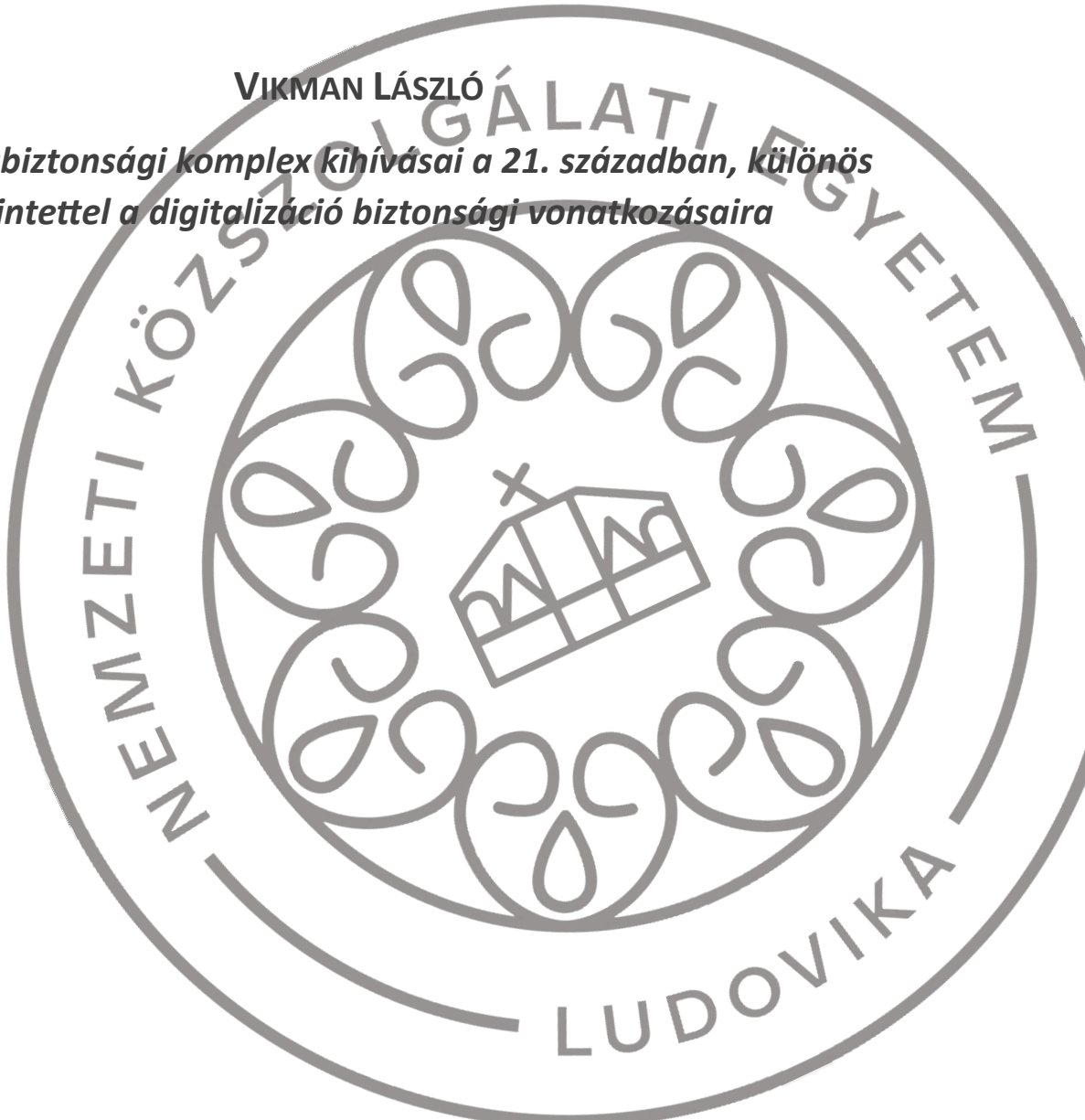
**NEMZETI KÖZSZOLGÁLATI EGYETEM**
**VÉDELMI-BIZTONSÁGI SZABÁLYOZÁSI ÉS KORMÁNYZÁSTANI KUTATÓMŰHELY**

# VÉDELMI-BIZTONSÁGI SZABÁLYOZÁSI ÉS KORMÁNYZÁSTANI MŰHELYTANULMÁNYOK

2023/13.

**VIKMAN LÁSZLÓ**

***Az ellátásbiztonsági komplex kihívásai a 21. században, különös tekintettel a digitalizáció biztonsági vonatkozásaira***



## Rólunk

A műhelytanulmány (working paper) műfaja lehetőséget biztosít arra, hogy a még vállaltan nem teljesen kész munkák szélesebb körben elérhetővé váljanak. Ezzel egyrészt gyorsabban juthatnak el a kutatási részeredmények a szakértői közönséghez, másrészt a közzététel a végleges tanulmány ismertségét is növelheti, végül a megjelenés egyfajta védettséget is jelent, és bizonyítékot, hogy a később publikálandó szövegben szereplő gondolatokat a working paper közzétételekor a szerző már megfogalmazta.

A Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok célja, hogy a Nemzeti Közszolgálati Egyetem Védelmi-biztonsági Szabályozási és Kormányzástani Kutatóműhely küldetéséhez kapcsolódó területek kutatási eredményeit a formális publikációt megelőzően biztosítsa, segítve a láthatóságot, a friss kutatási eredmények gyors közzétételét, megosztását és a tudományos vitát.

A beküldéssel a szerzők vállalják, hogy a mű megírásakor az akadémiai őszinteség szabályai és a tudományosság általánosan elfogadott mércéje szerint jártak el. A sorozatban való megjelenésnek nem feltétele a szakmai lektorálás.

A műfaji jellegből adódóan a leadott szövegekre vonatkozó terjedelmi korlát és egységes megjelenési forma nincs, a szerzőtől várjuk az absztraktot és a megjelentetni kívánt művet oldalszámozással, egységes hivatkozásokkal.

A szerző a beküldéssel hozzájárul, hogy a művét korlátlan ideig a sorozatban elérhetővé tegyük, továbbá vállalja, hogy a working paper alapján megírt végleges szöveg megjelenési helyéről a szerkesztőséget legkésőbb a megjelenéssel egy időben értesíti.

A kiadvány ötletét az MTA Jogtudományi Intézet Law Working Papers sorozatának sikeréből merítettük.

# *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2023/13*

***Szerző:***
*Dr. Vikman László*

***Kiadja***
*Nemzeti Közszolgálati Egyetem*
*Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely*

***Kiadó képviselője***
*Dr. Kádár Pál PhD dandártábornok*

***ISSN szám***
*2786-2283*

*A kézirat lezárva: 2023. szeptember 25.*

***Elérhetőség:***
*Nemzeti Közszolgálati Egyetem*
*Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely*
*1441 Budapest, Pf.: 60*
*Cím: 1083 Bp., Ludovika tér 2.*
*Központi szám: 36 (1) 432-9000*

Vikman László

# Az ellátásbiztonsági komplex kihívásai a 21. században, különös tekintettel a digitalizáció biztonsági vonatkozásaira[1]

## 1. Bevezetés

Az információbiztonság, a kiberbiztonság és a hálózatbiztonság témái[2] a digitiális információs kor kiemelt prioritásai közé tartoznak, és talán a leginkább reflektorfényben lévő és a tömegmédia is tematizált vonatkozásai az IKT-technológiák, az internet és a globális gazdaság által determinált társadalmi, gazdasági, kulturális és szociális viszonyainknak. Korszakunkban ez a fokozott behálózottság és interdependencia az állami és nem állami szereplők, ellenérdekelt felek között versengésekben, konfliktusokban is egy sajátos kompetíciós arénát hozott magával, amelyet összefoglalóan a hibrid fenyegetések kategóriájával jellemzünk, mely kiterjedt és tabudöntögető eszköztárával, sokszínű szereplőivel, totális szemléletével az államok védelmi-biztonság szervezeteit korábban nem látott spektrumú kihívások elé állítja[3].

