NEMZETBIZTONSÁGI SZEMLE
10. évfolyam (2022) 2. szám 40–55. • DOI: 10.32561/nsz.2022.2.3

Kovács Zoltán[1]

A rendfenntartó szervek 21. századi kihívásai

Kiberbiztonság a 21. században

The Challenges of Law Enforcement Agencies in the 21st Century

Cybersecurity in the 21st Century

A 21. század elején a rendfenntartó szervek számos kihívással szembesülnek. Ezek között van olyan, amely újonnan jelentkezett, a teljes világon átrohanva, alapjaiban változtatva meg mindannyiunk életét, mint a Covid–19 miatti pandémiás helyzet. Van olyan, amely régóta meglévő, de ma is aktuális probléma, mint a migráció. De van olyan is, amely nem olyan régi gyökerű, de azért már jó pár éve velünk van, ilyen a kiberbiztonság. 2021. szeptember 23-án tartott „A rendfenntartó szervek 21. századi kihívásai" című workshopon ezek közül többről is tartottak előadást a felkért szakemberek. Jelen cikk a kiberbiztonsággal kapcsolatos kihívásokról szóló előadás anyagát tartalmazza. Példákon keresztül mutatja be a kiberbiztonság jelentőségét és néhány fontosabbat azok közül a tendenciák közül, amelyek a napjainkban jellemzik azt. Foglalkozik a Covid–19, az összekapcsolt hálózatok, felhőalapú szoftverek, növekvő adatmennyiség, valamint a mesterséges intelligencia és gépi tanulás hatásával a kiberbiztonságra.

Kulcsszavak: *kiberbiztonság, mesterséges intelligencia, felhő, Covid–19, kibertámadás*

The law enforcement agencies had to face several challenges in the beginning of the 21st century. Some of these are new, sweeping across the world, fundamentally changing everyone's life, like the Covid-19 pandemic. There is another challenge, the migration, which is still relevant today. However, there is another, which is not as old as migration, but has appeared several years ago. This is cybersecurity. In the workshop, called „The Challenges of Law Enforcement Agencies in the 21st Century" the invited speakers held several presentations about these issues and other challenges. This

[1] Biztonsági igazgató, Vodafone Magyarország Zrt.; tanársegéd, Nemzeti Közszolgálati Egyetem Bűnügyi, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék, e-mail: zkovacs.24@gmail.com

article contains the material of the presentation on the challenges of cybersecurity. It emphasizes the importance of cybersecurity and some important trends through examples that characterise it today. The article addresses the impact of Covid-19, connected networks, cloud computing, growing amount of data, artificial intelligence and machine learning on cybersecurity.

Keywords: *cybersecurity, Artificial Intelligence, cloud, COVID-19, cyber attack*

1. Bevezetés

Jelen cikk „A rendfenntartó szervek 21. századi kihívásai" című workshopra készült előadás anyagát tartalmazza. Amint az a workshopon részt vevő előadók előadásaiból is plasztikusan kiderült, a rendfenntartó szervek nagyon sok és szerteágazó kihívással szembesülnek a 21. század elején.

Ezek között vannak olyan, a pandémiás helyzettel kapcsolatos feladatok, amelyek az elmúlt évszázadban egyáltalán nem voltak jelen a rendfenntartó szervek munkájában, az elmúlt években ez azonban amellett, hogy a világ minden más tevékenységére hatást gyakorolt, a rendfenntartó szervek munkáját is nagymértékben befolyásolta.

A 21. század kihívásai közül talán a kiberbiztonságiak jelennek, jelentek meg eddig a legmarkánsabban, ezek okozták a legnagyobb „fejtörést", ezek igényelték, igénylik a legtöbb új képzést, a korábbi gondolkodásmód jelentős átalakítását. A pandémiás helyzet azonban erre is óriási kihatással volt, ezt is alapjaiban változtatva meg.

Jelen cikk kereteit messze meghaladja a kiberbiztonsági kihívások teljes körű bemutatása, így azok közül csupán a szerző által legfontosabbaknak ítélteket emeli ki. Azon legfontosabbakat, amelyek talán – a szerző megítélése szerint mindenképpen – a legnagyobb hatással vannak a rendvédelmi szervek munkájára. Ennek során az alábbi kérdésekkel foglalkozik:

- a Covid–19 hatása a kiberbiztonságra;
- összekapcsolt hálózatok, felhőalapú szoftverek, növekvő adatmennyiség hatása;
- AI és gépi tanulás hatása.

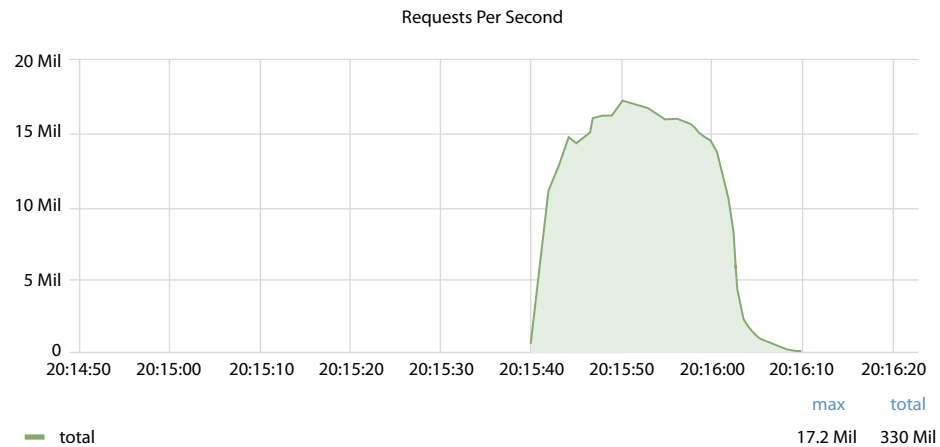
Jelen cikk – összhangban a workshop gondolatvilágával és a fentebb megfogalmazottakkal – elsősorban problémafelvető és nem problémamegoldó. Ennek megfelelően tartalma a főbb hatások ismertetésére és a kihívások megfogalmazására terjed ki.

