati szervezeteket és a kutatóintézeteket, 13% a médiát, 12% az oktatási rendszert vette célba, és a maradék 12% volt az egyéb támadás.[64]

Az amerikai kormány és szövetségesei 2021 júliusában kiadtak egy nyilatkozatot, amelyben kijelentették, hogy Kína rosszindulatú kibertevékenysége komoly fenyegetést jelent az Egyesült Államok és szövetségeseinek gazdaságára és biztonságára. Ebben a nyilatkozatban a Hafnium APT-csoportra is történt utalás, amelyet a kínai polgári hírszerzéshez, a KNDK Állambiztonsági Minisztériumához kötöttek. Mint ismeretes, a kínai APT-csoportok több tízezer számítógépet és informatikai hálózatot törtek fel világszerte egy széles körű „kiberhírszerzési" kampány keretében, amely leginkább a magánszektorból szedett áldozatokat.[65]

A kínai kibertevékenység érintette az amerikai választásokat is. A Zirconium APT-csoport az elnökválasztást megelőzően folyamatosan alkalmazott e-mailekbe ágyazott külső forrásokra mutató tartalmakat, amelyekkel követni tudta a felhasználói aktivitást. Ezzel elsősorban olyan egyéneket vett célkeresztbe, akik információval rendelkezhettek az esetleges amerikai politikai változásokról. A kínai kiberműveletek azonban a szomszédos országokat sem hagyták érintetlenül. A Microsoft szerint 2020 júliusától a Chromium nevű APT-csoport indiai, malajziai, mongóliai, pakisztáni és thaiföldi célpontok ellen indított támadásokat, de Hongkongban és Tajvanon is tevékenykedett. Sőt, a Chromium a hongkongi és a tajvani egyetemek ellen volt talán a legaktívabb, de a célpontjainak listáján kormányzati szervezetek és külföldi telekommunikációs szolgáltatók is szerepeltek. Mindemellett Latin-Amerikában és Európában is folytattak hírszerző műveleteket. A Nickel APT-csoport tevékenysége szintén kiterjedt a kormányzati szervezetekre, de elsősorban Közép- és Dél-Amerikában. A kínai befolyás növekedésével a jövőben várhatóan egyre több támadást hajtanak majd végre a Kínához köthető hackerek, hogy információt szerezzenek a befektetésekről, tárgyalási folyamatokról, és hogy még nagyobb befolyásra tehessenek szert.[66]

A New York-i Margin Research kiberbiztonsági kutatóintézet szerint miközben jó úton halad afelé, hogy kiber-szuperhatalom legyen, Kína lassan felszámolja a civil-kereskedelmi ipari szektorok és az állam közötti határokat. Ezáltal pedig a jelentős potenciált mutató vezető kínai technológiai vállalatok – de elsősorban a kiberbiztonsági cégek – komoly erőforrásokkal szolgálhatnak a kínai kormány és a fegyveres erők számára.[67] Az elmúlt évtizedekben nagyon gyors ütemben fejlődött a kínai kiberbiztonsági szektor,

[64] További Kínához köthető APT-csoport még a Manganese, a Zirconium, a Nickel és a Chromium. Microsoft (2021): i. m. 60.

[65] *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China.* [online], The White House, 2021. július 19. Forrás: whitehouse.gov [2022. 05. 17.].

[66] Microsoft (2021): i. m. 62.

[67] Patrick Howell O'Neill: *How China Built a One-of-a-Kind Cyber-Espionage Behemoth to Last.* [online], MIT Technology Review, 2022. február 28. Forrás: technologyreview.com [2022. 05. 28.].

az egymás után alakuló informatikai biztonsággal foglalkozó cégek pedig egyre szigorúbb kormányzati politikai keretek között kell hogy működjenek.[68]

Mint ismeretes, Kínában évente megrendezik a Tianfu Cup névre keresztelt hekkerbajnokságot, ahol gyakorlatilag a térség legjobb kiberbiztonsági szakemberei mérkőznek meg egymással, és a résztvevők általában sikerrel használnak ki olyan sérülékenységeket, amelyek segítségével könnyen feltörik akár a Windows 10 operációs rendszert, az Adobe pdf-olvasót, az Ubuntu operációs rendszert, az Apple iOS 15 mobil operációs rendszert, a Safari és a Google Chrome internetböngészőket[69] és még számos más fontos programot és applikációt.[70] Kína általánosságban nem támogatja, hogy a kiberbiztonsággal foglalkozó kutatói részt vegyenek külföldi hekkerversenyeken, különösen olyanokon nem, ahol nulladik napi sérülékenységek is napvilágot láthatnak. Akiknek mégis jóváhagyják a részvételét ilyen nemzetközi szakmai megmérettetéseken, azoktól elvárt, hogy a versenyt megelőzően adják át az általuk felfedezett sérülékenységről szóló információkat a kínai kormánynak. Mindemellett egy újabb jogi szabályozás szerint az egyéneknek és a vállalatoknak is két napon belül meg kell osztaniuk a kormánnyal, ha nulladik napi sérülékenységet találtak. A Kínában megrendezett hekkerversenyeken bemutatott sérülékenységeket pedig rendszerint ki is használják a kormányhoz köthető kibertevékenység keretében még a hibajavítások megjelenése előtt, ahogy az korábban előfordult már a Google vagy az Apple esetében is. A Margin Research kutatóintézet ezzel kapcsolatban megjegyzi, hogy a kínai kiberképességek rohamos fejlődése miatt kiemelt fontosságú a kínai technológiai szektor szereplőivel megőrizni a kapcsolatot, nemcsak technológiai és gazdasági okokból, de kiberbiztonsági szemszögből is. A kínai szakértők ugyanis a legjobbak közé tartoznak a sérülékenységek kutatásában, és mélyreható ismeretekkel rendelkeznek az offenzív és a defenzív technikák terén is, ami mind szükséges a kibertámadások elhárításához. Éppen ezért, az amerikai–kínai információcsere megszüntetése a kiberbiztonság terén ellehetetlenítené a szolgáltatók védekezési képességét, és az ellenséges kibertevékenység változása is nehezebben lenne nyomon követhető.[71]