Az egymás követő technikai újítások, innovációk és újszerű megközelítések az értékteremtésük mellett szinte kivétel nélkül magunkban hordoznak a felhasznált hardverből, szoftverből, üzemeltetésből, a felhasználási célból vagy formából esetleg egyszerűen csak a felhasználókból fakadóan több olyan sérülékenységet, biztonsági kockázatot, amelynek kezelésére a fejlesztő több okból sem ad eleve megoldást. Ennek konkrét oka széles spektrumon lehet megtalálható, egészen onnan, hogy ez valamilyen objektív okból nem képzelhető el, de származhat az alkalmazó hanyagságából, bármely fél költségtakarékossági törekvéseiből és végül, a legrosszabb esetben akár előre eltervezett módon, leplezett szándékkal is. Nincs olyan élenjáró, diszruptív, új csúcstechnológia a digitalizáció előretörése során, aminek esetében nem merült volna fel valamely komoly kockázat. Gondolhatunk akár a minden elektronikus eszközt szenzorokkal és hálózati kapcsolati képességekkel felszerelő „dolgok internetére”[4], a társadalmi információs teret, a médiát, és szociális viszonyainkat átformáló és a hagyományos

[1] A mű TKP201-NVA-16 számú projekt keretében, a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a Tématerületi Kiválósági Program 2021 pályázati program finanszírozásában valósult meg

[2] Lásd pl.: Török Bernát (szerk.): Információ- és kiberbiztonság: Fenntartható biztonság és társadalmi környezet tanulmányok V, Budapest, Ludovika Egyetemi Kiadó, 2020, https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf;jsessionid=BF61800E8CD9ADAB6552D15901E5C6F1?sequence=1 ; Krasznay Csaba: Kiberbiztonság a XXI. században, Budapest, Katonai Nemzetbiztonsági Szolgálat, 2022

[3] Lásd: Farkas Ádám: Babelic Confusion? Systemic issues in the adaptation to defence and security challenges in the transatlantic states, with special regard to the Eurasia-idea as a special aspect of hybridity. Budapest, Iustum Aequum Salutare, XIX. 2023. 1., 17–31. o. https://ias.jak.ppke.hu/20231sz/02_FarkasA_normal_IAS_2023_1.pdf ; Farkas Ádám: The Status and Role of Law and Regulation in the 21st-Century Hybrid Security Environment, Cluj, Acta Univ. Sapientiae, Legal Studies, 11, 2 (2022) 113–124. o., https://acta.sapientia.ro/content/docs/112_07.pdf ; Krasznay Csaba (szerk.): Taktikák és stratégiák a kiberhadviselésben, Budapest, Ludovika Egyetemi Kiadó, 2023

[4] Lásd: Tóth András: Az IoT-eszközök védelmi célú alkalmazásának információbiztonsági kihívásai, In: M., Szabó Miklós (szerk.) A hadtudomány aktuális kérdései napjainkban : I. kötet, Budapest, Ludovika Egyetemi Kiadó, 2022, 77-93. o.



Nemzeti Kutatási Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

médiát visszaszorító közösségi médiára[5], vagy a jelenleg leginkább dominálo, számos jogi, etikai kérdést felvető mesterséges intelligenciára[6].

Az ellátásbiztonság talán az a biztonsági kategória, ami a legszorosabb összekapcsolódást mutatja a hagyományos(an elkülönülő) biztonsági gondolkodás és a "civil" élet kulcsterületei között. Ez a szoros és kölcsönösen függőségi jellegű kapcsolat pedig megkerülhetetlenné teszi, hogy a célzott - konkrét problémakörökre fókuszáló és operatív jellegű - szemléletmód mögött mindig ott tartsuk a háttérben azt az elvi-gondolkodásmódbeli újdonságot, hogy a különféle életviszonyok megfelelő értelmezésében ma már megkerülhetetlen a biztonsági szemléletmód mögöttes érvényesítése, de fordítva is igaz, hogy hatékony biztonságot nem lehet építeni, ha nem tekintünk ki a kulcsterületek tágabb vonatkozásaira és kérdéseire. Az ellátásbiztonságot történelmi szempontból értékelve is megkülönböztethetjük, hiszen mint kategória és szempontrendszer nem kötődött a korábbi évszázadokban a digitalizáció eredményeihez, megelőzte azokat, mivel teljesen analóg, sőt akár ipari forradalom előtti korszakokban is abszolút értelmezhető, értékelhető, mérhető minősége volt a társadalom számára kritikus alapszolgáltatásoknak, erőforrások rendelkezésre állásának. Az IKT-eszközök fejlődése és ezek széles körű elterjedése ezekben az alapszolgáltatásokban viszont magával hozta azok biztonsági környezetét, és annak kockázatait is. A koronavírus-járvány sokkja[7] és az arra megindult rohamtempójó válaszkeresés olyan helyzetet idézett elő, ami a békeidőben (ha ez még értelmezhető kifejezés egyáltalán) egyébként nem különösebben romantikus olyan alapszolgáltatásokat mint áram-, és vízellátás, köztisztaság, élelmiszerbiztonság, alapvető egészségügyi felszerelések és eszközök központi témává tették, és súlyosan zord emlékeztetőt adott arra vonatkozóan, hogy miért *létfontosságú* a rendszerelem, miért *kritikus* az infrastruktúra. Az ellátásbiztonságot így nem minden alap nélkül egyfajta prerekvizítumként is kezelhetjük a többi biztonság-kategória vonatkozásában[8].

Az elmúlt néhány évben számos olyan nagy hatású támadás ért kritikus infrastruktúrákat – és nem csak az orosz-ukrán háborús zónában – amelyek súlyos hatásokat, jelentős zavarokat okoztak az államok, társadalmak, gazdaságok működésében. A társadalmat tömegesen kiszolgáló hálózatos alapon működő (közmű)szolgáltatások ellátásbiztonságának megteremtésében a szolgáltatást nyújtó és azokat közvetlenül támogató rendszereken túl kell

[5] Lásd: Tóth András: A figyelem alapú piacok káros hatásainak szabályozási csökkentése, In: Homicskó, Árpád Olivér (szerk.) A technológia fejlődés társadalmi kihívásai és hatása a jogi szabályozásra, Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2022, 183-207. o. , Klein Tamás: Az újmédia szabályozásának új iránya? – A Digital Services Act alapjogvédelmi mechanizmusa, In: Török, Bernát; Ződi, Zsolt Digitalizálódó társadalom : Tanulmányok az új technológiák társadalmi-jogi hatásairól, Budapest, Ludovika Egyetemi Kiadó, 2023, 117-140. o.

[6] Török Bernát, Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai: Tanulmányok a mesterséges intelligencia és a jog határterületeiről, Budapest, Ludovika Egyetemi Kiadó, 2021

[7] Lásd: Bonnyai Tünde, Kiss Adrienn, Margitics József: Társadalom és gazdaság járvány idején: Létfontosságú információs rendszerek biztonsága - kihívások különleges jogrend idején, In: Koltay, András, Török Bernát (szerk.) Járvány sújtotta társadalom: A koronavírus a társadalomtudományok szemüvegén keresztül, Budapest, Ludovika Egyetemi Kiadó, 2021, 179-202. o., Greiner István: Gyorsreagálás a pandémiára, ellátásbiztonság, Budapest, Scientia et Securitas, 2. évfolyam, 2. szám 172-176. o., 2021, https://akjournals.com/view/journals/112/2/2/article-p172.xml

[8] Ennek alátámasztására lásd pl.: Molnár Ferenc: Ellátásbiztonság a biztonságért, Budapest, Biztonságtudományi Szemle II. évf. 1. szám, 89-106. o., 2020, https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/v iew/80/67

tekinteni, amikor egy magas szintű védelem és ellenállóképesség elérése a cél. A különböző szempontú és forrású fenyegetéselemzések és tapasztalat-feldolgozások alapján a beszállítói rendszerek ugyanúgy jelentős kulcstényezők, és kiberbiztonsági szempontból folyamatos mitigációt igénylő elemei az adott szervezet működésének, mint a közvetlen befolyás alatt álló belső folyamatok és rendszerek. Nem csoda, hogy ez a tényező – az egyre szofisztikáltabb támadási módozatok[9] mellett – egyre hangsúlyosabb figyelmet kap nem csak a stratégiai elemzésekben, de a konkrét szabályozókban is.

