NEMZETBIZTONSÁGI SZEMLE

Kiemelt közlemények

11. évf. (2023)
1. szám

ISSN 2064-3756 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

Impresszum

Nemzetbiztonsági Szemle
A Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézetének elektronikus (online) megjelenésű tudományos folyóirata

HU ISSN 2064-3756 (elektronikus)

Kiadó
Nemzeti Közszolgálati Egyetem | Ludovika Egyetemi Kiadó
Kapcsolat: www.ludovika.hu; kiadvanyok@uni-nke.hu
Székhely: 1083 Budapest, Ludovika tér 2.
A kiadásért felel: Deli Gergely rektor
Olvasószerkesztők: Bujdosó Hajnalka, Gergely Zsuzsánna, Resofszki Ágnes
Tördelőszerkesztő: Kőrösi László

Tartalom

NEMZETBIZTONSÁGI SZEMLE
11. évfolyam (2023) 1. szám 3–20. • DOI: 10.32561/nsz.2023.1.1

Bogdanovits András,[1] Kovács Zoltán[2]

A vezetékes információs rendszerek védelmének speciális szabályai, eszközei a jogszabályokban, ajánlásokban

Specific Rules and Tools for the Protection of Wired Information Systems in Legislation and Recommendations

Jelen cikk célja, hogy különösen a hírközlési szolgáltatók rendszereire fókuszálva feltárja, szükséges-e a külön is foglalkozni az elektronikus információs rendszerek vezetékes elemeinek a védelmével, vagy azok már az elektronikus információs rendszerek védelmének komplex megközelítése okán kellően védettnek tekinthetők a jelenlegi jogszabályokban, ajánlásokban leírt kontrollok alkalmazásával. Ezért a cikk az információs rendszerek védelmének alapelveiből kiindulva áttekinti a vezetékes és vezeték nélküli hálózatok biztonságának főbb jellemzőit, a vezetékes hálózatokra fókuszálva röviden ismerteti az infokommunikációs hálózatok biztonságához kapcsolódó fontosabb hazai jogszabályokat és (a mérvadónak tekinthető angolszász) nemzetközi ajánlásokat, bemutatja azok kifejezetten vezetékes és vezeték nélküli hálózati elemekre vonatkozó kontrolljait, valamint a biztonság fokozása érdekében javaslatot tesz a továbblépésre.

Kulcsszavak: *elektronikus információs rendszerek, vezetékes hálózatok, kiberbiztonság, Ibtv., NIST 800-53*

The aim of this article is to explore, with a particular focus on the systems of communications service providers, whether the protection of the wired elements of electronic information systems needs to be addressed separately, or whether they can be considered sufficiently protected by the application of controls described in current legislation and recommendations, due to the complex approach to the protection of electronic information systems. Therefore, starting from the basic principles of information systems security, the article reviews the main characteristics of wired

[1] MSc, vezetékes tervezés és nyilvántartás menedzser, Vodafone Magyarország Zrt., e-mail: bogdanovits@gmail.com
[2] PhD, vezérigazgató, NISZ Zrt.; tanársegéd, Nemzeti Közszolgálati Egyetem Bűnügyi, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék, e-mail: zkovacs.24@gmail.com

and wireless network security, briefly describes the main domestic legislation and international recommendations (the most authoritative being Anglo-Saxon) related to the security of information communication networks, describes their controls specifically applicable to wired and wireless network elements, and suggests a way forward to enhance security.

Keywords: *electronic information systems, wired networks, cybersecurity, NIST 800-53*

Bevezetés

Az információs társadalom alapját az infokommunikációs infrastruktúrák képezik. Az információs társadalom megléte, hatékony működése az említett infrastruktúrák fejlettségétől függ. Az infokommunikációs technológiák elterjedése alapjaiban alakította át a gazdasági tevékenységeket és a társadalmi kapcsolatrendszereket, ugyanis a gyors információcsere napjaink gazdaságának, társadalmának meghatározó alappillére. Az infokommunikáció sajátossága, hogy a technika, a tudomány fejlődésével mindig újabb fajtái jelennek meg, ezek pedig alapvetően befolyásolják a társadalmi-gazdasági fejlődést, mivel az infrastruktúra folyamatosan alakítja, változtatja ezeket a folyamatokat. Ezek pedig új igényeket generálva visszahatnak az előbbiek fejlődésére, így egyfajta spirált képezve gyorsítják, erősítik egymást.[3]

A felhasználót a legtöbb esetben nem foglalkoztatja, hogy milyen technológia biztosítja a munkájához szükséges hátteret, őt csupán az érdekli, hogy az adott rendszer az igényeinek megfelelő szolgáltatásokat biztosítsa, és biztonságosan működjön. Éppen ezért nem könnyű vállalkozás kizárólag a hírközlési szolgáltatók vezetékes információs rendszerei védelmének speciális szabályairól, a jogszabályi eszközeiről, ajánlásairól írni. Ugyanis a jogszabályok és ajánlások alkotói – helyesen eljárva – holisztikusan kezelik az elektronikus információs rendszerek biztonságának kérdéseit és védelmét, így jobbára a vezetékes hálózatok, különösen a szolgáltatók hálózatai védelmét külön nem emelik ki.

Ugyanakkor két jellemző vezetékes hálózati rész miatt érdemes megvizsgálni ezt a speciális kérdéskört is. Az első a felhasználókat az utolsó mérföldön kiszolgáló hálózati rész. Ebben az esetben a hírközlési szolgáltatók azon hálózati elemei, amelyek itt kizárólag vezetékes módon szolgálják ki a felhasználókat, még mindig nagy forgalmat bonyolítanak le, és általában nagyobb sebességet és megbízhatóságot kínálnak, mint a vezeték nélküli megoldások. Ráadásul a vezeték nélküli hálózati elemek segítségével az információk csak rövid távolságot tesznek meg a levegőben, ezt követően jellemzően nagy kapacitású vezetékes kapcsolatokon keresztül továbbítják azokat. Ez pedig a második olyan szegmens, amely miatt célszerű a vizsgálatot elvégezni. Ráadásul sok biztonsági kérdés mindkét esetben megjelenik.

[3] Kovács 2021.

Az utolsó mérföldön kiszolgáló hálózati részekkel kapcsolatban azonban elmondható, hogy a világon ma már sokkal több ember rendelkezik vezeték nélküli kommunikációs eszközzel, mint csupán vezetékes kapcsolatot biztosítóval. Ezt jól mutatják a magyarországi adatok is. Amíg 2022 első félévében mintegy 3 millió darab volt a lakossági helyhez kötött internet-előfizetések száma,[4] addig csak az internetforgalmat bonyolított okostelefonos SIM-kártyák száma közel 7,5 milliót tett ki.[5] Ráadásul napjainkban már a kizárólag vezeték nélküli kapcsolódási lehetőséggel rendelkező okostelefonok és táblagépek száma meghaladja a személyi számítógépekét, bár ez utóbbiak – elsősorban a hordozható kivitelűek – jellemzően szintén rendelkeznek vezeték nélküli kapcsolódási lehetőségekkel.[6] Az okostelefonok és táblagépek tömeges elterjedésével, a 3G/4G, majd az 5G mobilhálózatok bevezetésével és a wifihozzáférési pontok nagy arányú kiépítésével a vezeték nélküli adatforgalom robbanásszerűen nőtt az elmúlt években. Ám ezekben a hálózatokban is a rádiós szakasz után megjelennek a vezetékes elemek. Így a mobil adatátvitel növekedése valójában növeli a vezetékes hálózatok iránti keresletet is, ezért az infokommunikációs rendszerek biztonságát jelentősen befolyásolja a hírközlési szolgáltatók vezetékes információs rendszereinek a biztonsága. Hazánkban az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény szerint:

> „14b. elektronikus információs rendszer:
> a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;
> b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy
> c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;"[7]

Így az idézett rész a) pontja szerint érdemes és kell is a hírközlési szolgáltatók hálózatainak védelmi kérdéseivel foglalkozni.

A CIA-elv

Az elektronikus információs rendszer biztonsága a rendszer olyan állapota, amelynek védelme a rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. Az elektronikus információs rendszerek biztonságfogalmát tovább elemezhetjük az alábbi követelmények szerint, ami angol kifejezések kezdőbetűinek összeolvasásából CIA-elv néven fogalmazható meg:

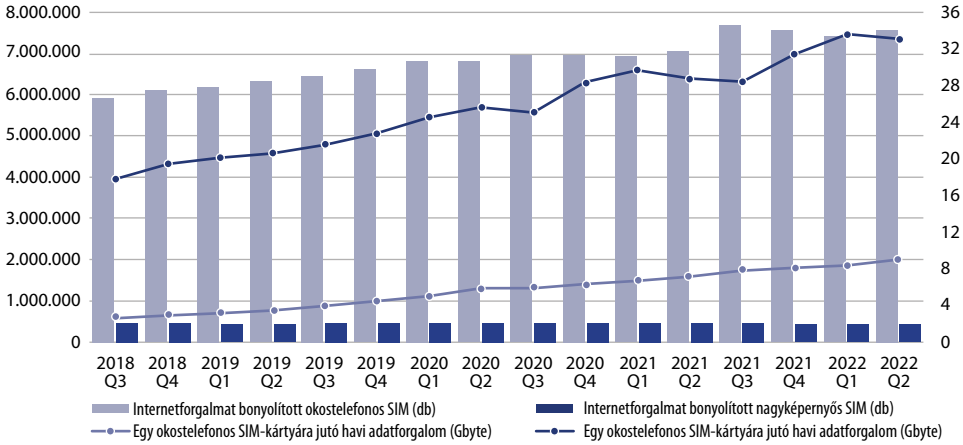
4 NMHH 2022a.
5 NMHH 2022b.
6 Lásd: www.broadbandsearch.net/blog/mobile-desktop-internet-usage-statistics
7 2013. évi L. törvény.

- *Bizalmasság (Confidentiality)* követelménye azt jelenti, hogy egy adott információt csak az arra jogosultak és csak a jogosultságaik szerint ismerhetik meg, használhatják fel, vagy rendelkezhetnek annak felhasználásáról. Azaz illetéktelenek csak nagy erőbefektetéssel, költséggel, vagy kis valószínűséggel legyenek képesek az adott információhoz hozzájutni. A követelmény biztosítására például hozzáférésvédelmi rendszereket, kriptográfiai eljárásokat használnak, amelyek segítik illetéktelenek hozzáférésének megakadályozását az adott információhoz.
- *Sértetlenség (Integrity)* követelménye azt jelenti, hogy az adat tartalma és tulajdonságai megegyeznek az elvárttal, egy adott információt vagy rendszert csak az arra jogosult változtathat meg. Ebbe beletartozik, hogy az adott adat hiteles (az elvárt forrásból származik) és letagadhatatlan (bizonyítható annak származása). A véletlenül megváltozott információt is figyelembe véve, ez a követelmény nagy hangsúlyt fektet a módosítás észlelésére. A követelmény biztosítására az előző bizalmasság követelmény biztosítására szolgáló eszközökön kívül többek között használatos a digitális aláírás és különböző hitelesítő eljárások.
- *Rendelkezésre állás (Availability)* követelménye azt jelenti, hogy az adott adatot vagy rendszert az arra jogosultak a szükséges időben és időtartamban használni tudják, azaz megmutatja, hogy egy adott rendszernek milyen megbízhatósággal kell ellátni a feladatát. A követelmény olyan objektív statisztikai jellemzőkkel jellemezhető, mint az üzemidő, rendelkezésre állási tényező és a sebezhetőségi ablak.[8]

Vezeték nélküli és vezetékes hálózati elemek biztonsága

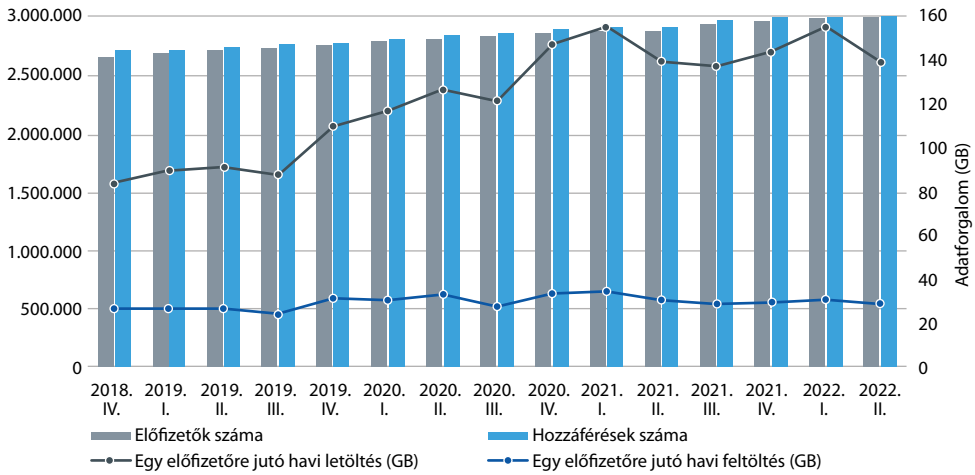
Amikor elektronikus információs rendszerek, infokommunikációs hálózatok (jelen cikk ezeket egymás szinonimájaként használja) biztonságáról beszélünk, legyenek azok vezetékesek vagy vezeték nélküliek, akkor a fent ismertetett CIA-elv alapján vizsgáljuk azokat. Manapság sok szervezet a felhasználókat közvetlenül kiszolgáló vezetékes hálózati elemeit vezeték nélküli hálózatokra cseréli, mivel a vezeték nélküli hálózatok könnyebben teszik lehetővé a számítástechnikai rendszereik elérését, kevesebb kábelt és csatlakozót igényelnek. Így tesznek a hírközlési szolgáltatók is, hiszen a vezeték nélküli internetelérés egyre nagyobb részarányt tesz ki a portfóliójukban. A mobilinternet növekedését mutatja az alábbi, 1. számú ábra.

[8] Muha 2015.



1. ábra: Internetforgalmat bonyolított SIM-kártyák számának és fajlagos forgalmának alakulása szolgáltatási szegmensenként
Forrás: NMHH 2022b

Ugyanakkor az NMHH felmérése szerint a helyhez kötött internetelérések száma és a rajtuk folytatott adatforgalom is növekszik, bár a mobilnál jelentősen lassabb ütemben. Ezt mutatja a 2. számú ábra.



2. ábra: Lakossági helyhez kötött internet-előfizetések és -hozzáférések számának, valamint a fajlagos forgalomnak az alakulása
Forrás: NMHH 2022a

A teljes hálózaton alkalmazott vezetékes technológiát sokkal biztonságosabbnak tartották, mint amikor vezeték nélküli rendszerelemeket is felhasználtak.[9] Köszönhetően azonban a fejlődő technológiáknak és a biztonsági előírásoknak, a vezeték nélküli hálózati részek megfelelően biztonságosnak tekinthetők, mint a vezetékesek, már amennyiben azok tartalmazzák az előírt biztonsági kontrollokat és megfelelően vannak konfigurálva. Ennek okán a biztonsági ajánlások, előírások vizsgálatakor azt láthatjuk, hogy a vezeték nélküli hálózati elemek biztonságára lényegesen több részletszabályt dolgoztak ki, mint speciálisan a vezetékesre.

A vezeték nélküli hálózati elemek biztonságára több ok miatt is nagyobb figyelmet fordítottak korábban. Egyrészt a vezeték nélküli hálózati elemekhez való hozzáférés nem igényel fizikai hozzáférést például egy hálózati csatlakozóhoz vagy kábelhez, mint a vezetékes hálózatok esetében. Másrészt a vezeték nélküli hálózati elemek a végfelhasználók és a hálózat közötti adatátvitelhez rádióhullámokat használnak, és ezeket a rádióhullámokat nem lehet például a vállalat működési területénél (például kerítés) megállítani. Ezért lehetséges, hogy valaki az épület mellett vagy a parkolóban ülve lehallgatja a vezeték nélküli hálózati kommunikációt, sőt adott esetben aktívan be is avatkozhat a hálózati forgalomba, így például akár manipulálhatja az ott található adatok tartalmát is. Márpedig ezeket sokszor a felhasználók nem ismerték, vagy nem foglalkoztak vele kellő mértékben.

Ugyanakkor a belső fenyegetések, a kívülről érkező célzott támadások, valamint a vállalati hálózatokhoz való fizikai hozzáférés megszerzéséhez pszichológiai manipulációt (ismert angol elnevezéssel: social engineering) és mérnöki módszereket is alkalmazó hackerek világában a hálózat vezetékes részének biztonságát is szem előtt kell tartani. Különösen igaz ez a hírközlési hálózatok hosszú, sok esetben utak mellett a földben elvitt vagy akár légvezetékes hálózati elemeire is. Éppen ezért érdemes megvizsgálni, hogy az elektronikus információs rendszerek egészére, valamint azok vezeték nélküli hálózati elemeire vonatkozó biztonsági előírások mellett milyen kifejezetten a vezetékes hálózati elemek védelmét szolgáló ajánlások, előírások léteznek, és azok a hírközlési szolgáltatók hálózatai esetében elégségesek-e a mai világban.

A tisztán vezetékes hálózati elemekkel kialakított hálózatok előnyei

Megfelelő telepítés és konfigurálás esetén a vezetékes hálózati elemek megbízhatóságot és stabilitást nyújtanak. A hálózati elemek és a kábelezés (például optikai vagy Ethernet-kábelek) telepítése után a végeredmény egy rendkívül megbízhatóan működő rendszer lesz. Bár a vezeték nélküli kapcsolatok folyamatosan fejlődnek, a vezetékes hálózatok elérése általában stabilabb és megbízhatóbb. A vezetékes hálózatok azért is megbízhatók, mert a jelet nem befolyásolják a rádiós terjedési viszonyok. Ha például egymáshoz közeli, ugyanazon a csatornán működő wifihálózatok[10] vannak, az egyik

[9] NIST 2020.

[10] Wifi: Az engedély nélkül használható 2,4 és az 5 GHz-es frekvenciasávban működő vezeték nélküli helyi hálózat (WLAN) kialakítására szolgáló, széles körben elterjedt szabvány (IEEE 802.11).

jel zavarhatja a másikat, ami veszélyeztetheti a stabilitást. De ha a közelben reflexiót okozó tereptárgyak vannak, ez hatással van a vezeték nélküli kapcsolatra, míg a vezetékes hálózati kapcsolatot ezek a tényezők nem befolyásolják. Ezenkívül a vezetékes hálózatokban természetesen nem lép fel az ellátatlan területek problémája, amelyek a vezeték nélküli kapcsolatokban időnként a lefedettség hiánya vagy terjedési anomáliák miatt előfordulnak. Ez azért van így, mert minden egyes eszköznek a hálózathoz való csatlakoztatásához külön kábelt használnak, és mindegyik kábel – megadott hosszig – azonos sebességgel továbbítja az adatokat.

A vezetékes hálózatok másik előnye, hogy általában gyorsabbak, mint a vezeték nélküli hálózatok. Bár az adatsebesség folyamatosan javult a vezeték nélküli technológiák (például 5G hálózatok, a wifi 6[11] routerek, wifi mesh hálózatok) megjelenésével, ám jelenleg még mindig a vezetékes hálózaton érhető el nagyobb átviteli sebesség.

A harmadik említésre méltó előny a hozzáférés biztonsága. Illetéktelen felhasználó nem, vagy csak sokkal nehezebben tud csatlakozni egy tisztán vezetékes hálózathoz, mint vezeték nélküli technológiát is használó társához. Egy tisztán vezetékes hálózat ugyanis mind fizikailag (például kerítéssel, rácsok, őrség stb. alkalmazásával), mind logikailag (a szükséges, jól konfigurált biztonsági eszközökkel és alkalmazásokkal) jobban védett lehet az illetéktelen hozzáféréstől, mint egy vezeték nélküli elemekkel kiegészített hálózat. Ez utóbbi esetében gondoljunk például arra, hogy a wifihálózatok még a korszerű levegő interfész titkosító protokollt használva (például WPA2, WPA3) is könnyen hozzáférhetők.[12]

A vezetékes hálózati elemek hátrányai

Elsőként megemlíthetnénk a mobilitás hiányát, ugyanis a vezetékes hálózatok rugalmatlanok a mobilitás szempontjából. Ahhoz, hogy a felhasználó az eszközt egy másik helyen használhassa, extra kábeleket és/vagy beállításokat kell használnia. Például egy vállalatnál használt rendszer biztonságának alapvető eleme, hogy adott portról csak adott (előre konfigurált) eszköz(ök) használhassa(k) a hálózatot, de egy hírközlési szolgáltató által fix helyre kiépített vezetékes szolgáltatás áthelyezése is sok időt és szolgáltatói közreműködést igényel.

A vezetékes hálózat telepítése hosszabb időt vehet igénybe és drágább, mivel több komponensre van szükség a folyamat befejezéséhez. Az infrastruktúra méretigényétől függően a telepítés hosszadalmas és összetett lehet, mivel ki kell építeni a kábelezést, és minden egyes eszközt fizikailag is csatlakoztatni kell a hálózathoz.

Egy tisztán vezetékes hálózat esetén nemcsak a kiépítés, hanem a karbantartás is költségesebb. Ráadásul a kábeleket véletlenül vagy akár szándékosan is el lehet vágni, ki lehet húzni stb.

[11] A wifiszabvány legújabb generációja a wifi 6, más néven 802.11ax, amely akár 4,8 gigabit/sec adatátviteli sebességet is lehetővé tesz.

[12] Khandelwal 2019.

Megállapítás a vezetékes hálózati elemekről

Összességében megállapítható, hogy az előnyök és hátrányok mérlegelése mellett, elsősorban a költséghatékonyság és a javuló biztonság miatt a hírközlési szolgáltatók kínálatában is egyre terjednek a vezeték nélküli megoldások. Ugyanakkor a vezeték nélküli hálózati részekkel rendelkező hálózatok esetében is minden esetben vannak vezetékes részek, ráadásul ezek a hírközlési szolgáltatók hálózatában jellemzően nagy sebességű, nagy földrajzi kiterjedésű optikai hálózatokat is jelentenek. Így az infokommunikációs hálózatok esetében elmondható, hogy legtöbb esetben hibrid megoldással, azaz a két technológia kombinációjával találkozhatunk. A fent leírtak okán mindenképp érdemes elemezni a vezetékes hálózati elemekre vonatkozó biztonsági előírásokat, ajánlásokat, majd megvizsgálni, hogy ezek teljes mértékben elegendők-e a mai viszonyok mellett, vagy speciális, kifejezetten a vezetékes technológiát jobban védő kontrollokra is szükség van. Ennek teljes feldolgozása messze meghaladja jelen cikk kereteit, így a továbbiakban a főbb szabályzatok, ajánlások ismertetése következik.

Vezetékes hálózati elemek biztonsági kontrolljainak önálló megjelenése a fontosabb jogszabályokban, ajánlásokban

Az elektronikus információs rendszerek biztonságával foglalkozó és konkrét kontrollokat előíró fontosabb jogszabályok és ajánlások áttekintése alapján elmondható, hogy ezek jórészt komplex megközelítéssel dolgoznak. Ez azt jelenti, hogy a biztonsági kontrollok úgy jelennek meg, hogy azok függetlenek attól, hogy a hálózatot vezetékes vagy vezeték nélküli módon valósították-e meg. Ez egyrészt teljesen érthető és helyes megközelítés. Másrészt viszont vannak, lehetnek olyan speciális elemek, különösen a hírközlési szolgáltatók hálózatában, amelyek csak vezetékes, vagy csak vezeték nélküli rendszerelemeknél jelentkeznek. Épp emiatt ezekben a jogszabályokban, ajánlásokban megjelennek olyan kontrollpontok is, amelyek kifejezetten vezeték nélküli vagy vezetékes hálózati elemekre vonatkoznak. Érdemes ezeket áttekinteni és megvizsgálni, vajon a kifejezetten vezetékes rendszerelemekre vonatkozó kontrollpontok elégségesek-e, megfelelnek-e a mai viszonyoknak.

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)[13] és a 41/2015. (VII. 15.) BM rendelet[14]

Az Ibtv. célja a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon védelme érdekében az elektronikus információs rendszereikben kezelt adatokra vonatkozóan

[13] 2013. évi L. törvény.
[14] 41/2015. (VII. 15.) BM rendelet.

a bizalmasság, a sértetlenség és a rendelkezésre állás követelményeinek érvényesítése. Ahhoz, hogy az Ibtv. hatálya alá tartozó elektronikus információs rendszerek zárt, teljes körű, folytonos és kockázatokkal arányos védelmét garantálni lehessen, a 41/2015. (VII. 15.) BM rendelet az osztályba sorolásnak megfelelő logikai, fizikai és adminisztratív védelmi intézkedések bevezetését írja elő. A kockázatarányosságot az elektronikus információs rendszerek biztonsági osztályba soroltatásával, valamint az elektronikus információs rendszerrel rendelkező szervezetek biztonsági szintjének meghatároztatásával érték el.

Az Ibtv.-ben az elektronikus információs rendszer fogalma igazodott 2019 elejétől a NIS irányelv hálózati és információs rendszer fogalmához, de úgy, hogy tartalmazza az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózatokat is.

A 41/2015. (VII. 15.) BM rendeletben kimondottan vezetékes hálózati elemekre nincsenek kontrollpontok, ugyanakkor vezeték nélkülire igen. A 3. számú mellékletben található kontrollpontot az alábbi, 1. táblázat tartalmazza.

1. táblázat: Részlet a 41/2015. BM 3. mellékletéből

1.	Sorszám	Intézkedés típusa	Alapelvek											
2.			Bizalmasság				Sértetlenség				Rendelkezésre állás			
3.			Biztonsági osztályok											
4.			2	3	4	5	2	3	4	5	2	3	4	5
112.	3.3.10.	Hozzáférés ellenőrzése												
144.	3.3.10.14.	Vezeték nélküli hozzáférés	0	X	X	X	0	X	X	X	0	X	X	X

Forrás: 41/2015. (VII. 15.) BM rendelet

Az adminisztratív, fizikai és logikai biztonsági követelmények szöveges magyarázatát tartalmazó 4. mellékletben az alábbi, 2. táblázatban található példák olvashatók.

2. táblázat: Részlet a 41/2015. BM 4. mellékletéből

Sorszám	Kategória	Példák az ellenőrzésekre
1.2.4.	Technológiai eltérések	Példaként említi a vezeték nélküli kommunikációt, hogy az erre vonatkozó előírások csak akkor alkalmazandók, ha használják is.
3.3.10.14.	Vezeték nélküli hozzáférés	Az alkalmazandó speciális biztonsági feladatokat írja le: • szabályozás, technikai útmutató, valamint engedélyezési eljárás; • hitelesítés és titkosítás; • felhasználó konfigurálás tiltása; • antennák; tekintetében.