3.4. Irán kibertevékenysége

A perzsa állam jellemzően a regionális ellenfeleivel szemben szokott destruktív kibertámadásokat végrehajtani, az Egyesült Államokat illetően viszont Teherán a nukleáris

[68] A Margin Research kutatóintézet szerint kilenc olyan kiberbiztonsági cég van Kínában, amelyekre érdemes odafigyelni a kiberbiztonsággal és a kínai politikai és katonai stratégiával foglalkozó szakembereknek. Ez a kilenc cég a Tophant, a Cyber Kunlun, a Chaitin Tech, a BugBank, a KnownSec, a SlowMist, az Ansai Technology, a BlockSec és a PeckShield. Ezek a vállalatok többnyire sérülékenységek kutatására, fenyegetések detektálására, biztonsági hírszerzésre koncentrálnak, az általuk nyújtott szolgáltatások és termékeik pedig védelmet kínálnak ügyfeleik számára az offenzív kibertevékenységgel szemben. A vezető ipari vállalatok és internetszolgáltatók pedig a Sangfor Technologies, a Huawei, a New H3C Technologies, a Qi An Xin Technology, a Beijing Venustech Inc., a Topsec Technologies Group, az NSFocus Technologies Group Co Ltd, az Alibaba Cloud, a Qihoo 360 és a Tencent. *The Chinese Private Sector Cyber Landscape.* [online], Margin Research, 2022. április 25. Forrás: margin.re [2022. 05. 17.].

[69] Catalin Cimpanu: *Windows 10, iOS 15, Ubuntu, Chrome Fall at China's Tianfu Hacking Contest.* [online], The Record, 2021. október 17. Forrás: therecord.media [2022. 05. 17.].

[70] Selján–Selján (2021): i. m. 39–40.

[71] Margin Research (2022): i. m.

tárgyalások esetleges sikerében és a szankciók feloldásában bízva inkább kivárásra játszott. A Microsoft szerint bár 2021 folyamán Teherán valóban kevésbé agresszív magatartást mutatott a kibertérben az Egyesül Államok irányába, az amerikai entitások Irán regionális ellenfeleihez képest továbbra is kiemelt célpontok maradtak az iráni APT-csoportok számára. Az iráni hekkerek által leginkább támadott országok között így az Egyesült Államok volt az első (49%), Izrael a második (24%) és Szaúd-Arábia a harmadik (15%).[72]

Izrael és Irán fokozódó szembenállása miatt tehát az offenzív iráni kibertámadások elsősorban a zsidó államra összpontosítottak, noha Teherán egy másik regionális ellenfelére is kiterjedtek. A legkedveltebb támadási módszerük pedig a vizsgált időszakban a zsarolóprogramok alkalmazása volt. 2020-ban figyelték meg az Agrius névre keresztelt APT-csoportot, amelyet iráni kötődésűnek tartanak, és a jelek szerint hírszerzési és adattörlő tevékenységet is folytatott. A SentinelLABS kutatóinak megfigyelései szerint 2021 májusában egy újabb, Iránhoz és egy n3tw0rm zsarolóprogrammal operáló csoporthoz köthető diszruptív kibertámadásra került sor Izrael ellen, az Agrius és a n3tw0rm közötti összefüggések alapján pedig mindkét csoport művelete valószínűleg egy széles körű iráni stratégia része volt.[73] 2020 júliusában a Unit 42 nevű kiberbiztonsági kutatócsoport is azonosított egy, a Közel-Keleten és Észak-Afrikában két állami szervezettel szemben végrehajtott kibertámadást, amely a Thanos néven emlegetett zsarolóprogram egyik verzióját alkalmazta.[74]