Korábbi írásomat[10] amelyben a közműszolgáltatók rezilienciájával, a reziliencia nemzeti, EU és NATO stratégiai hátterével foglalkoztam, a téma még átfogóbb körüljárására ezúttal az ellátásbiztonságot aktuális fenyegető fő tényezőkkel, és az ezekre a tényezőkre megadott válaszként elfogadott – részben megvalósítás és végrehajtás alatt álló – új uniós szabályozási csomag releváns elemeinek megvilágításával egészíteném ki.

## 2. Fenyegetések

A cégek, állami intézmények kiberstratégiáinak állandó, „kötelező" tartalmi eleme a fenyegetések értékelése, így ezekkel – komolyan vett védelmi tevékenység esetén – érdemes jogi szempontból is foglalkozni. A jelentős kockázatok figyelembevétele, a kockázatkezelési-mátrixokba való felvétele, esetleges ellenlépések, mitigációs intézkedések előzetes tervezése elengedhetetlen a védelmi architektúrát alapjaiban meghatározó rendszer kialakításának, a hatékony védelemhez szükséges képességeknek, valamint az ehhez szükséges humán- és technológiai fejlesztéseknek a meghatározásában. Komplex megközelítésben azonban a kibervédelem[11] nem csupán a korszerű technológia és a kompetens mérnök-csapat összessége. Ha mindennek hátteréből hiányzik a hatékony szervezeti felépítés a fenyegetésekhez igazítottan gyors döntési mechanizmusokkal, a megfelelő szabályozási háttérrel és annak magabiztos értelmezési gyakorlatával, továbbá az operatív működés megfelelő jogi támogatásával[12] az a hatékony védelem kialakítására tett erőfeszítéseket gátolhatja, akár meg is béníthatja.[13]

---

[9] Lásd: Haig Zsolt: A kibertéri műveletek fejlődése: a számítógép-hálózati műveletektől a kibertéri befolyásolásig. In: Krasznay, Csaba (szerk.) Taktikák és stratégiák a kiberhadviselésben. Budapest, Magyarország : Ludovika Egyetemi Kiadó, 2023, 41-60. o.

[10] Lásd: dr. Vikman László: A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra, Budapest, Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/14., https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK_M%C5%B1helytanulm%C3%A1nyok_2021_14_Vikman%20L%C3%A1szl%C3%B3_A%20k%C3%B6zm%C5%B1szolg%C3%A1ltat%C3%A1sok%20%C3%A9s%20a%20reziliencia%20egyes%20k%C3%A9rd%C3%A9sei,%20k%C3%BCl%C3%B6n%C3%B6s%20tekintettel%20a%20kiberbiztons%C3%A1gra.pdf

[11] A kiberbiztonságot mint fogalmat jelen tanulmány keretei között alapvetően egy rendszert jellemző, minőségi mutatóként, a kibervédelmet pedig mint aktív tevékenységet, képességet használom.

[12] Például az adott szervezet üzemmenetéhez, felelősségi- és kockázati szintjéhez igazított beszállítói szerződések, melyek a megkívánt mértékben szabályozzák az egyes termékfelelősségi, személyes adatok védelméhez kapcsolódó, szerzői jogi, és rendelkezésre állási kérdéseket is.

[13] Ennek rendszerszintű állami és jogi kérdéseiről lásd: Vytautas BUTRIMAS: Defending critical infrastructure: The challenge of securing industrial control systems. Helsinki, Hybrid COE Working Paper 18, 2022 https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220602-Hybrid-CoE-Working-Paper-18-Defending-critical-infrastructure-WEB.pdf ; Garrett DERIAN-TOTH, Ryan WALSH, Alexandra SERGUEEVA, Edward KIM, Alivia COON,

Azt, hogy egy adott szervezet – sőt tágabban akár az állam – a kiberbiztonsági stratégiájában milyen fenyegetés-térképpel számol, nem csupán a kibertér realitásai határozzák meg, nyilván az adott szervezet profilja, kitettsége, erőforrásai is. Nem egyszer bebizonyosodott már, hogy egy ragyogóan kidolgozott, minden támadási vektorra kiterjedő szemlélettel és részletes kockázatkezelési mátrixxal felépített stratégia önmagában csak néhány darab papír marad, ha a menedzsment nem áll demonstratívan a kitűzött biztonsági célok mögé a szükséges anyagi- és humán-erőforrásokkal, amennyiben indokolt, akár külső szolgáltatók bevonásával. Azonban képzésre és fejlesztésre nem csak az elsődlegesen kézenfekvő vonalakon van szükség, hanem az IT-terület támogatói oldalán is. A HR, a beszerzés, és a vitathatatlanul fontos „érzékenyítő", tájékoztató tevékenység mellett[14] a jog is egy olyan kritikus támogató terület, amelynek művelőit szintén speciálisan fel kell készíteni a szaktevékenységek releváns elméleti és gyakorlati aspektusaiból.

Azzal a megközelítéssel is érdemes tehát az egyes fenyegetés-elemzéseket, támadásról szóló híradásokat és kommünikéket vizsgálni, hogy a technikai elhárító/helyreállító lépések az eseménykezelés után hogyan kerültek beillesztésre az adott szervezet döntési láncába, az ezzel megbízott szervezeti egységek hogyan illeszkednek a szervezet vezetési-irányítási struktúrájába, mi garantálja a megfelelő humán-adminisztratív-anyagi támogatásukat, és hogy az egyes támadás-típusok, krízisek milyen jogi következményekkel és tapasztalat feldolgozással járnak, esetleg milyen előzetes óvintézkedések tehetők jogi szempontból a felmerült problémák hatékonyabb kezelése érdekében. Látni kell ugyanis, hogy a nem megfelelő reagálásnak nem csak az állami közegben, de a civilszférában is jelentős visszahatásai lehetnek jogi értelemben is (pl. adatvédelmi, vagyoni és nem vagyoni károkozás, goodwill, reputáció és jó hírnév sérelme).

A NATO Kooperatív Kibervédelmi Kiválósági Központja (a továbbiakban: CCDCOE[15]) a katonai szövetség egyik tudományos értelemben is legaktívabb szakosított tudáscentruma. Elemzéseinek, publikált tanulmányainak és magasan értékelt konferenciáinak szakmai üzenetei és megállapításai – az infokommunikációs technológiák össztársadalmi jelentőségének köszönhetően is – széles körben tarthatnak számot a figyelemre és megfontolásra, a hagyományos értelemben vett védelmi-biztonsági szférán[16] túl is. Bár a 2022-es évnek az orosz–ukrán háború a biztonságpolitikai szempontból legjelentősebb és

---

Hilda HADAN, Jared STANCOMBE: *Opportunities for Public and Private Attribution of Cyber Operations.* In: *Tallinn Paper No. 12.*, Tallinn, NATO CCD COE, 2021.; FARKAS Ádám: *A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapvonalai.* In: *Jog Állam Politika* 2019/2. szám, 63-79. o.; FARKAS Ádám: A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.; KELEMEN Roland: *Cyberfare State – Egy hibrid állammodell 21. századi születése*. In: *Military and Intelligence CyberSecurity Research Paper* 2022/1. szám.; Farkas Ádám: Questions and Options for the Emerging Reform of the Hungarian Security and Defence Regulation, MTA Law Working Papers 14., 2022.

[14] Érdekes és abszolút korszerű magyar kezdeményezés a Nemzetbiztonsági Szolgálat széles közönségnek szánt „Kibertámadás!" című podcastja: https://nki.gov.hu/podcast/ , illetve az SZTFH által indított „Minden kiberül!" című podcast.

[15] https://ccdcoe.org/

[16] FARKAS Ádám: Az állam fegyveres védelmének alapvonalai, Budapest, Katonai Nemzetbiztonsági Szolgálat, 2019., FARKAS Ádám: A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon, Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.

valószínűleg hosszú évtizedes hatásokkal és súlyos következményekkel járó eseménye – amelynek szintén fontos elemei a kibertérben mindkét fél által végrehajtott tevékenységek – de ettől a kijózanítóan zord eseménytől elvonatkoztatva is érdemes összefüggéseiben áttekinteni az elmúlt évek fő kiberfenyegetési formáit és a közeli jövőben prognosztizálhatóan erősödő tendenciákat, mivel ezek mérlegelése a saját szervezet szempontjából segíthet kibervédelmi törekvéseinknek a fenyegetési környezethez adekvát kalibrálásában, illetve tágabban a hazai kooperatív kiberbiztonsági kutatások ösztönzésében.[17]

A CCDCOE 2022. januárjában kiadott „Recent Cyber Events" 14. száma[18] a szerzők által 2021-ben leginkább dominánsnak tekinthető három kibertéri fenyegetésről szól. Ezek a zsarolóprogramok, az IT-ellátási láncok kompromittálásával végrehajtott támadások és a kémszoftverek, avagy megfigyelésre alkalmas szoftverek voltak.