2. Példák és trendek a közelmúltból

Számtalan példát lehetne hozni hétről hétre a kibertámadásokra, ezekből a szerző kettőt ragadott ki véletlenszerűen. Ezek azonban nagyon jól jellemzik a probléma súlyát, és megmutatják a kibertérben jelentkező veszélyek hatásait mindennapjainkra és a rendfenntartó szervek munkájára egyaránt. 2021 augusztusában történt két incidens, amelyet a workshopon a szerző példának hozott fel:

Mirai botnet DDoS támadás pénzügyi iparági szereplő ellen[2]

A Cloudflare nevű cég tette közzé, hogy az eddigi legnagyobb mértékű, úgynevezett volumetrikus elosztott szolgáltatás-megtagadásos támadást (DDoS[3]) észlelte, amely egy meg nem nevezett pénzügyi iparágban működő szereplő ellen irányult. A támadást egy botnet,[4] a Mirai botnet[5] segítségével hajtották végre. A támadás során mért csúcssebesség 17,2 millió lekérdezés/másodperc (*request/second,* rps) volt, amely 3-szor nagyobb a korábban észlelt és mért eddigi legnagyobb mértékű támadásnál. A támadás lefolyását mutatja az alábbi, 1. ábra.



1. ábra: Az eddigi legnagyobb volumetrikus DDoS támadás lefolyása
Forrás: Lakshmanan (2021): i. m.

A támadásban több mint 20 ezer fertőzött eszköz vett részt, amelyek világszerte 125 országban voltak megtalálhatók. Ezek mintegy 15%-a négy országban, Indonéziában, Brazíliában, Vietnámban és Ukrajnában működött.

[2] Ravie Lakshmanan: Cloudflare Mitigated One of the Largest DDoS Attack Involving 17.2 Million rps. *The Hacker News,* 2021. augusztus 20.

[3] DDoS: *Distributed Denial of Service.*

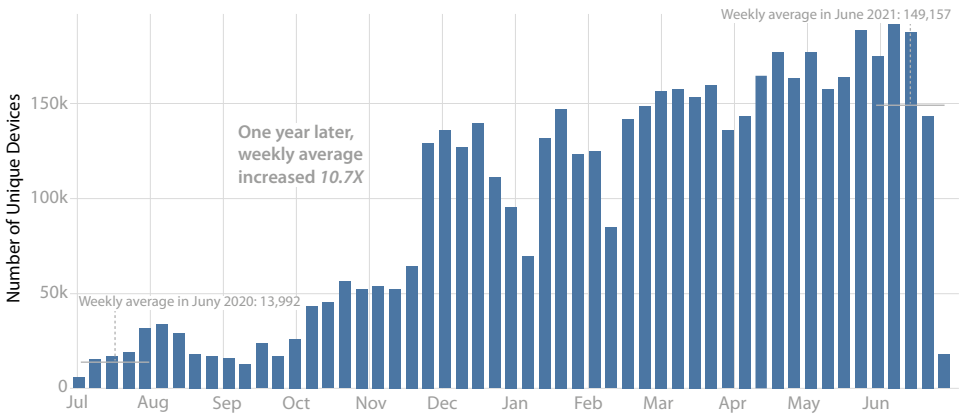
[4] Botnet: A *„robot"* és a *„network"* szavak összevonásával létrehozott kifejezés. Jelentése: botokkal fertőzött számítógépek (IT-alapú eszközök) halmaza. A bot egy rosszindulatú szoftver, amely parancsokat kap egy mester géptől. Ez a „bot" elnevezés a régi Internet Relay Chat (IRC) csevegőszolgáltatásból származik, ahol a felhasználók úgynevezett „botokat" fejleszthetnek, amelyek életben tudják tartani a csatornákat. A számítógép akkor fertőződik meg, amikor egy féreg vagy vírus telepíti a botot, vagy amikor a felhasználó meglátogat egy rosszindulatú webhelyet, amely kihasználja a böngésző sebezhetőségét.

[5] A Mirai egy rosszindulatú program, amely a Linuxot futtató hálózati eszközöket távvezérelt botokká alakítja, amelyek a botnet részeként használhatók nagyszabású hálózati támadásokban. Elsősorban az online fogyasztói eszközöket célozza meg, például az IP-kamerákat és az otthoni routereket.

Az USA-beli T-Mobile-tól több mint 50 millió ügyféladatot lopott el egy 21 éves hacker[6]

Egy hacker egy nem megfelelően védett routeren keresztül bejutott a Washington államban található adatközpontba, és ott az USA-beli T-Mobile szolgáltató több mint 100 szerveren tárolt adataihoz fért hozzá. Több mint 50 millió személyes adatot sikerült megszereznie a távközlési vállalat szervereiről. Köztük olyan érzékeny adatokat, mint név, születés időpontja, társadalombiztosítási szám, de hozzáfért a felhasználó által használt előfizetéshez tartozó készülék IMEI[7]- és SIM[8]-kártya IMSI[9]-kódjához is.

A két kiragadott példát követően érdemes néhány trendről is szót ejteni. A Fortinet kiberbiztonsági cég által 2021 augusztusában közzétett *Global Threat Landscape Report*[10] című időszakos dokumentumban található az alábbi, 2. ábra, amely a detektált zsarolóvírusok számát mutatja a 2020 júliusa és 2021 júniusa közötti időszakban.

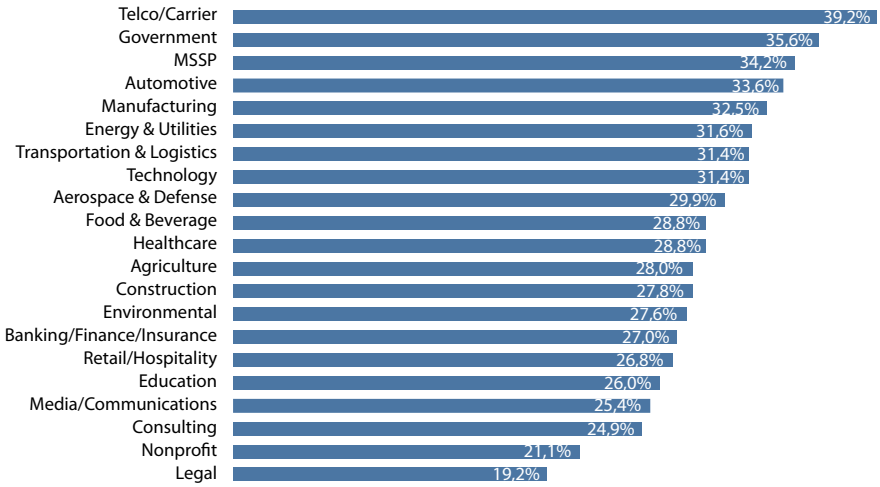


2. ábra: Zsarolóvírus-detektáció az elmúlt 12 hónapban
Forrás: Fortinet (2021): i. m.