A Microsoft és a kiberfenyegetések felderítésével foglalkozó Flashpoint szerint nem egyértelmű, hogy Irán anyagi haszonszerzés céljából is használta-e a zsarolóprogramokat, ugyanis legalább egy alkalommal inkább csak figyelemelterelésként alkalmazták egy valójában destruktív szándékú támadáshoz, amely során egy adattörlő programot telepítettek egy cég informatikai hálózatára és váltságdíjat is követeltek.[75] A Microsoft 2020 novemberétől kezdve az Izrael elleni iráni kibertámadások számának növekedését tapasztalta, amelynek része volt a zsarolóprogramok sorozatos alkalmazása is. Valószínűleg a Microsoft által Rubidiumnak nevezett iráni APT-csoport hajtotta végre a Pay2Key és a n3tw0rm nevű zsarolótámadásokat, amelyek szinte csak Izrael ellen irányultak 2020 végén és 2021 elején.[76] A Rubidium zsarolókampányai többnyire tengeri szállítmányozással foglalkozó izraeli logisztikai vállalatokat érintettek, a célpontok kiválasztása pedig arra enged következtetni, hogy ezek a kibertámadások részét képezték az Izraelnek szánt válaszlépéseknek a zsidó állam és Irán közötti feszült helyzetben.[77] Ami az Egyesült Államok elleni iráni kiberműveleteket illeti, az amerikai célpontok elleni tevékenység célját tekintve kettős volt. Teherán egyrészt igyekezett információkat szerezni az amerikai politika

[72] Microsoft (2021): i. m. 63–64.

[73] Amitai Ben Shushan Ehrlich: *From Wiper to Ransomware. The Evolution of Agrius.* [online], SentinelLABS, 2021. május 25. Forrás: sentinelone.com [2022. 05. 18.].

[74] Robert Falcone: *Thanos Ransomware: Destructive Variant Targeting State-Run Organizations in the Middle East and North Africa.* [online], Unit 42, 2020. szeptember 4. Forrás: unit42.paloaltonetworks.com [2022. 05. 18.].

[75] *A Second Iranian State-Sponsored Ransomware Operation "Project Signal" Emerges.* [online], Flashpoint, 2021. április 30. Forrás: flashpoint-intel.com [2022. 05. 18.].

[76] *Pay2Kitten, Pay2Key Ransomware – A New Campaign by Fox Kitten.* [online], Clear Sky Security, 2020. december. Forrás: clearskysec.com [2022. 05. 18.].

[77] Microsoft (2021): i. m. 63.

alakulásával kapcsolatban, másrészt próbált olyan informatikai hálózatokhoz hozzáférést szerezni, amelyek a nukleáris megállapodásról szóló tárgyalások kudarca, illetve a szankciók feloldásának elmaradása esetén még jól jöhetnek számára.[78]

Észak-Korea dobogós helyen

2020 júliusa és 2021 júniusa között Észak-Korea különösen aktív volt a kibertérben, figyelembe véve, hogy a többi nemzetállami szereplőhöz képest egy kisebb méretű és korlátozottabb erőforrásokkal rendelkező országról van szó, az államokhoz köthető kibertámadások tekintetében viszont mégis dobogós helyezést ért el a vizsgált időszakban. A Microsoft szerint az észak-koreai támadások első számú célpontjai a felhasználói programok voltak, és ezeknek a támadásoknak a többségét a Thallium és a Zinc APT-csoportok hajtották végre, azzal a céllal, hogy nyilvánosan nem hozzáférhető diplomáciai és geopolitikai szempontból releváns információkat szerezzenek. Ennek érdekében az észak-koreai APT-csoportok elsősorban diplomáciai tisztségviselőket, akadémikusokat és kutatóintézetek munkatársait vették célba világszerte. A legtöbb áldozatuk Dél-Koreában, az Egyesült Államokban és Japánban volt, ugyanakkor az észak-koreai aktorok Európában, de még Kínában és Oroszországban is vettek célba akadémikusokat és kutatókat, noha Peking és Moszkva is jó kapcsolatokat ápol Észak-Koreával.[79]

1. táblázat: A fontosabb APT-csoportok összefoglaló táblázata (2020. július – 2021. június)

Nemzetállam és a hozzá köthető támadások százaléka	Csoportnév és a hozzá köthető támadások százaléka	Egyéb elnevezések	Célpontok
Oroszország (58%)	Strontium	APT28, Fancy Bear	kormányzatok, diplomáciai testületek, védelmi szektor, kutatóintézetek, nem kormányzati szervezetek, felsőoktatás, hadiipari magánvállalatok, informatikai szoftver és szolgáltatók
	Nobelium (59%)	UNC2452	kormányzat, diplomáciai célpontok, védelmi szektor, informatikai szolgáltatók, telekommunikációs szektor, kutatóintézetek, nem kormányzati intézmények, katonai magánvállalatok
	Bromine	Energetic Bear	kormányzatok, energiaszektor, polgári légi közlekedés, védelmi ipar

[78] 2020 második felében például a Phosphorus nukleáris politikai szakértőket vett célba az iráni atomalkut (*Joint Comprehensive Plan of Action,* JCPOA) aláíró országokban, hogy információkat szerezzen a demokrata amerikai elnökjelölt, Joe Biden megválasztását követően várhatóan újrainduló tárgyalásokat megelőzően. 2020 őszén a Phosphorus kibertámadásokat hajtott végre a közelgő Müncheni Biztonságpolitikai Konferencia és a Think 20 csúcstalálkozó résztvevői ellen. Tom Burt: *Cyberattacks Target International Conference Attendees.* [online], Microsoft, 2020. október 28. Forrás: blogs.microsoft.com [2022. 05. 19.].

[79] Microsoft (2021): i. m. 66–67.