Forrás: 41/2015. (VII. 15.) BM rendelet

A Nemzeti Kibervédelmi Intézet által kiadott *Felhasználói kézikönyv a 41/2015. BM rendelet által meghatározott védelmi intézkedésekhez* című dokumentum[15] az alábbiakat tartalmazza a 3.3.10.14. számú kontrollpont vonatkozásában:

3. táblázat: Részlet a Felhasználói kézikönyv A 41/2015. BM rendelet által meghatározott védelmi intézkedésekhez dokumentumból

Védelmi intézkedés sorszáma	Védelmi intézkedés megnevezése	Magyarázat, cél	Biztonsági osztály			Példa, előremutató gyakorlat, iparági legjobb gyakorlat, értelmezés
			B	S	R	
3.3.10.14.	Vezeték nélküli hozzáférés	A Szervezet definiálja a vezeték nélküli hálózatra vonatkozó korlátozásokat, konfigurációs lehetőségeket és az engedélyezési eljárást.	3	3	3	A Szervezet az azonosításra és hitelesítésre vonatkozó eljárásrendben vagy az IBSZ-ben felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán (mint például UHF/VHF, 802.11x, and Bluetooth, wifi); továbbá meghatározza az engedélyezési eljárást.
3.3.10.14.2.	Hitelesítés és titkosítás	Az EIR-rendszerben hitelesítéssel és a forgalom titkosításával védik a vezeték nélküli hozzáférést.	5	5	5	Tanúsítvány alapú hitelesítés és forgalomtitkosítás használata a 802.11i szabvány szerint.
3.3.10.14.3.	Felhasználói konfigurálás tiltása	Csak arra felhatalmazott – jogosultsággal rendelkező – felhasználó és csak vezetékes LAN-kapcsolatról végezhet bárminemű konfigurációs tevékenységet a vezeték nélküli hálózatot illetően.	5	5	5	Adminisztrációs célra szeparált, dedikált VLAN használata, amely VLAN-nak csak vezetékes végpontjai vannak, és csak ebből a VLAN-ból lehetséges a vezeték nélküli hálózat konfigurálása.
3.3.10.14.4.	Antennák	A Szervezet olyan antennákat és árnyékolási megoldásokat alkalmaz, amelyek csökkentik a jelek észlelésének esélyét külső fél számára.	5	5	5	A legfelső biztonsági szinten szükség van speciális védelmi intézkedésekre, például az elektronikai felderítés elleni védelemre. A jelek külső fél általi észlelésének az esélye csökkenthető: - Az eszközök sugárzásának korlátozásával (természetesen csak ameddig nem veszélyezteti az elsődleges használati célját). A korlátozás lehet időbeli, térbeli vagy teljesítménybéli. - Árnyékolási technikákkal. Jellemzően különböző fémezett szövetekkel oldható meg az árnyékolás. A fentieken túl a legfelkészültebb iparágak (jellemzően a hadiipar) irányított antennákat, mobil antennákat vagy akár megtévesztő antennákat is használhatnak.

Forrás: Nemzeti Kibervédelmi Intézet 2021

[15] Nemzeti Kibervédelmi Intézet 2021.

A 41/2015. (VII. 15.) BM rendeletben az egyetlen pont, ahol vezetékes hálózatot említik, az a következő:

> „3.10.14.3. Felhasználó konfigurálás tiltása
> Az érintett szervezet azonosítja a felhasználókat, és csak közvetlen jogosultság birtokában, a védett hálózaton kialakított vezetékes kapcsolaton keresztül teszi lehetővé számukra a vezeték nélküli hálózat független konfigurálását."[16]

Ám ebben a pontban is csupán említés szintjén jelenik meg és a védett hálózat részének tekinti a teljes vezetékes hálózatot.

Speciálisan a hírközlési szolgáltatók hálózatára és kifejezetten azok vezetékes hálózati elemeire külön utalás a 41/2015. (VII. 15.) BM rendeletben nem található.

A fentiekből megállapítható, hogy hazánkban jelenleg csupán a vezeték nélküli hálózatokra vannak speciális követelmények, kontrollpontok, a vezetékesre pedig nem, a hírközlési szolgáltatók esetében pedig specifikus követelményeket nem találunk.

NIST 800-53

A NIST az Egyesült Államok legrégibb fizikai kutató laboratóriuma, amely ma a Kereskedelmi Minisztérium alatt, szövetségi ügynökségként dolgozik. A honlapjukon is közzétett küldetésük az, hogy támogassák az Egyesült Államok beruházásait és ipari versenyképességét olyan tudományok, szabványok és technológiák fejlesztésével, amelyek segítségével javul az ország gazdaságbiztonsága és az itt élő emberek életminősége. Elért eredményeiket számos területen kamatoztatják, így az egészségügyi nyilvántartásoktól kezdve az atomórákon és nanoanyagokon át a számítógépes chipekig számtalan termék és szolgáltatás használja a NIST által kidolgozott technológiákat, szabványokat. A szervezet meghatározó szerepet játszik az infokommunikációs rendszerekkel és azok biztonságával kapcsolatos szabványok és ajánlások kidolgozásában is.[17]

Ez utóbbi kapcsán a NIST számos dokumentumot készített, amelyek a kritikus biztonsági elemek azonosításában is segítenek. Az infokommunikációs rendszerekkel kapcsolatban megjelentetett dokumentumai közül a téma szempontjából kiemelendő kategóriák:

- NIST Special Publication 500 Series, amelyben a különböző szabványokhoz és referenciaarchitektúrákhoz kapcsolódó anyagokat teszik közzé;[18]
- NIST Special Publication 800 Series, amelyben a biztonsági kérdésekkel foglalkozó anyagok találhatók. A sorozat iránymutatásokat, ajánlásokat, műszaki előírásokat és éves jelentéseket tartalmaz a NIST kiberbiztonsági tevékenységeiről. Az SP 800 kiadványokat az Egyesült Államok szövetségi kormánya információi és információs rendszerei biztonságának és adatvédelmi igényeinek kielégítésére és támogatására fejlesztették ki;[19]

[16] 41/2015. (VII. 15.) BM rendelet.
[17] National Institute of Standards and Technology: www.nist.gov
[18] Lásd: www.nist.gov/system/files/documents/2018/08/07/SP500LIST_2005-present_GOOD-ONE-8.pdf
[19] Lásd: www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

- NIST Special Publication 1800 Series, amelyben praktikus, használható kiberbiztonsági megoldásokat mutatnak be.[20]

Ezek közül a cikk célkitűzése szempontjából a legfontosabb a NIST 800-53,[21] amely az információs rendszerek szervezetek által használandó biztonsági és adatvédelmi kontrollok egyfajta katalógusa.

A NIST 800-53 meghatározza a Federal Information Processing Standard (FIPS) által megkövetelt biztonsági ellenőrzések minimális alapszintjét is az összes egyesült államokbeli szövetségi információs rendszerre vonatkozóan (kivéve a nemzetbiztonsággal kapcsolatos rendszereket), de ajánlásként szolgál más szervezet, így más országok szervezetei számára is. A NIST 800-53 első változatát 2005-ben adták ki, jelenleg már az ötödik verziója, az úgynevezett rev5 van hatályban. [A korábban említett 41/2015. (VII. 15.) BM rendelet is a NIST 800-53-on, bár annak egy korábbi verzióján alapszik.] A NIST 800-53 amellett, hogy tartalmazza információs rendszerek különböző fenyegetések – a természeti katasztrófáktól az ellenséges támadásokig – elleni védeleméhez alkalmazható biztonsági és adatvédelmi kontrollokat, még a megfelelő védelem kialakításához szükséges kontrollok kiválasztásához, értelmezéséhez szükséges útmutatást is biztosítja a felhasználók számára. Az egyes szervezeteknek ugyanis a saját rendszereik és az azokban tárolt adatok ismerete és a felhasználás célja alapján kell kiválasztaniuk az alkalmazandó kontrollokat. Ehhez természetesen szükség van az általuk elvégzett gondos kockázatértékelésre és a lehetséges incidenseknek az információs rendszereikre gyakorolt hatásainak elemzésére.

A NIST 800-53 rev.5 több mint 100 kontrollpontot tartalmaz, amelyeket további kategóriákba soroltak a készítők. Ezeket az alábbi, 4. táblázat mutatja be:

4. táblázat: NIST 800-53 kontrollkategóriái

ID	Kategória	Példák az ellenőrzésekre
AC	Hozzáférés-ellenőrzés	Fiókkezelés és -figyelés; legkisebb jogosultság elv betartása; a feladatok elkülönítése
AT	Tudatosság és képzés	A biztonsági fenyegetésekkel kapcsolatos felhasználói képzés; műszaki képzés a magasabb szintű jogosultsággal rendelkező felhasználók számára
AU	Ellenőrzés és elszámoltathatóság	Az ellenőrzési feljegyzések tartalma; elemzés és jelentéstétel; a feljegyzések megőrzése
CA	Értékelés, engedélyezés és felügyelet	Kapcsolódás nyilvános hálózatokhoz és külső rendszerekhez; behatolásvizsgálat
CM	Konfigurációkezelés	Engedélyezett szoftverpolitikák, konfigurációváltoztatás-ellenőrzés
CP	Vészhelyzeti tervezés	Alternatív feldolgozási és tárolási helyszínek; üzletmenet-folytonossági stratégiák; tesztelés
IA	Azonosítás és hitelesítés	A felhasználókra, eszközökre és szolgáltatásokra vonatkozó hitelesítési irányelvek; hitelesítő adatok kezelése
IP	Egyéni részvétel	Hozzájárulás és adatvédelmi engedélyezés

[20] Lásd: www.nist.gov/itl/publications-0/nist-special-publication-1800-series-general-information
[21] NIST 2020.

ID	Kategória	Példák az ellenőrzésekre
IR	Incidenskezelés	Incidensreakció-képzés, felügyelet és jelentéstétel
MA	Karbantartás	Személyzet és eszközök karbantartása
MP	Médiavédelem	Hozzáférés, tárolás, szállítás és médiahasználat
PA	Adatvédelmi engedély	Személyes adatok gyűjtése, felhasználása és megosztása
PE	Fizikai védelem	Fizikai hozzáférés; vészhelyzeti áramellátás; tűzvédelem; hőmérséklet-szabályozás
PL	Tervezés	Közösségi média és hálózati korlátozások; mélységében védett biztonsági architektúra
PM	Programmenedzsment	Kockázatkezelési stratégia; belső fenyegetések elleni program; vállalati architektúra
PS	Személyi biztonság	A személyzet átvilágítása, megszüntetése és áthelyezése; külső személyzet; szankciók
PI	Személyes adatokkal kapcsolatos eljárások és átláthatóság	Személyes adatok kezelési eljárásának dokumentálása; kezelhető személyes adatok körének meghatározása; hozzájárulások kezelése
RA	Kockázatértékelés	Sérülékenységvizsgálat; adatvédelmi hatásvizsgálat
SA	Rendszerek és szolgáltatások beszerzése	Rendszerfejlesztési életciklus; beszerzési folyamat; ellátási lánc kockázatkezelése
SC	Rendszer- és kommunikációvédelem	Alkalmazások particionálása; határvédelem; kriptográfiai kulcsok kezelése
SI	Rendszer- és információintegritás	Hibaelhárítás; rendszerfelügyelet és riasztás
SR	Ellátási lánc kockázatmenedzsment	NIST-modellekre épülő szállítókkal vagy szervezetekkel való megfelelés

Forrás: NIST 2020

A fenti kategóriákba tartozó kontrollpontok elemzésekor megállapítható, hogy a NIST 800-53 nem tartalmaz kifejezetten a vezetékes hálózatokra vonatkozó önálló kontrollpontokat, de a vezetékes hálózatot megemlíti az alábbi, 5. táblázatban szereplő pontokban:

5. táblázat: Vezetékes hálózat említése a NIST 800-53-ban

Kontrollpont	Ellenőrzés neve	Leírás	Vezetékes hálózat említése
SC-5	Denial-of-service védelem	Egy szolgáltatásmegtagadásos esemény számos belső és külső ok miatt bekövetkezhet, például egy ellenséges támadás vagy nem megfelelő tervezés miatt kialakuló kapacitás- és/vagy sávszélességhiány miatt. Ilyen típusú támadások a hálózati protokollok széles skáláján (pl. IPv4, IPv6) fordulhatnak elő. A szolgáltatásmegtagadási események keletkezésének és hatásainak korlátozására vagy kiküszöbölésére számos technológia, eszköz áll rendelkezésre.	A szervezet korlátozza az egyének azon képességét, hogy szolgáltatásmegtagadásos támadásokat indítsanak más rendszerek ellen. Ennek egyik része, hogy a szervezet korlátozhatja az egyének azon lehetőségét, hogy kapcsolódjanak és tetszőleges információkat továbbítsanak az átviteli közegen (pl. vezetékes hálózatokon).

Kontrollpont	Ellenőrzés neve	Leírás	Vezetékes hálózat említése
SC-43	Felhasználási korlátozások	Használati korlátozások és megvalósítási irányelvek megállapítása a szervezet által meghatározott rendszerelemekre, valamint az ilyen komponensek használatának engedélyezése, felügyelete és ellenőrzése a rendszeren belül.	A felhasználási korlátozások többek között minden vezeték nélküli és vezetékes perifériakomponenst érintenek. A használati korlátozások és megvalósítási irányelvek a rendszerelemek által a rendszerben okozott károk potenciális kockázatán alapulnak, és segítenek biztosítani, hogy csak az engedélyezett rendszerhasználat történjen.
SI-4	Rendszer-monitoring	A vezeték nélküli hálózatok alapvetően kevésbé biztonságosak, mint a vezetékes hálózatok, pl. lehallgatás ellen, ezért a vezeték nélküli hálózatból vezetékes hálózatba belépő forgalmat ellenőrizni kell.	A szervezet használjon behatolásérzékelő rendszert (intrusion detection system, IDS) a vezeték nélküli kommunikációs forgalom figyelésére, amikor a forgalom vezeték nélküli hálózatról vezetékes hálózatra halad át.

Forrás: NIST 2020

Összességében a NIST 800-53 kapcsán is elmondható, hogy kifejezetten a vezetékes hálózatokra és főképp a hírközlési szolgáltatókra vonatkozó speciális kontrollokat itt sem találunk.

ISO 27001

Az ISO/IEC 27001:2013[22] az a nemzetközi szabvány, amely keretrendszert biztosít az információbiztonsági irányítási rendszerek számára, hogy a szervezetek folyamatosan biztosítani tudják az információk és információs rendszerek bizalmasságát, sértetlenségét és rendelkezésre állását. Az ISO 27001 az egyetlen olyan információbiztonsági szabvány, amely alapján a szervezetek független auditált tanúsítást szerezhetnek. Ez szakértői biztosítékot nyújt a szervezetek számára, hogy az információbiztonságot a nemzetközi legjobb gyakorlatoknak megfelelően kezelik. A tanúsítás nem feltétlenül kell hogy az egész szervezetre vonatkozzon, akár egyes üzleti egységekre is lehet ilyen tanúsítást szerezni.

Az ISO/IEC 27002:2013 az ISO/IEC 27001:2013 szabványnak megfelelő ISMS[23] részekénti biztonsági ellenőrzések végrehajtására vonatkozó referencia. Az ISO 27001 előírja az ISMS specifikációját, beleértve a kockázatkezelési folyamatra vonatkozó követelményeket, amelyet a szervezet kockázatainak megfelelő biztonsági intézkedések kiválasztásához kell használnia.

A szabvány „A" mellékletében kaptak helyet azok a szabályzók, amelyek lefedik azon kontrollpontokat, amelyek fontos szerepet játszanak a szervezetek információbiztonságának megvalósításában. A szervezet az „Alkalmazhatósági nyilatkozatban" rögzíti, hogy mely kontrollpontoknak felel meg.

[22] Lásd: www.iso.org/isoiec-27001-information-security.html
[23] ISMS (information security management system) információbiztonsági irányítási rendszer (IBIR).

Az ISO 27002 keretrendszer az ISO 27001 „A” mellékletében felsorolt ellenőrzések alkalmazására vonatkozó bevált gyakorlatokra nyújt útmutatást. Támogatja az ISO 27001 szabványt, és azzal együtt kell olvasni, alkalmazni.

Az ISO kockázatkezelési keretrendszere is hasonló a NIST-éhez. A kockázatkezelést három lépésre bontják:

- a szervezet információit érintő kockázatok azonosítása;
- a kockázatnak megfelelő kontrollok kialakítása;
- a teljesítményük nyomon követése.

Az ISO 27001:2013 szabvány „A” melléklete 114 kontrollt sorol fel 14 ellenőrzési csoportra osztva, amelyek tartalmilag bővebben ki vannak fejtve az ISO 27002 szabvány 5–18. pontjai alatt.[24]

A 14 csoportot az alábbi, 6. táblázat ismerteti.

6. táblázat: ISO 27 001:2013 ellenőrzési csoportjai

Ellenőrzési csoport	Leírás
A.5 Információbiztonsági irányelvek	Az információbiztonságot a szervezet legfelsőbb szintjéről kell irányítani, és az irányelveket világosan közölni kell az összes alkalmazottal.
A.6. Az információbiztonság szervezete	Az irányítási keretrendszernek támogatnia kell a szervezet információbiztonsági műveleteit, mind a szervezeten belül, mind azon kívül.
A.7. Személyi biztonság	Az alkalmazottaknak és az alvállalkozóknak tisztában kell lenniük a szervezet információinak védelmében betöltött szerepükkel a foglalkoztatás előtt és alatt.
A.8 Vagyonmenedzsment	A szervezeteknek azonosítaniuk kell fizikai és információs eszközeiket, és meg kell határozniuk az egyes eszközökhöz szükséges megfelelő védelmi szintet.
A.9 Hozzáférés-szabályozás	Az információkhoz és az információfeldolgozó eszközökhöz való hozzáférés korlátozása. Biztosítani kell a rendszerekhez és szolgáltatásokhoz való hozzáférést a jogosult felhasználók számára, és meg kell előzni a jogosulatlan hozzáférést. A felhasználókat elszámoltathatóvá tenni a saját felhasználói azonosságkezelési információik védelméért. Meg kell akadályozni a felhatalmazás nélküli hozzáférést rendszerekhez és alkalmazásokhoz.
A.10 Titkosítás	A kriptográfiára és a kriptográfiai kulcsok használatára vonatkozó szabályzatokat kell kidolgozni, és végre kell hajtani az információk titkosságának, integritásának és/vagy rendelkezésre állásának védelme érdekében.
A.11 Fizikai biztonság	Ellenőrzéseket kell bevezetni az információfeldolgozó létesítményekhez való illetéktelen fizikai hozzáférés, károsodás és zavarás megakadályozása érdekében.
A.12 Üzembiztonság	Az információkat és az információfeldolgozó létesítményeket védeni kell a rosszindulatú szoftverektől, az adatvesztéstől és a technikai sebezhetőségek kihasználásától.
A.13 A kommunikáció biztonsága	Az információkat védeni kell a hálózatokban és az információ továbbítása során, mind a szervezeten belül, mind azon kívül.
A.14 A rendszer beszerzése, fejlesztése és karbantartása	Az információbiztonságot az információs rendszerek teljes életciklusa alatt kell megtervezni és meg kell valósítani, így már a tervezés, fejlesztés, beszerzés során is. A tesztadatokat is védeni kell.

[24] Lásd: www.itgovernanceusa.com/iso27002

Ellenőrzési csoport	Leírás
A.15 Szállítói kapcsolatok	A szervezet minden olyan információs eszközét, amelyhez a beszállítók hozzáférnek, megfelelően védeni kell.
A.16 Információbiztonsági incidensek kezelése	Az információbiztonsági incidenseket következetesen és hatékonyan kell kezelni.
A.17 Üzletmenet-folytonossági menedzsment információbiztonsági szempontjai	Az információbiztonság folytonosságát be kell ágyazni a szervezet működésfolytonosság-irányítási rendszereibe.
A.18 Követelményeknek való megfelelőség	Az információkat úgy kell védeni, hogy azok megfeleljenek a jogi, törvényi, rendeleti és szerződéses kötelezettségeknek, valamint a szervezet irányelveinek és eljárásainak.

Forrás: Irwin 2023

A kommunikációs biztonsággal, amelynek célja az információ védelme a hálózatokban, valamint annak továbbítása során, az A.13 melléklet[25] foglalkozik. Ebben a vezetékes és a vezeték nélküli hálózatokkal kapcsolatos releváns elemek a következők (7. táblázat).

7. táblázat:Vezetékes és vezeték nélküli hálózatokkal kapcsolatos elemek

Kontrollpont	Leírás
A.13.1 A hálózati biztonság menedzsmentje	A hálózatban lévő információk és az azokat támogató információ-feldolgozó létesítmények védelmének biztosítása.
A.13.1.1 Hálózati intézkedések	A hálózatokat menedzselni kell, hogy védjük az információkat a rendszerekben és az alkalmazásokban.
A.13.1.2 A hálózati szolgáltatások biztonsága	Minden hálózati szolgáltatásra meg kell határozni a biztonsági mechanizmusokat, a szolgáltatási szinteket és az irányítási követelményeket, beleértve a hálózati szolgáltatási megállapodásokat függetlenül attól, hogy ezeket a szolgáltatásokat házon belülről vagy kiszervezett formában nyújtják.
A.13.1.3 Elkülönítés a hálózatokban	A hálózati szolgáltatások, a felhasználók és az információs rendszerek csoportjait el kell különíteni a hálózatokban.

Forrás: Irwin 2023

Az ISO/IEC 27001 és az ISO/IEC 27002[26] egyaránt felülvizsgálat alatt áll, előreláthatólag 2022 közepe táján jelennek meg a változások. Várhatóan azonban nem lesz ISO/IEC 27001:2022 név alatt új kiadás, hanem egy módosítást adnak ki ISO/IEC 27001:2013+A1:2022 néven.

Az egyik fő változása az lesz, hogy az „A" melléklet hivatkozik az ISO/IEC 27002:2022 szabványban szereplő kontrollokra, amely tartalmazza az adott kontroll címét és a kontrollt magát. Amíg az ISO/IEC 27002:2013 114 kontrollt tartalmaz 14 területen, az átdolgozás után az ISO/IEC 27002:2022 93 kontrollt tartalmaz majd 4 területen.

Összességében az ISO/IEC 27001 kapcsán is elmondható, hogy speciálisan a vezetékes elemekre vonatkozó kontrollok nem jelennek meg, és kifejezetten a hírközlési szolgáltatókra vonatkozó speciális kontrollokat pedig itt sem találunk.

[25] Lásd: https://infocerts.com/iso-27001-annex-a-13-communications-security/
[26] Lásd: www.iso.org/standard/75652.html

Összefoglaló, tanulságok

A vezetékes és vezeték nélküli hálózatok nagy kiterjedése és összetettsége kihívást jelent a biztonsági szakemberek számára. Igaz ez a hírközlési hálózatokra is. A releváns, már konkrét kontrollokat is tartalmazó hazai jogszabályok és angolszász ajánlások áttekintését követően elmondható, hogy ezek komplex megközelítést alkalmaznak és jellemzően szervezetek saját információs rendszereinek védelmére fókuszálnak. Ennek megfelelően jellemzően csupán az egyébként biztonsági szempontból több figyelmet követelő vezeték nélküli szakaszokra, rendszerelemekre kerültek be speciális kontrollok, speciálisan a vezetékes hálózati elemek védelmére szolgáló kontrollokkal nem igazán lehet találkozni. Mint ahogy a hírközlési szolgáltatók infrastruktúra-elemeinek védelmét szolgáló speciális kontrollokkal sem, bár hazánkban az Ibtv. elektronikus információs rendszernek tekinti ezeket is, amelyeket ugyanazon elvek szerint, ugyanazon kontrollok segítségével szükséges védeni.

Ha megnézzük, hogy ma milyen veszélyek fenyegetik, fenyegethetik a hírközlési szolgáltatók vezetékes rendszereit, rendszerelemeit, akkor azt látjuk, hogy széles a paletta. Az optikai kábelek munkálatok (például építés vagy mezőgazdasági tevékenység) közbeni elvágásától az optikai kábelek meghajlításával való információkicsatolásig széles a skála. Éppen ezért célszerű tovább vizsgálni és felmérni, hogy milyen veszélyek fenyegetik pontosan a hírközlési szolgáltatók nagy kiterjedésű vezetékes rendszereit, rendszerelemeit, ezek mekkora problémát okozhatnak a szolgáltatóknak és a felhasználóknak, majd amennyiben szükséges, ajánlásokat, kontrollokat fogalmazni meg ezek kivédésére, enyhítésére.

Irodalomjegyzék

Irwin, Luke (2023): ISO 27001 Annex A controls explained. IT Governance, 2023. január 6. Online: www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained

Khandelwal, Swati (2019): Security Flaws in WPA3 Protocol Let Attackers Hack WiFi Password. *The Hacker News,* 2019. április 10. Online: https://thehackernews.com/2019/04/wpa3-hack-wifi-password.html

Kovács Zoltán (2021): *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai.* Budapest: Ludovika.

Muha Lajos (2015): *A kritikus információs infrastruktúrák védelme.* (h. n.): Relnet Technológia Kft. Online: http://real.mtak.hu/78935/1/A_kritikus_informacios_infrastrukturak_vedelme_u.pdf

NIST (2020): *NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations.* (h. n.): National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.SP.800-53r5

NMHH (2022a): *A Nemzeti Média és Hírközlési Hatóság helyhez kötött piaci jelentése.* 2018. IV. – 2022. II. negyedév. Nemzeti Média- és Hírközlési Hatóság. Online: https://nmhh.hu/dokumentum/234021/helyhez_kotott_piaci_jelentes_2018_negyedik_2022_masodik_negyedev.pdf

NMHH (2022b): *A Nemzeti Média és Hírközlési Hatóság mobilpiaci jelentése.* 2018. IV. – 2022. II. negyedév. Nemzeti Média- és Hírközlési Hatóság. Online: https://nmhh.hu/dokumentum/233271/mobilpiaci_jelentes_2022_elso_felev.pdf

Jogi források

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

Nemzeti Kibervédelmi Intézet (2021): *Felhasználói kézikönyv* a 41/2015. BM rendelet által meghatározott védelmi intézkedésekhez. 2021. december. Online: https://nki.gov.hu/wp-content/uploads/2021/12/Felhasznaloi-kezikonyv-vedelmi-intezkedesekhez-v1.0.pdf

NEMZETBIZTONSÁGI SZEMLE
11. évfolyam (2023) 1. szám 21–33. • DOI: 10.32561/nsz.2023.1.2

Márton Balázs[1]

A NIBEK-től a Nemzeti Információs Központig – nemzetbiztonsági fúziós központok Magyarországon

From NIBEK to the National Information Centre – National Security Fusion Centres in Hungary

Az 1990-es rendszerváltozást követően, egy hosszú állandóságot jelentő időszak után, a 2010-es évek elején, majd 2022 júniusában került sor Magyarország nemzetbiztonsági intézményrendszerének jelentősebb átalakítására. Nemzeti Információs Központ elnevezéssel a nemzetbiztonsági rendszer egészére teljeskörűen kiterjedő információfúziós központ létesült. Magyarországon már korábban is voltak a fúziós központok bizonyos jegyeit magukon viselő állami szervek. Történeti időrendben és folytonosságukban való áttekintésük alátámasztja azt a felvetést, hogy e szervezetek alakításával a jogalkotó a biztonságpolitikai környezet változásához szándékozik igazodni. A jelenlegi korszakot és feltehetőleg a következő éveket meghatározó tartós válsághelyzeti működés egy, az eddigieknél hatékonyabb kapacitás kiépítését igényelte.

Kulcsszavak: *nemzetbiztonság, fúziós központ, rendészet, biztonság, védelem, belügy, együttműködés, titkosszolgálat*

Following the political regime change in 1990, after a long period of permanence, significant transformation has been made, regarding the institutional structure of the national security of Hungary, in the early 2010s, and then in June 2022. Fusion centre called Centre of National Information was established that is fully encompasses the whole system of national security. State organs with certain characteristics of fusion centres had already been existed in Hungary earlier. An overview of their historical chronology and continuity is able to demonstrate the hypothesis that the legislator intends to adapt these organisations to the changing security policy environment.

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Rendészettudományi Doktori Iskola, e-mail: marbal@t-online.hu

The sustained crisis response that has defined the current era and, presumably, the forthcoming period, has required a more effective capacity to be built up.