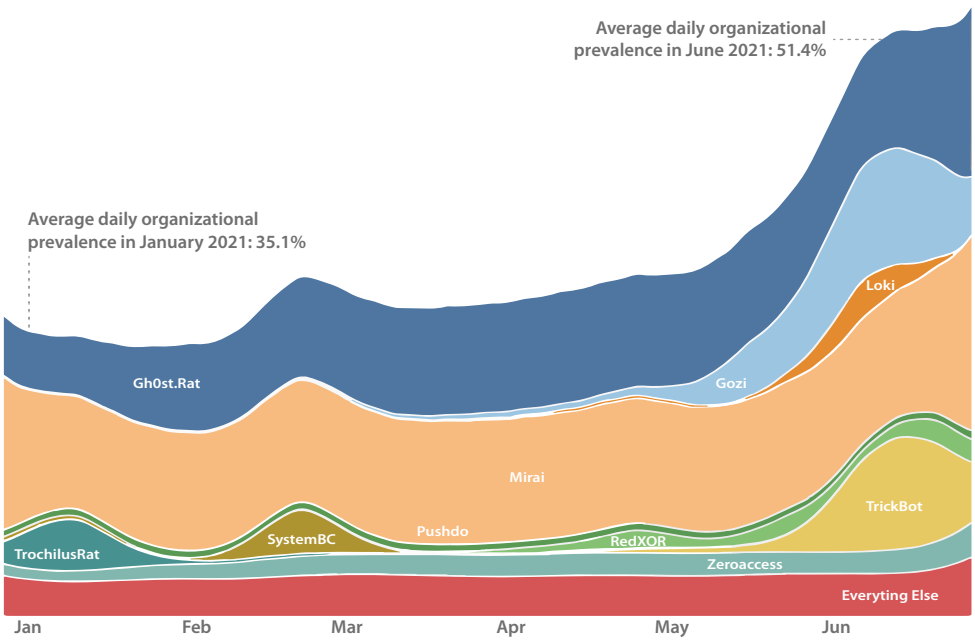
A kibervédelmi szakemberek korábban azzal számoltak, hogy a zsarolóvírusok a 2010-es évek második felében látott megjelenésüket és kiugró elterjedésüket követően továbbra is fennmaradnak a kibertámadók arzenáljában, ám számosságuk visszaáll egy jóval alacsonyabb szintre. Bár a visszaesés valóban be is következett, ám mint a 2. ábrán látható, az elmúlt évben ismét jelentősen megnőtt a zsarolóvírusos támadások száma, átlagosan 10,7-szer annyi támadást detektáltak 2021. júniusában, mint egy évvel korábban. Ennek egyik oka talán éppen a pandémiás helyzet okozta

6 Mitchell Clark: Hacker Claims Responsibility for T-Mobile Attack, Bashes the Carrier's Security. *The Verge,* 2021. augusztus 26.
7 IMEI: *International Mobile Equipment Identity,* nemzetközi mobilkészülék-azonosító, a mobiltelefon-készülékek egyedi azonosítószáma.
8 SIM: *subscriber identity module,* előfizetői azonosító modul, ez tárolja az előfizető azonosítására hivatott egyedi azonosítót.
9 IMSI: *International Mobile Subscriber Identity,* nemzetközi mobil előfizető azonosító, a SIM-kártyához rendelt egyedi azonosító szám.
10 Global Threat Landscape Report. A Semiannual Report by FortiGuard Labs. *Fortinet,* 2021. augusztus.

változás a világban, amely a kibertérre, és az abban tapasztalható veszélyek változására is alapvetően rányomta bélyegét. Erről a későbbiekben még bővebben is esik szó. Az alábbi 3. ábra mutatja a tanulmány készítői által 2021. első félévében észlelt zsarolóvírusos támadások megoszlását iparágak szerint.



3. ábra: Zsarolóvírusos támadások megoszlása iparágak szerint 2021. első félévében
Forrás: Fortinet (2021): i. m.

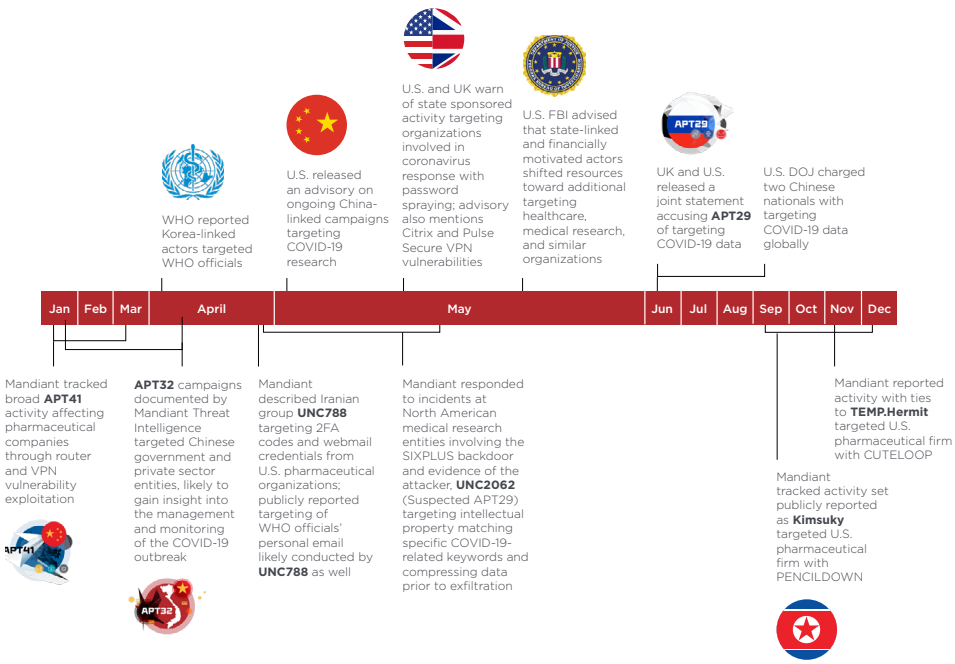


4. ábra: Botnet-detektáció 2021. első félévében
Forrás: Fortinet (2021): i. m.