A rosszindulatú programok egy külön kategóriája, a zsarolószoftverek nagy figyelmet kaptak a tavalyi évben. Ezek a rosszindulatú kódok nem csupán titkosítják, és olvashatatlanná teszik az áldozat rendszereiben tárolt adatokat, amelyeket csak „váltságdíj" ellenében oldanak fel a támadók, hanem a fenyegetés gyakran kettős, mivel a megszerzett adatok nyilvánosságra hozatalával történő nyomásgyakorlás hatására egy a hírnevére és működési prudenciájára érzékeny szervezet kétszeresen is szinte kilátástalan helyzetbe kerül (pl. egy ügyfélbizalomra építő pénzügyi szolgáltató; szenzitív adatokat kezelő szolgáltató cég; üzleti/szervezeti titkokra is rálátást nyerő auditor; stb.).

Másodlagos hatásai egy nem csupán adatokat tároló, de azokat folyamatosan a működésében használó entitás esetében időnként még komolyabbak lehetnek, mint ahogy azt előzetesen akár a támadók is megbecsülték. Gondolhatunk itt az egészségügyi szolgáltatókat ért támadásokra[19], melyek miközben szenzitív adatok sokaságára épülnek, emberéleteket és ellátásbiztonságot veszélyeztetnek, vagy az elemzésben külön is kiemelt májusi Colonial

[17] Ehhez lásd: KOVÁCS László: Hadviselés a 21. században: kiberműveletek, Budapest, Ludovika Egyetemi Kiadó, 2023.; KOVÁCS László: *A kiberbiztonság és a kiberműveletek megjelenése Magyarország új nemzeti biztonsági stratégiájában*. In: *Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata* 148 : 5 pp. 3-18. , 16 p. (2020); KOVÁCS LÁSZLÓ: *Kiberbiztonság és -stratégia*. Budapest, Dialóg Campus Kiadó, 2018.; KASSAI Károly: Kibertér - Aktuális változások, In: *Szakmai Szemle*, XVII. évfolyam 1. szám 2019. március, 116. o.; BIHARI László, MAGYAR Sándor: Mennyország helyett a pokolba, avagy az informatikai támogatás kihívásai. In: *Szakmai Szemle, A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata* 18:4. 158-169. o. (2020); Annamária BELÁZ, Csaba KRASZNAY, Zsolt SZABÓ: *Cybersecurity strategy and leadership management issues*. September 2020, In: *IMCSM Proceedings - An international serial publication for theory and practice of Management Science* (242-252 o.), University of Belgrade, https://www.researchgate.net/publication/348432259_Cybersecurity_strategy_and_leadership_management_issues; KELEMEN Roland, SZÉPVÖLGYI Enikő: A modern technológia és ami mögötte van - Konferencia a modern technológia biztonsági kockázatairól és állam- és jogtudományi kapcsolódásairól. In: *Katonai Jogi És Hadijogi Szemle* 4 pp. 191-197. o. (2021); KELEMEN Roland: A nem állami kibertéri műveletek egyes szereplőinek jelentősége a hibrid konfliktusokban. In: *SmartLaw Research Group Working Paper* 2 pp. 1-17. o. (2021); FARKAS Ádám: Biztonság – Geopolitika – Digitalizáció, avagy Amael Cattaruzza „A digitális adatok geopolitikája" című kötetének főbb üzenetei. In: *SmartLaw Research Group Working Paper* 1 pp. 1-13. , 13 p. (2021)

[18] Sungbaek CHO ET. AL.: Recent Cyber Events: Considerations for Military and National Security Decision Makers, Tallinn. CCDCOE, Recent Cyber Events No 14 / January 2022 https://ccdcoe.org/library/publications/recent-cyber-events-considerations-for-military-and-national-security-decision-makers-2/

[19] https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf

Pipeline-támadás[20] esetében, amely az USA keleti partján bénította meg a belföldi üzemanyagvezeték-rendszert vezérlő informatikai rendszereket, ezzel ellátási zavarokat és üzemanyagár-emelést is előidézve.

Ezek a támadások nem csak azt mutatták meg, hogy mennyire erősen összekapcsolódtak a társadalom és az információs rendszerek, hanem azt is, hogy mennyire sebezhetővé és függővé váltunk a kritikusnak tekinthető infrastruktúráink működésétől. A zsarolóprogramok jellemzően ilyen szolgáltatásokat céloznak meg, és ezek egymással igen gyakran a kiterjedt hálózatosság miatt még annyira erős kapcsolatban is állnak, hogy valamelyik kiesése képes lehet dominó-hatás kiváltására is. Egyre nyilvánvalóbb, hogy a rezilienciához nem elegendő a robosztus és redundáns digitális rendszerek kiépítése, de bizonyos létfontosságú funkciók vonatkozásában az „analóg" technológiák, a sziget-szerűen is működő helyi megoldások (pl. tartalék-generátorok) kialakítása is indokolt lehet. A kritikus infrastruktúrákat – vagy magyar terminológiával, létfontosságú rendszerelemeket – érintő veszélyek jelentőségét jól mutatja, hogy a kérdést már az USA-ban összkormányzati felelősségként és erőfeszítésként kezelik[21] és a nemzetközi összefogás is elengedhetetlen összetevője a hihető és kézzelfogható elrettentést is jelentő bűnüldöző tevékenységnek. Ezt erősíti az EU e téren tett törekvéseinek sora[22], és a kritikus infrastuktúra NATO rezilienciában betöltött szerepe[23].

Az informatikai rendszerek ellátási láncok biztonságával kapcsolatos aggályokat a még 2020 végén kezdődő, de igazán 2021-ben eszkalálódó Solarwinds-incidens[24] tette mindenki számára nyilvánvalóvá. A rosszindulatú kódrészletek eltávolítása az első, az amerikai kormányzati kiber- és kritikus infrastruktúrák védelméért felelős Cybersecurity and Infrastructure Agency[25] által kiadott útmutató publikálása után még hat hónappal sem fejeződött be teljesen minden érintett rendszerből. Az USA-ban szabványügyi kérdésekkel foglalkozó NIST[26] által kiadott útmutató[27] megállapítása szerint: „A szervezetek ma már nem biztosíthatják magukat egyszerűen a saját infrastruktúrájuk határvédelmével, mivel a határaikat ma már lehetetlen egzaktul meghatározni; a fenyegetések szándékosan a kibervédelmi szempontból fejlett

[20] https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (letöltve: 2023.08.16.)

[21] Akár katonai erőforrások bevonásával is, lásd: https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html

[22] Az EU kezdeményezéseihez lásd pl.: https://www.consilium.europa.eu/en/policies/eu-crisis-response-resilience/ ; illetve az Európai Helyreállítási és Reziliencia Eszközt: https://www.consilium.europa.eu/hu/policies/eu-recovery-plan/

[23] A Washington Szerződés 3. cikkelyében rögzített az reziliencia alapelve, mint elvárt törekvés a tagok részéről. A Szövetség számos dokumentumában részletezi az ezzel kapcsolatos közös célkitűzéseket és tervezett erőfeszítéseket, lásd pl.: Strengthened Resilience Commitment 2021 - https://www.nato.int/cps/en/natohq/official_texts_185340.htm ; NATO Climate Change and Security Action Plan 2021 - https://www.nato.int/cps/en/natohq/official_texts_185174.htm

[24] Kiterjedt volumenű kiberkémkedési incidens, amelyre 2020 decemberében derült fény. Állami támogatású – vélhetően orosz – hackerek hátsó ajtót (backdoor) telepítettek többek közt az USA kormányzati szerveinek és néhány EU-s szervezet rendszereibe. Lásd bővebben: https://nki.gov.hu/it-biztonsag/elemzesek/a-solarwinds-incidens-elemzese/ (letöltve: 2023.08.15.)