Keywords: *national security, fusion center, law enforcement, security, defence, internal affairs, cooperation, secret service*

A fúziós központokról általában

A bipoláris világrend megszűnése utáni átmeneti időszakot követően gyökeresen megváltozott a világ biztonságpolitikai fenyegetéseinek karakterisztikája. A teljesség igénye nélkül, a globalizáció előrehaladása, az információs társadalom kialakulása, a brutális technológiai fejlődés, a koronavírus-járvány és az orosz–ukrán háború kiváltó okai és egyúttal következményei is e változásnak. Népszerű és gyakran használt jelző manapság a hibrid szó, amely jól alkalmazható az általános biztonsági környezet megváltozására. Nagy számban jelentek meg olyan biztonságot veszélyeztető tényezők, amelyeket a Barry Buzan, Ole Wæver és Jaap de Wilde munkásságának köszönhetően öt szektorra (katonai, politikai, gazdasági, társadalmi, környezeti) osztott biztonsági koncepció szektoraihoz nehéz lenne egyértelműen besorolni, vagyis hibrid tényezők.[2] Ezek a folyamatok kombinálva a korunk nemzetközi rendjét Klaus Schwab szerint formáló interdependencia, sebesség és komplexitás hármasával[3] együttesen azt eredményezik, hogy a biztonságot veszélyeztető tényezők intenzitása az államokban – így Magyarországon is – általánosan emelkedett, ezért állandósult válsághelyzetek alakulhatnak ki.[4]

A biztonságot veszélyeztető tényezők ilyen módú változása és komplexitása folytán elengedhetetlenné vált a különböző területekre vonatkozó információk gyors, pontos és egységes kezelése, a többféle forrásokból érkező információk egybeolvasztása, fúziója. Erre a célra az államok fúziós információs központokat, vagy más néven információegyesítő és információmegosztó központokat létesítettek.[5] A fúziós központok koncepciójának gyökerei egészen az 1990-es évekre, az Amerikai Egyesült Államokba vezetnek vissza.[6] A kutatói körökben kialakult többségi álláspont szerint az 1996-ban a Los Angeles-i megyei rendőrség keretein belül létrehozott terrorizmusra vonatkozó előrejelzési központ (Los Angeles County Terrorism Early Warning Center) tekinthető az első fúziós központnak.[7] Jóllehet a terrorizmus mint nemzetközi és összetett biztonságot fenyegető tényező erősödése és a 2001. szeptember 11-i New York-i terrortámadás eredményezte a fúziós központok proliferációját és szélesebb körben való ismertté válásukat.

A szakirodalomban található definíció viszonylag tágra szabott és általános leírást ad a fúziós központokról. Gudrun Persson szerint a fúziós központok olyan entitások,

[2] Gazdag–Remek 2018.
[3] Schwab–Malleret 2020: 21–31.
[4] Gazdag–Remek 2018: 38.
[5] Jensen–McElreath–Graves 2017: 99.
[6] Masse–O'Neil–Rollins szerk. 2008: 15.
[7] Monahan 2010.

amelyekben a hírszerző és biztonsági közösség különböző egységei más ügynökségekkel közösen dolgoznak egy vagy több fenyegetés ellen.[8] A fúziós központok az egyes rendészeti, nemzetbiztonsági szerveknél szétszórtan meglévő információk újszerű kezelését tették lehetővé azáltal, hogy az ott dolgozók az információk elemzésével, valamint megosztásával képesek korai előrejelzésre, és az egyes közigazgatási intézmények, döntéshozók számára ajánlásokat fogalmazhatnak meg az új típusú fenyegetések kezelésére.[9] Persson meghatározásán túl még néhány olyan speciális tulajdonságot találhatunk, amelyek a fúziós központok többségére jellemzők. Ilyenek (a) a jelentős nyilvántartó kapacitások és adattárak megléte, (b) a képesség információfeldolgozó és elemző-értékelő tevékenység végrehajtására, (c) szoros összeköttetés a rendészeti és más szervekkel (ideértve a hírszerző és [állami] biztonsági közösség egyéb szerveit), aminek érdekében a központok kapcsolattartó pontokat is működtethetnek. (d) Az információk elsősorban terrorelhárításra, illetve a szervezett bűnözésre fókuszálnak, de a szélesebb értelemben vett nemzetbiztonsági és bűnüldözési spektrumra is kiterjeszthetők. (e) Elemzéseik és jelentéseik terjesztése legtöbbször a kormányzati tájékoztatást célozza, de előfordul, hogy ezeket az együttműködő szervekkel (partnerszolgálatokkal) is megosztják. (f) Kiegészítő funkcióként műveleti támogató és/vagy koordináló hatásköröket is gyakorolhatnak.[10]

A 2001-es eseményeket követően az euroatlanti térség országaiban egymás után létesültek a fúziós központok, eleinte kifejezetten a terrorizmus elleni fellépés hatékonyságának növelése céljából. Ahogyan arra Andrékó Gábor rámutat, a kétezres évek első felében alapított szolgálatokkal kapcsolatos szemléletmód az elnevezésükben is tetten érhető volt, a terrorral és az ellene való fellépéssel kapcsolatos jelzővel minden szervezet megkülönböztette magát az érintett állam más nemzetbiztonsági szerveitől. Körülbelül 2010-től kezdődött az az új fejlődési szakasz, amelyben e szervezetek működésében már hangsúlyosabban jelentek meg az államok biztonságát érintő további kihívások, amelyek túlmutattak a terrorizmussal kapcsolatos feladatokon. A döntéshozók felismerték, hogy a változó biztonsági környezetben nehézkes lehet elválasztani a terrorizmust a szervezett bűnözéstől, illetve magát a terrorfelderítést az egyéb irányokban folytatott titkos információgyűjtéstől.[11] Ez a felismerés vezetett ahhoz, hogy a szektorális helyett/mellett horizontális nemzetbiztonsági fúziós központok létesültek.

A horizontális nemzetbiztonsági fúziós központokra egyaránt igazak azok az alapvetések, amelyek a szektorális szervezetekre. Ezek az általános jellemzők a következők. (a) Elsődleges céljuk és feladatuk a kormányzati tájékoztatási tevékenység. A másik alapvető feladatuk az együttműködő szervek támogatása. Ennek az alapját a rendelkezésükre álló, és az együttműködő szervekhez képest szélesebb adatkörön megvalósított (úgynevezett összadatforrású) elemzői kapacitások biztosítják. (b) A fúziós központok a kormányzati döntéshozatali szerveknek alárendelten működnek. A partnerszervezetekkel való viszonyukban funkcionális feladatmegosztás érvényesül, amelybe gyakran beletartozik a partnerszolgálat oldalán keletkező információmegosztási

8 Persson 2013: 2.
9 Cieleszky–Kiss 2020: 66.
10 Sáfrán 2019: 84.
11 Andrékó 2021: 30–31.

kötelezettség, amelynek célja, hogy biztosítsa a hírszerző/biztonsági közösség által összegyűjtött információk rendelkezésre állását a fúziós központban. Ez a viszonyrendszer nem feltétlenül jelent közigazgatási jogi értelemben vett irányítási vagy felügyeleti jogokat, van, hogy „csak" jogszabály kötelezi az együttműködő szerveket az adatközlésre, amely a gyakorlatban *primus inter pares* helyzetet teremt. Az együttműködő szerveket tehát szinte minden esetben kógens jogszabályi rendelkezések kötik meghatározott információk fúziós központtal való megosztására, ezáltal is törekedve arra, hogy az információmegosztási hajlandóságot hátrányosan érintő, nem kívánt rivalizálást csökkentsék. (c) Az állami végrehajtó hatalom (kormányzat) a fúziós központ feletti közvetlen irányítási jogokat gyakorol (vö. előző pontok), a központok gyakran szervezetileg is vertikális módon tagozódnak be a rendészeti/nemzetbiztonsági igazgatás rendszerébe, ezáltal biztosítva az információmegosztási hajlandóság ellenőrizhetőségét és az elsődleges feladat ellátását. (d) A fúziós központ elsődlegesen a kormányzati döntéshozó által megfogalmazott hírigénynek megfelelő információk összegyűjtését, szükség esetén feldolgozását és továbbítását végzi. (e) Saját műveleti tevékenységet nem folytat, amely általános szabály alól vannak kivételek, amire példa a magyar fúziós központ (lásd lentebb). Az adatkezelésébe tartozó információkat az együttműködő szervektől szerzi be, amelyek között rendészeti és nemzetbiztonsági szervek, de van, hogy a közigazgatás rendszerén kívüli bűnüldöző szervezetek (például ügyészségi szervek) is megtalálhatók.[12] A következőkben a fúziós központok magyarországi kialakulását és fejlődéstörténetét tekintjük át a politikai szintig. Nem foglalkozunk részletesen a kormányzaton belül található, nemzetbiztonsági feladatokat végző szereplőkkel. Noha fontosnak tartjuk itt megjegyezni, hogy Magyarországon a koordinált hírszerzési együttműködés és a kormányzati becsatornázás folyamatában kulcsszerepet játszik a Miniszterelnöki Kabinetiroda szervezetén belül működő nemzeti információs államtitkár (NIÁT).[13] A NIÁT végzi a Kormány tagjai hírigényének gyors, hatékony eljuttatását a hírszerző, vagy azzal összefüggő tevékenységet végző szervek, így a fúziós központ felé, illetve a hírszerzési információkat eljuttatja a jogosult állami vezetők részére. Feladata azonban nem merül ki az információ „egyszerű" továbbításában, ennél jóval összetettebb. Nevezetesen, a Kormány tagjai által megfogalmazott információigényeket „átfordítja" a nemzetbiztonsági szakma nyelvére, meghatározza a főbb elemzési fókuszpontokat stb.[14]

A fúziós központ jogelődje Magyarországon: a Szervezett Bűnözés Elleni Koordinációs Központ (SZBKK)

Magától értetődik, hogy a nemzetközi biztonsági környezet változása hazánk biztonságpercepciójára is hatással van. Az előzőekben nagyvonalakban felvázolt, a fúziós központok kialakulására vonatkozó fejlődési folyamat nálunk is lezajlott, viszont ennek

[12] Márton 2021.
[13] 4/2022. (VI. 11.) MK utasítás.
[14] Hódos 2018.

ívét egyaránt árnyalták a hazai történelmi sajátosságok és a belbiztonsági környezet alakulása. Az 1990-ben bekövetkező rendszerváltoztatás után ugrásszerűen emelkedett a regisztrált bűncselekmények száma. Amíg a számuk 1990-ben 341 ezer körül volt, 1998-ban már a 600 ezret is átlépte.[15] Hovatovább, a nemzetközi bűnözői körök aktivitása emelkedett, és egyre nagyobb teret hódított a szervezett bűnözés. Az 1990-es évek második felében a lakosság olyan új jelenségeket élt meg, mint a szervezett bűnözői körök területfelosztó háborúja, a tömeges prostitúció, leszámolások, robbantásos merényletek stb.[16] Ebből kifolyólag szükségessé vált az összehangoltabb, koncentráltabb állami fellépés, a gyors és célirányos információcsere, amelyhez meg kellett szüntetni az indokolatlan párhuzamokat és átfedéseket. Ezért döntöttek egy önálló központi hivatal létrehozásáról, amely a Kormány irányítása alatt állt, négy tárca felelősségi körét érintette és tíz szervezet működéséhez kapcsolódott, de azoktól szervezetileg elkülönült.

A Belügyminisztérium alá rendelt szervezet neve Szervezett Bűnözés Elleni Koordinációs Központ (SZBKK) volt, és a bűnüldözési információk elemző-értékelő feldolgozását végezte, ezzel támogatva az együttműködő szervezetek tevékenységét.[17] Az SZBKK magán viselte a mai értelemben vett fúziós központok bizonyos jegyeit. A kormányzat irányítása alatt állt, és feladatai közé tartozott a kormányzati döntéshozatal támogatása, illetve a politikai döntéshozó tájékoztatása.[18] Az SZBKK-nak az együttműködő szervek felé koordinatív célú javaslattételi, értesítési és adattovábbítási jogosítványai voltak.[19] Az együttműködő szervek közé tartozott az összes korabeli nemzetbiztonsági szolgálat, a polgáriakat és a katonaiakat is ideértve, illetőleg a rendészeti szervek.[20] Mindazonáltal a következők miatt mégsem tekinthetjük az SZBKK-t adekvát értelemben vett fúziós központnak. A jogalkotó, bár kötelezte az együttműködő szerveket az SZBKK részére történő adatküldésre, ez alól olyan kivételt engedett, amely akár alkalmas lehetett arra is, hogy esetenként *de facto* az együttműködő szervezetet felügyelő miniszter adatmegosztással kapcsolatos diszkrecionális döntéséhez vezessen. Az együttműködő szervnek kivételesen, egyedi esetben, a forrás életének, testi épségének közvetlen veszélyeztetettsége esetén az együttműködő szervet irányító miniszter felmentést adhatott az adatközlés alól.[21] A koordinatív szerepkört az a rendelkezés nehezíthette, amely alapján az együttműködő szerv nemzetbiztonsági vagy kiemelt súlyú bűnüldözési érdekre tekintettel az átadott adat más együttműködő szervnek való megküldését megtilthatta, korlátozhatta, vagy előzetes hozzájárulásához köthette.[22]

Az SZBKK adatkezelését illetően fontos szűkítő körülmény volt, hogy mindezeket a jogalkotó kifejezetten csak a szervezett bűnözéssel kapcsolatba hozható jellemző bűncselekmények (például üzletszerű kéjelgés elősegítése, ha azokat bűnszervezet tagjaként követték el stb.) vonatkozásában tette lehetővé, és még ezek között is különbséget tett a büntetőeljárás elrendelését megelőzően és az ezt követően

15 Lásd: www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_zjb002.html
16 T/10307. számú törvényjavaslat Általános indokolás 34.
17 2000. évi CXXVI. törvény 1. §; 2000. évi CXXVI. törvény indokolása.
18 2000. évi CXXVI. törvény 11. § és 2. §.
19 2000. évi CXXVI. törvény 2. §.
20 2000. évi CXXVI. törvény 10. §.
21 2000. évi CXXVI. törvény 5. § (3).
22 2000. évi CXXVI. törvény 5. § (4).

továbbítható információkban.[23] A nemzetközi terrorizmus mint új jelenség előfordulása és a központ működésének első éveiből levont gyakorlati tapasztalatok 2005 decemberére indokolttá tették az SZBKK-t szabályozó törvény módosítását, amely módosítás eredményeként – egyebek mellett – a hatáskörei a terrorizmussal kapcsolatos bűncselekményekre is kiterjedtek.[24] Összességében a 2001. január 1-jétől működő központ 2007-re már több mint 15 ezer eljárás, 18 ezret meghaladó bűncselekmény, több mint 32 ezer célszemély és bűnös kapcsolatának adatait tartalmazta.[25] A magyar rendészettörténetben az SZBKK volt az első szervezet, amely deklaráltan információegyesítő, koordináló és stratégiai elemző feladatokra jött létre. Korlátozott mandátuma miatt inkább csak rendészeti fúziós központnak tekinthetjük. A központi hivatalként működő SZBKK a rendészeti közigazgatáshoz sorolandó, nem tartozott a nemzetbiztonsági szolgálatok közé.

A fúziós központ tervének megjelenése Magyarország nemzetbiztonsági szolgálatai között: a Nemzeti Információs és Bűnügyi Elemző Központ (NIBEK)

A rendszerváltoztatás óta állandósult nemzetbiztonsági struktúrában már régóta időszerű jelentősebb változtatásokat a 2010 utáni új kormányzat volt képes végrehajtani, hiszen rendelkezett a megfelelő politikai felhatalmazással ahhoz, hogy az érintett területeket részletesen szabályozó kétharmados törvények módosítását véghez vigye. Új rendvédelmi szervek jöttek létre, például a rendőrség terrorizmust elhárító szerveként a Terrorelhárítási Központ, vagy a polgári elhárítás szerve, a Nemzetbiztonsági Hivatal jogutódjaként az Alkotmányvédelmi Hivatal. A SZBKK korábban részletezett kialakításából fakadó gyengeségek a 2010-es évekre nyilvánvalóvá váltak, és a döntéshozók úgy látták, hogy az akkori jogszabályi környezetben és szervezeti formájában nem biztosítja az optimális működést és adatszolgáltatást.[26] Felismerték egy valódi nemzetbiztonsági fúziós központ hiányát, amely a bűnözéssel, a nemzetbiztonsági kockázatokkal összefüggő adatokat és információkat kormányzati szinten összesíti, szintetizálja, és a Kormány döntéseit összbiztonsági szemlélettel készült taktikai és stratégiai elemzésekkel, javaslatokkal segíti.[27] Egy 2011. novemberi törvényjavaslattal a nemzetbiztonsági szolgálatok körének módosítását indítványozták.[28] Az SZBKK alapjaira építve és annak jogutódjaként a Nemzeti Információs és Bűnügyi Elemző Központ (NIBEK) megalapítását irányozták elő, amely elődszervénél jóval szélesebb jogkörökkel és új feladatokkal egy valós és a fenti tulajdonságokat magán viselő fúziós

[23] 2000. évi CXXVI. törvény 4–6. §.
[24] 2006. évi XXVII. törvény.
[25] Istvanovszki 2008.
[26] T/5004. számú törvényjavaslat Általános indokolás, 48.
[27] T/5004. számú törvényjavaslat Általános indokolás, 48.
[28] T/5004. számú törvényjavaslat.

központ lett volna, amely a polgári nemzetbiztonsági szolgálatokért felelős miniszter (ekkortájt a belügyminiszter) irányítása alá tartozik.[29]

Az elgondolás szerint az együttműködő szervek köre az összes nemzetbiztonsági szolgálaton és a rendészeti szerveken túlmenően számos közigazgatási szervet is magában foglalt, például a közlekedési hatóságot és különböző nyilvántartó hatóságokat.[30] Az információmegosztás hiányából eredő esetleges kockázatokat kiküszöbölendő, a NIBEK az együttműködő szervekkel kiépített közvetlen elektronikus adatkapcsolat útján szerezte volna be a tevékenységéhez szükséges adatokat, ami lényegi változást jelentett volna az SZBKK együttműködő szervek aktív cselekvőségére hagyatkozó adatmegosztási szisztémájához képest.[31] Értelemszerűen az adatok köre már nem korlátozódott volna bizonyos bűncselekményekre, sőt, általában véve bűncselekményekre sem, hanem minden biztonsági, nemzetbiztonsági és bűnügyi adatra kiterjedt volna. Az adatáramlást korlátozó rendelkezések kizárólag a NIBEK koordinatív funkciójához tartozó, a NIBEK felőli adattovábbításhoz kivételes esetekben megkövetelt hozzájárulás formájában jelentkeztek.[32] A fúziós központokra jellemző módon a NIBEK titkos információgyűjtő tevékenység végzésére nem lett volna jogosult.[33] Ellenben új feladatként látta volna el a légi közlekedésről szóló törvénnyel összhangban utasinformációs egységként a légitársaságok által továbbított utasnyilvántartási és előzetes utasadatok (úgynevezett PNR[34]-adatok) kezelését, valamint értékelését és elemzését.

A NIBEK létrehozására vonatkozó törvényjavaslat politikai és szakmai vitákat is generált. A javaslatot számos kritika érte azért, hogy nem biztosítja megfelelően az alapjogok érvényesülését, vagy éppen túlzott adatvédelmi kockázatot jelent.[35] Olyan módosító indítványt is benyújtottak, amely szerint – tekintettel a szerv koordinációs és elemző-értékelő jellegére – nem kell biztosítani számára a „nemzetbiztonsági szolgálat" jogállást.[36] Végül – egy zárószavazást megelőző módosító indítványnak köszönhetően – nem került sor a NIBEK megalakítására, ennélfogva az SZBKK az akkori formájában működött tovább.[37] A SZBKK feladatai a 2015. január 1-jén hatályba lépett úgynevezett PNR törvénnyel[38] bővültek, ettől kezdve utasadat információs egységként (PIU[39]-egység) ellátta a PNR-adatok gyűjtését, elemzését, kezelését.

29 T/5004. számú törvényjavaslat 23. §.
30 T/5004. számú törvényjavaslat 27. §.
31 T/5004. számú törvényjavaslat 32. §.
32 T/5004. számú törvényjavaslat 32. § (3).
33 T/5004. számú törvényjavaslat 29. §.
34 *Passenger name record* – utasnyilvántartási adatállomány.
35 Nagycenki 2018; T/5004/24. számú módosító javaslat.
36 T/5004/22. számú módosító javaslat.
37 T/5004/43. számú zárószavazás előtti módosító javaslat.
38 2013. évi CXCVIII. törvény.
39 *Passenger Information Unit* – utasnyilvántartó hatóság.

Az első magyar fúziós központ: a Terrorelhárítási Információs és Bűnügyi Elemző Központ (TIBEK)

A 2015. november 13-án Párizsban történt terrortámadás-sorozatban dzsihádista öngyilkos merénylők hat helyszínen – egyebek között a Bataclan koncertteremben – több mint száz embert öltek meg. 2016. március 22-én az Iszlám Államhoz tartozó elkövetők a brüsszeli Zaventem repülőtéren, illetve a Maelbeek metróállomáson robbantottak, a támadások következtében 32 ember hunyt el. Az események következtében az európai országokban erősödött a terrorizmus megelőzésére összpontosító fellépés, ennek keretében hazánkban is törvénymódosításokra került sor.[40] A jogalkotó az SZBKK szervezett bűnözés elleni koordinációs feladatait terrorizmus elleni teendőkkel egészítette ki és az SZBKK-t átalakítva, a már meglévő kettő polgári és kettő katonai mellett, ötödik nemzetbiztonsági szolgálatként létrehozta a Terrorelhárítási Információs és Bűnügyi Elemző Központot (TIBEK). A törvény a TIBEK részére feladatul szabta – egyebek mellett – Magyarország biztonsági és bűnügyi helyzetének vizsgálatát, elemzését, a bűnügyi és terrorfenyegetettségi helyzet értékelését, közvetlen terrorfenyegetettség esetén biztonsági kérdésekben koordinációs tevékenység ellátását. Előzőeken túl kormányzati tájékoztató tevékenységet is ellátott. A politikai döntéstámogatás elősegítése érdekében nemzetbiztonsági, bűnügyi és terrorfenyegetettségi kérdésekben javaslatokat tehetett stratégiai döntések meghozatalára, időszerű feladatok ellátására, a terrorfenyegetettség szintjének meghatározására. Az együttműködő szervek számára hírigényeket szabhatott, illetve széles körű tájékoztató, támogató és koordinációs, illetve elemző-értékelő tevékenységet folytathatott.[41]

Az elemző-értékelő tevékenysége kiterjedt az együttműködő szervek hatáskörébe és illetékességébe utalt valamennyi információra, tehát nem korlátozódott csak a szervezett bűnözés vagy a terrorizmus körére. A TIBEK titkos információgyűjtés végzésére nem volt jogosult.[42] Az Nbtv.-ben rögzített hatáskörökből tisztán kirajzolódott, hogy a TIBEK megfelelt a fúziós központokról fentebb leírt általános és speciális kritériumoknak, ugyanakkor néhány olyan körülmény megemlítendő, amelyek ellensúlyozták a hatásköreinek hatékony gyakorlását.[43] A TIBEK a polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter irányítása alatt állt. A miniszter a TIBEK-en keresztül irányította az állami szervektől származó biztonsági és bűnügyi helyzetre vonatkozó információk elemzését, értékelését, valamint az e tárgyú kormányzati döntés-előkészítést támogató munkát.[44]

Bár a TIBEK Magyarország biztonsági és bűnügyi helyzetére vonatkozó vizsgálattal kapcsolatos hatásköréhez tartozott, hogy összeállítsa, aktualizálja, majd az együttműködő szervek irányába közvetítse a Kormány által megfogalmazott eseti és időszakos hírigényeket, tekintve, hogy a nemzetbiztonsági szolgálatok több miniszter irányítása alatt álltak, valójában a politikai döntéshozó hírigényei több

40 Nagycenki 2018: 98.
41 2016. évi LXIX. törvény 16. §.
42 2016. évi LXIX. törvény 22. §.
43 Márton 2021: 14–15.
44 2016. évi LXIX. törvény 18. §.

csatornán, a polgári hírszerzési tevékenység irányításáért felelős miniszter, a polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter vagy a honvédelemért felelős miniszter által irányított szolgálatokhoz, is érkezhettek, amelyek teljesíthették is ezeket, ennélfogva a rendszerben párhuzamosságok keletkezhettek. Ezek mindegyikét egy, az igazgatási hierarchiában egyenrangú fúziós központ sem lehetett képes feltárni. Ráadásul – ahogyan korábban már utaltunk rá – a szabályozás körülményeiből fakadóan az együttműködő szervek információmegosztási hajlandósága változó lehetett. A NIBEK-hez képest egyébként némileg csökkent az együttműködő szervek köre, néhány nyilvántartó hatóság kikerült, valamint a belső bűnmegelőzési és bűnfelderítési tevékenységet végző szerv ezen irányú feladataival kapcsolatos adatok beszerzésére nem volt lehetőség.[45] Noha a közvetlen elektronikus adatkapcsolat útján történő adatbeszerzés lehetősége fennállt, ez csak arra az esetre vonatkozott, ha az az együttműködő szerv törvényben meghatározott feladatainak hatékony ellátását nem veszélyezteti. Minden egyéb esetben az adathoz kizárólag kvázi megkereséssel juthatott hozzá a TIBEK.[46] Az SZBKK-hoz képest a TIBEK kétségkívül jelentős előrelépést jelentett az információfúziós központ evolúciójának hazai útján, de – részben a nemzetbiztonsági struktúrának és az ezt meghatározó szabályozásnak köszönhetően – valójában nem fejlődhetett a nemzetbiztonsági közösség csúcsszerveként funkcionáló, az amerikai Nemzeti Hírszerzési Igazgató Hivatalához (Office of the Director of National Intelligence) hasonló jogköröket gyakorló[47] szervezetté.

Az első valódi fúziós központ: a Nemzeti Információs Központ (NIK)

A 2022 februárjában kitört orosz–ukrán háború és az ennek következtében előálló gazdasági és energiaválság a megszokottól eltérő kontextusba helyezte Magyarország biztonsági környezetét, és ehhez illeszkedő, az új kihívásokhoz alkalmazkodni képes nemzetbiztonsági rendszert kívánt. 2022 májusában a nemzetbiztonsági struktúrában jelentősnek mondható átalakítás történt, aminek részeként a jogalkotó döntött a TIBEK jogutódlással történő megszüntetéséről és egy új nemzetbiztonsági fúziós csúcsszerv, a Nemzeti Információs Központ (NIK) létrehozásáról.[48] A NIK feladatai nagyrészt megegyeznek a TIBEK korábban ellátott feladataival, ugyanakkor néhány olyan módosítás történt, amelyek számottevő változást és feltehetőleg hatékonyságnövekedést eredményeznek.