Nemzetállam és a hozzá köthető támadások százaléka	Csoportnév és a hozzá köthető támadások százaléka	Egyéb elnevezések	Célpontok
Kína (8%)	Manganese	APT5, Keyhole Panda	kommunikációs infrastruktúra, hadiipar, szoftverfejlesztés
	Zirconium (3%)	APT31	kormányzati szervek és szolgáltatások, diplomáciai szervezetek, gazdasági szervezetek
	Hafnium	–	felsőoktatás, védelmi ipar, kutatóintézetek, nem kormányzati szervezetek, ügyvédi irodák, orvostudományi kutatások
	Nickel (2%)	APT15, Vixen Panda	kormányzati szervek és szolgáltatások, diplomáciai szervezetek
	Chromium	ControlX	energiaszektor, kommunikációs infrastruktúra, oktatás, kormányzati szervek és szolgáltatások
	Gadolinium	APT40	hajózás, egészségügy, felsőoktatás, regionális kormányzati szervezetek
Irán (11%)	Phosphorus (9%)	Charming Kitten	diplomáciai és nukleáris politikai közösségek, akadémikusok, újságírók
	Curium (2%)	Houseblend Tortoise Shell	amerikai katonai és hadiipari magánvállalatok, informatikai szolgáltatások, közel-keleti kormányok
	Rubidium	Fox Kitten Parasite	izraeli logisztikai vállalatok, informatikai szolgáltatások, védelmi szektor
Észak-Korea (23%)	Zinc	Lazarus, Labyrinth Chollima	felhasználói programok, magánvállalatok, kutatóintézetek, kiberbiztonsági kutatók
	Thallium (16%)	Kimsuky, Velvet Chollima	kutatóintézetek, diplomáciai tisztviselők, akadémikusok
	Cerium (5%)	Kimsuky	kutatóintézetek, diplomáciai tisztviselők, akadémikusok, védelmi szektor, űripar
	Osmium	Konni	diplomáciai tisztviselők, kutatóintézetek

Forrás: Microsoft (2021): i. m.

4. Futótűzként terjedő dezinformáció

A Microsoft a 2021. októberi jelentésében külön fejezetet szentelt a dezinformációk fokozódó terjedésének. Bár a téves információk szándékos terjesztése a közvélemény befolyásolásának céljából nem új találmány, az informatikai eszközök és a kommunikáció fejlődésével a dezinformációk új terjesztési módjai és formái kerültek előtérbe az elmúlt tíz évben, ami jelentős mértékben fokozta a dezinformációs kampányok befolyásának mértékét, illetve azok jelentőségét. Amíg a kibertámadások a digitális rendszerek megbízhatóságát, integritását és hozzáférhetőségét veszélyeztetik, addig a dezinformáció az egyén logikus, elemzői és kritikus gondolkodásának gyenge pontjait vagy éppen hiányosságait

használja ki.[80] A közösségi oldalak, a tartalomgyártói platformok, keresőmotorok és üzenetküldő szolgáltatások pedig ma már kitűnő terepül szolgálnak az államok és a nem állami szereplők számára is a dezinformációk terjesztésére. Emellett a különböző közösségimédia-szolgáltatások lehetővé teszik a rosszindulatú aktorok számára a dezinformációs kampányok rendszeres ismétlését, sikerük követését, ellenőrzését és optimalizálását is.[81]

Az online platformokat már évek óta előszeretettel alkalmazzák politikai befolyásolásra, a társadalmi polarizáció fokozására. Mindemellett a gépi tanulás fejlődésével és a grafikai lehetőségek bővülésével ma már korábban szinte lehetetlen minőségben és mértékben lehet hitelesnek tűnő audiovizuális tartalmakat *(deepfake)* is előállítani, amely még meggyőzőbbé teszi a fogékony közönség számára a dezinformációs kampányok üzenetét. A helyzetet tovább bonyolítja, hogy a mesterséges intelligencia segítségével a nemzetállamok és a nem állami szereplők egyaránt képesek az emberi gondolkodásról tanúskodó adatok és kutatási eredmények alapján pszichológiai műveleteket végrehajtani, egyéneket és csoportokat profilozni, és személyre szabott dezinformációs kampányokat indítani az emberek véleményének és magatartásának befolyásolására. Mindezek következtében jelentős mértékben felgyorsult a dezinformáció terjedése, ami súlyos következményekkel fog járni az iskolázott és tájékozott állampolgárokra utalt demokráciák esetében, és mindenképpen fenyegetést jelent a nyílt vitára, illetve a szabad és modern társadalmakra nézve.[82] Ráadásul az ellenséges aktorok a dezinformációs kampányokat és a kibertámadásokat jellemzően együtt is alkalmazzák a céljuk elérése érdekében. Egy jól koordinált dezinformációs kampánnyal például el lehet árasztani a hírcsatornákat téves információkkal, a mondvacsinált és kitalált narratívákkal pedig olyan szintű információs zajt lehet kelteni, hogy a hazugságok özönében az emberek többsége számára végül gyakorlatilag elveszik az igazság.