A fenti ábra jól mutatja, hogy a telekommunikációs ipar és a kormányzat voltak elsősorban a zsarolóvírusos támadások célpontjai, míg a más típusú kibereszközökkel egyébként erősen támadott egészségügy és oktatás ebben a félévben lényegesen kevesebb zsarolóvírusos támadást szenvedett el az előzőkhez képest.

Egy másik aggasztó jelenség, amint az az első példából is jól látszott, az úgynevezett botnetek terjedése. Ennek trendjét szintén jól mutatja az alábbi, 4. ábra. A 4. ábrán látható sávok szélessége reprezentálja, hogy az adott botnetet hány szervezetnél detektálták 2021 első félévében. Ebből jól látszik, hogy a fenti példában bemutatott Mirai mellett a Gh0st.Rat nevű botnethálózat játszik még kiemelkedő szerepet a kibertámadások során.

Az elmúlt években a Covid–19 a világ minden területére rányomta a bélyegét. Nincs ez másképp a kibertérrel sem. Ennek egyik releváns példáját mutatta be a FireEye nevű cég szokásos évi értékelő jelentésének, az *M-Trends*-nek 2021-es számában. A Covid–19 elleni vakcina kifejlesztése minden ország számára nemzetbiztonsági és gazdasági szempontok alapján is kiemelt kérdés volt. Épp ezért a vakcina fejlesztésének legintenzívebb időszakában, 2020-ban jelentős, ezt célzó ipari kémkedés folyt a kibertérben is. Ennek kiemelt és a FireEye cég által megismert eseteit mutatja be az alábbi, 5. ábra.



5. ábra: Covid–19-kutatásokat célzó, államilag támogatott kibertámadások
Forrás: FireEye–Mandiant: M-Trends 2021. Special Report (2021).

3. A rendfenntartó szervek főbb kiberbiztonsági kihívásai

Az előző fejezetben ismertetett két kiragadott példa és néhány kiberbiztonsági trend szemléletesen bemutatta, hogy a 21. század elejének egyik legnagyobb kihívását a kiberbiztonság jelenti mindannyiunk, így a rendfenntartó szervek számára is. A kiberbiztonsági kihívásokat sokféle jellemző szerint lehetne csoportosítani, rengeteg olyan aktuális trendet lehetne felvázolni, amelyek akár jelentősen hatnak, hathatnak a rendfenntartó szervek munkájára. A workshop előadásainak időkerete természetesen nem tette lehetővé a mély, mindenre kiterjedő elemzést, magának a workshopnak sem ez volt a célja, így a szerző önkényesen három olyan témakört emelt ki az előadásában, amelyek szerinte talán a legnagyobb hatást gyakorolhatják az említett szervek munkájára. Ezek az alábbiak voltak:

- a Covid-19 hatása a kiberbiztonságra;
- összekapcsolt hálózatok, felhőalapú szoftverek, növekvő adatmennyiség hatása;
- mesterséges intelligencia és gépi tanulás hatása.

3.1. Covid–19-kihívások

A pandémiás helyzet kiberbiztonságra vonatkozó hatásait az előző fejezet vége már felvezette. Attól azonban sokkal szerteágazóbb hatásai voltak, hogy csupán az oltóanyag kapcsán jelentkező, kibertérben elkövetett kémkedést emeljük ki. A Covid–19 kibertérre és a kiberbiztonságra gyakorolt hatásával sok cikk, blogbejegyzés stb. foglalkozik.[11] Az általuk leírt hatások közül a rendfenntartó szervek szemszögéből talán az alábbiak emelhetők ki:

• Geopolitika helyett teljesen *globális hatás a kibervédelemre.*

A kibertérben jól tudjuk, hogy nincsenek határok. Az olyan jelenségek, mint a bankkártyákkal való visszaélések vagy a nigériai csalás korábban is globálisak voltak. Azonban eddig az államilag támogatott kibertámadások kapcsán jelentős részben geopolitikai hatások voltak felfedezhetők. Valamilyen kisebb térségben kialakult probléma, egymáshoz ellenségesen álló országok konfliktusai sok esetben kiterjedtek a kibertérre is. Legtöbbször a beszélt nyelv miatt ez a kiberbűnözésre is igaz volt. A Covid–19 ezt is jelentősen befolyásolta, ahogy az az 5. ábrán is látható. Ma már sokkal inkább beszélhetünk globális hatásról, akár az államilag támogatott kibertámadások kapcsán is.

[11] Például Impact of COVID-19 on Cybersecurity. *Deloitte,* (é. n.); ENISA: *COVID19: Stronger Together in Fighting Cyber Threats* (2020); Leonid Grustniy: The Great Lockdown: How COVID-19 has Affected Cybersecurity. *Kaspersky,* 2021. március 24.; Bernardi Pranggono – Abdullahi Arabo: COVID-19 Pandemic Cybersecurity Issues. *Internet Technology Letters,* 4. (2021), 2. 1–6; Tabrez Ahmad: *Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity.* 2020.

• Vállalatok próbáltak alkalmazkodni – *a kibertámadók kihasználták a helyzetet.*

A Covid–19 hatásaihoz a vállalatok megpróbáltak alkalmazkodni. A munkavállalók jelentős részét *home office*-ból dolgoztatták, gyorsan és sokszor hiányos biztonsági elemekkel, beállításokkal tették elérhetővé számukra távolról a vállalati infrastruktúrát. Ez kedvező alkalom volt a kibertámadók részére is, hiszen sok esetben esetleges megoldásokkal, biztonságos, titkosított kapcsolat nélkül kezdtek el távolról dolgozni a korábban home office-t nem alkalmazó cégek. Ráadásul sokszor a munkavállalók is ismeretlen terepen mozogtak, így az ő megtévesztésük is lényegesen könnyebben ment ebben az időszakban. A támadók pedig kihasználták ezeket a – számukra nagyon kedvező – lehetőségeket.

• A globális járvány megváltoztatta az üzleti tevékenységet, és ennek eredményeként *változott a legtöbb vállalkozás támadási felülete és kockázati profilja*

Sok vállalatnak nemcsak azt kellett megszerveznie, hogy a munkát másképp tudják elvégezni a dolgozók, de sok esetben az üzleti modellen is változtatniuk kellett. Korábban a weben nem, vagy csak elhanyagolható mértékben termékeket, szolgáltatásokat kínáló cégek tevékenysége jelentős mértékben tevődött át az internetre. Ez azonban kockázati profiljukat is jelentősen befolyásolta, megváltoztatta, hiszen korábban nem ismert vagy kismértékű kockázatok értékelődtek fel számukra, a korábban használt kockázatelemzéseiket sok esetben alapjaiban kellett újragondolniuk.