A NIK Magyarország biztonsági és bűnügyi helyzetének vizsgálata során a nemzetbiztonságot érintően kiemelt kockázatot jelentő biztonsági fenyegetésekkel kapcsolatos kérdések vonatkozásában szakmai koordinációs tevékenységet lát el az érintett szervezetek bevonásával és kockázatelemzést is végez.[49] Érdemi változás, hogy a NIK már

45 2016. évi LXIX. törvény 28. §.
46 2016. évi LXIX. törvény 28. §.
47 Best 2010.
48 2022. évi IV. törvény 43. §.
49 2022. évi IV. törvény 30. §.

nem csak kormányzati tájékoztató tevékenységet lát el, a nemzetbiztonsági szolgálatok közül – a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott kivétellel, valamint az irányító miniszter igényén kívül – hírigényt csak a NIK teljesíthet.[50] Tekintve, hogy a polgári nemzetbiztonsági szolgálatok és a polgári hírszerzés irányításáért való felelősség a 2022-ben megalakult új kormányban már egyazon miniszter felelőssége, így a második kitétel a honvédelemért felelős miniszter irányítása alatt maradt katonai nemzetbiztonsági szolgálat vonatkozásában értelmezhető.[51] A hírigény eredményes teljesítése érdekében minden nemzetbiztonsági szolgálat részére kógens szabályként írta elő a törvény, hogy a feladataik ellátása során megszerzett, és a NIK hatásköreinek gyakorlásához szükséges információkat haladéktalanul kötelesek biztosítani a részére.[52] Ha a hírigény teljesítése érdekében szükséges, a NIK bármely együttműködő szervet az általa kezelt adatok kiegészítésére, pontosítására hívhatja fel, amelyet az együttműködő szerv köteles határidőn belül teljesíteni.[53]

A NIK megerősített szerepe tehát azt a célt szolgálja, hogy a hírigények teljesítése „egycsatornás" módon történjen, a hírigényre jogosult szerv vagy személy kizárólag a NIK-et irányító miniszter megkeresésével és a kért tájékoztatást is ezen az úton megkapva juthasson hozzá az igényelt információhoz.[54] Egyúttal valamennyi nemzetbiztonsági szolgálat esetében világossá tette a jogalkotó, hogy külső hírigényt nem teljesíthet. Annak érdekében, hogy a rendszerben az információk átadása zavartalan legyen, feltétlen adatátadási kötelezettséget rögzítettek a NIK részére.[55] A hírigény-teljesítési tilalom feloldása indokolt volt a katonai nemzetbiztonsági szolgálat vonatkozásában, amely feladatainak ágazati sajátossága – biztosítja a honvédelemért felelős miniszter által vezetett minisztérium és a Magyar Honvédség Parancsnoksága védelmi, hadászati-hadműveleti tervező munkájához szükséges információkat, valamint működteti Magyarország katonai egységes felderítő rendszerét[56] – erre logikus magyarázatot nyújt. A hírigény-teljesítési tilalom alkalmazandó a Nemzetbiztonsági Szakszolgálat (NBSZ) külső szerv megrendelésére végzett információgyűjtésből származó adataira, ebben az esetben az adatszolgáltatás kötelezettje a külső szerv lesz.[57] E rendelkezés indokának megértéséhez – egyebek mellett – elég csak arra gondolnunk, hogy az NBSZ megrendelői között a kormányzaton kívüli (ügyészségi) szervek is megtalálhatók. A fúziós központokra általában jellemző módon a NIK sem jogosult titkos információgyűjtést folytatni, ez alól egyetlen kivételt jelent a saját állománya tekintetében ellátott belső biztonsági és bűnmegelőzési célú ellenőrzési feladatok, továbbá kifogástalan életvitel ellenőrzésének végrehajtása.[58] Új hatáskörként a NIK

50 2022. évi IV. törvény 24. §.
51 182/2022. (V.24.) Korm. rendelet 9. §.
52 2022. évi IV. törvény 25. §, 27. §, 28. §.
53 2022. évi IV. törvény 32. § (3) *m)* pont.
54 2022. évi IV. törvény 28–34. §-hoz fűzött általános indokolása.
55 2022. évi IV. törvény 24. §-hoz fűzött általános indokolása.
56 2022. évi IV. törvény 28. §-hoz fűzött általános indokolása.
57 2022. évi IV. törvény 29. §.
58 2022. évi IV. törvény 39. §.

ellátja a vízummentes országokból a schengeni térségbe belépők monitorozására szolgáló ETIAS[59]-rendszerrel kapcsolatos nemzeti egység feladatait.[60]

Összegzés

A biztonsági környezet stabilitásának, kiszámíthatóságának csökkenése, komplex és hibrid fenyegetések fennállása esetén a döntéshozónak még inkább törekednie kell gyorsan alkalmazkodó, párhuzamosságokat és a töredezettséget nélkülöző, világos felelősségi viszonyokon alapuló nemzetbiztonsági szervezetrendszer működtetésére, mint „békeidőben". A kilencvenes években a demokratikus jogállami keretek kialakításának árnyékában egy-egy konkrét jelenségre elkülönülten reagálni képes intézmény felállítása kötötte le a kapacitásokat, viszont a romló belbiztonsági állapotok és a szervezett bűnözés jelenségeinek kezelése érdekében intézményesíteni kellett az együttműködést és a koordinációt. A legegyszerűbb megoldásnak egy központi hivatal felállítása mutatkozott, amely jellegét tekintve a szektorális (rendészeti) fúziós központ elgondolását tükrözte.

A kétezres években világszerte terjedő horizontális fúziós központokkal járó számtalan előny szele megérintette a hazai szakpolitikai döntéshozókat, akik kísérletet tettek egy valódi, nemzetbiztonsági horizontális információegyesítő centrum létrehozására. Azonban a biztonsági kihívások ekkor még más összképet mutattak, ahogyan Szenes Zoltán is rámutat, 2010-re az államközi háborúk szinte megszűntek, illetve a tőlünk távolabbi területeken zajló konfliktusok közvetlen hatásai még kevésbé voltak érezhetők hazánkban.[61] Köszönhetően részben a stabil nemzeti biztonsági környezetnek, hiányzott a megfelelő társadalmi-politikai szándék a nemzetbiztonsági *status quo* megváltoztatásához. A 2010-es évtized közepén az illegális migráció erősödése, a nemzetközi terrorizmus európai megjelenése már elég erős hatásnak mutatkoztak ahhoz, hogy bizonyítsák egy nemzetbiztonsági fúziós központ létjogosultságát. A TIBEK létrehozása mérföldkőnek bizonyult a fúziós központok magyarországi történetében, amely „papíron" már igényt tartott a rendészeti információk körét meghaladó nemzetbiztonságot érintő információkra is, elsősorban terrorelhárítási megfontolásokból. Mindazonáltal a szabályozás nem tette alkalmassá arra, ami végső soron egy fúziós központ igazi célja volna, azaz nem tudott megkerülhetetlen szűrővé válni a politikai döntéshozó irányába vezető hírigényt biztosító csatornán. Magyarország 2020. évi Nemzeti Biztonsági Stratégiája szerint

> „biztonsági környezetünk változásai olyan gyorsak, mélyrehatóak és alapvetőek, hogy egy új világrend kialakulásáról beszélhetünk. A világban zajló nagyléptékű gazdasági, társadalmi, demográfiai és környezeti változások és az egyre szűkösebb globális erőforrásokért folyó verseny jelentős feszültségek forrása. A változások elsődleges jellemzője, hogy azok sokszor összeolvadnak, felgyorsulnak és komplex kihívásokat generálnak".[62]

[59] European Travel Information and Authorisation System – Európai Utasinformációs és Engedélyezési Rendszer.
[60] 2022. évi IV. törvény 32. §.
[61] Szenes 2017: 82–83.
[62] 1163/2020. (IV. 20.) Korm. határozat 45.

A Nemzeti Információs Központtal egy olyan horizontális, a nemzetbiztonsági rendszer egészét átfogni képes fúziós központ jön létre, amely – egyéb feladatai mellett – a hírigény kizárólagos teljesítőjeként tájékoztatási (bemeneti) oldalon képes lesz észlelni a párhuzamosságokat, sőt akár ki is használni ezeket a „mozaikok" összeillesztésével, így szolgáltatva pontosabb, ellenőrzöttebb, gyorsabb információkat a kormányzati döntések meghozatalához. Kimeneti oldalon pedig immáron a szükséges felhatalmazás birtokában ténylegesen koordinálhatja a nemzetbiztonsági rendszer szereplőit.

Irodalomjegyzék

Andrékó Gábor (2021): A TIBEK – mint fúziós információs központ – centripetális hatása a magyar kormányzati döntésekre, különös tekintettel az értékelés és a tájékoztatás szerepére. *Nemzetbiztonsági Szemle,* 9(2), 29–43. Online: https://doi.org/10.32561/nsz.2021.2.3

Best, Richard A. Jr. (2010): *Intelligence Reform After Five Years: The Role of National Intelligence (DNI).* (h. n.): Congressional Research Service. Online: https://sgp.fas.org/crs/intel/R41295.pdf

Cieleszky Péter – Kiss Máté Attila (2020): Ébredő nemzedékek. *Nemzetbiztonsági Szemle,* 8(1), 62–73. Online: https://doi.org/10.32561/nsz.2020.1.4

Gazdag Ferenc – Remek Éva (2018): *A biztonsági tanulmányok alapjai.* Budapest: Dialóg Campus.

Hódos László (2018): Gondolatok a nemzeti hírszerző képesség koordinációjáért felelős szerv közjogi helyzetéről. *Szakmai Szemle,* 16(4), 5–16.

Istvanovszki László (2008): A Szervezett Bűnözés Elleni Koordinációs Központ helye, szerepe, tapasztalatai a határon átnyúló veszélyek és fenyegetések megelőzésében, kezelésében. *Felderítő Szemle,* 7(Különszám), 63–72.

Jensen, Carl J. – McElreath, David H. – Graves, Melissa (2017): *Bevezetés a hírszerzésbe.* Budapest: Antall József Tudásközpont.

Márton Balázs (2021): Fúziós központok az Európai Unióban – A bűnügyi és biztonsági információmegosztás uniós intézményei. *Nemzetbiztonsági Szemle,* 9(2), 3–19. Online: https://doi.org/10.32561/nsz.2021.2.1

Masse, Todd – O'Neil, Siobhan – Rollins, John szerk. (2008): *Information and Intelligence (Including Terrorism) Fusion Centers.* (h. n.): Nova Science Publishers Inc.

Monahan, Torin (2010): The Future of Security? Surveillance Operations at Homeland Security Fusion Centers. *Social Justice,* 37(2–3), 84–98.

Nagycenki Tamás (2018): Központokkal a szervezett bűnözés ellen. *Belügyi Szemle,* 66(9), 82–106. Online: https://doi.org/10.38146/BSZ.2018.9.5

Persson, Gudrun (2013): *Fusion Centres – Lessons Learned.* (h. n.): Swedish National Defence College – Center for Asymmetric Threat Studies.

Sáfrán József (2019): A Fúziós Központok és alapvető képességeik. *Nemzetbiztonsági Szemle,* 7(4), 83–95. Online: https://doi.org/10.32561/nsz.2019.4.7

Schwab, Klaus – Malleret, Thierry (2020): *Covid-19: The Great Reset.* Geneva: Forum Publishing.

Szenes Zoltán (2017): Katonai biztonság napjainkban. Új fenyegetések, új háborúk, új elméletek. In Finszter Géza – Sabjanics István (szerk.): *Biztonsági kihívások a 21. században.* Budapest: Dialóg Campus, 69–104.

Jogi források

2000. évi CXXVI. törvény a Szervezett Bűnözés Elleni Koordinációs Központról
2006. évi XXVII. törvény A Szervezett Bűnözés Elleni Koordinációs Központról szóló 2000. évi CXXVI. törvény módosításáról
2013. évi CXCVIII. törvény a nemzeti utasadat-információs rendszer létrehozása érdekében szükséges, valamint a rendőrséget érintő és egyes további törvények módosításáról
2016. évi LXIX. törvény a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról
2022. évi IV. törvény egyes törvényeknek a Magyarország minisztériumainak felsorolásáról szóló 2022. évi II. törvényhez kapcsolódó módosításáról
182/2022. (V. 24.) Korm. rendelet a Kormány tagjainak feladat- és hatásköréről
1163/2020. (IV. 20.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
4/2022. (VI. 11.) MK utasítás a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról
T/5004. számú törvényjavaslat az egyes rendvédelmi tárgyú törvények módosításáról, valamint az azzal összefüggő további törvénymódosításokról
T/5004/22. számú módosító javaslat
T/5004/24. számú módosító javaslat
T/5004/43. számú zárószavazás előtti módosító javaslat
T/10307. számú törvényjavaslat indokolással – a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról

NEMZETBIZTONSÁGI SZEMLE
11. évfolyam (2023) 1. szám 34–48. • DOI: 10.32561/nsz.2023.1.3

Budavári Krisztina[1]

A védelmi ipar és a nemzetbiztonság kapcsolata az aktuális 21. századi környezetben

National Security and the Defence Industry in the 21st Century

A globális biztonsági, gazdasági és technológiai környezetben zajló folyamatok következtében, számos hatás eredőjeként az országok védelmi ipari bázisai jelentősen felértékelődtek a 2010-es évektől kezdődően. Ugyanezek a hatások a nemzetbiztonsági rendszereket is széleskörűen és mélyen érintik. A védelmi ipar stratégiai iparág jellegéből adódóan komplex kapcsolatban áll az állam működésével és a nemzetbiztonsággal is. Így az országok biztonsága szempontjából jelentős szerepe van a nemzetbiztonsági rendszerek hatékony és eredményes működésének a védelmi ipari bázisokhoz kapcsolódó kihívások, kockázatok és fenyegetések kezelésében, amelyek azonban a folyamatosan romló globális biztonsági környezetben és exponenciális technológiai fejlődés mellett egyre sokrétűbbek, változók és egyre nehezebben előrejelezhetők.

Kulcsszavak: *nemzetbiztonság, nemzetbiztonsági szolgálatok, védelmi ipar, technológiai fejlődés, kiberbiztonság, ellátási láncok biztonsága, hírszerzés, elhárítás*

Defence Industrial Bases (DIB) have gained in significance lately, as a result of a number of impacts derived from the global security, economic and technological environment. The same environmental factors affected the national security systems extensively and deeply. Due to the strategic nature of the defence industry, it also has a complex relationship with the proper functioning of the state, also with the national security. Thus, the efficient and effective operation of national security systems has a significant role to play in addressing the challenges, risks and threats associated with Defence Industrial

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: krisztina.budavari.7@gmail.com

Bases that are increasingly diverse, changing and unpredictable in a deteriorating global security environment and under the influence of exponential technological advances.

Keywords: *national security, national security agency, defence industry, technological advancement, cyber security, supply chain security, intelligence, counterintelligence*

Bevezetés

A védelmi ipar jelenlegi hazai fejlesztése minőségileg és nagyságrendileg más feladatot jelent a nemzetbiztonsági rendszerre nézve a korábban évtizedekig fennálló helyzethez képest. A feladatok meghatározása elengedhetetlenné teszi a potenciális kihívások, kockázatok és fenyegetések azonosítását, azonban az adott globális biztonsági, gazdasági, technológiai és társadalmi környezetben ez nagyon jelentős kihívás. A környezet alapvető jellemzője ugyanis a komplexitás, az előrejelezhetetlenség, valamint a cirkuláris okság (ahol a viszonyokat és eseményeket kölcsönhatások interdependens hálózata határozza meg, vagyis az események és a szereplők viselkedése egyszerre oka és következménye is a másik viselkedésének vagy egy másik eseménynek). Továbbá a probléma nem egyszerűsíthető lokális szintre, mert a védelmi ipar vagy védelmi ipari bázisok nemzeti biztonsággal és nemzetbiztonsággal való kapcsolata a jelenlegi komplex környezetben csak globális kontextusban értelmezhető.

A védelmi ipar és a nemzetbiztonság viszonyának elemzése keretében ezért az elvégzett kutatás célja az is volt, hogy megtalálja ezeknek a potenciális kihívásoknak, kockázatoknak és fenyegetéseknek vagy egy elméleti osztályozási rendszerét, vagy egy olyan megközelítését, amely alkamas azok rendszerezésére, így a nemzetbiztonsági rendszer leendő feladatai szempontjából átlátható és konkrét cselekvési irányokat mutathat a stratégiai tervezés, a kapcsolódó szakpolitikák és a nemzetbiztonsági rendszer számára, továbbá elméleti szinten feltárja a védelmi iparhoz, illetve védelmi ipari bázishoz kapcsolódó, nemzetbiztonság szempontjából legkritikusabb kockázatokat. A kutatás azonosította azt a két területet – kiberbiztonság és ellátási láncok biztonsága – amely a legjelentősebb releváns nemzetbiztonsági kihívásokat, kockázatokat és fenyegetéseket rendszerként integrálja, ebből adódóan az ezek felőli megközelítés segíti azok logikus átláthatóságát és rendszerezését.

A kutatásban kihívást jelentett a nemzetbiztonság-fogalom többféle hazai értelmezése – mikro vagy szervezeti/funkcionális és makro vagy politikai/kormányzati,[2] vagy más megközelítésben a nemzetbiztonsági szolgálatok összessége szemben a kiterjesztőbb nemzetbiztonsági rendszer[3] értelmezéssel –, valamint ehhez kapcsolódóan kihívás

[2] Farkas 2020.

[3] „A szakterülettel foglalkozó kutatók közül néhányan a nemzetbiztonsági tevékenységben érintett, illetve azzal szorosan összefüggő szervezetek összességét mint nemzetbiztonsági szervezetrendszert definiálják. E felfogás szerint ebbe beletartoznak – többek között a hírszerző, elhárító, adatszerző, adatvédelmi feladatokat ellátó – nemzetbiztonsági szolgálatok és e szolgálatok irányítói. Ide sorolandók továbbá a nemzetbiztonsági szolgálatokat ellenőrző szervezetek, amelyek a szolgálatok működését, különböző szempontok szerint – anyagi, törvényességi, szakmai és a legújabb területként adatvédelmi – vizsgálják. Végül, de nem utolsósorban a nemzetbiztonsági szervezetrendszer elemei a szolgálatok közötti koordinációért felelős, azt végrehajtó szervezetek.” Mezei 2022: 85.

a nemzetbiztonság makro vagy politikai/kormányzati megközelítése és a biztonságelméletekben és biztonság- és védelempolitikában alkalmazott „nemzeti biztonság" fogalmak közötti viszony is. A kutatás megközelítésében a nemzetbiztonság politikai/kormányzati megközelítését alkalmaztam, és bár a három szint nagyon átfed, azokat a tényezőket, amelyek kizárólag a szélesebb, nemzeti biztonsághoz kapcsolódnak, a vizsgálódás próbálta nem fókuszba helyezni (bár kérdés, hogy például a gazdasági biztonságot veszélyeztető tényezők honnantól [hatókör, hatás erőssége stb.] jelentenek nemzetbiztonsági problémát stb.)[4] A védelmi ipar témakörével kapcsolatban pedig kihívást jelentett (nemcsak ebben a kutatásban, hanem folyamatosan), hogy egyrészt a hazai védelemgazdaság-tan nemcsak a nemzetközi folyamatokat nem követte le, hanem alapvető fogalmak (védelmi ipar, védelmi ipari bázis stb.) definíciója is hiányzik. Összességében a védelmi ipar tekintetében az a tényező, hogy a hazai tudomány az aktuális globális folyamatokat nem követte le, azt jelenti, hogy nem is tudja megfelelően kezelni a problémát. Mindez nemcsak a stratégiák, szakpolitikák, a teljes nemzetbiztonsági rendszer, hanem a nemzetbiztonsági szolgálatok működési szintjén is problémákat fog okozni (például a jelenlegi állás szerint nem tudható, hogy konkrétan mi az a vállalati kör, amely a védelmi ipart vagy védelmi ipari bázist jelenti Magyarországon, amellyel kapcsolatban a nemzetbiztonsági szolgálatoknak feladata van/lesz, vagy még inkább, kellene lennie).[5]

Globális környezet – a kihívások, kockázatok, fenyegetések eredete

A globális biztonsági környezetben az utóbbi években bekövetkezett változások oda vezettek, hogy a globális hatalmi erőviszonyok változásnak indultak, jelenleg a nemzetközi rendszer globális architektúrájának átstrukturálódása zajlik,[6] amit Oroszország Ukrajna elleni jelenleg is zajló agressziója még inkább felgyorsított. A 2010-es évektől folyamatosan romló biztonsági környezet és az USA (Donald Trump ciklusában) alkalmazott külpolitikája miatt a védelmi költségvetések folyamatos emelkedése a védelmi ipari keresletet globálisan jelentősen növelte, és megnövekedett az országok védelmi ipari bázisainak és a technológiai bázisainak jelentősége. A nagyhatalmi versengés visszatért, jelenleg is fokozódik. A legjelentősebb szereplők, az Egyesült Államok, Kína és Oroszország a hatalmi pozíciójuk növelését a globális technológiai vezető

[4] Gyakorlati értelemben az alkalmazott megközelítés azt jelenti, hogy pl. a technológiai fejlődést nem olyan szempontból lényeges értékelni, hogy az milyen új eszközöket képes biztosítani a nemzetbiztonsági szolgálatok számára, és az pl. milyen szervezeti változásokat indukálhat, hanem abból a szempontból, hogy a védelmi iparban keletkező új technológiai eredményeket a rendszernek meg kell védenie (pl. ipari kémkedés kérdése, kritikus IP jogokkal kapcsolatos szabályozás stb.).

[5] Természetesen vannak különböző besorolások, a kötelező szabályozások végrehajtásából (különböző engedélyesek, listákon szereplők, statisztikai adatszolgáltatásra kötelezettek, különböző ellenőrzések vagy tanúsítások alá esők stb.) eredően képződő csoportok, álláspontok (pl. Védelmiipari Szövetség stb.), de amint tudományos vizsgálódás tárgyává tesszük ezeket, láthatóvá válnak a problémák. Vagyis a legegyszerűbb feladat esetében, az iparágról szisztematikusan gyűjtendő adatok esetében már az sem határozható meg megalapozottan, hogy azt konkrétan kitől és kiről kellene gyűjteni, a leendő új belépőket nem is említve.

[6] Budavári 2021: 172.

szerep megszerzésében látták, és olyan stratégiákat kezdtek el alkalmazni, amelyek elsősorban a védelmi technológiai fejlesztésekben és elsősorban a feltörekvő és diszruptív technológiák területén globális fejlesztési hajszához, valamint fegyverkezési versenyhez vezettek.

A globális hegemón és a kihívó nagyhatalmak pedig a teljes nemzetközi rendszerre hatással vannak. Több területen paradigmatikus változások indultak el már a 2010-es években, vagy azt megelőzően (5. generációs hadviselés, NATO 4.0, Ipar 4.0), valamint a számos komplex hatás a globális védelmi ipar transzformációját is elindította (Aerospace & Defense 4.0). A védelmi ipar átalakulása (is) egyrészt közvetlenül visszahat a biztonsági, gazdasági és technológiai folyamatokra. Másrészt a paradigmatikus változások, például az exponenciális technológiai fejlődés eredményei mélyreható, széles körű, strukturális változásokat is okoznak és még inkább fognak okozni a jövőben, ami társadalmi és környezeti hatásokat is eredményez. A 2010-es évektől jellemzően bizonytalan és előrejelezhetetlen környezet pedig a jelenlegi orosz–ukrán konfliktus miatt még kiszámíthatatlanabb lett, és a nemzetközi rendszer szereplői közötti bizalom jelentős átrendeződését okozta. A globális, összekapcsolt világgazdaságban, ahol az erőforrások, tőke, termelési tényezők és technológia áramlása korábban jelentős fejlődést eredményezett, egyben jelentős aszimmetrikus függőségeket is, jelenleg beláthatatlan következményekre kell számítania az államoknak.[7] Mindez pedig egy olyan helyzetben, amikor a nagy kihívások (Grand Challenges), a klímaválság, demográfiai kihívások stb. egyre súlyosabb és sürgetőbb problémákat jelentenek, és amelyek kezeléséhez nemzetközi konszenzusok, globális és megosztott áldozatvállalás és olyan mennyiségű pénzügyi forrás lenne szükséges, amelyet csak a teljes rendszer együttesen tud előállítani. Az eddig fennálló nemzetközi rend alapvető értékei kérdőjeleződnek meg, és a globális problémák megoldására létrehozott nemzetközi szervezetek válnak működésképtelenné.

21. századi nemzetbiztonság

A változások és az ezredfordulót követően „kitáguló" biztonságpolitikai problémák (fegyveres konfliktusok, humanitárius vészhelyzetek, tömeges illegális migráció, terrorizmus felerősödése, környezeti és egészségügyi veszélyek) napjainkra visszafordíthatatlanul befolyásolják az egyes nemzetek biztonságát, amelyek már nem egy jól látható másik féltől származnak, hanem az összetett nemzetközi politikai, gazdasági, társadalmi és technológiai kérdéskörök mentén formálódnak.[8] „A biztonságot befolyásoló tényezők jelentős arányban már nem az államok közigazgatási határain belül keletkeznek, továbbá a korábbi határok szigorú elválasztó szerepe is leértékelődött."[9] A „nemzetbiztonsági rendszerek egyre több, nélkülözhetetlen szálon kapcsolódnak az állam és a társadalom egyéb szektoraihoz",[10] és „a modern társadalmak egyre

7 Budavári 2021: 75–85.
8 Dobák 2022a: 13.
9 Dobák 2022a: 15.
10 Dobák 2022a: 15.

sebezhetőbbé váltak".[11] A merev funkcionális elkülönülés lebontása (a társadalmi, gazdasági és tudományos fejlődés miatt) egyre sürgetőbbé válik,[12] a komplex kihívások miatt pedig a minél szélesebb körű együttműködések, szektoron belül, szektoron kívül és a civil szereplőkkel is. A kialakult konvergencia a fenyegetések oldaláról[13] elengedhetetlenné teszi a konvergenciát a fenyegetések kezelése oldaláról is.[14]

> „Az infokommunikációs megoldások robbanásszerű fejlődése – annak az államra és a társadalomra gyakorolt […] pozitív hatásai mellett – ugyanakkor közelebb is hozta a biztonságot fenyegető kihívásokat."[15] Az információrobbanás (évtizedek óta exponenciálisan nő a világon az újonnan keletkezett információk mennyisége) hatása is széles körben hat a nemzetbiztonsági rendszerre. Mivel a „releváns információk megszerzését célzó információgyűjtés a nemzetbiztonsági szolgálatok fő feladata, így minden, ami ezzel összefügg, jelentősen befolyásolja a nemzetbiztonsági szolgálatok működését".[16]

Egyre fontosabbá válik a biztonságra, védelemre és a hadviselésre a jövőben hatást gyakorló különböző technológiák folyamatos monitorozása is, és annak megállapítása, hogy azok a jövőben kulcsfontosságúnak tekinthetők-e, hogyan befolyásolják egy adott nemzet védelmi képességeit, biztonsága növelésének lehetőségeit, valamint a nemzeti ipar szintjén rendelkezésre állnak-e annak fejlesztési képességei.[17] A feltörekvő technológiák közül a mesterséges intelligencia stratégiai szinten fogja befolyásolni a nemzetbiztonságot is, valamint a biztonság minden szektorára hatással lesz. Az Amerikai Egyesült Államok 2018. évi *Nemzeti Védelmi Stratégiá*ja a mesterséges intelligenciát a feltörekvő technológiák azon csoportja közé sorolja, amely „megváltoztatja a háború jellegét és kihívást jelenthet a régóta fennálló háborús elvekre".[18] Egyes elemzők szerint a mesterséges intelligencia a védelmi szektorokban olyan mértékű transzformációt fog eredményezni, mint a nukleáris fegyverek, repülőgépek, számítógépek és a biotechnológia.[19] Ez potenciálisan egy új hadügyi forradalomhoz vezethet,[20] és talán a védelem fogalmának újradefiniálásához.[21] A mesterséges intelligencia katonai alkalmazásának várhatóan messzemenő következményei lesznek a kormányzás, az emberi jogok, a nemzetközi hatalmi erőviszonyok és a hadviselés terén egyaránt,[22] és civil alkalmazása esetében hasonló transzformatív hatásokra kell számítani.