A dezinformációk ellensúlyozása érdekében növelni kellene a médiatudatosságot, fel kellene készíteni az embereket a dezinformáció és a téves információ felismerésére,[83] valamint fel kellene hívni a figyelmet a források és a médiaorgánumok megbízhatósága ellenőrzésének szükségességére. Elengedhetetlen továbbá a független és minőségi újságírás, valamint a megbízható hírszervezetek támogatása, a helyi tudósítók munkájának segítése. A jövőben várhatóan rendelkezésre állnak majd a mesterséges intelligencia alkalmazásán alapuló technikai lehetőségek a dezinformációk és az azokat terjesztő források kiszűrésére.[84] A mesterséges intelligencia fejlődésével azonban minden bizonnyal a dezinformációk terjedése is egyre komolyabb problémát fog okozni, hiszen ezáltal gyakorlatilag korlátlanul tud majd terjedni a nagyon hihetően megalkotott dezinformáció a közösségi

[80] A Microsoft szerint a dezinformációk és a számítógépes propaganda jelentette fenyegetés gyakorlatilag kognitív hekkelés *(cognitive hacking),* amelynek az a célja, hogy dezinformációk segítségével változtassa meg a célközönség gondolkodását és manipulálja valóságértelmezését. Microsoft (2021): i. m. 112.

[81] Microsoft (2021): i. m. 110.

[82] Microsoft (2021): i. m. 110–111.

[83] *Misinformation* (téves információ): nem szándékosan terjesztett, tényként bemutatott, valójában azonban téves információ (véletlen hiba). *Disinformation* (dezinformáció): a közvélemény megtévesztését szolgáló, szándékosan terjesztett, propagandacélokra szánt téves információ (manipulált audiovizuális tartalom, összeesküvés-elmélet, pletyka). *Malinformation* (rossz információ, félretájékoztatás): privát információk szándékos nyilvánosságra hozatala személyes érdekből, eredeti tartalom kontextusának megváltoztatása, dátum és idő módosítása.

[84] Microsoft (2021): i. m. 111.

oldalakon és általában az interneten. Ezt a helyzetet nyilvánvalóan a kibertér valamennyi szereplője ki fogja használni, így például Oroszország és Kína is.[85]

Azt, hogy a mesterséges intelligencia hogyan transzformálja át a nemzetközi biztonsági környezetet és ezáltal milyen komoly biztonsági kihívásokat fog majd jelenteni az elterjedése, már a NATO is felismerte.[86] Tudva, hogy a mesterséges intelligencia hatással lesz majd a kollektív védelemre, a válságkezelésre és a kooperatív biztonságra egyaránt, a NATO 2021 októberében kiadta a mesterségesintelligencia-stratégiáját.[87] Mivel a forradalmi technológiák a béke, a válságok és a fegyveres konfliktusok természetét is megváltoztatják, a NATO számára elengedhetetlen, hogy erőfeszítéseket tegyen a technológiai fejlettségének megőrzése és javítása érdekében. Ez azért is kiemelt fontosságú, mert például Kína a következő tíz éven belül a világ vezető hatalmává szeretne válni a mesterséges intelligencia terén. A NATO ugyanakkor a mesterséges intelligencia mellett további területeket is prioritásként jelölt meg a forradalmi technológiák közül a maga számára, mint például a big data, az autonóm rendszerek, a kvantumtechnológia, a biotechnológia, a hiperszonikus technológia és az űrtechnológia.[88]

5. Összegzés

A Microsoft megfigyelései szerint 2021 őszéig abban nem történt változás, hogy még mindig a hírszerzés és az információgyűjtés mutatkozott a nemzetállamok egyik fő célkitűzésének, ami jellemzően sokkal gyakrabban fordul elő, mint a destruktív célú támadások. Irán az egyetlen állam, amely rendszeresen hajt végre destruktív céllal kibertámadásokat, elsősorban Izrael ellen.[89] Ahogy azt a Microsoft 2021-es jelentésében is megjegyezte, Irán és a zsidó állam között jellemzően feszült politikai helyzetben és kölcsönösen kerül sor kibertámadásokra direkt károkozás céljából, amikor egymást érik az incidensek, nem kímélve egymás szállítóhajóit sem. Iránnal szemben azonban más fontosabb állami szereplők – mint például Észak Korea, Oroszország vagy Kína – általában igyekeznek tartózkodni a destruktív jellegű kibertámadások végrehajtásától, ugyanakkor folytatják azok előkészítését arra az esetre, ha a feszültség fokozódása miatt a kormányzat esetleg a kiberháború eszkalációja mellett döntene. Az államokhoz köthető támadások közel 80%-a kormányzati szerveket, nem kormányzati szervezeteket vagy kutatóintézeteket érintett, de például Észak-Korea már anyagi haszonszerzés céljából is hajtott végre kibertámadásokat, jellemzően kriptovaluta-kereskedelemmel foglalkozó cégek ellen, amelyektől vagy kriptovalutát vagy esetleg kutatáshoz kapcsolódó szellemi tulajdont próbált ellopni. Az elmúlt évek legkomolyabb változása, amely mind a négy említett állami szereplőre (Oroszország,

---

[85] Jonathan Haidt: *Why the Past 10 Years of American Life Have Been Uniquely Stupid.* [online], The Atlantic, 2022. április 11. Forrás: theatlantic.com [2022. 05. 26.].