[25] Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/

[26] National Institute of Standards and Technology, https://www.nist.gov/

[27] https://csrc.nist.gov/publications/detail/nistir/8276/final

szervezetek beszállítóit célozzák, kihasználva a leggyengébb láncszemet." A Kaseya[28], BigNox[29] és Gigaset[30] incidensek szintén aláhúzták ennek a veszélynek a fontosságát.

Szintén fontos támadási irány, az „újrahasznosított" és akár nyílt forrású átvett programrészletek, csomagok és könyvtárak megfertőzése, melyeken keresztül a támadó célú kódot maga a későbbi áldozat emeli be saját környezetébe, de előfordult a szoftver-fejlesztő környezetek, eszközök kompromittálása is (Codecov[31]).

Az ellátási-beszállítói lánc biztosítása érdekében a beszállítóknak maguknak kell felelősséget vállalniuk először a saját tevékenységeik vonatkozásában – megfelelő teszteléssel, a nyílt internettől szegregált fejlesztéssel, biztonságos konfiguráció menedzsmenttel, tanúsítvány-kezeléssel és az automatikus frissítéseket is terjesztő szoftver-platformok megerősítésével. Ha a fejlesztési folyamat egy része kiszervezésre kerül, mindenképpen védeni kell a forráskódot, és további ellenőrzéseket kell végrehajtani az esetleges sérülékenységek és rosszindulatú kódok feltárására. A beszerzések esetén a részletes specifikáció vizsgálatának egészen komponens-szintig le kell mennie, és érdemes megfontolni a beszerzett termékkel szemben valamilyen megbízható harmadik fél, egy tanúsító szervezet általi certifikációját is (akár a Common Criteria, vagy az ISO 27001 szabvány mentén)[32].

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) 2021 októberben publikált Threat Landscape 2021[33] című dokumentuma nyolc fő fenyegetéscsoportot azonosított, amelyek a 2020-2021-es időszakban meghatározták a kiberteret:

- zsarolószoftverek (ransomware);
- rosszindulatú szoftverek (malware), amelyek valamilyen negatív hatást fejtenek ki egy rendszer bizalmasságára, integritására vagy rendelkezésre állására;
- rejtett kriptobányászat (cryptojacking), amelyben a célrendszer számítási kapacitásait rejtetten kriptovaluta bányászatára használják fel;
- e-mail-el kapcsolatos visszaélések, amelyek elsősorban az e-mail olvasóját célozzák, veszik rá valamire;

[28] Felhőalapú szoftver-szolgáltatást a beszállítói láncon keresztül érintő amerikai ransomware-incidens, amely azóta kvázi-tananyagként ajánlott feldolgozásra: https://blog.isc2.org/isc2_blog/2023/07/kaseya-incident-two-years-later-what-has-changed-what-have-we-learned.html ; https://niccs.cisa.gov/education-training/catalog/skillsoft/secops-tools-and-2021-security-incidents-kaseya-ransomware (letöltve: 2023.08.16.)

[29] Hong kong-i, tajvani és sri lanka-i célpontokat érintő, szintén a beszállítói láncon keresztül érkező támadás 2021-ben: https://www.zdnet.com/article/hacker-group-inserted-malware-in-noxplayer-android-emulator/ (letöltve: 2023.08.16.)

[30] Android-alapú mobiltelefonok megfertőző támadás, amely szoftverfrissítésként került az eszközökre egy külső szolgáltató szerveréről: https://www.zdnet.com/article/hacker-group-inserted-malware-in-noxplayer-android-emulator/ (letöltve: 2023.08.16.)

[31] A Codecov cég szoftverfejlesztő célszoftverének felhasználásával jutottak el a támadók a Codecov termékét felhasználó szervezetek belső hálózataiba. https://www.reuters.com/technology/codecov-hackers-breached-hundreds-restricted-customer-sites-sources-2021-04-19/ (letöltve: 2023.08.16.)

[32] További szempontokért lásd: Executive Order on Improving the Nation's Cybersecurity, May 12, 2021, Sec. 4. Enhancing Software Supply Chain Security, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[33] ENISA Threat Landscape 2021, 8.o. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (letöltve: 2022.04.04.)

- adatok elleni fenyegetések, amelyek során bizalmas és/vagy szenzitív adatok kiszivárgása, megszerzése történik;
- fenyegetések a rendszerek rendelkezésre állása vagy integritása ellen, azaz jellemzően DoS- vagy web-alapú támadások;
- dezinformáció és félrevezetés, amely a vizsgált időszakban leginkább talán a COVID-járványhoz volt kapcsolható, de a jelenben az orosz-ukrán háborúnak is kritikus jelentőségű kísérőjévé vált;
- nem rossz-szándékú veszélyforrások, mint a helytelen rendszer-konfigurációk, fizikai meghibásodások, emberi hibák.

Az ENISA dokumentumának trendelemzéséből[34] érdemes kiemelni néhány eddig még nem érintett szempontot is:

- minden támadástípusnak megjelenik a bérbevehető, szolgáltatásként is igénybe vehető formája, üzleti modellje, ami az attribúció feladatát[35] még inkább nehezíti: zsarolószoftverek, DoS-támadások, phishing-kampányok vagy dezinformáció esetében;
- a kiberbűnözők egyre inkább haszonszerzésre törekednek, és jellemzően kriptovaluta-alapú kifizetéseket követelnek;
- a kibertámadások egyre inkább kritikus infrastruktúrákat támadnak;
- az üzleti szféra és egyéb szervezetek elektronikus levelezése kiemelt célpont;
- a dezinformációhoz egyre fejlettebb mesterséges intelligenciát is bevetnek a támadók.

A brit központtal, de globális ügyfélkörrel (több, mint 500 ezer szervezet) működő Sophos 2022-re kiadott fenyegetési jelentését[36] is érdemes kiemelni. Ez az anyag 5 fontos témakört tárgyal mélyebben, elsőként a zsarolószoftverek várható jövőjét elemzi, jelezve a szolgáltatási-modell terjedését és a zsarolási spektrum szélesedését is. Ezt követik a rosszindulatú szoftverek (malware és disztribúciós rendszereik) valamint a mesterséges intelligencia, mint technológia

[34] ENISA i. m. 9. o.

[35] Az attribúcióról bővebben lásd: Herbert LIN: Attribution of Malicious Cyber Incidents. Washington, Hoover Institute – Stanford University, 2015.; Timo STEFFENS: Attribution of Advanced Persistenst Threats. How to Identify the Actors Behind Cyber-Espionage. Berlin, Springer Vieweg, 2020.; Garrett DERIAN-TOTH – Ryan WALSH – Alexandra SERGUEEVA – Edward KIM – Alivia COON – Hilda HADAN – Jared STANCOMBE i.m. (2021); PÁLL-OROSZ Piroska: Attribúció (betudás) a kibertérben In: Kenedli Tamás (szerk.): Nemzetbiztonsági Tanulmányok II. Budapest, Katonai Nemzetbiztonsági Szolgálat, 2021., 66-84. o.;
Az attribúcióhoz azonban másik oldalról számításba kell venni a támadó műveletekkel kapcsolatos szakmai gondokodást és szakpolitikai irányokat is, melyről lásd: KOVÁCS László: Offenzív kiberműveletek 1.: Az offenzív kiberműveletek természete. *Hadmérnök* 2021/2., 187-204. o.; KOVÁCS László: Offenzív kiberműveletek 2.: Kibererők és képességeik. *Hadmérnök* 2021/3., 119-137. o.; Max SMEETS – Herbert S. LIN: Offensive Cyber Capabilities: To What Ends? (https://ccdcoe.org/uploads/2018/10/Art-03-Offensive-Cyber-Capabilities.-To-What-Ends.pdf); Maren LEED: Offensive Cyber Capabilities at the Operational Level. The Way Ahead. Washington, Center for Strategic & International Studies, 2013.; James A. LEWIS: The Role of Offensive Cyber Operations in NATO's Collective Defence. Tallinn, CCDCOE, 2015.; Herbert LIN – Amy ZEGART (ed.): Bites Bombs and Spies. The Strategic Dimensions of Offensive Cyber Operations. Washington, Brooking Institution Press, 2018.; BÁNYÁSZ Péter – KRASZNAY Csaba – TÓTH András: A NATO kibervédelmi szakpolitikája. In: Szenes Zoltán (szerk.): A mai NATO: A szövetség helyezete és feladatai. Budapest, Zrínyi Kiadó, 2021, 130-149. o.