A kihívások és változások a nemzetbiztonsági gondolkodásra és az érintett szervek feladataira is közvetlenül hatottak,[23] és a nemzetbiztonság értelmezése is

11 Dobák 2022a: 15.
12 Bács 2022: 42–43.
13 Bács 2022: 48.
14 Bács 2022: 50–51.
15 Dobák 2022a: 15.
16 Mezei 2022: 95.
17 Dobák 2022b: 62.
18 Porkoláb–Négyesi 2019: 4.
19 Allen–Chan 2017: 1.
20 De Spiegeleire – Maas – Sweijs 2017.
21 Tonin 2019: 1.
22 Wilner 2018: 1.
23 Dobák 2017: 236.

egyre kiterjesztőbbé vált. „Ezen változások talán a legjelentősebbeknek tekinthetőek a hidegháború befejezése óta, amely a nemzetbiztonsági, illetve titkos információgyűjtési képességekkel rendelkező biztonsági struktúrák szerepének felértékelődését eredményezték."[24] „Azt, hogy mit hoz a század további része […] nehéz megjósolni. A változás dinamikája és az érintett területek sokasága alapján azonban rövid időn belül jelentős változásokra kell felkészülni."[25] „A kockázatok sokszorozódása, a határon átnyúló jellege, súlyossága okán tovább kell erősíteni az országokon belüli, illetve a nemzetközi együttműködéseket. […] A technológiai robbanás, a kibertér jelentőségének folyamatos növekedése következtében további, új típusú nemzetbiztonsági szintű kockázatok megjelenése várható."[26]

> „A titkosszolgálatok technikai vonatkozású szegmenseit […] a biztonság oldaláról jelentkező fenyegetések változása, valamint a technikai környezet fejlődése formálja majd a továbbiakban is. A fenyegetések terén a már most is látható hangsúlyeltolódások új hírszerzési célokat, és ezek mentén új és újabb információgyűjtési megoldásokat eredményeznek majd. […] Egyértelmű szerepet kap a technológiai fölény kérdése, amely a korszerű, határokon átnyúló, globális méretű információgyűjtési képesség mentén megjósolhatatlan előnyöket biztosíthat az ezekkel rendelkező országoknak. Mindezek mögött új alkalmazási elvek, módszerek jöttek és jönnek létre, ideértve mind az információgyűjtés, mind az információk elemzésének és értékelésének kiemelten fontos területeit is, és mindezek […] kihathatnak az érintett nemzetbiztonsági szervezetek struktúráira is."[27]

Ezekre a változásokra az egyes államoknak és azok nemzetbiztonsági rendszereinek ma még csak részben állnak rendelkezésére a megfelelő kezelési technikák.[28]

A védelmi ipar mint stratégiai iparág

A védelmi ipar szereplői tevékenységük jellegéből adódóan számos szempontból speciális üzleti, politikai, szabályozási környezetben működnek, speciális kapcsolatokkal, speciális piacokon, ahol más piacokhoz képest sokkal jellemzőbbek a piacot, a versenyt, az árakat, a tranzakció összelőnyét torzító anomáliák. Ráadásul az állammal együtt részt vesznek a védelem mint közjószág előállításában. A védelemhez szükséges termékek és szolgáltatások jelentős és kritikus részét a védelmi ipar állítja elő, vagyis működése és teljesítménye közvetlen kapcsolatban áll az ország védelmi képességeivel, a védelemgazdasági potenciállal és a katonai potenciállal, szélesebb körben a biztonság- és védelempolitikával stratégiai szinten. Másrészt (általában jelentős) gazdasági szereplő, ezen keresztül hatással van a makrogazdasági teljesítményre, valamint (általában széles körű) külkereskedelmi tevékenysége révén hatással van a fizetési mérlegre, ezeken keresztül a gazdaságpolitikára. Továbbá (leghangsúlyosabban) a fegyverkereskedelem és a védelmi technológiai transzferek

[24] Dobák 2017: 236.
[25] Mezei 2022: 102.
[26] Mezei 2022: 102.
[27] Boda–Dobák 2016: 23–24.
[28] Dobák 2022a: 13.

révén az alkalmazható külpolitikára is.[29] A védelmi ipari külkereskedelem, kiemelten a fegyverkereskedelem szabályozása szintén nemzetbiztonsági kérdés is. A védelmi iparnak az is sajátossága, hogy a biztonsági környezet romlása – ami egyébként a nemzetbiztonsági kockázatokat növeli – az emelkedő védelmi költségvetések révén számára pozitív kilátásokat jelent.

A globális védelmi ipar mai jellemzőit – ami azonban jelenleg ismét transzformálódik –, két jelentős időszak alakította, a hidegháború lezárulását követő időszak, amikor a védelmi költségvetések jelentősen csökkentek, és az államok biztonsági percepciói jelentősen megváltoztak, valamint az utóbbi évtized, a biztonsági környezet ismételt jelentős romlása, valamint az exponenciális technológiai fejlődés.[30] Ennek következtében az iparág mára egyrészt transznacionális értékláncok hálózataként értelmezhető, másrészt egyre nagyobb a koncentrációja, harmadrészt pedig egyre inkább együttműködik civil piaci szereplőkkel. Ez a rendszer egyre inkább híján van az átláthatóságnak, és a profitmaximalizálási célok mellett egyre nehezebb egyensúlyozni a biztonsági szempontokkal.

Látható, hogy a védelmi ipar működése komplex kölcsönhatásban van az állammal, a nemzeti biztonsággal és a nemzetbiztonsággal is. Ebből eredően számos és máshol nem jellemző, sajátos tényezők is nemzetbiztonsági kihívásként, kockázatként és fenyegetésként jelenhetnek meg az iparággal kapcsolatban, vagy onnan eredően. Példaként, a védelmi ipar esetében akár az iparág struktúrája is jelenthet nemzetbiztonsági kockázatot. Az USA-ban például jelenleg nemzetbiztonsági kockázatként értékelik az elmúlt időszak egyik iparági trendjéből (jelentős számú felvásárlás és összeolvadás, igen nagyértékű tranzakciók, „megamerger"-ek)[31] adódó iparági struktúrát. Az USA védelmi minisztériuma által nemrég kiadott jelentés szerint a védelmi ipar extrém konszolidációja a piaci versenyt olyan mértékben csökkentette, amely már nemzetbiztonsági kockázatot jelent.[32] További példaként említhető a klaszterizácó, amelynek számos gazdasági előnye van, például a járműiparban kiterjedten alkalmazzák, de más iparágaktól eltérően a védelmi iparban viszont jelentősen növeli a kockázatokat (a vállalati szintű, a piaci szintű és a nemzetbiztonsági kockázatokat egyaránt). A védelmi iparra jellemző speciális beszerzési metódusok szintén befolyásolják a piacot, valamint az iparágban kiemelt jelentőségű szellemi tulajdonhoz fűződő jogok (IP-) védelmének szabályozása is. (Mindkét tényező az utóbbi időben több országban jelentős stratégiai újragondolások tárgyává vált.) A két tényező külön-külön is alkalmas a piacot torzító jelenségeket létrehozni (éppen ezért hátrányokat kikerülő, akár illegális akciókat kiváltani), azonban ha figyelembe vesszük a köztük lévő kapcsolatot, a helyzet még bonyolultabb, ráadásul a legdrágább fegyverrendszereknél jelenik meg leginkább. Olyan komplex jelenségekről is beszélhetünk továbbá (piactorzító hatású jelenség, egyben nemzetbiztonsági kockázat), mint a katonai-ipari hatalmi komplexumok, amely egy erőteljes, kiterjedt és erőforrásban gazdag koalíció, amelynek önmagát fenntartó és megerősítő természete van, és a legfőbb közös célja a katonai szektor

29 Budavári 2021: 20–21.
30 Budavári 2021: 20–27.
31 Iparági trendekről és vállalati stratégiákról bővebben: Budavári 2021: 109–123.
32 The White House 2022.

folyamatos bővítése függetlenül a tényleges szükségletektől.[33] A védelmi iparban kifejlesztett és katonai felhasználásra alkalmazott új technológiák szintén relevánsak lehetnek nemzetbiztonsági szempontból. Az USA nemrég közzétette azoknak a technológiáknak a listáját, amelyeket a gazdasági biztonság és nemzetbiztonság szempontjából a legnagyobb hatásúaknak tart, ezek a mesterséges intelligencia, bioökonómia, autonóm rendszerek, kvantumtechnológia és félvezetők.[34]

Az összes potenciális kockázat bemutatása a reális vállalás kereteit jelentősen túllépné, azok meghatározása a nemzetbiztonsági rendszerek feladata, azonban látható a kihívás nagyságrendje, amivel a jelenlegi környezetben szembesülnek.

Hazai környezet

Magyarországon a védelmi ipar fejlesztése kormányzati stratégiai célkitűzés a *Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program*[35] – jelenleg Honvédelmi és Haderőfejlesztési Program (HHP) – 2017. évi elindulása óta. A program egyszerre tűzte célul a haderő haditechnikai korszerűsítését és a magyar védelmi ipar intenzív fejlesztését egy komplex gazdaság-, társadalom-, valamint biztonság- és védelempolitikai célrendszer részeként. A védelmi képességcélokon kívül a kormány a gazdaság diverzifikáltságának növelését, új munkahelyek teremtését, versenyképes és magas hozzáadott értéket termelő iparágak létrehozását, az ország innovációs képességeinek javítását is el kívánja érni. Védelmi területen pedig kiemelt célok az importfüggőség csökkentése, az ellátásbiztonság megteremtése, valamint a nemzeti ellenállóképesség növelése.[36] Mindezek a célok a legújabb stratégiai dokumentumokkal – 2020. évi Nemzeti Biztonsági Stratégia (NBS),[37] 2021. évi Nemzeti Katonai Stratégia (NKS),[38] 2021. évi Védelmi Ipari Stratégia (VIS)[39] – is igazolhatók. Mind az NBS, mind az NKS nagy súlyt helyez a védelmi ipar szerepére a nemzeti biztonság garantálásában. A nemzetbiztonsági megközelítés egy helyen jelenik meg az NBS-ben: „A hazai védelmi ipar, azon belül is a kutatás-fejlesztés és az innováció támogatása *nemzetbiztonsági érdek*, mivel ezek által csökkenthető az import függőség, növelhető az ellátásbiztonság és hazai gyártmányokkal korszerűsíthetőek a védelmi eszközök."[40]

Az iparág ilyen léptékű fejlesztése, ami a biztonság minden szektorára jelentős hatásokat gyakorolhat (és a célja is az, hogy jelentős biztonsági és makrogazdasági hatásokat érjen el), a nemzetbiztonsági rendszer számára a korábbi feladatokhoz képest minőségileg és nagyságrendben is sokkal jelentősebb feladatot fog jelenteni. Mindezt összevetve a regionális és globális biztonsági környezet jelenlegi folyamatos, jelentős romlásával és annak hatásaival és következményeivel (szankciók, embargók

33 Budavári 2021: 26.
34 NCSC 2021.
35 1298/2017. (VI. 2.) Korm. határozat.
36 Budavári 2021: 152–153.
37 1163/2020. (IV. 21.) Korm. határozat.
38 1393/2021. (VI.24.) Korm. határozat.
39 A VIS titkos minősítésű dokumentum, tartalmával kapcsolatban nyilvános, hiteles forrás: www.parlament.hu/documents/static/biz41/bizjkv41/HOB/2106081.pdf
40 1163/2020. (IV. 21.) Korm. határozat 105. pont.

szintjétől a nemzetközi rendszer szereplői közötti bizalomban történt átrendeződésig, a védelempolitikákban, védelmi költségvetésekben, a globális védelmi iparban, valamint a technológiai fejlesztések terén már ismertetett folyamatok felgyorsulásáig) még inkább.

Hazai tekintetben lényeges, és az eddigi folyamatokból már látható, hogy az újonnan épülő iparágban a hazai vállalatok a létrejövő transznacionális értékláncokba alacsony szinten fognak bekapcsolódni. Ezek az értékláncok rendkívül komplexek (például a Leopard II harckocsi ellátási lánca több mint 1500 vállalatból áll[41]). Viszont „az ellátási lánc annyira erős, mint a leggyengébb láncszeme".[42] Az is jellemző, hogy főleg kkv-k kapcsolódnak be a védelmi iparba (mivel nagyvállalatok nincsenek). Ezzel kapcsolatban az USA Védelmi Ipari Szövetségének kutatása kimutatta, hogy (az USA-ban) összefüggés van a vállalatok mérete és az általuk jelentett kockázat között: minél kisebb a vállalat, annál nagyobb a biztonsági rés.[43] Lényeges továbbá, hogy sem az iparági szereplők, sem az állam nem rendelkezik jelentős tapasztalattal, sem jelentős erőforrásokkal,[44] a szabályozás és a teljes rendszer (beleértve a teljes innovációs rendszert) az évtizedekig fennálló korábbi helyzetet ismeri. Ráadásul az iparág nem organikusan fejlődik, hanem irányítottan. Továbbá nemzetbiztonsági kockázatot jelenthet hazai szinten, és főként a nagyhatalmak közötti viszony elmúlt időszakbeli jelentős romlása mellett, az iparpolitika (nyugati védelmi ipari nagyvállalatok betelepítése minél nagyobb számban) és a külpolitikában a keletinyitás-politika (infrastrukturális beruházások, szállítási útvonalak, logisztikai csomópontok finanszírozási és tulajdonosi háttere) kombinációja is. A jelenlegi helyzetben az orosz–ukrán háború hatása is jelentős a hazai védelmi iparhoz kapcsolódó nemzetbiztonsági kockázatokra. Az elhúzódó konfliktus nagyon jelentős keresletnövekedést okozott, ami egyre nagyobb nyomást helyez (piaci és biztonsági tekintetben egyaránt) a védelmi ipari bázisokra globálisan, és komplex hatások révén számos kockázatot, veszélyt, fenyegetést keletkeztet. (Például egy hazánk szempontjából releváns kockázat, hogy az adott globális ellátásilánc-problémák mellett, rövid távon az alacsony stratégiai jelentőségű és alacsony alkuerejű országok – mint hazánk a régióban – jelentős ellátási problémákkal szembesülhetnek, ami gyengítheti a védelmi képességüket.)[45]

A hazai nemzetbiztonsági rendszer számára így a jelenleg épülő új iparág jelentős kihívásokat fog jelenteni, nemcsak az iparág speciális adottságaiból adódóan, hanem a globális és regionális folyamatokból, a lokális adottságokból és képességekből, valamint nem kevésbé a hazai alkalmazott politikák közötti stratégiai összhang esetleges hiányából adódóan.

41 The European Parliament 2014.
42 Lásd: www.cisa.gov/resources-tools/groups/ict-supply-chain-risk-management-task-force
43 Bourbon 2019.
44 A világ legnagyobb védelmi ipari vállalatainak néhány éves önálló költségvetése csak az új termékek fejlesztésére, egyes esetekben több mint a Zrínyi HHP teljes 10 éves költségvetése. Budavári 2021: 165.
45 Kandrík 2022.

A legjelentősebb kockázatok – kiberbiztonság és ellátási láncok biztonsága

A kutatás alapján a már említett két terület mint rendszer jelenti a legjelentősebb nemzetbiztonsági kockázatokat a védelmi ipar szempontjából: a kiberbiztonság és az ellátási láncok biztonsága. Tekintettel a hazai szakirodalom hiányosságaira is, a tárgyi témában az Amerikai Egyesült Államok (USA) – mint a világ legnagyobb védelmi ipari bázisával rendelkező, a globális technológiai vezető szerepet még birtokló, és messze a legmagasabb védelmi költségvetéssel rendelkező ország[46] – gyakorlatát vizsgáltam.[47]

A kiberbiztonság kiemelt, nemzetbiztonsági szintű kezelése már Magyarországon, a gyakorlatban is megvalósul. Viszont a védelmi ipar tekintetében figyelemre méltó, és a hazaitól teljesen eltérő szemléletet tükröz, hogy az USA-ban a védelmi ipari bázis külön szektort képez a kritikus infrastruktúrán belül (16 szektor összesen) a Kiberbiztonsági és Infrastruktúra Biztonsági Ügynökség (Cybersecurity & Infrastructure Security Agency, CISA) rendszere alapján. Minden szektor rendelkezik saját kockázatkezelési ügynökséggel, a védelmi ipari bázis szektor kockázatkezelési ügynöksége a Védelmi Minisztérium (Department of Defense, DoD). Az ügynökségek ágazatspecifikus tervet készítenek, az állami és a magánszektorbeli partnerek összehangolt együttműködésével, amely részletezi, hogyan valósul meg a Nemzeti Infrastruktúra Védelmi Terv kockázatkezelési keretrendszere az ágazat egyedi jellemzőinek és kockázatainak kontextusában.[48]

A védelmi szempontból kritikus ellátási láncok kockázatainak nemzetbiztonsági szintű kezelése tekintetében viszont szisztematikus hazai kormányzati gyakorlat nem igazolható. Az USA azonban az ellátási láncok problémáját a gyakorlatban is kiemelten, nemzetbiztonsági szinten kezeli. A Nemzeti Hírszerzési Igazgató Hivatalában (Office of the Director of National Intelligence, ODNI) a Nemzeti Elhárítási és Biztonsági Központ (National Counterintelligence and Security Center, NCSC) feladatkörébe tartozik az ellátási láncok fenyegetéseinek kezelésével kapcsolatos prioritások meghatározása és a Hírszerző Közösség (U.S. Intelligence Community, IC) erőfeszítéseinek összehangolása ezen a területen. A két terület össze is függ, vagyis a kiberbiztonság az ellátási láncokban és az IKT ellátási láncok biztonsága a legkritikusabb nemzetbiztonsági kihívásoknak tekinthetők. Az USA gyakorlatában az NCSC-n belül az Ellátási Lánc és Kiberigazgatóság (Supply Chain and Cyber Directorate, SCD) a két területért egyben felelős, feladata a nemzeti ellátási láncok biztonságának és a kiberbiztonság fokozása, tájékoztatás, irányítás és koordináció a stratégiai partnerekkel együttműködve a kockázatokkal kapcsolatos integrált döntések és reagálás érdekében.[49]

46 Bővebben: Budavári 2021: 72–123.
47 Lásd az irodalomjegyzéket.
48 Lásd: www.cisa.gov/defense-industrial-base-sector
49 Lásd: www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats

Az ellátási láncok[50] emberek, folyamatok, technológiák, információk, erőforrások alkotta globálisan kiterjedt és összekapcsolt hálózatok, amelyek termékeket és szolgáltatásokat hoznak létre és juttatnak el a vevőhöz. A globális ellátási láncok dinamikusak, sokrétűek és komplexek. Az átláthatóság és a követhetőség hiánya biztonsági kockázatot jelent, mert minden egyes komponensnek megvan a saját ellátási lánca, ami számos lehetőséget jelent az ellenséges szándékú szereplők számára, hogy szabotálják bármelyik összetevőt (az alapanyagoktól a gyártási folyamatokon keresztül, a szállításon és csomagoláson át, számos ponton).[51] Továbbá nemzetbiztonsági szempontból az egyes lánctípusok megkülönböztetésének is van jelentősége. A védelmi ellátási láncok vagy védelem szempontjából kritikus ellátási láncok az állam szemszögéből értelmezendők, a védelmi ipari ellátási láncok (amelyek részei az előbbieknek) pedig az iparág szemszögéből. Az állam biztonságközpontú érdeke az ellátási láncai tekintetében – ami befolyásolja azok ellenőrzését, védelmét és szabályozását – ugyanis nem minden esetben esik egybe az iparág és a vállalatok profitközpontú érdekeivel a saját láncaikra vonatkozóan. Természetesen az államnak is érdeke a gazdasági biztonság szempontjainak, ezért a vállalatok profittermelési képességeinek figyelembevétele, de a vállalatok profitelvárásaikban nem az ország gazdasági biztonságának ideális szintjéből indulnak ki. Az egyensúlytalanság, a nem megfelelő szabályozás, a túlzott korlátozások ezen a területen pedig automatikusan generálhatják a nemzetbiztonsággal ellentétes, akár illegális tevékenységeket (a szabályozások be nem tartásától kezdve, amelyek olyan biztonsági réseket okozhatnak, ahol a haderő vagy a kormányzat információi is kiszivároghatnak,[52] külföldi „outsourcing" vagy „offshoring" kritikus technológiai információk kiszivárgásának veszélyével, embargók megkerülése, illegális [fegyver]kereskedelem stb.).

A védelmi ellátási láncok nemzetbiztonsági kockázataival kapcsolatban az USA védelmi minisztériuma kiadott egy jelentést, amelyben átlátható csoportosításban összegzi azokat, elsősorban az *elhárítási kihívások* felőli megközelítésben:

„Nemzetbiztonsági kockázatok (Counterintelligence Risks):

1. Ellátási láncok nem megfelelő átláthatósága
   a) Képtelenség azonosítani a külföldi joghatóság vagy külföldi kormány irányítása alá tartozó alsóbb szintű beszállítókat
   b) A fenyegetések, sebezhetőségek és kockázatok azonosításának nehézségei az alsóbb szintű ellátási láncokban lehetővé teszik hamisított vagy kompromittált alkatrészek behelyezését az ellátási láncba

[50] Mivel a kiberbiztonsággal kapcsolatos kutatások hazai szinten is jelen vannak, és széleskörűen áll rendelkezésre a téma szakirodalma, illetve igazolhatóan a téma jelentősége felismert, ezért a fejezet a továbbiakban az ellátási láncokkal foglalkozik.

[51] Ferry–Poindexter 2016: 19.

[52] Az USA Nemzeti Védelmi Ipari Szövetségének (National Defense Industrial Association, NDIA) egy kutatása kimutatta, hogy az USA hazai védelmi beszállítói közül a kkv-k kevesebb mint 60%-a olvassa el azt a dokumentumot, amely a védelmi beszállítókra vonatkozó minimum biztonsági sztenderdeket tartalmazza. Lásd Bourbon 2019.

2. Elavult beszerzési politikák és eljárások
   a) A hazai befektetők elriasztása a magas tőkebefektetési igények miatt
   b) Az inkonzisztens minisztériumi beszerzési gyakorlatok instabilitást okoznak az alsóbb szintű beszállítóknál és akadályozzák a befektetéseket újabb technológiákba
3. Külföldi tulajdon, irányítás vagy befolyás
   a) A Védelmi Minisztérium kereslete nem elég jelentős ahhoz, hogy a szabványosítást és a technológiai modernizációt ösztönözze
   b) Erőteljes függés külföldi országoktól és kizárólagos beszállítóktól a kritikus komponensek tekintetében, az erodálódott hazai ellátási láncok miatt
4. A Védelmi Minisztériummal kapcsolatban álló hálózatok kiberbiztonsági pozíciója
   a) Egyre gyakoribbak a védelmi ipari bázist érintő kifinomult, megfelelő erőforrásokkal támogatott kibertámadások
   b) A védelmi ipari bázisban a szoftverfejlesztés és -terjesztés csatornáinak nem megfelelő a kiberbiztonsági helyzete, ami a védelmi ipari bázis kitettségét fokozza mind a hagyományos kibertámadásokkal, mind a szoftverek ellátási láncaiban végrehajtott kibertámadásokkal szemben."[53]

A fent azonosított kockázatok körvonalazzák azt a számtalan kockázatot, amellyel a védelmi ipari bázisnak szembe kell néznie. Azonban hangsúlyozni kell, hogy az információs és kommunikációs technológiák (IKT) ellátási láncainak biztonsága kiemelten hat a védelmi ellátási láncokban a kritikus termékekre és szolgáltatásokra. Ezért a védelmi ipari bázist támogató IKT ellátási láncok biztonságát előtérbe kell helyezni, így az IKT ellátási lánc védelme erősokszorozó a védelmi ellátási láncok tekintetében.[54]

Összefoglalás

A jelenlegi komplex környezetben mind a védelmi ipar, mind a nemzetbiztonsági rendszerek jelentős változásokon mennek keresztül. A globális biztonsági környezet romlásával mindkét terület felértékelődött az utóbbi években, ami továbbra is, gyorsulva folytatódik. A változások másik legfőbb okozója pedig a rohamos technológiai fejlődés. A nemzetbiztonsági rendszereknek így a védelmi ipari bázisok kapcsán nagyon jelentős kihívásokat, kockázatokat és fenyegetéseket kell kezelniük, úgy, hogy közben maguk is változnak. A kockázatok, kihívások és fenyegetések sokrétűek, komplex kölcsönhatásban állnak, egyre inkább előrejelezhetetlenek, váratlan forrásokból, országhatárokra tekintet nélkül jelentkeznek. Ebben a helyzetben a releváns kockázatokat és az azokból következő feladatokat is rendkívül nehéz meghatározni.

[53] NCSC 2022.
[54] NCSC 2022.

A kutatás alapján levonható az a következtetés, hogy nemzetbiztonsági szempontból, a védelmi ipar tekintetében a védelmi ellátási láncok kiberbiztonsági kockázatai a legjelentősebbek, a legmélyebb hatásokat tudják gyakorolni a nemzetbiztonságra, és a legsürgetőbb azok kezelése.

Irodalomjegyzék

Allen, Greg – Chan, Taniel (2017): *Artificial Intelligence and National Security.* Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs. Online: www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

Bács Zoltán György (2022): Viribus Unitis, avagy civil-professzionális konvergencia a 21. században. In Dobák Imre (szerk.): *Nemzetbiztonság a 21. század elején. Szemben a kihívásokkal.* Budapest: Ludovika, 42–51.

Boda József – Dobák Imre (2016): Titkosszolgálatok fejlődése – technikai szemmel. *Nemzetbiztonsági Szemle,* 4(4), 17–25. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1879/1168

Bourbon, Ben (2019): Agencies Look to Minimize Supply Chain Risks. *FedTech Magazine,* 2019. november 6. Online: https://fedtechmagazine.com/article/2019/11/agencies-look-minimize-supply-chain-risks

Budavári Krisztina (2021): *A magyar védelmi ipar helyzete és fejlődési lehetőségei.* Budapest: Magyar Hadtudományi Társaság. Online: https://doi.org/10.51491/vedelmi.ipar2021

De Spiegeleire, Stephan – Maas, Matthijs – Sweijs, Tim (2017): *Artificial Intelligence and the Future of Defense: Strategic Implications for Small- and Medium-Sized Force Providers.* The Hague: The Hague Centre for Strategic Studies. Online: https://bit.ly/3NVI0qn

Dobák Imre (2017): Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében. *Hadmérnök,* 12(2), 235–249. Online: http://hadmernok.hu/172_19_dobak.pdf

Dobák Imre (2022a): A nemzetbiztonság 21. századi értelmezése és jellemzői. In Dobák Imre (szerk.): *Nemzetbiztonság a 21. század elején. Szemben a kihívásokkal.* Budapest: Ludovika, 13–28.

Dobák Imre (2022b): Társadalom – technológiai környezet – nemzetbiztonság. In Dobák Imre (szerk.): *Nemzetbiztonság a 21. század elején. Szemben a kihívásokkal.* Budapest: Ludovika, 52–67.

The European Parliament (2014): *Defence Industrial Supply Chains and the Role of SMEs in the Sector.* Online: https://bit.ly/3LAPaNR

Farkas Ádám (2020): Gondolatok a nemzetbiztonság fogalmáról. *Szakmai Szemle,* 18(3), 5–20. Online: www.knbsz.gov.hu/hu/letoltes/szsz/2020_3_szam.pdf

Ferry, Heath – Poindexter, Van (2016): Supply Chain Risk Management. An Introduction to the Credible Threat. *Defense AT&L,* 2016. július–augusztus. 19–22. Online: www.dau.edu/library/defense-atl/DATLFiles/Jul-Aug2016/Ferry_Poindexter.pdf

Kandrík, Matej (2022): The Defense Impact of the Ukraine War on the Visegrád Four. *German Marshall Fund,* 2022. július 28. Online: www.gmfus.org/news/defense-impact-ukraine-war-visegrad-four

Mezei József (2022): A szervezetrendszerek módosítása, strukturális válaszok. In Dobák Imre (szerk.): *Nemzetbiztonság a 21. század elején. Szemben a kihívásokkal.* Budapest: Ludovika, 85–102.