[86] *NATO Science & Technology Trends 2020–2040.* [online], NATO Science & Technology Organization, 2020. március. 50–58. Forrás: nato.int [2022. 05. 26.].

[87] Zoe Stanley-Lockman – Edward Hunter Christie: *An Artificial Intelligence Strategy for NATO.* [online], 2021. 10. 25. Forrás: NATO nato.int [2022. 05. 26.].

[88] *NATO 2030 Factsheet.* [online], NATO, 2021. június. Forrás: nato.int [2022. 05. 26.].

[89] Farnaz Fassihi – Ronen Bergman: *Israel and Iran Broaden Cyberwar to Attack Civilian Targets.* [online], The New York Times, 2021. november 27. Forrás: nytimes.com [2022. 05. 10.].

Észak-Korea, Irán, Kína) jellemző, hogy elkezdtek informatikai szolgáltatókat is megcélozni annak érdekében, hogy még hatékonyabban tudják támadni azok ügyfeleit. Ezekre a támadásokra az orosz SolarWinds és a Microsoft Exchange szervereken található sérülékenységeket kihasználó kínai támadások szolgáltak kitűnő például, s bár ezek voltak talán az utóbbi évek legnagyobb visszhangot kiváltó kiberbiztonsági incidensei, Irán és Észak-Korea is hasonló, közvetett támadási taktikákat használtak az igazi célpontjaik ellen.[90]

A megfigyelt támadások többségének 2020. július és 2021. június között is az Egyesült Államokban található szervezetek voltak a célpontjai, ezért is esett szó Joe Biden amerikai és Vlagyimir Putyin orosz elnök június 16-i genfi csúcstalálkozóján a kibertámadások kérdéséről.[91] Ugyanakkor az egyes államok közötti feszültség fokozódásával párhuzamosan észlelhető volt a célpontok és a támadások intenzitásának változása is. Ennek megfelelően, például míg az Oroszországhoz köthető Nobelium nevű APT-csoport a megelőző költségvetési évben a Microsoft mindössze hat ügyfele ellen hajtott végre kiberműveletet, addig az érintett ügyfelek száma 2021 nyarára már 1200-ra ugrott. Mindez elsősorban annak volt betudható, hogy Oroszország jelentős mértékben növelte a támadások számát azon ukrán kormányzati célpontok ellen, amelyek a határmenti orosz csapatösszevonással szemben igyekeztek nagyobb támogatottságot szerezni. 2021 első felében azonban más változás is történt. Izrael esetében például megnégyszereződött a támadások száma, ami elsősorban Irán számlájára volt írható.[92]

Ahogy a technológia egyre fontosabb szerepet kezd betölteni a mindennapi életünkben, úgy a kiberbiztonság szavatolása is lassan egyre égetőbb kérdéssé fog majd válni az egyének, a vállalatok és a kormányzatok számára egyaránt. Ugyanis a technológiai fejlődéssel párhuzamosan együtt jár a támadók által kihasználható sérülékenységek számának a növekedése, azaz lényegében egyre többféleképpen lehet majd bármilyen informatikai rendszert feltörni, legyen szó csak egy mobiltelefonról, vagy akár az amerikai védelmi minisztérium levelezőrendszeréről. A támadók pedig lehetnek „csupán kiberbűnözők" vagy akár nemzetállamok által támogatott hekkercsoportok is, amelyek egyre kifinomultabb eszközökkel és egyre több erőforrással rendelkeznek, így már képesek komplex kiberműveleteket végrehajtani. A kibertámadásokkal szembeni védekezés érdekében ezért itt is érdemes hangsúlyozni a jó kiberhigiénia[93] és a kiberbiztonsági alapszabályok betartásának fontosságát, illetve az informatikai támadási felületek csökkentésének szükségességét.

---

[90] Microsoft (2021): i. m. 52.

[91] A találkozón Biden elnök szóba hozta az amerikai Colonial Pipeline elleni támadást és megjegyezte, hogy fel fog lépni minden orosz kibertámadás ellen. Putyin orosz elnök tagadta, hogy Oroszországnak bármi köze lett volna akár csak egy amerikai célpont elleni kibertámadáshoz. Ezt követően a felek megállapodtak a kiberbiztonsági tárgyalások megkezdéséről. A 2022. február 24-én indult ukrajnai orosz invázió és az annak keretében kibontakozó ukrajnai kiberháború fényében azonban kijelenthető, hogy az elnöki csúcstalálkozón elhangzottak nem hoztak pozitív változást a kibertér biztonságát tekintve. Georges De Moura – Tal Goldstein: *What the Biden-Putin Summit Reveals about Future of Cyber Attacks – And How to Increase Cybersecurity.* [online], World Economic Forum, 2021. június 17. Forrás: weforum.org [2022. 09. 11.].

[92] Microsoft (2021): i. m. 52.

[93] *Krasznay Csaba: az új kulcsszó a kiberhigiénia.* [online], Infostart, 2022. január 18. Forrás: infostart.hu [2022. 06. 06.].

FELHASZNÁLT IRODALOM

A Second Iranian State-Sponsored Ransomware Operation "Project Signal" Emerges. [online], Flashpoint, 2021. április 30. Forrás: flashpoint-intel.com [2022. 05. 18.]