[36] Sophos 2022 Threat Report – Interrelated threats target an interdependent world, https://assets.sophos.com/X24WTUEQ/at/b739xqx5jg5w9w7p2bpzxg/sophos-2022-threat-report.pdf (letöltve: 2022.04.04.)

növekvő jelentősége és hozzáférhetővé válása a fenyegetések aktorai számára. Az előrejelzést a mobilplatformokon növekedő malware-fenyegetés és a kritikus infrastruktúrák elleni támadások jellemzőinek elemzésével zárják.

A szintén angliai székhelyű BAE Systems, amely amellett, hogy Európa legnagyobb hadiipari beszállítója, például a SWIFT-rendszer üzemeltetésében is közreműködik, szintén kiadott egy 2022-re vonatkozó előrejelzést[37]. Ebben ők hét várható trendet vázolnak fel:

- a COVID várható lecsengésével a pénzügyi szféra ismét kiemelt célponttá válik;
- a zsarolószoftverek üzemeltetői a Bitcoin-on túllépve, más kriptovalutákban kívánnak majd tranzakciókat végrehajtani, amelyek nyomon követése nehezebb (pl. Monero[38]);
- az egyes szervezeteket célzó támadások egyre inkább a személyes használatú alkalmazotti eszközökön keresztül, akár social engineering módszerek alkalmazásával valósulnak majd meg, ami szükségessé teszi majd a szervezeti biztonsági előírások frissítését;
- a támadók az IoT-eszközökre jellemző kezdeti, vagy lassan javított sérülékenységeket kihasználva fogják megszerezni a kezdeti hozzáférést a rendszerekbe[39];
- várható, hogy meghatározott személyek hangjának utánzásával, „deepfake”-eszközökkel és social engineering módszerekkel együtt igyekeznek majd a támadók hozzáféréseket megszerezni telefonhívásokon keresztül;
- a rendszereken behatolási teszteket végrehajtó és a rendszert védő szakemberek között szervezeti falak lebontása várható, mivel a folyamatban lévő támadások korai felismerését a „Red Team” szemlélet jócskán segítheti;
- egyre kisebbnek tűnő hibák okozhatnak egyre komolyabb üzemzavarokat, legyen szó kritikus infrastruktúra kieséséről (pl. Colonial Pipeline zsarolószoftverrel bénítása) vagy közösségi csevegő szolgáltatásról (pl. Whatsapp konfigurációs hibája[40]).

3. Változó uniós keretek[41]

A 2016/1148 irányelv (NIS) megalkotásakor nagy eredményeket hozott azzal, hogy EU-szinten meghatározta a kiberbiztonság alapvető kereteit, de irányelvi jellegéből fakadóan a benne lévő

[37] 2022 Cyber Predicitions, https://www.baesystems.com/en/cybersecurity/feature/2022-cyber-predictions (letöltve: 2022.04.04.)

[38] A Monero rendszere nagyobb valószínűséggel őrzi meg a kriptovaluta birtokosának a valós személyazonosságát, mint pl. a Bitcoin, így a ransomware-támadások elkövetői inkább már az ehhez hasonló megoldásokat választják. https://www.getmonero.org/ ; https://www.newsweek.com/monero-developer-criminal-groups-use-crypto-ransoms-justin-ehrenhofer-1600884 (letöltve: 2023.08.16.)

[39] IoT (Internet of Things, „dolgok internete”): a működési hatékonyság és a kényelem érdekében különböző ipari és háztartási eszközök hálózati, szenzoros és számítási kapacitásokkal való továbbfejlesztése, amelyek mint önálló IKT-eszközök szintén támadások célpontjaivá válhatnak. Lásd pl.: JOHANYÁK Zsolt Csaba, PÁSZTOR Attila: IoT rendszereket fenyegető támadások, Gradus, 2023/1. szám, https://gradus.kefo.hu/archive/2023-1/2023_1_CSC_001_Johanyak.pdf (letöltve: 2023.08.16.)

[40] 3,5 milliárd fehasználót érintett és zárt ki 6 órára az online csevegő-alkalmazásból egy rossz beállítás. https://www.reuters.com/technology/facebook-instagram-whatsapp-partly-reconnecting-after-nearly-six-hour-outage-2021-10-04/ (letöltve: 2023.08.16.)

[41] A hazai szabályozás részletes elemzésére, értékelésére lásd: Mógor Judit, Angyal István: A létfontosságú rendszerek védelmére vonatkozó szabályozás fejlesztése, Budapest, Scientia et Securitas, 3. évfolyam, 2. szám, 118-125. o., 2022, https://akjournals.com/view/journals/112/3/2/article-p118.xml

mozgástér meglehetősen sokféle nemzeti megoldást hozott magával, amelyek mostanra akadályává váltak a folyamatosan romló biztonsági környezet által is megkövetelt magas szintű koordinációnak, és az egyes kérdések nemzeti sajátosságok elismerése melletti, de korreláló megközelítésének.

2022 év végén, közösségi szinten hosszas előkészítés után – tekintettel az orosz-ukrán háború tapasztalataira is – a tagállamok kiberbiztonságát alapjaiban meghatározó és alakító új szabályozók jelentek meg, a NIS 2 irányelv[42], és a pénzügyi szféra szempontjából meghatározó „lex specialis", a DORA rendelet[43] (valamint NIS 2-vel szorosan, hatályba lépésben is együtt mozgó, a kritikus rendszerelemek szempontjából fontos CER irányelv[44]). A már meglévő szabályok újragondolását a fokozott fenyegetésekre hozott nemzeti intézkedések ismételt közös nevezőre hozása, az együttműködés, de egyúttal a szabályozási fókusz kibővítése is magával hozta. Az új szabályozók főbb újításait (mint. pl. az új kategorizálást: alapvető – kiemelten fontos), az elől irányelv kereteit kiszélesítő, továbbfejlesztő rendelkezéseit már számos hírben, rövid tanulmányban feldolgozták[45], ehelyütt az ellátásbiztonságra, szoftverfejlesztésre- és üzemeltetésre és a IKT eszközök kereskedelmére várhatóan jelentős hatást gyakorló néhány részletet emelnék csak ki.

A NIS 2 irányelvnek való megfelelést a tagállamoknak 2024. október 17-ig kell biztosítaniuk. Preambulumában kiemeli, hogy az ellátási láncokban komoly szerepet játszó kis- és középvállalkozások válnak egyre inkább támadások célpontjaivá, ezért az ő fokozottabb kiberbiztonságuk is fontos cél. Konkrét technikai-műszaki intézkedésekről a 24. cikk (2) bekezdésében, mint a kockázatelemzés, eseménykezelés és jelentéstételi-kötelezettség, üzletmenet-folytonosság, ellátási-lánc biztonság és kockázatértékelés, szabályzatok és eljárások, kriptográfia és HR-biztonság inkább felsorolás-szerűen, általános értelemben beszél, ezzel inkább kereteket biztosít[46]. A beszállítói rendszerek kapcsán a (3) bekezdésben a tagállamok felelősségévé teszi, hogy az irányelv hatálya alá tartozó szervezetek, amikor mérlegelik az egyes intézkedések megfelelőségét, figyelembe vegyék az egyes közvetlen beszállítókra és szolgáltatókra jellemző sérülékenységeket, valamint a beszállítóik és

[42] Az Európai Parlament és a Tanács 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2)

[43] Az Európai Parlament és a Tanács 2022/2554 rendelete a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (DORA)

[44] Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (CER)

[45] Lásd pl: Domokos Márton, Bertók Gábor, Huszár Daniella: NIS2 – az EU új Kiberbiztonsági Irányelve, https://www.jogiforum.hu/hir/2023/01/03/nis2-az-eu-uj-kiberbiztonsagi-iranyelve/ (letöltve: 2023.07.25.); Hüvelyes Péter: DORA: hatékony és egységes kockázatkezelési gyakorlatok a pénzügyi szektornak, https://euroone.blog.hu/2023/02/14/dora_hatekony_es_egyseges_kockazatkezelesi_gyakorlatok_a_penzugyi_szektornak (letöltve: 2023.07.25.)