NCSC (2021): *NCSC Fact Sheet – Protecting Critical and Emerging U.S. Technologies from Foreign Threats.* 2021. október 21. Online: www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Fact-sheet_10_22_2021.pdf

NCSC (2022): *Fortifying the Defense Industrial Base (DIB) Supply Chains.* 2022. február. Online: www.dni.gov/files/NCSC/documents/supplychain/dod-supply-chain-spotlight-2022-4C850B07-.pdf

Porkoláb Imre – Négyesi Imre (2019): A mesterséges intelligencia alkalmazási lehetőségeinek kutatása a haderőben. *Honvédségi Szemle,* 147(5), 3–19. Online: https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/208

Tonin, Matej (2019): *Artificial Intelligence: Implications for NATO's Armed Forces.* NATO Parliamentary Assembly, Science and Technology Committee (STC), Sub-Committee on Technology Trends and Security (STCTTS), 2019. október 13. Online: https://bit.ly/3Vu9lS8

The White House (2022): *Fact Sheet: Department of Defense Releases New Report on Safeguarding our National Security by Promoting Competition in the Defense Industrial Base.* 2022. február 15. Online: https://bit.ly/3LAEChK

Wilner, Alex S. (2018): *Artificial Intelligence and Deterrence: Science, Theory and Practice.* (STO-MP-SAS-141) NATO Science and Technology Organization. Online: www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-141/MP-SAS-141-14.pdf

Jogi források

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

2011. évi CLXXI. törvény a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény katonai nemzetbiztonsági szolgálatok összevonásával kapcsolatos módosításáról, valamint az azzal összefüggő további törvénymódosításokról

2014. évi CIX. törvény a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény, valamint egyes törvényeknek a nemzetbiztonsági ellenőrzéssel összefüggő módosításáról

1298/2017. (VI. 2.) Korm. határozat a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról
1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
1393/2021. (VI.24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról
128/2011. (XII. 2.) HM utasítás a katonai nemzetbiztonsági szolgálatok összevonásával kapcsolatos egyes feladatokról
60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról

NEMZETBIZTONSÁGI SZEMLE
11. évfolyam (2023) 1. szám 49–61. • DOI: 10.32561/nsz.2023.1.4

Ákos Bunyitai[1]

Insider Threat Mitigation in High Security Facilities

The biggest challenge for the security in high security facilities is the insider threat, humans as the weakest link of the system. The insider is an invisible enemy of the security, because it has unique capabilities. Although perfect security cannot exist, the aim of the present study – besides showing the threat represented by insider offenders – is to introduce the measures for risk mitigation.

Keywords: *security, protection, prevention*

The story of the Trojan Horse used during the Trojan War is well known. The Trojans pulled into the protected city of Troy a huge wooden horse, with Greek soldiers inside. At night the Greek force crept out from the horse and opened the gates of the city under siege for the rest of their army. The Greek army entered the city of Troy and destroyed it. Success was due to the assistance given to the external part of the Greek army from inside the well protected city walls, by the soldiers from the wooden horse. From the time of Homer's ancient epic poem, Iliad, a "Trojan Horse" means any trick or stratagem that makes someone "invite" a foe into a securely protected area who then attacks from the inside. The problem of the possible hostile element in any secured area is still relevant. As Matthew Bunn and Scott D. Sagan wrote: "Insider threats are perhaps the biggest and most difficult part of the security challenge."[2]

Who are the 'insiders'?

To put it simply, an insider is an internal adversary, who has capabilities and opportunities to perform malicious actions; therefore, an insider is a security threat. Let us see the most relevant/important definitions used by the supporting guides of the International Atomic Energy Agency (hereinafter: IAEA). The IAEA was among the first to recognise

[1] MSc, Security Engineer, Student of Óbuda University Blasting Technology Engineer Postgraduate Specialist Training, e-mail: bunyitai.akos@gmail.com

[2] Bunn–Sagan 2016: 171.

the threat of an insider and published its definitions and suggestions for the mitigation of possible harms from the point of view of nuclear security:

Adversary

An adversary is any individual performing or attempting to perform a malicious act. They may be an insider or an outsider.[3]

Insider

"An individual with authorized access to associated facilities or associated activities or to sensitive information or sensitive information assets, who could commit, or facilitate the commission of criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security."[4]

Threat

"A likely cause of harm to people, damage to property or harm to the environment by an individual or individuals with the motivation, intention, and capability to commit a malicious act."[5]

Malicious act

"An act or attempt of unauthorized removal or sabotage."

The illegal, malicious act that may cause any harm or damage may vary by every facility. It depends on the local legal background, the profile of the company, and many other factors. For example, the main goal for the physical protection system in nuclear facilities is to protect radioactive material from unauthorised removal and also to protect nuclear facilities from sabotage and – in case of sabotage – minimising the radiological consequences.[6]

3 IAEA 2020.
4 IAEA 2013: 12.
5 IAEA 2008: 1.
6 IAEA 2011: 52.

Who can be an insider?

In order to understand the scale of the threat, let us clarify the persons, who can become insiders. It can be anybody who has permission to enter the site and/or authorised access to the systems of the facility, thus in particular, but not exclusively:

- officials of the management of the facility
- employees of the facility
- security personnel, guards
- system administrators of the IT system
- external contractors, partners
- maintenance personnel
- official persons
- employees of public utilities (electricity, gas, water, sewer, Internet, waste management)
- vendors, courier
- visitor

Insider types

The division of the insiders by types is largely theoretical, its practical significance is negligible. In the majority of cases, the identity of the insider is revealed only once the illegal act had been committed (before that, they can be considered 'potential' insiders if they are suspected of hostile activities). In the preparation phase, it is difficult to predict how they would act, what is their motivation, whether they would act aggressively. In many cases, their intentionality is also questionable. The following categories are used to review the insiders and to be ready to face the threat. Types of insiders:

1. passive (always non-violent, only provide information)
    - unintentional or unwitting[7]
    - intentional
2. active (always intentional)
    - non-violent insider (perpetrates an act himself/herself or assists others to committing)
    - violent insider (ready to use physical violence against personnel or others)

Possible insider tactics

According to the IAEA's statement, an "insider can pose many different types of threats to a facility".[8] The insider when committing an illegal act, can act alone or in

[7] Unwitting insider: the unwitting insider is unaware of their involvement in the attack.
[8] IAEA 2020.

cooperation with – even in preparation for an external attack – other colleagues or a group from outside the facility. Their action can be quick (e.g. cutting a hole on the fence) or even protracted in time (e.g. protracted theft, smuggling in small amounts of explosives). Some of the actions are very difficult to detect.

1. Possible passive insider tactics
    - transfer of available sensitive information to an external person (regarding the weakness of the security system, the facility and its operation)
    - transfer of own access rights (knowledge-based or physical token)
    - loss of sensitive information
    - testing the security capabilities of the facility
    - other non-violent acts

"The passive insider provides only the information that he or she can readily obtain and divulge without fear of detection."[9] In many cases, the employee unknowingly, unintentionally, accidentally and with good intentions helps the malicious act (e.g. as a victim of social engineering), thus becomes a passive, unwitting insider. He or she can gossip (e.g. CEO's hobby), or transfer useful or even sensitive information (e.g. new security guards), can be inattentive, and forget an access card somewhere, can 'piggybacking'[10] or take any subject avoiding the security control, breaking the security culture, rules and legislative regulation.

2. Possible active insider tactics
    - unauthorised entry (e.g. breaking of locks)
    - testing the security capabilities of the facility
    - disinformation of the security organisation
    - theft (e.g. keys)
    - manipulation of sensitive information
    - falsification of database or blueprint
    - tamper or sabotage of security system
    - sabotage (e.g. by improper handling, damage, explosives)
    - preventing authorised access
    - cyberattack (it can result in physical damage also)
    - neutralisation of security staff or response forces
    - disruption of the normal operation of the facility, jeopardising business continuity
    - other non-violent or violent acts

The real difference between passive and active insiders is how they carry out their activities. An active insider is always an active participant in the plot, risking of being caught. If the insider gives his or her own key to the adversary, he or she is a passive

[9] Sandia National Laboratories 2019.
[10] Piggybacking: when an authorised person opens the door for an unauthorised person to enter.

insider; but if he or she steals or copies his or her colleague's key, he or she becomes an active insider.

An active, non-violent insider uses stealth and deceit, not force, against personnel; while an active, violent insider is ready to use force against personnel. An active insider cannot be an unwitting one, because he or she is always aware that what he or she is doing is helping the attack.

It is noteworthy, that damage can be caused not only by unauthorised access to something, but also by intentional (or unintentional) damage by authorised access and by unauthorised blocking of access as well. Anyone who has logical and/or physical access to something, has a good chance of being able to block it from others (e.g. blocking access to fire water, blocking access to utilities or blocking the doors of the security personnel). Picking a lock and replacing it with your own lock may be a preparatory step for an attack: ensuring that the obstacle is overcome more quickly and less conspicuously during the attack. Both, the passive or active – even violent – insiders may be responsible for testing the security capabilities of the facility (e.g. response time of the guards), even with actions disguised as innocent mistakes.

Motivation

The possible motivation of the insider can help to understand their behaviour and to prevent becoming an insider. The security personnel cannot be sure that the insider's act is rational. An unwitting insider does not have motivation. As stated in the Sandia National Laboratory's publication: "Motivation is an important indicator for both level of malevolence and likelihood of attempt."[11]

Some of the possible motivations:

- financial
- ideological
- coercion
- psychological
- revenge/embarrassment
- ego
- mental stability
- combination of the above

Attributes and advantages

The advantages of insiders is that they are able to: be "invisible" for the security organisation, because no one suspects them; they can explore their options freely and unobtrusively; test the security capabilities without consequences; choose the best time; select the most vulnerable target; may associate with other insiders or outsiders. "Insiders possess at least one of the following attributes that provide

[11] Sandia National Laboratories 2019.

advantages over external adversaries when attempting malicious activities: authorized access, authority, knowledge."[12]

1. An insider may have authorised logical and/or physical access[13] to information, equipment, system, thus in particular, but not exclusively:

- databases
- IT and communication system
- regulations
- protocols and procedures
- plans, even to security plan and contingency plan
- premises, even to office, storage, armoury, server room
- equipment
- tools
- vehicles
- systems, even to security system

In summary: an insider may have authorised access to everything that is factually in use by the company.

2. An insider may have authority when performing his/her duties thus in particular, but not exclusively:

- management of certain systems (e.g. remote system control, shutdown, disconnect)
- managing subordinates (e.g. override internal rules by verbal instruction)

3. An insider may have knowledge and skills in particular, but not exclusively:

- facility-level knowledge
  - location
  - access routes
  - buildings, floor plans
  - utility networks
  - operational information
- organisation-level knowledge
  - management
  - organisation structure
  - position of employees
  - contact details of employees
  - subordinate–superior relationships
  - rules, protocols, procedures, policies
  - personal information (family and friendships, hobby, etc.)
- professional-level knowledge

[12] IAEA 2020

[13] Logical access to virtual, non-material items; physical access to material items (for more information see IAEA 2011; IAEA 2018).

- security-level knowledge
  - detection and delay equipment's type, location, number, guard's location, patrol routes, security protocols
  - vulnerabilities
  - offensive tactics, weapons, martial arts skills, explosives
  - external response force
- external partners, suppliers
  - contracts
  - expected deliveries and dispatches
  - waste collection arrangements
  - mechanics, maintenance

As detailed above, it can be seen that the possibilities for insiders range widely, the circumstances are in their favour. What can the security organisation do? "Quis custodiet ipsos custodes?"[14]

Insider threat mitigation

After the target has been identified, the first step is to specify defensive measures to mitigate insider threat. Understanding preventive and protective measures are the keys to mitigate the insider threat; to detect, to delay and to respond to the malicious act and also to minimise the effects of the adversary act.

1. Preventive measures: "Identifying undesirables behavior or characteristics, which may indicate motivation prior to allowing them access; minimize the opportunities for malicious acts by limiting access, authority and knowledge."

2. "Protective measures: Detect, delay and respond to malicious act."[15]
The key is to reduce the opportunities to perpetrate any malicious act to the lowest possible level with preventive measures, as shown in Figure 1. In case if there is still another insider with opportunity for malicious act, protective measures have to help to detect, delay and respond to minimise the negative consequences of the insider's act. The deterrent factor of the preventive and protective measures is also effective, however, it is hardly measurable.

[14] "Quis custodiet ipsos custodes?" is a Latin phrase from Juvenal's Satire VI meaning: "Who will guard the guards themselves?"
[15] IAEA 2021.

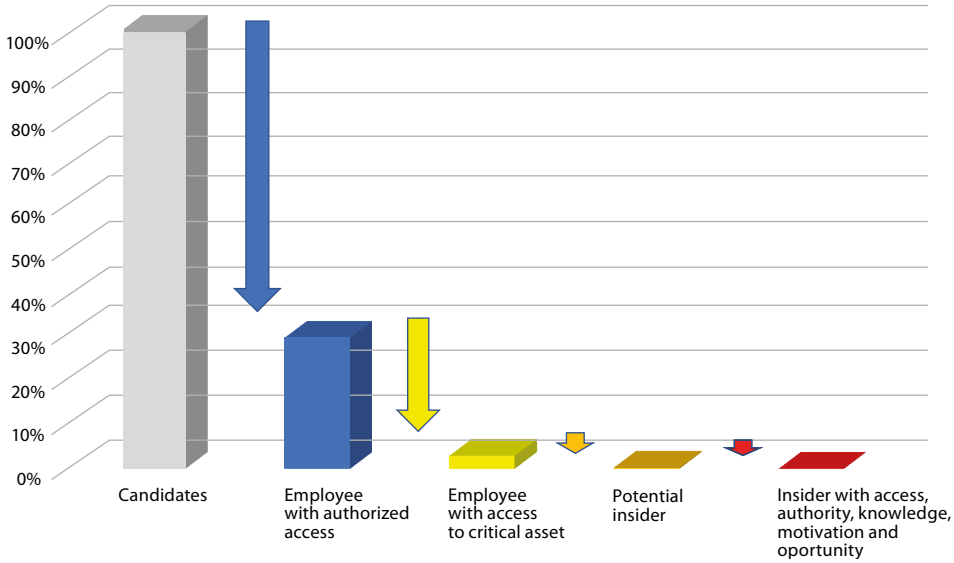


Figure 1: Reduce the opportunities with preventive measures
Source: compiled by the author

3. Main steps and useful tools to mitigate the insider threat

The effective tools to mitigate the insider threat are in the hands of the Management, the Human Resources Management and the Security Department of the facility. These contain preventive and protective elements of corporate policy, partnerships, internal rules, procedures, protocols and security system.

- Prevention of transformation into an insider globally
  At the macro-economic level i.e. at the level of the general regulation, the State sets out the normative legislation and lower level regulatory act which in disfavourable cases may trigger someone to become an insider. On the other hand, good insurance, favourable employment conditions and a good taxation system can avoid the conversion of individuals into insiders.
- Avoid the problem
  It means that inside the company a good recruitment process has to be developed to avoid recruiting people with high security risks. Do not employ someone who is a potential threat!
  The employment of a risky individual is avoidable by:
  – cooperation with authorities, intelligence services and investigating authority
  – cooperation, exchange of information and experience with other high security facilities
  – employing the best possible and reliable staff necessary for the operation of the facility and for the performance of security tasks in-house

  - developing appropriate recruitment requirements for jobs (e.g. security clearance, psychological screening, avoiding persons with dependency or other factors owing to which an individual could be coerced later)
- Prevent the transformation from employee to insider[16]
  The company encourages loyalty by offering favourable conditions to its employees to prevent their dissatisfaction.
  - clear management communication and management reporting to employees on issues that affect everyone (e.g. employee forums, regular meetings)
  - open communication between departments
  - a clear and transparent organisational structure (hierarchies, responsibilities)
  - corporate security culture, security awareness training (entry-level and refresher training, out-of-sequence training if necessary)
  - encouraging questioning behaviour
  - maintaining alertness (e.g. reducing workload, taking rest periods)
  - supporting the integration of new employees (mentorship program)
  - developing a system that encourages employee loyalty, low turnover and employee satisfaction, and retention: a stable and predictable working environment, a career development model, good relations between employees and between management and employees, a high pay and reward system, fringe benefits, positive feedback
  - encouraging less inter- and intra-departmental rivalry and teamwork (e.g. by organising training sessions)
- Reduce the opportunities
  The security organisation reduces the opportunity of malicious act with regulators and controls.
  - introducing a tiered licensing system – sharing of rights – to reduce the likelihood of extortion, coercion, threats and abuse
  - encouraging continuous training, further training and self-training of the security organization (learning new tools, tactics and methods)
  - developing an audited supplier system
  - avoiding an over-regulated environment[17]
  - creating, communicating and enforcing a regulatory environment that is logical, reasonable, transparent, understandable, clear, strict but fair and enforceable, and applies equally to all
  - enforcing compliance where necessary (e.g. through the operation of security system, consistent sanctions for non-compliance and exceptions)
  - keeping the regulations up to date, revising and amending them as necessary
  - enforcing the escort of persons without independent entry permit
  - application of security service, with patrolling guards

[16] "Prevention of insider threats is a high priority, but leaders and operators should never succumb to the temptation to minimize emergency response and mitigation efforts in order to maintain the illusion that there is nothing to fear" (Bunn–Sagan 2016: 171).

[17] "In many cases the security rules are so complex that employees violate them inadvertently" (Bunn–Sagan 2016: 171).

  - applying the DiD[18] principle
  - the redundant and diverse design of the security system, its continued operation in a decentralised, "offline" mode in the event of sabotage
  - restricting access to elements of the security system (e.g. control panel of the walkthrough metal detector, software update)
  - access control with multi-level personal identification, restriction of access and key acquisition rights, adaptation to area and job; strive to ensure that no more licenses are issued than are minimally necessary for the operation of the facility (necessary and sufficient principle)
  - security screening (search of prohibited items) of persons, luggage, vehicle ("remote screening"[19] where applicable) at entry points
  - screening and refusal of entry to suspicious persons and persons under the influence of alcohol or narcotics
  - applying the principles of confidentiality and integrity: restricting physical and logical access to sensitive information (e.g. different levels of software privileges, encrypted communication, use of information splitting (fragmentation of critical information, codes, passwords), digital signatures)
- Vigilance
  Paying attention to changes in employee behaviour.
  - monitoring changes in employee behaviour (e.g. family problems, radicalisation, addiction problems) through daily work contact
  - encouraging the reporting of suspicious persons or incidents to the direct manager and/or the security organisation
  - identification[20] and periodic scanning of critical systems and system components (to detect preparation for sabotage)[21]
  - incentives for cross-checking (holders with permanent entry permit may ask others to prove their identity)
  - periodic reassessment of the trustworthiness, watch the changes of the colleagues (e.g. severe dissatisfaction with his/her private or professional life)
  - training of security staff, e.g. training in the use of security screening equipment (entry, periodic/refresher, non-routine) for operating staff, incorporate possible insider tactics into the training and exercise program
  - periodic vulnerability assessment, assessing the effectiveness of the security system with taking into account the possible insider(s),[22] including with the evaluation of the results

18 Defence in depth: The increasingly stringent – from the outside towards the installation to be protected – layers of the elements of the security system, which requires more and more time, equipment, knowledge and preparation to penetrate by adversary.

19 Remote screening: the operator of the screening machine is not in the same room as the luggage, so he/she cannot see who the luggage belongs to (based on the "black box" principle).

20 "The first step involves identifying those components or areas that could be potentially vulnerable to acts of insider sabotage and are targets within a target set" (Sandia National Laboratories 2019).

21 For more information on the extreme manifestations of sabotage tools that can be used see Daruka 2012: 33.

22 Always keep in mind that "any vulnerability assessment which finds no vulnerabilities or only a few is worthless and wrong" (Johnston 2013).

  - updating the protection plan by adapting new vulnerabilities and insider tactics
  - a quality assurance system (periodic and random checks of security system, periodic review of the effectiveness of preventive and protective measures, with testing of equipment at the time of taking over the service)[23]
- Insider inside
  In case if there is still an insider with opportunity for malicious act, protective measures have to face violence: detect, delay and respond, in order to minimise the negative effects of the insider's act and mitigate the caused damage.
  - developing and practicing entry and exit, emergency, security incident management and other plans and protocols
  - installing sabotage-proof, tamper resistant access control, intrusion detection and video surveillance systems at critical locations (e.g. zone barriers, zone barrier hatches, emergency exits) with time-stamped logging and traceability of events and alerts (for incident assessment)
  - maintaining the efficiency of the security system by ensuring adequate availability (e.g. by employing operators and repair and maintenance staff)
  - restricting and slowing down the access to priority premises (access protocol: interlock, time lock, two-person rule[24])
  - application of the "guardian angel policy"[25] for protecting the security staff

Effective defence against an insider becomes more difficult by the fact that most of the time it is only possible to identify the insider if the insider's tactics are known. Insiders' tactics achieve their goal by exploiting a perceived or real vulnerability in the security system. The potential fundamental elements of protection are: the legislation and normative acts; the national security services; the law enforcement structures; the judiciary system; the corporate policy and strategy; regulations (policies, procedures); trainings (security awareness training, entry-level and refresher training); trustworthiness assessment; security system (mechanical protection, integrated intrusion detection, access control and video surveillance system, security service).

Given the creative nature of the human mind and the unpredictability of human actions, possible passive and active insider tactics and protective measures to prevent, identify and mitigate the damage caused by insiders are listed above from the point of view of a security manager of a high security facility.

---

23 "Do not assume, always asses and assess (and test) as realistic as possible. Unfortunately, realistic testing of how well insider protections work in practice is very difficult; genuinely realistic tests could compromise safety or puts testers at risk, while tests that security personnel and other staff know are taking place do not genuinely test the performance of the system" (Bunn–Sagan 2016: 174).

24 Two-person or "two-man rule is a strategy where two people must be in an area together, thus mitigating insider threats to certain critical areas" (U.S. Department of Defense 2019). The effectiveness of the two-person rule can be increased by rotating teams of two (to prevent over-confidentiality).

25 Guardian angel policy is an effective defensive measure. The policy means that against a possible insider attack at least one person always has to remain armed and vigilant. It can be applied to form a team of three guards (Bunn–Sagan 2016: 116).

It is noteworthy, that the most effective measures and actions against insiders can also lead to very radical actions. In these cases, an extreme action usually causes the destruction of environmental factors and has a potential for maximum damage.[26]

By implementing the measures detailed above, the security system will have effective, largely preventive, and better incident detection tools against insiders.

Summary

The fight against insiders is an imbalanced fight. There is no universal or organisation-specific antidote to avoid 100% such attacks while the human factor is present. What can we do? We can strive for prevention, watch our colleagues, implement risk mitigation measures, test, practice and keep the vigilance high all the time. Keep in mind that the threat represented by insiders is a real and major security challenge and never forget that the conspiracies of multiple insiders are also possible.[27]

References

Bunn, Matthew – Sagan, Scott D. eds. (2016): *Insider Threats.* Ithaca: Cornell University Press. Online: https://doi.org/10.7591/9781501705946

Daruka, Norbert (2012): Terroristák és taktikák, avagy védekezz, ha tudsz. *Repülés-tudományi Közlemények,* 24(2), 33–41.

Daruka, Norbert (2018): A jövő háborúi az improvizált robbanószerkezetek alkalmazásának tekintetében. *Seregszemle,* 16(2), 7–22.

IAEA (2008): *Preventive and Protective Measures against Insider Threats. NSS-8.* Vienna: International Atomic Energy Agency.

IAEA (2011): *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). NSS-13.* Vienna: International Atomic Energy Agency.

IAEA (2013): *Objective and Essential Elements of a State's Nuclear Security Regime. NSS-20.* Vienna: International Atomic Energy Agency.

IAEA (2018): *Computer Security of Instrumentation and Control Systems at Nuclear Facilities. NSS-33T.* Vienna: International Atomic Energy Agency.

IAEA (2020): *Preventive and Protective Measures Against Insider Threats. NSS-8G.* Vienna: International Atomic Energy Agency.

IAEA (2021): "Preventive and Protective Measures against Insider Threats", e-learning. International Atomic Energy Agency.

Sandia National Laboratories (2007): *Nuclear Power Plant Security Assessment.* Technical Manual, Sandia Report. SAND2007-5591. Albuquerque: Sandia National Laboratory.

[26] Read more about radicalised acts and their means in Daruka 2018: 7–22.

[27] "Conspiracies of multiple insiders, familiar with the weakness of the security system (and in some cases including guards or managers), are among the most difficult threats for the security systems to defeat" (Bunn–Sagan 2016: 156).

Sandia National Laboratories (2019): *Insider Analysis*. 27th International Training Course. New Mexico: Sandia National Laboratory.
Johnston, Roger G. (2013): *Security Maxims: Vulnerability Assessment Team.* Argonne National Laboratory.
U.S. Department of Defense (2019): Unified Facilities Criteria (UFC) Electronic Security Systems. UFC 4-021-02, Change 1.
U.S. Department of the Army (2001): *Physical Security.* FM 3-19.30. Washington, D.C.: U.S. Army Headquarters.

NEMZETBIZTONSÁGI SZEMLE
11. évfolyam (2023) 1. szám 62–77. • DOI: 10.32561/nsz.2023.1.5

Kegyes Tamás,[1] Süle Zoltán,[2] Abonyi János[3]

Az információmenedzsment szerepe az ABV-védelemben[4]

The Role of Information Management in CBRN Protection

Az atom-, bio- és vegyi (ABV-) incidensek felderítése kiemelt fontosságú feladat, amely évtizedek óta intenzíven kutatott téma. A folyamatos technológiai, adatfeldolgozási és automatizálási vívmányok újabb és újabb fejlesztési potenciált nyitnak az ABV-védelem terén is, amely napjainkra komplex, interdiszciplináris tudományterületté vált. Ennek megfelelően kémikusok, fizikusok, meteorológusok, katonai szakértők, programozók és adattudósok egyaránt közreműködnek a kutatásokban. A hazai ABV-védelmi képességek hatékony növelésének a kulcsa is abban rejlik, hogy megfelelően strukturált koncepció mentén folyamatos és célirányos fejlesztés történjen. Kutatásunk célja, hogy áttekintést adjunk a modern ABV-védelmi technológiák főbb komponenseiről, ezen belül összefoglaljuk az ABV-felderítés, illetve a döntéstámogatási lépések koncepcionális követelményeit, és bemutatjuk az információmenedzsment szerepét és legújabb lehetőségeit a folyamatokban.

Kulcsszavak: *ABV-védelem, információmenedzsment, döntéstámogató rendszer, ABV-architektúra*

The detection of chemical, biological, radiological and nuclear (CBRN) incidents is a high priority and has been an intensively researched topic for decades. Ongoing technological, data processing and automation advances are opening up new development potentials in the field of CBRN protection, which has become a complex, interdisciplinary field. Accordingly, chemists, physicists, meteorologists, military experts, programmers and data scientists are all involved in the researches. The key to effective enhancement of domestic CBRN defence capabilities also lies in continuous and directed development along a well-structured concept. The aim of our research is to provide an overview of the

[1] ELKH-PE Komplex Rendszerek Figyelemmel Kísérése Kutatócsoport, e-mail: kegyes.tamas@mik.uni-pannon.hu
[2] Pannon Egyetem Műszaki Informatikai Kar, e-mail: sule.zoltan@mik.uni-pannon.hu
[3] ELKH-PE Komplex Rendszerek Figyelemmel Kísérése Kutatócsoport, e-mail: janos@abonyilab.com
[4] A közlemény a TKP2021-NVA-10 számú projekt keretében az Innovációs és Technológiai Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a 2021. évi Tématerületi Kiválóság Program pályázati program finanszírozásában valósult meg.

main components of modern CBRN defence technologies, including a summary of the conceptual requirements for CBRN reconnaissance and decision support steps, and to present the role and recent opportunities of information management in these processes.