Alert (AA22-083A), Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector. [online], Cybersecurity and Infrastructure Security Agency, 2022. március 24. Forrás: cisa.gov [2022. 05. 24.]

Alert (AA22-110A), Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. [online], Cybersecurity and Infrastructure Security Agency, 2022. április 20. Forrás: cisa.gov [2022. 05. 28.]

Burt, Tom: *Another Nobelium Cyberattack.* [online], 2021. május 27. Forrás: blogs.microsoft.com [2022. 05. 14.].

Burt, Tom: *Cyberattacks Target International Conference Attendees.* [online], Microsoft, 2020. október 28. Forrás: blogs.microsoft.com [2022. 05. 19.]

Cimpanu, Catalin: *Windows 10, iOS 15, Ubuntu, Chrome Fall at China's Tianfu Hacking Contest.* [online], The Record, 2021. október 17. Forrás: therecord.media [2022. 05. 17.]

Clapper, James R. – Marcel Lettre – Michael S. Rogers: *Joint Statement for the Record to the Senate Armed Services Committee, Foreign Cyber Threats to the United States*. [online], Senate Armed Services Committee, 2017. január 5. Forrás: armed-services.senate.gov [2022. 05. 29.]

Cole, Brendan: Russia Puts U.S. Top of 'Unfriendly Countries' List. [online], Newsweek, 2021. április 27. Forrás: newsweek.com [2022. 05. 15.]

Conceptual Views on the Activity of the Armed Forces of the Russian Federation in Information Space. Ministerstvo Oborony Rossiyskoy Federatsii, 2011. [online]. Forrás: pircenter.org [2022. 05. 24.]

Conger, Kate: With Eye to Russia, Biden Administration Asks Companies to Report Cyberattacks. [online], The New York Times, 2022. március 23. Forrás: nytimes.com [2022. 05. 26.]

Conger, Kate: Hackers' Fake Claims of Ukrainian Surrender Aren't Fooling Anyone. So What's Their Goal? [online], The New York Times, 2022. április 5. Forrás: nytimes.com [2022. 05. 25.]

Conger, Kate: Ukraine Says It Thwarted a Sophisticated Russian Cyberattack on Its Power Grid. [online], The New York Times, 2022. április 12. Forrás: nytimes.com [2022. 05. 25.]

Conger, Kate – David E. Sanger: U.S. Says It Secretly Removed Malware Worldwide, Pre-empting Russian Cyberattacks. [online], The New York Times, 2022. április 6. Forrás: nytimes.com [2022. 05. 25.]

Conger, Kate – David E. Sanger: *Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds.* [online], The New York Times, 2022. április 27. Forrás: nytimes.com [2022. 05. 25.]

Connell, Michael – Sarah Vogler: *Russia's Approach to Cyber Warfare.* [online], CNA, 2017. március. Forrás: cna.org [2022. 05. 28.]

Cyber Attacks against Estonia (2007). [online], Cyber Law Toolkit, 2007. április 27. Forrás: cyberlaw.ccdcoe.org [2022. 06. 04.]

De Moura, Georges – Tal Goldstein: *What the Biden-Putin Summit Reveals about Future of Cyber Attacks – And How to Increase Cybersecurity.* [online], World Economic Forum, 2021. június 17. Forrás: weforum.org [2022. 09. 11.]

Edward Snowden: Leaks that Exposed US Spy Programme. [online], BBC, 2014. január 17. Forrás: bbc.com [2022. 06. 04.]

Ehrlich, Amitai Ben Shushan: *From Wiper to Ransomware. The Evolution of Agrius.* [online], SentinelLABS, 2021. május 25. Forrás: sentinelone.com [2022. 05. 18.]

Falcone, Robert: *Thanos Ransomware: Destructive Variant Targeting State-Run Organizations in the Middle East and North Africa.* [online], Unit 42, 2020. szeptember 4. Forrás: unit42.paloaltonetworks.com [2022. 05. 18.]

Fassihi, Farnaz – Ronen Bergman: *Israel and Iran Broaden Cyberwar to Attack Civilian Targets.* [online], The New York Times, 2021. november 27. Forrás: nytimes.com [2022. 05. 10.]

Gatlan, Sergiu: *Microsoft: Russian State Hackers Behind 53% of Attacks on US Govt Agencies.* [online], 2021. október 8. Forrás: bleepingcomputer.com [2022. 05. 15.]

Georgia–Russia Conflict (2008). [online], Cyber Law Toolkit, 2008. július–augusztus. Forrás: cyberlaw.ccdcoe.org [2022. 06. 04.]