• A támadási technikák nagyrészt ismertek voltak, de a *támadások kifinomultsága és a használt eszközök aránya változott.*

A pandemiás időszak alatt a kibertámadásokban használt támadó eszközök, technikák jelentős része már korábban is ismert volt. Ezen eszközök felhasználása volt az, ami a szakemberek számára újdonság volt. A támadásokat jobban előkészítették, azok kifinomultabbak lettek, a támadók igyekeztek azokat mindig hozzáigazítani a célpont aktuális eszközeihez, működési módjához stb.

3.2. Összekapcsolt hálózatok, felhőalapú szoftverek, növekvő adatmennyiség

A távközlési trendekről is számos tanulmány született, ezek közül a téma, azaz a rendfenntartó szervek szemszögéből vizsgálódva az egyik legrelevánsabb összegzés talán a *Nemzetbiztonság általános elmélete*[12] című könyv *„Új technológiák hatása*

[12] Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, NKE Nemzetbiztonsági Intézet, 2014.

a hírszerzésre" című fejezetében található. Ebben a leírásban, mint meghatározó távközlési megatrend, többek között megtalálható:

- a globalitás trendje;
- a mobilitás trendje;
- a konvergencia trendje;
- a szélessávú infrastruktúra előretörése;
- az elektronikus úton folytatott kommunikáció változása;
- a kommunikációs szokások változása;
- a technológiák konvergenciája;
- a növekvő adatmennyiség.

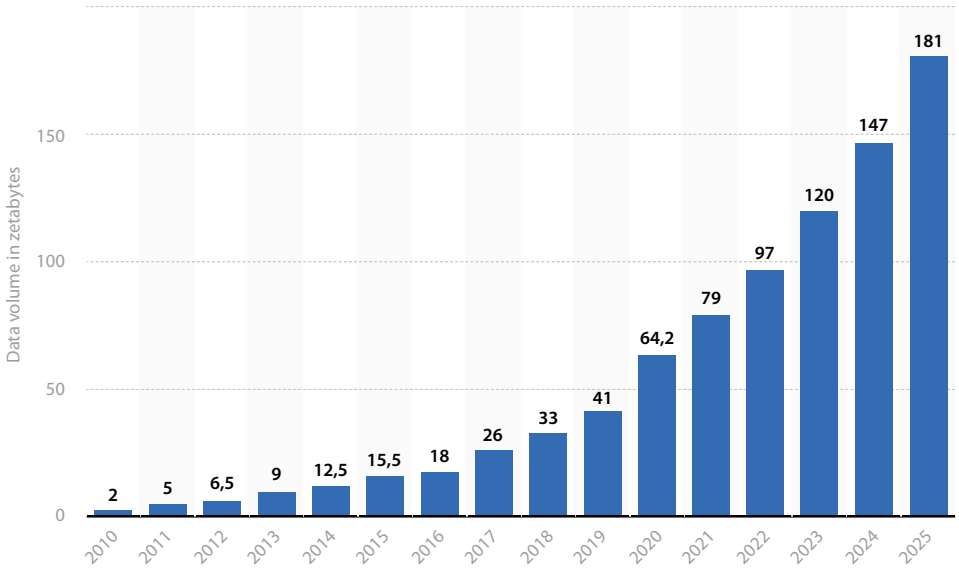
A fent említett felsorolásból talán az alábbi három dolgot érdemes kiemelni, amelyek a legnagyobb hatással lehetnek a rendfenntartó szervek munkájára.

A *hálózatok összekapcsolása* azt jelenti, hogy egyre több hálózat kapcsolódik egymáshoz, jellemzően az interneten keresztül, így azok kívülről, ártó szándékú emberek, csoportok számára is elérhetők, vagy legalábbis támadásra is alkalmas felületet nyújtanak. Ma már egy több telephellyel rendelkező vállalat, de akár állami intézmény is, minden telephelyén biztosítani akarja ugyanazokat az infokommunikációs lehetőségeket munkatársai számára a hatékony munkavégzéshez, amelyek a központi épületében megtalálhatók. Épp ezért az egyes telephelyeken telepített rendszereket is összeköti, amihez jellemzően az internetet mint legolcsóbb összeköttetési lehetőséget veszik igénybe. Természetesen lehetnek olyan rendszerek, amelyeket dedikált hálózattal kötnek össze, ám ezeknek csupán csekély száma nem rendelkezik publikus kijárattal. Ezeknél a hálózatoknál ugyanis a külsős elektronikus levelezést és a webelérést is biztosítani szokták. Ez viszont azt is jelenti, hogy a támadó bárhol lehet, nem kell hogy azonos országban vagy akár csak azonos földrészen legyen a megtámadottal. Ráadásul a támadók általában fedik a nyomaikat, például proxyszervereken keresztül jutnak el a célpontig. Ez pedig azt is jelenti, hogy az ellenük való védekezés és fellépés is nemzetközi összefogást igényel. Ez pedig csak jól kialakított és bejáratott nemzetközi együttműködéssel és közös fellépéssel lehetséges.

A *felhőalapú rendszerek és szoftverek* ma már megkerülhetetlenek. Az egyének, a kisebb-nagyobb vállalatok, de akár állami szervek is igénybe veszik ezeket. Ennek egyik fő oka a ráfordított pénzügyi erőforrás, hiszen ezek általában összességében kedvezőbb konstrukcióban érhetők el, mintha mindent saját magunknak kellene megvásárolni, telepíteni, üzemeltetni a megfelelő tudású szakemberekkel stb. A másik fő oka, hogy a fejlesztők is jellemzően ilyeneket fejlesztenek. Egyre több olyan szoftver van, amelynek van valamilyen felhős lába (gondoljunk itt például a szinte mindenki által használt Microsoft termékekre, mint az Office365, Teams, OneDrive stb., valamint ezek integráltságára), de vannak olyan szoftverek is, amelyek kizárólag felhőalapon érhetők el havi előfizetési díj ellenében. A felhőalapú rendszerek és szoftverek esetében azonban számos biztonsági kérdés is felmerül. Ilyenek például, hogy a szolgáltatónál ki és milyen feltételekkel fér hozzá az adatainkhoz, információinkhoz? A szolgáltató beszállítói, azaz harmadik felek hozzáférhetnek-e – és ha igen, akkor mikor és milyen feltételekkel – ezekhez? Mi történik, ha a szolgáltató rendszerét feltörik,

és adatainkat, információinkat innen szerzik meg? Vagy mi történik, ha a szolgáltató valamiért (például csőd miatt) lekapcsolja, vagy más ok (például fizetési vita) miatt elérhetetlenné teszi számunkra saját adatainkat, információinkat? Bár Magyarországon nagyon előremutató módon működik a kormányzati felhő, ettől még a rendfenntartó szervek találkozhatnak ezekkel a kérdésekkel, például egy magáncéggel kapcsolatos nyomozás során.