Keywords: *CBRN protection, information management, decision support system, CBRN architecture*

Bevezetés

Az atom-, bio- és vegyi (ABV-) védelmi tevékenységeket eleinte a nagyhatalmak hadászati potenciálja, illetve azok folyamatos, bár változó intenzitású fenyegetései indukálták. Napjainkban sokkal inkább az államok által nem kontrollálható terrorista csoportok jelentenek fenyegetést, de tovább bővíti az ABV-katasztrófák bekövetkezésének veszélyét az iparosodott, politikai, gazdasági és kulturális ellentétekkel terhelt időszakunk is.[5] Bár Magyarországon is több évtizedes múltja van az ABV-védelemnek, azonban a gyorsan változó világunkban újabb és újabb fejlesztési irányok nyílnak. Ezek közül többre vonatkozóan készültek már rövid, közép- és hosszú távú megvalósítási tervek, azonban végrehajtásuk egyéb prioritások mellett hosszú és időigényes folyamat.[6]

A célunk, hogy a napjainkban elérhető szakmai és tudományos eredményekre alapozva áttekintést nyújtsunk a modern ABV-védelem koncepcionális követelményeiről, ezáltal támogatva a célirányos és magas potenciált rejtő fejlesztési beruházások meghatározását. Munkánk során a releváns hazai és nemzetközi szakirodalom feltárásán túl rendszereztük az ABV-védelem funkcionális komponenseit, azonosítottuk azok hatékonyságnövelő lehetőségeit, feltártuk az adott műveletekhez kapcsolódó legjobb gyakorlatokat közvetlenül az ABV-védelem területéről, illetve az ekvivalens problémák esetén közvetve az ipari és termelési területekről is.

Cikkünk második fejezetében ismertetjük az ABV-védelem felépítését, ezen belül áttekintjük az ABV-felderítés eszközeit, azok jelenlegi potenciálját a „régi típusú" eljárásrendhez képest. Ezt követően bemutatjuk az információmenedzsment szerepét és lépéseit a nyers adatok feldolgozásában, majd meghatározunk néhány alapvető fontosságú célfüggvényt, amelyek lehetővé teszik az iparban széleskörűen alkalmazott optimalizációs technológiák felhasználását az ABV-felderítés területén is. A harmadik fejezetben áttekintjük a gépi tanulás alkalmazási lehetőségeit az ABV-védelmi folyamatokban, valamint ismertetjük a modelleknek az adatokra és azok feldolgozására vonatkozó előkövetelményeit, és a legjobb gyakorlatokon keresztül bemutatjuk a gépi tanulás nyújtotta hatékonyságnövelő képességeket. A negyedik fejezetben megvizsgáljuk a döntéstámogató rendszerek új fejlesztési irányait, különös tekintettel a hálózati döntéstámogatás tulajdonságaira. Röviden összefoglaljuk a hálózati és a hierarchikus megközelítések főbb különbségeit, kiemelve a jelentősebb eltéréseket eredményező aspektusokat. Az ötödik fejezetben javaslatot teszünk egy lehetséges ABV-védelmi rendszer magas szintű architektúrájára, bemutatunk egy prototípus-víziót, majd azonosítjuk

[5] Juhász 2001.
[6] Berek–Szabó 2012; Szabó 2017.

a főbb tervezési feladatcsoportokat. Végül a hatodik fejezetben összefoglaljuk az eredményeinket és a konklúziókat, valamint kiemelünk néhány magas potenciállal kecsegtető kutatási témát, amelyek tovább javíthatják az ABV-felderítési képességeket.

Az ABV-védelem felépítése

Az ABV-védelem rendkívül szerteágazó feladatok és lépések sorozata, azonban a tudományos konszenzus alapján öt főbb funkcionális területre bontható.[7]

- Felderítés: az ABV-incidens vagy -szennyezés érzékelése, kiterjedésének meghatározása, valamint az időbeli változásának nyomon követése. Az ABV-felderítés főbb feladatai a kimutatás, az azonosítás és a monitorozás. A kimutatás a levegőben lévő mérgező anyag érzékelését jelenti. Ez történhet kémiai vagy fizikai úton, humán vagy gépi közreműködéssel, egy vagy több szenzor felhasználásával, mechanikus vagy digitális érzékelőkkel, illetve ezek különböző kombinációjával. A főbb érzékelési eljárások az alábbiak:
  - hordozható kézi érzékelők;
  - okosszenzorok;
  - pilóta nélküli járművek;
  - földi/légi/vízi megfigyelő eszközök;
  - elektronikus adatforrások;
  - humán érzékelés.

A modern katonai szenzorhálózatok jellemzően lényegesen nagyobbak és komplexebbek, mint a civil szenzorhálózatok,[8] azonban az elmúlt évtizedek jelentős fejlesztései ellenére ezen érzékelők még mindig költségesek. Ezzel szemben a civil felhasználásban már megjelentek az alacsony költségű érzékelők, amelyek tömeges alkalmazásával figyelemre méltó eredményeket értek el.[9]

A méréseket végző érzékelők tekintetében a statikus, fix telepítésű szenzorokkal szemben egyre inkább teret nyernek a mobil érzékelők. Ezeknek három fajtáját különböztetjük meg:

- Nem vezérelt szenzorokat leginkább mozgó járművekre telepítenek.[10]
- Központilag vezérelt szenzorok esetén a megvizsgálandó területre lehet irányítani az eszközt, vagyis dinamikus, a környezeti mérések eredményeitől függően irányított megoldást alakítanak ki.[11]
- Autonóm vezérlésű szenzorok alkalmazásakor központi irányítás nélkül, de a mérési eredményektől függően lokális irányítású érzékelőket használnak.[12]

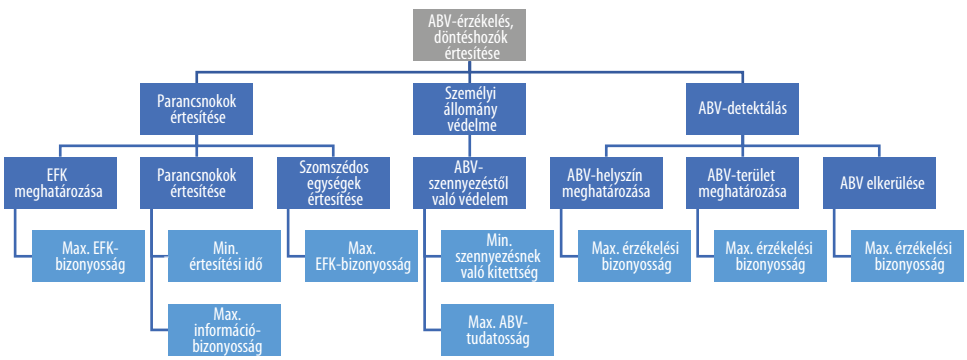
- Információmenedzsment: az ABV-felderítési adatok összegyűjtése, feldolgozása és továbbítása, amibe beletartoznak az információátviteli és -kiaknázási

[7] Berek 2016.
[8] Islam et al. 2009.
[9] Zhang–Madhani–Berg 2005.
[10] Madhani–Tauil–Zhang 2005.
[11] Kon et al. 2012.
[12] Bouhamed et al. 2020.

lépések is. Az utolsó évtizedekben lezajlódó informatikai forradalom során gyökeresen megváltozott a felhasználható eszköztár. A korábban elképzelhetetlen adatbőség és számítási kapacitás lehetőséget kínál arra, hogy az ABV-védelemben közreműködő személyi állomány helyett mind több műveletet gépi úton végezzenek el az emberi teljesítményt jelentősen meghaladó precizitással, megbízhatósággal és alacsony feldolgozási idővel. Azonban a szenzorokban képződő adatok feldolgozó rendszerek felé való továbbítása kapcsán számos követelménynek kell megfelelni:

- Hibamentesség: a mérési adatokat mindennemű megváltozási lehetőség kiiktatásával, a szenzor mérési pontosságával kell beküldeni.
- Alacsony késleltetési idő: a mérési időpillanattól számított legrövidebb időn belül kell továbbítani az adatokat.
- Energiahatékonyság: az alacsony késleltetési idő kritériumával szemben a folyamatos adatkapcsolat rendkívül energiaigényes lehet, ezért a – jellemzően akkumulátorról működő – szenzorok üzemidejének növeléséhez az adatküldési gyakoriság optimalizálása szükséges.
- Biztonság: a rendszer jellegéből fakadóan az adatok eltéríthetetlensége és megmásíthatatlansága alapvető fontosságú.
- Üzembiztosság: az érzékelési rendszer csak folyamatos működés mellett tudja ellátni legfőbb célját, így ennek biztosítása is kiemelt jelentőségű.

A mérési adatok központi összegyűjtését követően az információ kinyerése és a döntéstámogató műveletek elvégzése következik, amely az ABV-védelem legkritikusabb pontja.[13] Az 1. ábra egy ABV-védelmi döntéstámogató eszköz funkcionális felépítését ismerteti. Ennek alapján az elsőbbségi felderítési követelmények (EFK) relevanciájának bizonyosságára, az értesítési időkre, a szennyezésnek való kitettség mértékére és az érzékelési bizonyosságra vonatkozóan megfogalmazhatók egzakt célfüggvények, amelyek megnyitják az utat az ipari, gazdasági és kutatási területeken már sikeresen alkalmazott optimalizációs eljárások felhasználása előtt.



1. ábra: ABV döntéstámogató eszköz funkcionális felépítése
Forrás: Cascio et al. 2019

[13] Cascio et al. 2019.

- Fizikai védelem: az ABV-szennyezéssel veszélyeztetett állomány, valamint egyes tárgyi vagy gépi eszközök megóvása.
- Veszélykezelés: az ABV-szennyezés alóli mentesítési műveletek elvégzése.
- Egészségügyi ellenintézkedések és biztosítás: az állomány által elszenvedett ABV-ártalmaknak megfelelő orvosi ellátás biztosítása.

Cikkünk további részében elsősorban az információfeldolgozó és a döntéstámogató folyamatok hatékony szervezését tekintjük át. Ennek előfeltétele az ABV-felderítés módszereinek megismerése, így az alábbiakban ezt mutatjuk be részletesebben.

A gépi tanulás alkalmazási lehetőségei az ABV-megoldásokban

Napjainkban sorra jelennek meg újabb és újabb technológiák és módszerek, amelyek jelentős teljesítményjavulást és hatékonyságnövekedést eredményeznek az ipar és a gazdaság számos területén. Többek között a mesterséges intelligencia, a gépi tanulás, a robotok, az okoseszközök, az önvezető járművek, a drónok, a virtuális-valóság-megoldások, a nanotechnológia és a szintetikus organizmusok különböző alkalmazásai és felhasználásai olyan mértékben alakítják át életünket, hogy a negyedik ipari forradalomként hivatkoznak rájuk. Mindezen lehetőségek kiaknázása az ABV-védelem területén is elkezdődött, és a jelentős kihasználatlan potenciál miatt, vélhetően tartósabb folyamattá válik. Ebben a fejezetben áttekintjük az új technológiák alkalmazásainak számos „jó gyakorlatát" az ABV-védelem területén.

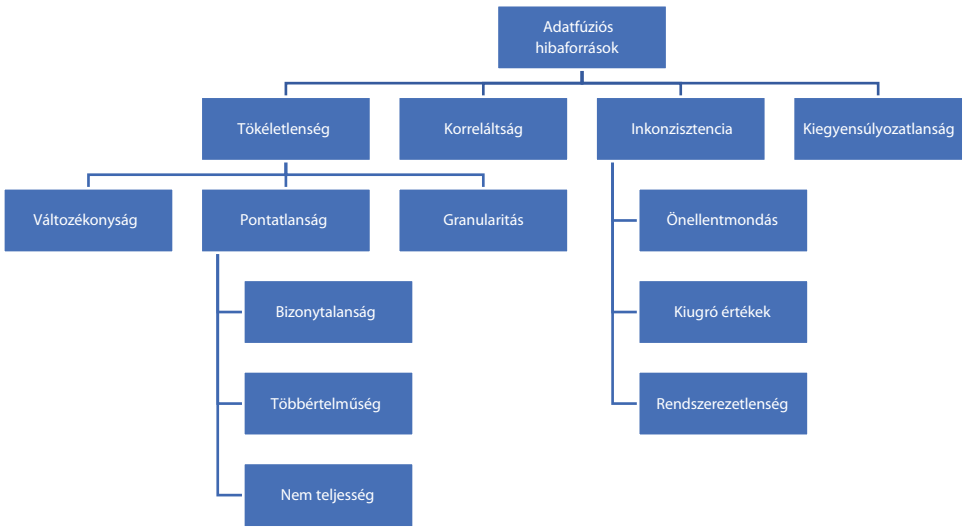
A gépi tanulási rendszerek használata során négy egymásra épülő réteget különböztetünk meg. Az első rétegben szerepelnek a forrásadat-előállítási műveletek. Ahhoz, hogy megfelelően ki lehessen aknázni a gépi tanulás nyújtotta lehetőségeket, elsősorban megfelelő mennyiségű, minőségű, terjedelmű és gyakoriságú adat szükséges, amelyeket össze kell kapcsolni, majd integrálni.

A gépi tanulási megoldások második rétegét az adattárolási, adatfeldolgozási és adat-előkészítési lépések alkotják. Mivel a különböző gépi tanulási módszerek bemeneti adatra vonatkozó előkövetelményei eltérők, így az adatstruktúrák és gépi tanulási módszerek kölcsönösen korlátozhatják egymást. A jól strukturált adatokhoz korlátozott autonómiájú felügyelt tanulási módszerek alkalmazhatók. A kép- és hangadatok esetében a megerősítéses tanulási módszerek használhatók, amelyek adaptív öntanuló funkciója a szituációs tapasztalathoz tud igazodni. A természetes nyelvi feldolgozó algoritmusok mindenféle hangfelismerésre, hangértelmezésre és hangorientáció vizsgálatára alkalmasak. A big data jellegű, nagy mennyiségű adat feldolgozását igénylő műveleteket leginkább neurális hálózatokkal lehet támogatni. Ezenfelül a mechanikus érzékelők okoseszközökkel (*Internet of Things,* IoT) integrálhatók, így az adatáramlás felgyorsítható, és sok esetben a távoli vezérlés is biztosítható.[14]

A gépi tanulási rendszerek harmadik rétegébe az adatfúziós és a modellalkotási feladatok tartoznak. Az ezzel foglalkozó szakemberek szerint a kifejlesztett modellek csak annyira lehetnek pontosak, amennyire a forrásadatok megfelelőek, így

[14] Ahmed 2022.

nem lehet eléggé hangsúlyozni, hogy milyen fontos a legmagasabb adatminőségre való törekvés. A 2. ábra bemutatja az adatfúziós hibaforrások típusait.[15] Ezek közül a mérési tökéletlenség típusai lényegében elkerülhetetlenek, amire a mérőeszközök minősítése során meghatározott várható mérési hibamérték figyelembevételével lehet felkészülni. Továbbá a mérőeszközök telepítési tervezésével és a mérőeszközök megfelelő kiválasztásával elérhető, hogy a mérési hibák a kívánt toleranciasávon belül maradjanak. Nagyrészt szintén tervezési kérdés a korreláltsági és kiegyensúlyozatlansági hibák kezelése, míg az inkonzisztencia fennállásának azonosítása és kiküszöbölése az adatfeldolgozási folyamatok validációs lépéseiben kezelhető.



2. ábra: Az adatfúziós hibaforrások típusai
Forrás: Khaleghi et al. 2013

Az adatfeldolgozási folyamatnak mindenképpen érdemes tartalmaznia egy robosztus adaptív programozási keretrendszert, amely képes korrigálni az adatok sokféleségét, tökéletlenségét, pontatlanságát és egyéb hibaforrásait.

A gépi tanulási módszerek rendkívül szerteágazók, de az alábbiakban bemutatjuk az ABV-védelem kapcsán már sikeresen alkalmazott és magas potenciállal rendelkező megoldásokat:

- *Okoseszközök (IoT), szenzorhálózatok*: Az ABV-érzékelés hagyományosan a humán személyzet által működtetett specifikus céleszközökkel történt. Ezzel a vizsgált szennyezéstípusok már alacsony koncentráció esetén is kimutathatók, azonban a személyzetnek a vizsgálati területre való kivonulása, a mérések elvégzése és az esetleges laboratóriumi kiértékelések jelentős átfutási időt követeltek egy olyan helyzetben, amikor minden perc számíthat. Ráadásul az ilyen érzékelési feladatra képes humán egységek száma is korlátozza az ABV-érzékelési képességeket.

[15] Khaleghi et al. 2013.

E kihívásokra hatékony választ nyújtanak az okoseszközök közé tartozó szenzorok, illetve az azokból felépülő szenzorhálózatok és szenzorklaszterek. A mögöttes elgondolás az, hogy az ABV-észlelési idő csökkentésével lehetőség nyílik a gyorsabb reagálásra. Ehhez leginkább a korai figyelmeztető rendszerek (*early warning systems,* EWS) kialakítása szükséges, amelyek akár alacsonyabb mérési pontosságú, de kiterjedtebb érzékelőkre, illetve az ezekből felépülő szenzorhálózatokra épülnek.[16] Emellett egyre növekvő figyelmet kapnak a különböző érzékelési technológiákat ötvöző szenzorklaszterek.[17] Mindkét esetben a mérési adatok feldúsítása a cél, amiből a feldolgozás során statisztikailag szignifikáns következtetések készíthetők, ráadásul a humán érzékeléshez képest alacsonyabb költségszinten és rövidebb észlelési időkkel.

- *Szenzorfúzió*: A modern ABV-védelmi megoldásokban több különböző típusú szenzort használnak egymással párhuzamosan. Ezek közül vannak nagy hatótávolságú érzékelők, mint a radar, az infravörös, illetve az elektrooptikai eszközök, valamint rövid hatótávolságú érzékelők, mint a Raman-spektrométerek, továbbá a pontérzékelők, mint az ionmobilitás-spektrométerek (IMS) és a kémiai ágens elemző eszközök. Az ABV-felderítés egyik kritikus pontja az, hogyan sikerül a különböző mérési eredmények integrálása a minél pontosabb helyzetértékeléshez. A szenzorfúziós technikák alkalmazásával kidolgoztak egy alacsony paraméterszámú aggregációs modellt, amely a szennyezési felhő kiterjedését a különböző típusú szenzorok mérési eredményeit ötvözve becsli meg.[18] Az ABV-védelmi információáramlás sértetlenségét biztosítva az esetleges mérési hibákat nem eliminálja, hanem a megbízhatósági indikátorok kis értékeivel jelzi annak alacsony bizonyosságát. A módszer könnyen automatizálható és valós idejű adatfeldolgozást tesz lehetővé, azonban a modell előzetes paraméterezése szükséges. A modellbe a humán megfigyelések a pontszerű mérőeszközök mintájára integrálhatók.
- *Szennyezési felhők dinamikájának modellezése:* A légkörbe jutó és az onnan kiülepedő szennyező anyagok általában nem koncentráltan, hanem hosszú távon, nagy területen fejtik ki hatásukat, így a döntési folyamatok során nélkülözhetetlen olyan módszerek alkalmazása, amelyek minél gyorsabban, a lehető legpontosabb képet szolgáltatják a katasztrófák várható következményeiről.[19] A szennyezések légköri terjedésének meghatározásához különféle időjárási adatok szükségesek: a szél iránya, sebessége, változékonysága, napi menete, vertikális profilja; a hőmérséklet rétegződése; a relatív nedvesség és csapadék, valamint a légköri stabilitás. Ezen adatok alapvető fontosságúak a szennyezés dinamikájának meghatározásához, ami jól mutatja azt is, hogy az érzékelési rétegben nem elegendő csupán a szennyezés meglétét és mértékét mérni, hanem további, például időjárási szenzorálás is szükséges. A mért értékek, valamint az előrejelzési modellek adatai alapján a szinoptikus szakemberek állítják elő a talajmenti meteorológiai információkat tartalmazó kódolt üzenetet

16 Marinelli et al. 2015.
17 Lawrence–Kuhne–Swindle 2020.
18 Lundberg–Paffenroth–Yosinski 2010.
19 Viengdavanh 2012.

(CDM), de az előrejelzett mezők alapján emberi beavatkozás nélkül, algoritmusok segítségével is készülhetnek az üzenetek.[20]
Számos automatizált ABV-szennyezési modellező szoftver áll már éles használatban, amelyeknek jellemzően az alábbi funkcionalitásai vannak: ABV-üzenetek készítése, küldése, fogadása, feldolgozása standardizált formátumban; adatátvitel különböző protokollok szerint; ABV-csapások és nem csapásból származó kibocsátások értékelése, sugárdózis és a sugárszint kiszámítása, térinformatikai megjelenítés, gyakorlatok tervezése, beépített veszélyhelyzet-elhárítási kézikönyv.[21] A feldolgozások során változatos, az adott részfeladatra optimalizált gépi tanulási modelleket használtunk fel, amelyek részletes bemutatása túlmutat jelen cikk keretein. Amit viszont fontos kiemelni, hogy a szennyezési felhők dinamikájának és kiterjedésének közel valós idejű gépi modellezése olyan számítási és előtanulási kapacitásokat mozgósít, amelyek a humán szakértők számára elérhetetlenek.

- *Szimulációs döntéstámogatás:* ABV-esemény bekövetkezésekor rendkívül komplex helyzetben kell meghozni a döntéseket, ami igen megterhelő a folyamatban részt vevő személyzet számára, mert bizonytalan, összetett és dinamikusan változó helyzetre kell optimálisan reagálniuk. Mindezt fokozza az a lelki teher, hogy döntéseiken közvetlenül emberéletek múlhatnak. Ráadásul az ABV-események jelentős hatású, de kis valószínűséggel bekövetkező, ritka események, következésképpen nehezen tipizálhatók, és nem igazán hasonlíthatók össze egymással, mert más földrajzi helyen, eltérő körülmények között következnek be. Mindezen tényezők azt támasztják alá, hogy az ABV-védelem döntési folyamataiban a lehető legátfogóbb információkra van szükség, hogy a hibás döntések kockázatát minimalizálni lehessen.[22]
  Ehhez a rendelkezésre álló és a folyamat korábbi lépései során előállított adatokat és információkat felhasználva a rendszer sorrendezi a hatályos műveleti eljárásrend szabályait azok relevanciája alapján, és a döntések következményeire valószínűségi számításokat végez. Így az illetékes döntéshozó számára jelentős támogatást nyújt azáltal, hogy a megfelelő műveleti lépéseket azonosítja, és az egyes szcenáriók bekövetkezési esélyeit számszerűsíti.
- *Virtuális ikerkörnyezet:* Az ABV-védelmi kiképzés általában fizikai gyakorlatként történik, ami alapvetően szükséges és hasznos, azonban időigényes és költséges is. Az ipari gyártóüzemek működésének elemzéséhez és optimalizálásához egyre nagyobb arányban használnak digitális ikerkörnyezetet *(digital twin),* amely tulajdonképpen az üzem virtuális mása. Ebben gyorsan és költséghatékonyan végezhetők el a gyártósori változtatások komplex elemzései. Az ABV-védelemmel érintett területek teljes virtuális másának elkészítése sajnos minden realitáson túlnyúló feladat lenne, azonban a kiképzési gyakorlatok céljára már készítettek virtuális ikerkörnyezeteket.[23] Ennek keretében virtuális valóság, kevert virtuális valóság és személyi számítógépes megoldásokat alakítottak ki,

[20] Viengdavanh 2012.
[21] Viengdavanh 2012.
[22] Drury–Ullah–Madden 2018.
[23] Altan et al. 2022.

amelyeket több, a fizikai gyakorlatokat korábban teljesítő résztvevő bevonásával értékeltek. Az eredmények alapján a virtuális ikerkörnyezetek fontos szerepet kaphatnak a jövőbeni ABV-védelmi kiképzések során.

A gépi tanulási rendszerek negyedik rétegét az információmegosztási műveletek alkotják. Az ABV-védelem vonatkozásában ez a meghozott döntéseken túl a folyamat megelőző részeiben keletkező származtatott és számított információkat is magában foglalja. Az elmúlt évek során ezen a területen is új megközelítések nyertek teret, amit önálló fejezetben tárgyalunk.

A döntéstámogató rendszerek új irányai

A vezeték nélküli hálózatok, az okoseszközök és a személyzet nélküli érzékelők széles körű elterjedése hasonló mértékben változtatja meg az információs rendszerek működését, mint negyed évszázada az internet. Ezen átalakulás során a hálózat és a hálózati működés az információs rendszerek uralkodó paradigmájává vált, és az általa lehetővé tett páratlan összekapcsolódottság gyökeresen megváltoztatta az egyének, a vállalatok, a kormányok és a társadalmak működését, kommunikációját. Ebben a fejezetben a hálózati döntéstámogató rendszerek (*network decision support system,* NWDSS) felépítését mutatjuk be, kezdve azok alapvető tulajdonságaival:[24]

- *Képlékeny hálózat heterogén elemekkel.* A koncepció lényege a strukturális felépítésen alapul. A hálózat csomópontjai egyaránt lehetnek személyek, érzékelők vagy szoftverágensek. A személyi csomópontok önállóan egyénként vagy csoportosan is alkothatnak egy egységet. Ez utóbbi jellemzően valamilyen szervezeti egységet jelent, például katonai egységet, bűnüldöző szervet, tűzoltókat vagy különféle helyi és kormányzati intézményi csoportokat. A hálózat személyi csomópontjai rendre tartalmaznak döntéshozókat, noha a hálózati intelligencia bizonyos alacsony szintű döntéseket meghozhat a szoftverágensek segítségével, így például a hálózat kezelését és ellenőrzését is.
  A hálózat képlékenysége annak folyamatos változásából fakad: a részt vevő személyek kikapcsolhatják a telefonjukat, az érzékelők lemerülhetnek vagy csendes üzemmódra válthatnak. A hálózati csúcspontok összekapcsoltsága is dinamikusan változik, így a hálózat pontos felépítése lényegében állandó változásban van.
- *Érzékelőbőség.* A hálózat a definíciója szerint tartalmazhat emberi és nem emberi komponenseket érzékelőként. A gépi szenzorok miniatürizálódása és számosságának robbanásszerű növekedése jelenti a hálózati döntéstámogató rendszerek kialakulásának legfőbb hajtóerejét, különös tekintettel a katasztrófaelhárítási, a honvédelmi és a katonai műveleti területeken.
- *Egyidejű ember–gép, gép–gép és ember–ember interakciók*. A személyzet nélküli érzékelők jelentősen megnövelik az ember–ember interakciókon túli együttműködési tevékenységek iránti követelményeket. A tradicionális döntéstámogató

[24] Bordetsky–Dolk 2013.

rendszerek elsősorban az ember–gép interakciókra (*human-computer interaction,* HCI) fókuszáltak, de a szenzorok számosságának növekedésével ez kezelhetetlenné vált. Ember–szenzor kapcsolat szükséges, amikor az eszközt irányítani vagy vezérelni kell. Szenzor–ember kommunikáció indokolt akkor, ha az érzékelő valamilyen figyelemre méltó esemény bekövetkezését észleli. Szenzor–szenzor kapcsolat segítségével irányítható egy személyzet nélküli jármű. Végül az ember–ember interakciók továbbra is nélkülözhetetlen csatornát jelentenek az információáramlásban.