HAFNIUM Targeting Exchange Servers with 0-day Exploits. [online], Microsoft Threat Intelligence Center (MSTIC), 2021. március 2. Forrás: microsoft.com [2022. 05. 16.]
Haidt, Jonathan: *Why the Past 10 Years of American Life Have Been Uniquely Stupid.* [online], The Atlantic, 2022. április 11. Forrás: theatlantic.com [2022. 05. 26.]
Hanna, Andrew: *The Invisible U.S.–Iran Cyber War.* [online], The Iran Primer, 2019. október 25. Forrás: iranprimer.usip.org [2022. 06. 04.]
Federal Bureau of Investigation: Internet Crime Report 2021. [online], FBI, 2021. Forrás: ic3.gov [2022. 05. 05.]
Krasznay Csaba: az új kulcsszó a kiberhigiénia. [online], Infostart, 2022. január 18. Forrás: infostart.hu [2022. 06. 06.]
Martin, Alexander: *US Military Hackers Conducting Offensive Operations in Support of Ukraine, Says Head of Cyber Command.* [online], Sky News, 2022. június 1. Forrás: news.sky.com [2022. 06. 04.]
McLaughlin, Jenna: *Top Biden Cyber Official: SolarWinds Breach Could Turn from Spying to Destruction 'in a Moment'.* [online], Yahoo News, 2021. április 8. Forrás: news.yahoo.com [2022. 05. 15.]
Microsoft: *Microsoft Digital Defense Report.* [online], Microsoft, 2021. október. Forrás: microsoft.com [2022. 04. 29.]
Nafisi, Ramin – Andrea Lelli: GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM's Layered Persistence. [online], Microsoft, 2021. március 4. Forrás: microsoft.com [2022. 05. 14.]
NATO 2030 Factsheet. [online], NATO, 2021. június. Forrás: nato.int [2022. 05. 26.]
NATO Science & Technology Trends 2020–2040. [online], NATO Science & Technology Organization, 2020. március. Forrás: nato.int [2022. 05. 26.]
O'Neill, Patrick Howell: *How China Built a One-of-a-Kind Cyber-Espionage Behemoth to Last.* [online], MIT Technology Review, 2022. február 28. Forrás: technologyreview.com [2022. 05. 28.]
Pay2Kitten, Pay2Key Ransomware – A New Campaign by Fox Kitten. [online], Clear Sky Security, 2020. december. Forrás: clearskysec.com [2022. 05. 18.]
Perlroth, Nicole – Noam Scheiber – Julie Creswell: *Russian Cybercriminal Group Was Behind Meat Plant Attack, F.B.I. Says.* [online], The New York Times, 2021. június 2. Forrás: nytimes.com [2022. 05. 28.]
Recent Ransomware Attacks. [online], Checkpoint Research, é. n. Forrás: checkpoint.com [2022. 06. 04.]
Rekowski, Michał – Tomasz Piekarz – Barbara Sztokfisz – Robert Siudak – Izabela Albrycht – Przemysław Roguski – Paweł Kostkiewicz et al.: *Geopolitics Of Emerging and Disruptive Technologies.* [online], Krakow, The Kosciuszko Institute, 2020. Forrás: ik.org.pl [2022. 05. 29.]
Russian SVR Targets U.S. and Allied Networks. [online], NSA, CISA & FBI, Cybersecurity Advisory, 2021. április 5. Forrás: media.defense.gov [2022. 05. 15.]
Sanger, David E. – Kate Conger: *Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds.* [online], The New York Times, 2022. május 10. Forrás: nytimes.com [2022. 05. 28.]
Selján Gábor: The Remarkable 10th Anniversary of Stuxnet. *AARMS,* 19. (2020), 3. 85–98. Online: https://doi.org/10.32565/aarms.2020.3.6
Selján Péter – Selján Gábor: Kiberbiztonsági kitekintés. *Nemzet és Biztonság,* 14. (2021), 1. 24–47. Online: https://doi.org/10.32576/nb.2021.1.3
Smith, Brad: *Digital Technology and the War in Ukraine.* [online], Microsoft, 2022. február 28. Forrás: blogs.microsoft.com [2022. 05. 24.]
Soesanto, Stefan: *The IT Army of Ukraine.* [online], Center for Security Studies, 2022. június. Forrás: css.ethz.ch [2022. 09. 11.]
Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine. [online], Microsoft Digital Security Unit, 2022. április 27. Forrás: microsoft.com [2022. 04. 28.]
Stanley-Lockman, Zoe – Edward Hunter Christie: *An Artificial Intelligence Strategy for NATO.* [online], NATO, 2021. október 25. Forrás: nato.int [2022. 05. 26.]
The 10 Biggest Ransomware Attacks of 2021. [online], Touro College Illinois, 2021. november 12. Forrás: illinois.touro.edu [2022. 05. 05.]
The Chinese Private Sector Cyber Landscape. [online], Margin Research, 2022. április 25. Forrás: margin.re [2022. 05. 17.]

The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior tot he People's Republic of China. [online], The White House, 2021. július 19. Forrás: whitehouse.gov [2022. 05. 17.]

Voo, Julia – Irfan Hemani – Simon Jones – Winnona DeSombre – Daniel Cassidy – Anina Schwarzenbach: *National Cyber Power Index 2020. Methodology and Analytical Considerations.* [online], Belfer Center, 2020. szeptember. Forrás: belfercenter.org [2022. 08. 06.]

Шойгу рассказал о задачах войск информационных операций. [online], РИА Новости, 2017. február 22. Forrás: ria.ru [2022. 05. 24.]

York, Dan: *What Is the Splinternet? And Why You Should Be Paying Attention.* [online], Internet Society, 2022. március 23. Forrás: internetsociety.org [2022. 05. 31.]