A *növekvő adatmennyiség* ma természetes velejárója az információs társadalomnak, amelyben élünk. Egyre több adatot termelünk, amelyet azután felhasználunk és újrahasznosítunk, így állítva elő újabb információkat. Ez az információs társadalom természetes működése. A világon előállított adatok mennyiségét és annak várható növekedését mutatja a Statista 2021-ben készített alábbi, 6. ábrája.



6. ábra: A világszerte létrehozott, rögzített, másolt és felhasznált adatok/információk mennyisége 2010 és 2025 között (zettabyte-ban)
Forrás: www.statista.com/statistics/871513/worldwide-data-created/

Ez pedig több oldalról is kihívások elé állítja a rendfenntartó szerveket. Egyrészt saját maguk is egyre több adatot állítanak elő, amelyeket fel kell dolgozzanak, tároljanak, továbbítsanak stb. Másrészt ezeket az adatokat meg kell védeniük az illetéktelenek általi hozzáféréstől, megszerzéstől, módosítástól vagy törléstől. Harmadrészt törvényes ellenőrzést végzőként ki kell ezekből válogatni a számukra relevánsakat és azokat fel kell tudni dolgozniuk, használniuk a munkájuk során.

Ráadásul a növekvő adatmennyiséget úgy állítjuk elő, hogy időről időre új eszközök, rendszerek, alkalmazások jelennek meg, amelyeket felhasználunk ehhez. Ez pedig mind a felhasználás, mind pedig a törvényes ellenőrzés oldaláról újabb és újabb kihívások elé állítja a rendfenntartó szerveket.

3.3. Szerepkörök, amelyekre gondolni kell

A fentiek alapján jól látszik, hogy a rendfenntartó szerveknek több szerepkörrel is számolniuk kell, amikor a 21. század kiberbiztonsági kihívásaival szembesülnek és kívánják azokat megoldani. Ezek a szerepkörök pedig az alábbiak:

• *Felhasználó*

Ez azt jelenti, hogy azokat az új lehetőségeket, amelyeket az egyre fejlődő technika kínál, a rendfenntartó szervek maguk is ki akarják használni. Hiszen ezek segítségével ők is gyorsabban, hatékonyabban, jobban képesek ellátni feladataikat. Ez csak úgy lehetséges, ha saját eszközeiket, rendszereiket és nem utolsósorban belső folyamataikat, eljárásrendjüket is időről időre megújítják. Ez pedig megfelelő szakértelmet, a szükséges beruházási és fenntartási költségek biztosítását, a működtető állomány ki- és továbbképzését is jelenti.

• *Saját rendszerek védelmét ellátó*

Ha a rendfenntartó szervek már rendelkeznek a fent is leírt hatékony eszközrendszerrel, akkor ezeket és az ezekben tárolt adatokat is meg kell védeniük. Ez azonban a hagyományos módszerekkel sok esetben nem vagy csak részben végezhető el. Egyrészt újabb és újabb támadási formákkal kell szembe nézni, amelyeknek sok esetben már a felismerése sem egyszerű. Másrészt a korábban említett felhőalapú rendszerek esetében a védekezés nem megoldható a hagyományos elvek mentén. Még abban az esetben is, ha állami szervezet szolgáltatja a felhőalapú rendszert (mint például hazánkban a NISZ Zrt.), akkor is a rendszer védelmét meg kell osztani, és ebben meg kell állapodni a szolgáltatóval. Mindezek mellett olyan kérdések is felmerülnek, amelyek a korábbi modellben, amikor minden eszköz és adat az adott szervezetnél volt, nem is léptek fel. Ilyenek például a harmadik felek (például karbantartást végző külső szolgáltatók) hozzáférése az adatokhoz, vagy a szolgáltató csődje esetén az adataink elérése.

• *Törvényes ellenőrzést végző*

Az új, internetes technológián alapuló, elsősorban felhőalapú rendszerek, alkalmazások megjelenése nemcsak a használat, de az ellenőrzés szempontjából is kihívások elé állítja a rendfenntartó szerveket. Ahogy azt a fenti, növekvő adatmennyiség kérdéskörnél már vázoltuk, ki kell tudni választani a releváns rendszereket, és meg kell oldani azok ellenőrzését. Ez több dolog miatt sem egyszerű. Egyrészt azért, mert az, hogy melyik országban melyik rendszer ellenőrzését érdemes, szükséges megoldani, eltérő lehet, hiszen eltérők a felhasználási szokások is. Míg például az Egyesült Államokban a Twitter rendkívül népszerű platform, addig Magyarországon alig akad

használója. Másrészt ezeket a rendszereket le kell tudni hallgatni. Ám amíg például a telefónia esetében jól bejáratott, szabványos ajánlások vannak ennek kialakítására, addig az internettechnológián alapuló hírközlést (is) biztosító rendszerek felépítése nagymértékben eltérhet egymástól, és nincsenek kész, polcról levehető megoldások. Ráadásul, ha még ki is alakít egy szervezet egy ilyen monitoringrendszert, lehet, hogy az akár rövid időn belül elavul az alkalmazott technológia változása vagy a felhasználók más platformra való áttérése okán. Harmadrészt a szolgáltatóval való együttműködés elengedhetetlen, ám ennek kikényszerítéséhez nincsenek meg a megfelelő, nemzetközi szintű szabályzók.