[46] Azzal a fontos kiegészítéssel, hogy 2024. október 17-ig a Bizottság végrehajtási jogi aktusokat fogad el, amelyekben meghatározza az intézkedések technikai és módszertani követelményeit a DNS-szolgáltatók, a legfelső szintű doménnévnyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, az online piacterek, az online keresőprogramok és a közösségimédiaszolgáltatási platformok szolgáltatói, valamint a bizalmi szolgáltatók tekintetében.

szolgáltatóik termékeinek és kiberbiztonsági gyakorlatainak – többek között biztonságos fejlesztési eljárásaiknak – az általános minőségét. A tagállamoknak biztosítaniuk kell, hogy a szervezetek – amikor azt mérlegelik, hogy az intézkedések közül melyek megfelelők – kötelesek legyenek figyelembe venni a 22. cikk (1) bekezdésének megfelelően a kritikus ellátási láncok vonatkozásában, a tagállamok közötti stratégiai együttműködés és információcsere céljából létrehozott tagállami együttműködési csoport által elvégzett összehangolt biztonsági kockázatértékelések eredményeit[47].

A 13., 23. és 29. cikk szerinti széles körű értesítési és jelentéstételi kötelezettség valamint információmegosztás szabályozása a határokon átnyúló vagy ágazatközi jelentős események vonatkozásában EU-szintre emeli az eseményekről, kiberfenyegetésekről való értesülést, sőt újításként behozza majdnem bekövetkezett eseményt is, így a gyártók és beszállítók szempontjából sem mindegy, hogy bármely jelentős biztonságot érintő minőségi probléma nagyon gyorsan közismertté válik, ezzel növelve a hanyag fejlesztés reputációs kockázatait. Az együttműködés lehető legszélesebb körének kialakítása érdekében a nemzeti CSIRT-hálózat, az uniós szintű válságok kezelésére létrejött EU-CyCLONe[48] és a már említett tagállami együttműködési csoport kerül létrehozásra.

A szabványosításról szóló 25. cikk előírja a tagállamoknak, hogy – részrehajlás nélkül - ösztönözzék a hálózati és információs rendszerek biztonsága tekintetében releváns európai és nemzetközi szabványok és műszaki előírások alkalmazását. Az ENISA pedig ebben a témában a tagállamokkal együttműködve és adott esetben az érintett érdekelt felekkel folytatott konzultációt követően tanácsokat és iránymutatásokat dolgozhat majd ki. Az irányelv tudatosan és következetesen többször hivatkozik[49] a folyamatosan fejlődő műszaki szabványkörnyezetre, ezzel nyilván elkerülve, hogy fontos részei valamely innováció következtében anakronisztikussá, meghaladottá, vagy egyenesen alkalmazhatatlanná váljanak.

A DORA rendelet különlegességét az adja, hogy az IKT-technológiák alkalmazásában élenjáró, tevékenysége miatt örök célpontot jelentő pénzügyi szféra biztonsági színvonalát – digitális működési rezilienciáját[50] – emelje és egységesítse az EU-ban egy magas szintre és működési alapelveken túl konkrétabb intézkedések megtételét is előírja. Ennek egyik legfontosabb eszközrendszere a közösségi pénzügyi piacot felügyelő európai felügyeleti hatóságok[51] által

[47] Aminek előképeként hivatkozza a telekommunikációs 5G-hálózatok kiberbiztonsága kapcsán korábban kiadott (EU) 2019/534 Bizottsági ajánlást.

[48] https://www.enisa.europa.eu/topics/incident-response/cyclone

[49] A felhőszolgáltatásokkal kapcsolatban az ISO/IEC 17788:2014, a sérülékenységkezeléssel kapcsolatban az ISO/IEC 30111, ISO/IEC 29147, a kiberbiztonsággal kapcsolatban általánosságban az ISO/IEC 27000 szabványsorozat kerül megemlítésre hivatkozási pontként.

[50] 3. cikk 1. pont: „a pénzügyi szervezet képessége arra, hogy kiépítse, biztosítsa és felülvizsgálja működési integritását és megbízhatóságát azáltal, hogy harmadik fél IKT-szolgáltatók által nyújtott szolgáltatások igénybevételével közvetlenül vagy közvetetten biztosítja azon hálózati és információs rendszerek biztonságának kezeléséhez szükséges IKT-vonatkozású képességek teljes körét, amelyeket a pénzügyi szervezet használ, és amelyek a pénzügyi szolgáltatások folyamatos nyújtását és minőségét támogatják, többek között zavarok fennállásakor is;"

[51] Ezek az 1093/2010/EU európai parlamenti és tanácsi rendelettel létrehozott európai bankfelügyeleti hatóság (Európai Bankhatóság, EBA), az 1094/2010/EU európai parlamenti és tanácsi rendelettel létrehozott európai felügyeleti hatóság (Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság, EIOPA) és az 1095/2010/EU európai

2024. július 17-ik kiadott szabályozástechnikai-standardok és végrehajtás-technikai standardok lesznek[52]. A rendelet alapján elvárás az IKT-kockázatok kezelése, az események osztályozása és jelentése, a sérülékenység ellenőrzése, a beszállítói kockázatok kezelése (a rendeletben harmadik féltől eredő IKT-kockázat), és a piaci szereplők között kiberfenyegetésekre vonatkozó információmegosztás – mindezek egy szinttel konkrétabban és részletesebben, mint a NIS 2 esetében, így az azonosításra, védelemre, reagálásra és helyreállításra, sőt a mentési gyakorlatra is szabályok megadásával. A rendelet január 16-án lépett hatályba és rendelkezéseit 2 év felkészülési idő után kell alkalmazni.

A kritikus szervezetek rezilienciájáról szóló CER irányelv célja, hogy megerősítse ezek ellenállóképességét a felmerülő fenyegetésekkel szemben, beleértve a természeti veszélyeket, a terrortámadásokat vagy a szabotázst, valamint a közegészségügyi vészhelyzeteket. Az irányelv melléklete tizenegy ágazatot vont a fókuszába: energia, közlekedés, banki szolgáltatások, pénzügyi piaci infrastruktúra, egészségügy, ivóvíz és szennyvíz, digitális infrastruktúra, közigazgatás, világűr és élelmiszer-ipar.

Az új szabályok szerint a tagállamoknak nemzeti stratégiát kell elfogadniuk, és rendszeres kockázatértékelést kell végezniük a társadalom és a gazdaság számára kritikusnak vagy létfontosságúnak tartott szervezetek azonosítása érdekében. A államoknak támogatást kell nyújtaniuk a létfontosságú szervezeteknek ellenálló képességük fokozásához, valamint egymással együtt kell működniük.

A szervezeteknek magukra vonatkozóan is kockázatértékelést kell végezniük, és műszaki, biztonsági és szervezeti intézkedéseket kell hozniuk ellenálló képességük fokozása és az incidensek bejelentése érdekében. A 21. század kihívásaira való reagálást jó jelzi, hogy az éghajlatváltozás való alkalmazkodást célzó intézkedések szükségességére is kitér az irányelv az olyan „hagyományosnak” vagy kézenfekvőnek tűnő követelmények mellett, mint a kockázat- és válságkezelési eljárások, az üzletmenet-folytonossági intézkedések, az alternatív ellátási láncok vagy a hatékony munkavállalói biztonságirányítás. A humán-elem felismert jelentőségét még jobban alátámasztja a háttérellenőrzések előírása, amely alapján a kritikus szervezetek számára megengedett, hogy kellően indokolt esetben kérelmet nyújtson be érzékeny szerepet betöltő személyek ellenőrzésére a hatáskörrel rendelkező nemzeti hatóságok felé.

A Bizottság támogatást fog nyújtani a tagállamoknak és a szervezeteknek azáltal, hogy uniós szintű áttekintést készít a határokon átnyúló és ágazatokon átívelő kockázatokról, a legjobb gyakorlatokról, az útmutató anyagokról, a módszerekről, a határokon átnyúló képzési tevékenységekről és gyakorlatokról, amelyek célja a határokon átnyúló és ágazatokon átnyúló kockázatok vizsgálata.

Az új uniós keretrendszer hatásai minden érintett tagállamban a hálózatbiztonsági teljes vertikumának felülvizsgálatát, kiszélesítését és a biztonság színvonalának emelését célzó új (szakmai-technikai eredetű) jogintézmények létrehozását hozza majd. A jellemzően

parlamenti és tanácsi rendelettel létrehozott európai felügyeleti hatóság (Európai Értékpapírpiaci Hatóság, ESMA).