• *Állami rendszereket, védett vezetőket védő*

A fentebbi pontban már volt szó arról, hogy a rendfenntartó szerveknek saját rendszereik védelmét biztosítaniuk kell. Azonban feladatkörükből adódóan több-kevesebb feladatuk lehet védett intézmények vagy vezetők eszközeinek, rendszereinek védelme kapcsán is. Adott esetben egy megtörtént kiberbiztonsági incidens kivizsgálásában is részt kell venniük. Ez pedig speciális felkészültségű szakembereket és speciális eszközöket is igényelhet. E mellett a biztonságtudatos használat az egyik leghatékonyabb és nem utolsósorban legolcsóbb módja a kibervédelemnek. Így célszerű a védett intézmények és vezetők részére biztonságtudatossági képzéseket kialakítani és rendszeresen tartani.[13]

3.4. Mesterséges intelligencia (MI vagy AI)[14] és gépi tanulás a kiberbiztonságban

Ma már a mesterséges intelligencia és a gépi tanulás azok közé a *buzzwordök* közé tartoznak, amelyeket lépten-nyomon hallhatunk. Ugyanakkor számos tudományos cikk, a témával foglalkozó fórum és blogbejegyzés foglalkozik a témával. Ma már elmondhatjuk, hogy a mesterséges intelligencia és a gépi tanulás is a mindennapok részévé vált a kiberbiztonságban, és sajnos nemcsak a védő, de a támadó oldalon is.

A védő oldalon megjelenő, mesterséges intelligenciával és gépi tanulással felvértezett eszközökről a gyártók is előszeretettel kommunikálnak, ám ezek hasznosságát, felhasználhatóságát a kibervédelemmel foglalkozó szakemberek is fel- és elismerik. Egy 2018-ban megjelent interjú szerint egy közepes méretű vállalat naponta körülbelül 200 ezer biztonsági eseménnyel találkozik.[15] Ezek feldolgozása pedig csupán emberi erőforrással nem lehetséges. Egy 2021-ben megjelent tanulmány[16] szerint a mesterséges intelligencia használatának a kiberbiztonságban az alábbi fő előnyei vannak:

---

13 Kovács Zoltán: *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai.* Budapest, Ludovika Egyetemi Kiadó, 2021.

14 AI: *artificial intelligence* vagy MI: mesterséges intelligencia.

15 Dan Patterson: How AI, IoT, and Big Data Will Shape the Future of Cybersecurity. *TechRepublic,* 2018. augusztus 13.

16 Daniel Martin: 8 Benefits of Using AI for Cybersecurity. *Cyber Management Alliance,* 2021. május 4.

A mesterséges intelligencia:

- idővel egyre többet tanul, így jól fogja ismerni az üzleti folyamatokat, a hálózati forgalmat, az ott zajló folyamatok normál viselkedését;
- azonosítja az ismeretlen fenyegetéseket, amelyeket az ember sok esetben nem ismer fel;
- sok adatot képes kezelni, így az egyre növekvő mennyiségű logot, riasztást, eseményt stb. is;
- jobb sérülékenységmenedzsmentet biztosít, mert gyorsabb értékelést és felmérést biztosít;
- jobb általános biztonságot nyújt, mert rengeteg támadási formát képes felismerni és priorizálni azokat;
- csökkenti az ismétlődő folyamatokat, így fizikai és lelki terhelést is levesz a kiberbiztonsági szakemberekről;
- felgyorsítja az észlelési és válaszidőt, ezáltal jelentősen növeli a hálózat biztonságát;
- biztonságosabb hitelesítést biztosít, mert számos eszközt tud használni ehhez (például biometrikus azonosítások, CAPTCHA,[17] *brute force*[18] felismerés stb.)

A mesterséges intelligencia védő oldali használatával kapcsolatban a FireEye kiberbiztonsági cég 2018-as „FireEye Cyber Defense Summit 2018" című konferenciáján volt egy kerekasztal-beszélgetés. Ezen David Gunning, a DARPA[19] mesterségesintelligencia-kutató programmenedzsere azt jósolta, hogy a kibervédelemben az úgynevezett Tier1 szintű operátorokat 5 éven belül kiváltja a mesterséges intelligencia. A Tier1 szintű operátorok azok a szakemberek, akik a riasztások, kiberbiztonsági események közvetlen és gyors feldolgozását végzik, vagy gyorsan lezárva az adott vizsgálatot (vagy mert ismert, vagy mert téves, azaz *fals positive* riasztás volt), vagy ha az további vizsgálatot igényel, akkor továbbítják azokat az úgynevezett Tier2 elemzőknek. Bár az Egyesült Államokban a Tier1 operátorok feladatköre meglehetősen egyszerű és jórészt betanított feladatokból áll, azért ez a jóslás így is jól szemlélteti a mesterséges intelligencia fejlődését és előretörését napjainkban.

A mesterséges intelligencia természetesen a támadó oldalon is megjelenik. A támadók a mesterséges intelligenciát – valamint annak részhalmazát, a gépi tanulást – is használják hatékonyabb, automatizáltabb, agresszívebb és összehangoltabb támadások indítására. Ezek segítségével ugyanis jobban fel tudják térképezni és meg tudják érteni, hogy a célpontszervezetek hogyan védik a rendszereiket. Erre példák az ügyfélszolgálatokon is használt nyelvi feldolgozó eszközök, amelyek a támadók kezében kifinomultabb adathalász levelek előállítását teszi lehetővé.[20]

---

17 CAPTCHA: *Completely Automated Public Turing test to tell Computers and Humans Apart,* azaz teljesen automatizált nyilvános Turing-teszt a számítógép és az ember megkülönböztetésére. Ez egy olyan teszt, amely képes megkülönböztetni az emberi felhasználót a robottól (számítógéptől).

18 *Brute force,* magyarul nyers erő. Ez egy titkosításokkal, jelszóvédelemmel szemben alkalmazott támadási módszer, amely során minden lehetséges variációt kipróbál a jelszóra a támadó.

19 DARPA *(Defense Advanced Research Projects Agency),* az Egyesült Államok Védelmi Minisztériumának kutatásokért felelős részlege.

20 Mercedes Cardona: When Bad Guys Use AI and ML in Cyberattacks, What Do You Do? *Security Roundtable,* (é. n.).

A támadók a támadás különböző szakaszaiban használják, használhatják a mesterséges intelligenciát. Így például az „önállóan működő kártékony kód elkészítéséhez és bejuttatásához, a hálózaton belüli terjedéshez, a védelmi technológiák intelligens megkerüléséhez, a kis méretű és alacsony sebességű adatlopáshoz vagy a felhasználó »élethű« szimulálásához stb."[21] A DarkWeb piacterein számos mesterséges intelligenciát és gépi tanulást használó hackereszközt kínálnak, és a kibertámadásokra egy ökoszisztéma épült fel, amelyben a támadást mint szolgáltatást[22] is igénybe lehet venni.[23] A gyakorlati tapasztalatok is azt mutatják, hogy bizony, a támadó felek használják már ezeket a technológiákat.

A fentiek alapján napjainkban a mesterséges intelligencia használata a támadó és a védő oldalon is a gépek-gépek, sőt az intelligencia-intelligencia elleni küzdelemről szól. A 2019-ben megrendezett RSA konferencián, amely a világ legnagyobb kiberbiztonsági eseménye, az egyik előadásban élőben bemutatták a gyakorlatban is, milyen az, amikor mesterséges intelligenciával támadunk és mesterséges intelligenciával védekezünk. Bár a bemutató olyan volt, mint az 1990-es években, amikor a sakkszoftvereket/robotokat játszatták egymással, azért néhány dologra így is ráirányította a figyelmet. Az első, hogy ma már mindkét oldalon demonstrálható módon működik a technológia. A második, hogy mindkét oldalon hatékonyan fel is lehet használni ezt. A harmadik pedig az, hogy a bemutatottnál fejlettebb, egy vagy néhány, de adott feladat(ok)ra fókuszáló technológiával már rendelkezik mindkét oldal.

4. Összegzés, következtetések

A workshopon elhangzott előadáson és ebben a cikkben a fent leírtak alapján megállapítható, hogy a kiberbiztonság a rendfenntartó szervek számára a 21. század egyik legnagyobb kihívása. Egy folyamatosan változó, fejlődő kiberkörnyezetben kell több szerepkörben (felhasználó, saját rendszereit védő, törvényes ellenőrzést végző, védett intézmények, személyek eszközeit, rendszereit védő) feladatot ellátniuk, helyt állniuk. Mindezt olyan tényezők is jelentősen befolyásolják, mint a Covid–19, a mesterséges intelligencia fejlődése, no meg persze az állandóan fejlődő infokommunikációs eszközök, rendszerek.

Kiberbiztonság kérdéskörében rengeteg kérdés van, talán mindig több, mint amennyi válasz. Ahhoz, hogy ezekre a kihívásokra megfelelő és kellően gyors válaszokat adhassanak a rendfenntartó erők, tudatos tervezésre, fejlesztésre és az állomány folyamatos képzésére van szükség. Mindezt úgy szükséges megtenniük, hogy a fent leírt szerepkörök mindegyikét egyaránt és megfelelő súllyal figyelembe kell venniük.

---

21 *The Next Paradigm Shift AI-Driven Cyber-Attacks.* Research White Paper. San Fransisco – Cambridge, DarkTrace, 2018.

22 *Cyber-Attack-as-a-service* (CAaaS).

23 Keman Huang et al.: *Casting the Dark Web in a New Light: A Value-Chain Lens Reveals a Growing Cyber Attack Ecosystem and New Strategies for Combating It.* Massachusetts Institute of Technology, 2019.

Felhasznált irodalom

Ahmad, Tabrez: *Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity.* 2020. Online: https://doi.org/10.2139/ssrn.3568830

Impact of COVID-19 on Cybersecurity. *Deloitte,* (é. n.). Online: www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

Cardona, Mercedes: When Bad Guys Use AI and ML in Cyberattacks, What Do You Do? *Security Roundtable,* (é. n.). Online: www.securityroundtable.org/when-bad-guys-use-ai-and-ml-in-cyberattacks-what-do-you-do

Clark, Mitchell: Hacker Claims Responsibility for T-Mobile Attack, Bashes the Carrier's Security. *The Verge,* 2021. augusztus 26. Online: www.theverge.com/2021/8/26/22643277/t-mobile-hacker-data-leak-claims-responsibility-criticizes-security

Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, NKE Nemzetbiztonsági Intézet, 2014.

ENISA: *COVID19: Stronger Together in Fighting Cyber Threats* (2020). Online: www.enisa.europa.eu/topics/wfh-covid19/media/covid19-stronger-together-in-fighting-cyber-threats

FireEye – Mandiant: *M-Trends 2021.* Special Report (2021). Online: www.arrow.com/ecs-media/16352/fireeye-rpt-mtrends-2021.pdf

Global Threat Landscape Report. A Semiannual Report by FortiGuard Labs. *Fortinet,* 2021. augusztus. Online: www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-landscape-2021.pdf

Grustniy, Leonid: The Great Lockdown: How COVID-19 has Affected Cybersecurity. *Kaspersky,* 2021. március 24. Online: www.kaspersky.com/blog/pandemic-year-in-infosec/39123/

Huang, Keman – Michael Siegel – Keri Pearlson – Stuart Madnick: *Casting the Dark Web in a New Light: A Value-Chain Lens Reveals a Growing Cyber Attack Ecosystem and New Strategies for Combating It.* Massachusetts Institute of Technology, 2019. Online: https://doi.org/10.2139/ssrn.3459128

Kovács Zoltán: *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai.* Budapest, Ludovika Egyetemi Kiadó, 2021.

Lakshmanan, Ravie: Cloudflare Mitigated One of the Largest DDoS Attack Involving 17.2 Million rps. *The Hacker News,* 2021. augusztus 20. https://thehackernews.com/2021/08/cloudflare-mitigated-one-of-largest.html

Martin, Daniel: 8 Benefits of Using AI for Cybersecurity. *Cyber Management Alliance,* 2021. május 4. Online: www.cm-alliance.com/cybersecurity-blog/8-benefits-of-using-ai-for-cybersecurity

The Next Paradigm Shift AI-Driven Cyber-Attacks. Research White Paper. San Fransisco – Cambridge, DarkTrace, 2018. Online: www.oixio.ee/sites/default/files/the_next_paradigm_shift_-_ai_driven_cyber_attacks.pdf

Patterson, Dan: How AI, IoT, and Big Data Will Shape the Future of Cybersecurity. *TechRepublic,* 2018. augusztus 13. Online: www.techrepublic.com/article/how-ai-iot-and-big-data-will-shape-the-future-of-cybersecurity

Pranggono, Bernardi – Abdullahi Arabo: COVID-19 Pandemic Cybersecurity Issues. *Internet Technology Letters,* 4. (2021), 2. 1–6. Online: https://doi.org/10.1002/itl2.247

Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025(in zettabytes). *Statista.com.* Online: www.statista.com/statistics/871513/worldwide-data-created/