[52] Ezek kidolgozása már folyamatban van, az első nyilvános anyagok már elérhetők: https://www.eba.europa.eu/esas-consult-first-batch-dora-policy-products (letöltve: 2023.07.26.)

jogforrásban kihirdetett nemzeti kiber- avagy hálózatbiztonsági stratégiák[53] az új szempontrendszerek szerint frissítendők lesznek, amire a jelentős gyorsasággal változó technikai közeg, a geopolitikai súlypontváltozás és az orosz-ukrán konfliktus (és tanulságai) miatt egyébként is szükség van. A részletesen tárgyalt új jogintézmények mellett kiemelendő a lehető legszélesebb körű kooperáció és információmegosztás, aminek gyakorlati megvalósulása még érdekes adatvédelmi, nemzetbiztonsági, üzleti titokvédelmi akadályokba ütközhet és balanszírozott részletszabályozásuk nehéz jogi feladatot jelent majd.

4. Összegzés

A szuprancionális, nemzeti és szakmai keretek változása minden bizonnyal több lényegi változást, fejlődést hoz majd magával[54]. Állami, szakpolitikai szinten a NIS 2 7. cikke által is érintett nemzeti kiberbiztonsági stratégia átdolgozása lesz szükséges, amely az alapvető és fontos szervezetekre koncentrálva, részletes ágazati és tematikai alábontásaiban is konzekvens módon, egy központi víziót követve, határoz meg intézkedési irányokat és stratégiai törekvéseket. Véleményem szerint időhorizontját tekintve a stratégia nem szaladhat 5 évnél sokkal előbbre az állandóan változó, innovatív közeg miatt, amely a stratégia helyzetértékelési, fenyegetettség-elemző, és prioritás-mátrixát is gyorsan elavulttá teszi. A stratégia kidolgozásáért felelős Nemzeti Kiberbiztonsági Koordinációs Tanácsnak[55] érdemes lenne hangsúlyt fektetnie a stratégiai célok éves szintű lebontására, mérhető paraméterekkel, hogy a megtett erőfeszítések értékelhetők, visszamérhetőek legyenek.

A cél nemzeti szinten az EU-s keretek között mozgó, rugalmas és az iparági jó gyakorlatokat bátorító regulatív modellek felépítése, amely az IKT fejlesztésben és üzemeltetésben közreműködő minden szakemberrel szemben – az adott feladat által megkövetelt biztonsági szinthez és az üzemeltetett rendszerhez igazított – szakmai elvárásokat támaszt, ellenőriz és számonkér. A NIS 2 által megfogalmazott együttműködések erősítése érdekében élő és folyamatosan működő kommunikációs csatornák kialakítására van szükség az IT ipar (kooperáció a biztonság növelése érdekében), az egyetemi és szakképzési szféra (K+F+I, az iparági szakemberigények közvetítésére, a szükséges HR-erőforrás rendelkezésre állásának előmozdítására) és a fogyasztói csoportok tudatosságának növelésére (szemléletformálás, tudatos és kockázatcsökkentő online működés érdekében).

[53] https://www.enisa.europa.eu/topics/national-cyber-security-strategies

[54] Az aktuális helyzet áttekintéséhez lásd: Bányász Péter, Krasznay Csaba, Tóth András: A kibervédelem szakpolitikai szintjének helyzete és kihívásai Magyarországon, az EU-ban és a NATO-ban, Budapest, Military and Intelligence Cybersecurity Research Paper 2022/8., Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/MIC_RP-2022_8%20B%C3%A1ny%C3%A1sz%20P%C3%A9ter%20-%20Krasznay%20Csaba%20-%20T%C3%B3th%20Andr%C3%A1s%20-%20A%20kiberv%C3%A9delem%20szakpolitikai%20szintj%C3%A9nek%20helyzete%20%C3%A9s%20kih%C3%ADv%C3%A1sai%20Magyarorsz%C3%A1gon,%20az%20EU-ban%20%C3%A9s%20a%20NATO-ban.pdf

[55] Lásd a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet

A szervezetek vezetői szempontjából kritikus felelősség ezeknek a kockázatoknak a felmérése, kezelése[56], az információbiztonsággal olyan szakemberek megbízása, akik szemléletmódjukban biztonság-orientáltak, és az üzleti/szervezeti célok elsődlegessége mellett képesek a rendelkezésre álló erőforrásokból a lehető legtöbbet kihozva a lehető legmagasabb biztonsági szintű üzemeltetési környezetet kialakítani. Ehhez a vezetés részéről messzemenő támogatásra, és folyamatos képzésre is szükség van az infrastruktúrába történő tervezett, és néha terven felüli invesztíciókon felül.

Nem szükséges egy szervezeten belül minden részfeladat magas szintű ellátását megoldani, a beszerzés, jogi támogatás, üzemeltetés, eseménykezelés, biztonsági felügyelet funkciói a szervezet erőforrásaitól és igényeitől is függően külsős, háttérellenőrzött, referenciákkal rendelkező beszállítókkal is megoldható, de mindenképpen érdemes és egyes esetekben kötelező megfelelő előrelátással ezeket jó előre lebiztosítani, és a kiválasztásuk során messzemenően körültekintően eljárni.

A fentiekben tárgyalt uniós jogi eszközök implementációja minden tagállamban, így hazánkban is remélhetőleg fokozni fogják létfontosságú rendszerelemek üzemeltetőinek, az IKT-szektor beszállítóinak, az elektronikus információs rendszerek állami és civil üzemeltetőinek felelősségtudatát valamint hálózataik elért biztonsági színvonalát, végül ezen keresztül az ellátásbiztonságot. Megcélzott hatása a közösségi jog standardizálásának egy olyan versenyelőny megteremtése, amelyet az adatvédelemben globálisan is versenyelőnynek és mintának tekintett GDPR rendelet[57] is hozott magával. Az állami szerepvállalás növekedése borítékolható, amely a megnövekedett hatósági ellenőrzések mellett megfelelő szervezéssel egy partneri jellegű viszonyra törekvő, segítő alapállással párosul majd. Az IKT közeg és a hálózatbiztonsági szabályozási kereteinek „rövid szavatossági ideje" és inflációja jelentős részben betudható a szabályozás technológia innováció által húzott jellegének, és annak a dinamikusan formálódó közegnek, ami a 21. század kibertere. A szabályozás terjedelmének és komplexitásának növekedése, a komoly szankciókkal, bírságokkal megtámogatott előírások miatt növekvő jogi kockázatok magukkal hozzák azt is, hogy minden szereplő értékelésében nagyobb szerepet fog kapni a jogalkalmazás, a konform működés feltételeinek kialakítása, és ezzel párhuzamosan hangsúlyt fektetnek majd a szükséges jogi kompetenciák megszerzésére és növelésére is.

[56] A C-suite tagjainak tuadatossága, ébersége és felelősségvállalása azért sem elkerülhető, hiszen személy szerint a saját maguk által is használt eszközökön keresztül, betöltött státuszuk miatt is kiemelt célpontnak számítanak. Lásd.: Magyar Sándor, Tóth András, Bányász Péter: The role of information security awareness for senior executives, In: İlyas, ERPAY; Necati, SÜMER 1st BİLSEL INTERNATIONAL AHLAT SCIENTIFIC RESEARCHES CONGRESS, Bitlis (Törökország), Bilgesina (2023) 1054-1061. o.; Bonnyai Tünde, Kiss Adrienn, Tóth András (szerk.): Nagyvállalati biztonságtudatosság és nyílt forrású információszerzés: Kiber- és információbiztonsági tanulmányok, Budapest, Nemzeti Közszolgálati Egyetem Ludovika Egyetemi Kiadó, 2023

[57] Jogi szempontból az alapjogvédelem mellett leginkább a megnövelt bizalom és hitelesség, az adatkezelés kereteinek egységesítése, színvonalának javítása, és az előírásoknak megfelelő szervezetek reputációjának növelése és a versenyfeltételek kiegyenlítése emelhető ki. Lásd pl.: https://www.techtarget.com/searchdatabackup/tip/6-business-benefits-of-data-protection-and-GDPR-compliance (letöltve: 2023.08.16.)