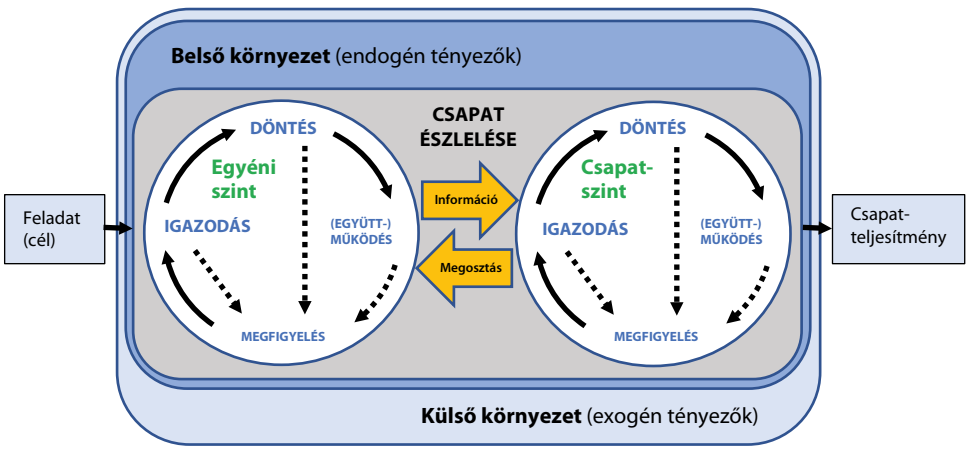
- *Nyitott, generatív és önszerveződő rendszer.* A hálózati döntéstámogató rendszerhez szabadon csatlakoztathatók újabb és újabb csúcspontok, ahogy az megfigyelhető számos internetalapú közösségi platformon is. A kialakuló rendszer generatív abban az értelemben, hogy egyszerű szabályok alapján működik, és hálózatelméleti módszerekkel leírható a viselkedése. Az így felépülő megoldások korábban jellemzően problémamegoldó fókusszal működtek, a koncepció újdonsága, hogy ez döntéstámogató céllal is hasznosítható. Mindazonáltal a polgári-katonai információmegosztási modell a kialakulóban lévő hálózatalapú parancsnoki és irányítási terület számára is hasznosítható egy információszűrő hálózatra épített új kockázatkezelési modell bevezetésével.[25]
- *Tudásháló és kialakuló tudásfolyamatok.* A hálózati döntéstámogató rendszerekben többféle emberi és nem emberi közreműködő együttműködése által keletkezhet információ, amelyek feltárásával a különböző célok elérése megvalósíthatóvá válik, például a különböző típusú incidensek azonosítása vagy egy fizikai terület megfigyelése. A kialakuló hálózati tudás minősége központi jelentőségű a közreműködő emberek, szenzorok és szoftverágensek együttműködésének hatékonyságára és eredményességére nézve. Tudásmenedzsment szempontból bármilyen hálózat értelmezhető tudáshálóként is az egyes csomópontokban elérhető kollektív információ mérésével. Az információáramlás dinamikája a tudásfolyamok kialakulásával (*emerging knowledge processes,* EKP) fejlődhet, amelyek a tudásközpontok közötti áramlások fokozásával vagy fejlesztésével javíthatók. A hálózat képlékenységéből fakadóan a tudásfolyamokat változó közreműködői halmazok és azok változó kapcsolódási struktúrája jellemzi. A résztvevők információismereti profilja előzetesen nem ismert, azok a működés során az információáramlatok letisztulása után rajzolódnak ki. A hálózati döntéstámogatási rendszerek kulcsfontosságú tudásfolyama a szakértői visszanyúlás, ahol a döntéshozóknak lehetőségük nyílik akár emberi, akár gépi tudásbázishoz való hozzáférésre.
- *Agilis, együttműködő döntéshozatal a „végeken".* A hálózati döntéstámogató rendszerek, különösen a vészhelyzeti reagálás vagy a harctéri taktikai hadműveletek esetén alkalmasak a decentralizált döntéshozatali folyamatok támogatására. Ezek gyakran kaotikusak, nem rendelkeznek előzetes forgatókönyvekkel, tele vannak nagy kockázatú helyzetekkel és erős időkényszerekkel, valamint nem teszik lehetővé a klasszikus hierarchikus döntési folyamatok alkalmazását sem. Ehhez igazodva a döntési folyamatokban együttműködő

[25] Chlebo–Christman–Johnson 2011.

résztvevők szervezete jellemzően ellaposodik, és a döntéshozatal nem központilag, hanem a „végeken” történik meg agilis módon.

- *Számítógépes modellezés és kísérletezés.* Az olyan generatív hálózatok elemzésére, mint amilyenek a döntéstámogató hálózatok is, leginkább számítógépes modelleket használnak. Ennek keretében egy virtuális környezetben szimulálják a hálózat működését, és az eredmények alapján finomhangolhatók a hálózati szabályok, elősegítve a hatékonyabb tudásáramok kialakulását.

A nem megfelelően kontrollált döntéshozatal könnyedén hibás lépésekhez vezethet.[26] Ahhoz, hogy jól működő információmegosztási protokollt lehessen kialakítani, érdemes figyelembe venni annak szerepét. Napjainkban már általános jelenség, hogy különböző méretű csapatokat vagy szervezeti egységeket használnak szervezeti célok eléréséhez. A csapatok egymástól kölcsönösen függő tagokból állnak, akik változatos interakciós folyamatokon keresztül koordinálják a munkájukat. Ezek az interakciós folyamatok kulcsfontosságúak a helyzetfelismerés és -értékelés elvégzésében akár dinamikusan változó környezetben is. A pontos, időszerű, megfelelően megosztott információk létfontosságúak a csapatfeladatok elvégzéséhez, különösen olyan akciócsoportoknál, amelyek összetett vagy időérzékeny műveleteket hajtanak végre. A csapatok észlelési folyamatmodelljét mutatja a 3. ábra.[27] E megközelítés erőssége, hogy a két irányú információmegosztási platform segítségével lehetőséget nyújt bizonyos döntések alacsonyabb szintű meghozatalához, amelynek kontrollálását az adott csapat végzi.



3. ábra: A csapatészlelési folyamat modellje
Forrás: Mullins 2021

[26] Mullins 2021.
[27] Mullins 2021.

A modern ABV-védelmi keretrendszer prototípusmodellje

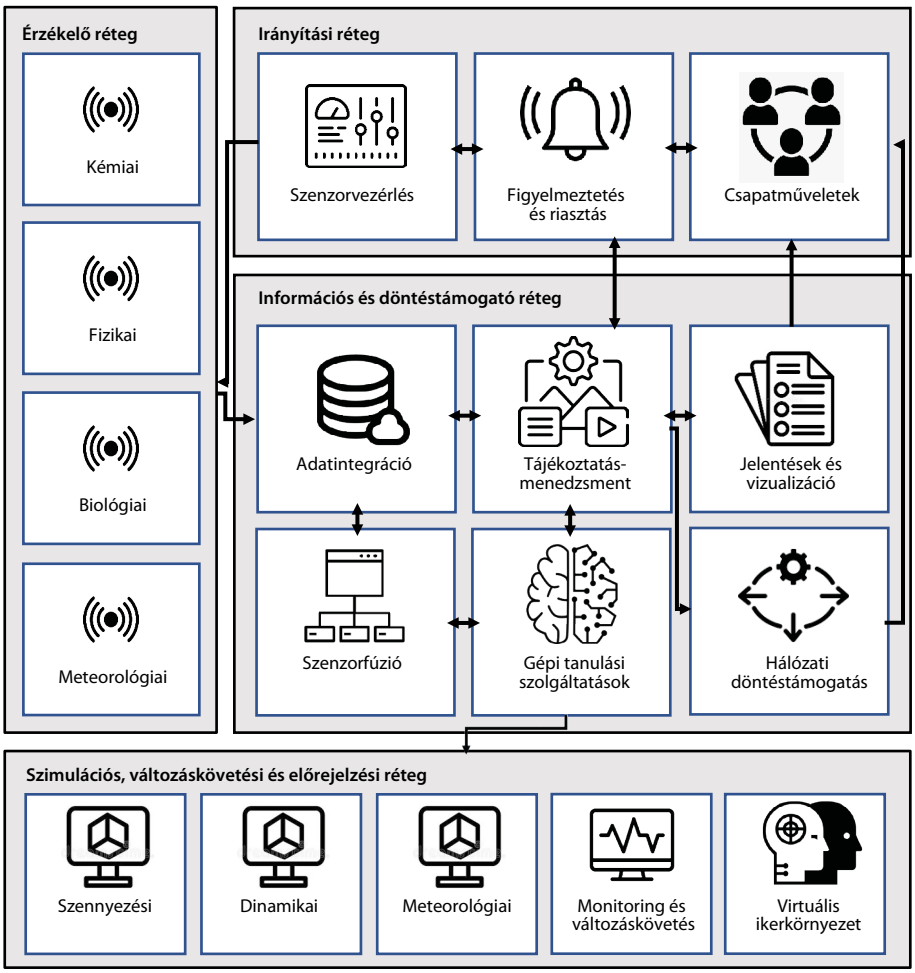
Ebben a fejezetben bemutatunk egy modern ABV-védelmi keretrendszert, amely jelentősen épít a lengyel mintára,[28] illetve a páneurópai EU-Sense projekt megállapításaira,[29] de azoktól több ponton is eltér. Hangsúlyozzuk, hogy a következőkben ismertetett keretrendszer egy prototípusmodell, amely – ha az igények indokolják – rugalmasan bővíthető további modulokkal, emellett a felépítéséből fakadóan a fejlesztések könnyen szakaszolhatók. Az alábbiakban áttekintjük a keretrendszer főbb komponenseit:

- *ABV szennyezésérzékelő réteg:* tartalmazza a fix telepítésű és a mozgó szenzorokat, valamint a humán megfigyelőket is. Jellege és típusa szerint heterogén felépítésű. Célja a vizsgálat alá vont területre vonatkozó adatgyűjtés.
- *ABV szenzorvezérlő réteg:* az érzékelés hatékonyságának maximalizálására törekedve irányítja a mozgatható szenzorokat, hogy megfelelő lefedettségű feltárást biztosítson a kapcsolódó folyamatokhoz.
- *ABV adatintegrációs réteg:* az érzékelőkből érkező nyers adatok összegyűjtésére, egységesítésére és tárolására szolgál.
- *ABV szenzorfúziós réteg:* a különböző érzékelőkből származó adatok összesítését és integrálását, majd a szennyezés fennállásának, jellegének, típusának és mértékének meghatározását végzi. A működtetéséhez előzetes paraméterezés és kalibráció szükséges. Ebbe a rétegbe beágyazhatók további adatminőség-ellenőrzési és validációs lépések is.
- *ABV monitoring és változáskövető réteg:* a szennyezés időbeli változásának és térbeli mozgásának dinamikai meghatározását végzi.
- *ABV szimulációs előrejelzési réteg:* a meteorológiai, a földrajzi és a szennyezésdinamikai adatok felhasználásával a szennyezés várható kiterjedését és eloszlását jelzi előre. Fejlettebb verzióban a különböző műveleti szcenáriókra vonatkozóan is értékeléseket készít, amelyből a közbeavatkozás várható hatásait, illetve azok humán és gépi erőforrásokon várható következmények kiértékelését végzi döntéstámogatási célból.
- *ABV információmenedzsment-réteg:* az érzékeléstől a releváns szabályozások vonatkozó részeinek meghatározásán, valamint a döntéstámogatási célú származtatott és kalkulált információkon és a meghozott döntéseken át az elvégzett és a folyamatban lévő műveletekig bezárólag a teljes ABV-védelmi megoldást átfogó információtovábbítási és -megosztási réteg. Felépítését tekintve minél magasabb fokon automatizált, szigorú jogosultságkezelést megvalósító, beépített naplózási funkciót biztosító platform és kommunikációs protokoll.
- *ABV-védelmi, gépi tanulási szolgáltatások:* olyan kötött és kötetlen módon használható eljárások és szolgáltatások halmaza, amelyek a meglévő információkból a felhasznált modelleken keresztül származtatott következtetéseket és kiterjesztéseket készítenek objektív, reprodukálható módon. Mivel napjainkban a számítási kapacitások lehetővé teszik, ezért a humán képességeket messze meghaladó komplexitású problémák megoldásában, az emberi feldolgozási

[28] Tarapata et al. 2021.
[29] Gawlik-Kobylińska et al. 2021.

idők töredéke alatt képesek elvégezni a rájuk delegált lépéseket. Tekintettel arra, hogy a folyamat számos pontján felhasználhatók a gépi tanulás képességei, ezért a javasolt architektúrában központi szolgáltatásként szerepelnek.
- *ABV vizualizációs és jelentésszolgálati réteg*: az információtovábbítás hatékonyságának maximalizálására optimalizált réteg, amely a standard formátumokon és a szabályzatokban meghatározott jelentéseken túl dinamikus, önkiszolgáló információs felülettel is rendelkezik.
- *ABV figyelmeztetési és riasztási réteg*: az ABV-védelmi folyamatban érintett teljes állományra kiterjedő információs mechanizmus.

Végül az általunk javasolt ABV-védelmi rendszer architekturális felépítését és a fentebb megadott komponensek összefüggéseit és kapcsolatait mutatja a 4. ábra.



4. ábra: Javasolt ABV-védelmi keretrendszer
Forrás: a szerzők szerkesztése

Összefoglalás

A közelmúltban számos területen történtek olyan technológiai és működésszervezési áttörések, amelyek hatékony segítséget nyújthatnak az ABV-védelem továbbfejlesztésében. Az ABV-érzékeléshez használt szenzortechnikákon túl legalább olyan fontos a hibrid (emberi-gépi) érzékelési hálózat információmegosztási és döntéstámogató rétegeinek megfelelő tervezése. Ennek eléréséhez javasolt az egyirányú információs csatornák többirányúvá tétele, validációs és kontrollmechanizmusok beépítése, az információfolyamok gördülékenységének támogatása, a gépi szenzorok és számítógépes mesterséges ágensek integrálása. Bemutattuk a hálózati döntéstámogató rendszerek jellemzőit, amelyek rámutatnak arra, hogy a statikus műveleti forgatókönyveken túl milyen struktúrával lehet hatékonyan reagálni a váratlan helyzetek kezelésére annak érdekében, hogy a kollektív tudás alapján optimális döntések születhessenek.

Mindezen lehetőségek önállóan is képesek az ABV-védelem egy-egy feladatát továbbfejleszteni, azonban a hatékonyságnövelési potenciáljuk magasabb fokú kihasználásához érdemes a teljes rendszerre vonatkozó fejlesztési koncepciót követni. Ezt elősegítendő átfogó javaslatot tettünk egy modern ABV-védelmi keretrendszerre vonatkozóan, amelyre modulárisan felfűzhetők az egyes komponenseket érintő fejlesztések. Ezek közös célja az érzékelési, feldolgozási és reagálási idők jelentős csökkentése, az információkiaknázási lépések megbízhatóságának és integráltságának növelése, az automatizált műveletek által az ABV-védelmi műveletek kapacitásainak kiterjesztése és legfőképp a döntések hatékony támogatása, valamint a szűk keresztmetszetek feloldása.

Irodalomjegyzék

Ahmed, Nizam Uddin (2022): Integrating Machine Learning in Military Intelligence Process: Study Of Futuristic Approaches Towards Human-Machine Collaboration. *National Defence College E-Journal,* 2(1), 59–89.

Altan, Burak – Gürer, Servet – Alsamarei, Ali – Demir, Damla Kıvılcım – Düzgün, H. Şebnem – Erkayaoğlu, Mustafa– Surer, Elif (2022): Developing Serious Games for CBRN-e Training in Mixed Reality, Virtual Reality, and Computer-Based Environments. *International Journal of Disaster Risk Reduction,* 77, 103022. Online: https://doi.org/10.1016/j.ijdrr.2022.103022

Berek Tamás (2016): LCD-3 széria, mint lehetséges hatékony eszköz az alegységek ABV védelmi felszerelés rendszerében. *Műszaki Katonai Közlöny,* 26(1), 68–79.

Berek Tamás – Szabó Sándor (2012): Az ABV mentesítő állomás Force Protection koncepciója. *Hadmérnök,* 7(3), 89–99.

Bordetsky, Alex – Dolk, Daniel (2013): *A Conceptual Model for Network Decision Support Systems*. In *46th Hawaii International Conference on System Sciences*. Wailea, 1212–1221. Online: https://doi.org/10.1109/HICSS.2013.32

Bouhamed, Omar – Ghazzai, Hakim – Besbes, Hichem – Massoud, Yehia (2020): A UAV-Assisted Data Collection for Wireless Sensor Networks: Autonomous

Navigation and Scheduling. *IEEE Access,* 8, 110446–110460. Online: https://doi.org/10.1109/ACCESS.2020.3002538

Cascio, Jordan – Hale, Morgan – Owens, Amy – Swann, Shafer – Weliver, Andrew – Jiménez, José (2019): Creating a Decision Support Tool for the Stryker NBC RV. In *Proceedings of the Annual General Donald R. Keith Memorial Conference.* West Point, NY: Department of Systems Engineering United States Military Academy, 124–129.

Chlebo, Paul Jr. – Christman, Gerard J. – Johnson, Roy A. "Al" (2011): Enhancing Collective C2 in the International Environment: Leveraging the Unclassified Information Sharing Enterprise Service. In *16th International Command and Control Research and Technology Symposium,* 1–49.

Drury, Brett – Ullah, Ihsan – Madden, Michael G. (2018): An Information Retrieval System for CBRNe Incidents. In *ECML PKDD 2018 Workshops.* Cham: Springer, 211–215. Online: https://doi.org/10.1007/978-3-030-13453-2

Gawlik-Kobylińska, Małgorzata – Gudzbeler, Grzegorz – Szklarski, Łukasz – Kopp, Norbert – Koch-Eschweiler, Helge – Urban, Mariusz (2021): The EU-SENSE System for Chemical Hazards Detection, Identification, and Monitoring. *Applied Sciences,* 11(21), 10308. Online: https://doi.org/10.3390/app112110308

Islam, Mohd. Noor – Jang, Yeong-Min – Choi, Sun-Woong – Park, Sang-Joon (2009): Key Technology Issues for Military Sensor Networks. *Information and Communications Magazine,* 26(3), 41–51.

Juhász László (2001): *Az ABV-felderítés béke és háborús feladatainak összehangolása a hazai gyakorlat és a NATO-elvek alapján.* PhD-disszertáció.

Khaleghi, Bahador – Khamis Alaa – Karray, Fakhreddine O. – Razavi, Saiedeh N. (2013): Multisensor Data Fusion: A Review of the State-of-the-Art. *Information Fusion,* 14(1), 28–44. Online: https://doi.org/10.1016/j.inffus.2011.08.001

Kon, Kazuyuki – Igarashi, Hiroki – Matsuno, Fumitoshi – Sato, Noritaka – Kamegawa, Tetsushi (2012): Development of a Practical Mobile Robot Platform for NBC Disasters and Its Field Test. In *2012 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR).* IEEE. Online: https://doi.org/10.1109/SSRR.2012.6523894

Lawrence, Kaitlin – Kuhne, Wendy – Swindle, Ashlee (2020): *Development of FRET clusters for CBRN Detection*. LDRD Report. Online: https://doi.org/10.2172/1651109

Lundberg, Scott – Paffenroth, Randy – Yosinski, Jason (2010): Algorithms for Distributed Chemical Sensor Fusion. *Signal and Data Processing of Small Targets,* 7698, 60–71. Online: https://doi.org/10.1117/12.849588

Madhani, Sunil – Tauil, Miriam – Zhang, Tao (2005): Collaborative Sensing Using Uncontrolled Mobile Devices. In *2005 International Conference on Collaborative Computing: Networking, Applications and Worksharing.* IEEE, 2005. Online: https://doi.org/10.1109/COLCOM.2005.1651206

Marinelli, William J. – Schmit, Thomas – Rentz Dupuis, Julia – Mulhall, Phil – Croteau, Philly – Manegold, David – Beshay, Manal – Lav, Marvin (2015): Cooperative Use of Standoff and UAV Sensors for CBRNE Detection. In *Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Sensing XVI.* 9455. Baltimore: SPIE. Online: https://doi.org/10.1117/12.2177023

Mullins, Steven J. (2021): Information Sharing Patterns in Action Teams: Understanding Cognitive Interactions in Dynamic Environments. In *25th International Command and Control Research and Technology Symposium, EasyChair Smart CFP.* Southampton, 1–23.

Szabó Sándor (2017): *Az új generációs mentesítő rendszerek hatása a hazai ABV mentesítő képesség átalakítására.* PhD-disszertáció. Budapest: Nemzeti Közszolgálati Egyetem.

Tarapata, Zbigniew – Antkiewicz, Ryszard – Najgebauer, Andrzej – Pierzchała, Dariusz (2021): Risk Analysis and Alert System for CBRN Threats: Features and Functions. In *Proceedings of the 37th International Business Information Management Association Conference*, Córdoba, Spain.

Viengdavanh Róbert Manivanh (2012): *Az atom-, biológiai- és vegyivédelem meteorológiai vonatkozásai.* Szakdolgozat. Budapest: ELTE.

Zhang, Tao – Madhani, Sunil – Berg, Eric van den (2005): Sensors on Patrol (SOP): using Mobile Sensors to Detect Potential Airborne Nuclear, Biological, and Chemical Attacks. In *MILCOM 2005, IEEE Military Communications Conference,* IEEE 2005. Online: https://doi.org/10.1109/MILCOM.2005.1606107

NEMZETBIZTONSÁGI SZEMLE
11. évfolyam (2023) 1. szám 78–107. • DOI: 10.32561/nsz.2023.1.6

Legárd Ildikó[1]

Információbiztonsági incidenstrendek a közigazgatásban[2]

Information Security Incident Trends in Public Administration

A közigazgatás a kibertér felől érkező fenyegetések egyik leggyakoribb célpontja, az állami és önkormányzati szervek elleni kibertámadások egyre célzottabbak, kifinomultabbak és egyre nagyobb kár okozására képesek. Az elektronikus információs rendszerek biztonsága érdekében hatékony fizikai, logikai és adminisztratív intézkedéseket szükséges alkalmazni, amelyek meghatározásához elengedhetetlen az aktuális információbiztonsági incidenstrendek ismerete.

Jelen tanulmány célja a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet által, 2019 és 2021 közötti időszakban detektált információbiztonsági események átfogó elemzése, a közigazgatást érintő hazai incidenstrendek azonosítása érdekében. Az írás kiemelten vizsgálja, hogy a kibertámadók hogyan reagáltak a Covid–19-világjárványra, és ez milyen módon jelenik meg a hazai incidenstrendekben. Az elemzés további célkitűzése annak megállapítása, hogy mely szektort érte a legtöbb incidens a vizsgált időszakban, és mely incidenstípusok jellemzők ebben az ágazatban. További kutatási kérdésként merült fel, hogy a pszichológiai manipuláció milyen százalékos arányban mutatható ki a detektált incidenstrendekben.

Kulcsszavak: *információbiztonság, incidenstrendek, közigazgatás, Nemzeti Kibervédelmi Intézet, kibertámadások, Covid–19*

Public administration is one of the most common targets of cyber threats. Cyberattacks against public and local governments are becoming increasingly targeted, sophisticated, and are capable of causing ever greater damage. Information systems security requires effective physical, logical and administrative measures, which needs knowledge of current trends in information security incidents.

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola, e-mail: ildiko.legard@gmail.com

[2] A tanulmány a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet támogatásával készült. Külön köszönöm dr. Munkácsi Viktor nb. alezredes úr, a Nemzeti CSIRT vezetőjének szakmai támogatását, tanácsait, amelyet az adatok elemzéséhez és a tanulmány megírásához nyújtott.

The aim of this study is to provide a comprehensive analysis of information security incidents detected by the National Cyber-Security Centre of Hungary between 2019 and 2021 in order to identify national incident trends affecting public administrations. The paper focuses on how cyber attackers have responded to the Covid–19 pandemic and how this is reflected in national incident trends. A further objective of the analysis is to identify which sector was affected the most by incidents during the period under review and which incident types are typical for this sector. A further research question was the percentage of social engineering in the detected incident trends.

Keywords: *information security, incident trends, public administrations, National Cyber-Security Centre of Hungary, cyber-attacks, Covid–19 pandemic*

Bevezetés

A *Nemzeti Digitalizációs Stratégia* (NDS) 2022–2030 kiemeli, hogy a „technológia fejlődésével az informatikai és kiberbiztonsági helyzet is egyre összetettebbé válik. Emiatt szükséges a biztonságtudatosság növelése, a megelőzés, az egyének, szervezetek és vállalkozások mélyrehatóbb biztonsági védelemének kialakítása”,[3] valamint „ágazati és központi szinten kiemelten szükséges az információbiztonsági elemek és a kibervédelmi kapacitások bővítése, összhangban a hazai és az EU-s szintű törekvésekkel”.[4] A stratégia a digitális állam pillér intézkedéscsoportjai keretében a megfogalmazott célok megvalósítása eszközeként a kormányzati elektronikus szolgáltatások információbiztonságának növelését jelöli meg. A kibertérben jelentkező és a kibertérből érkező fenyegetések és az ezzel járó kockázatok kezelése leghatékonyabban a megelőzésre épülő hatékony védelmi intézkedések útján valósítható meg, amihez elengedhetetlen az aktuális incidenstrendek ismerete.

A biztonsági események kezelése[5]

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) Preambuluma kimondja, hogy: „A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.” Az elektronikus információs rendszer biztonsága érdekében a szervezetnek

[3] Miniszterelnöki Kabinetiroda 2022: 149.

[4] Miniszterelnöki Kabinetiroda 2022: 68.

[5] Az angolszász terminológia elkülöníti a biztonsági esemény és a biztonsági incidens fogalmát: az előbbi alatt minden megfigyelhető előfordulást ért egy hálózatban vagy egy rendszerben, az utóbbi, tehát az incidens fogalmába a számítógépes biztonsági szabályzatok, az elfogadható felhasználási irányelvek megsértésének vagy közvetlen fenyegetésének veszélye tartozik. A magyar jogszabályok azonban nem határolják el e két fogalmat, kizárólag a biztonsági esemény fogalmát alkalmazzák, amely terminológia alatt valójában a biztonsági incidenseket értik. Krasznay et al. 2019: 136.

külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják:

a) a megelőzést és a korai figyelmeztetést,
b) az észlelést,
c) a reagálást,
d) a biztonsági események kezelését.[6]

Az Ibtv. értelmező rendelkezése – 1. § (1) – értelmében:

- biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;
- súlyos biztonsági esemény: olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
- biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.

A biztonsági események kezelését – az eltérő ellátotti körre tekintettel – az alábbi szervezetek látják el:

- NBSZ NKI, amely kezeli:
  - az Ibtv. 2. §-ában – az Ibtv. 19. § (2) bekezdése szerinti kivétellel – meghatározott szervek nyílt,
  - a bejelentésköteles szolgáltatók,
  - a honvédelmi létfontosságú rendszerelemek kivételével az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők,
  - a központosított informatikai és elektronikus hírközlési szolgáltató

  elektronikus információs rendszereit érintő biztonsági eseményeket és fenyegetéseket.
- Katonai Nemzetbiztonsági Szolgálat: az Ibtv. 19. § (2) bekezdése alapján a honvédelmi célú elektronikus információs rendszereket érintő biztonsági eseményeket és fenyegetéseket kezeli.

[6] Ibtv. 6. §.

Az NBSZ NKI-n, illetve a KNBSZ-en kívül speciális eseménykezelési feladatokat lát el a Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ),[7] amely az ügyfélkörébe tartozó közoktatási, felsőoktatási, közgyűjteményi intézmények és kutatóhelyek részére nyújtott informatikai infrastruktúra fejlesztéséhez és üzemeltetéshez kapcsolódóan kezeli az érintett intézmények biztonsági eseményeit is. A HUNCERT a magyar internetszolgáltatókat segíti a számítógépes hálózati incidensek kockázatainak kezelésében, valamint az ilyen incidensek esetén az incidensek felderítésében, kezelésében és elemzésében.[8]

Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet

A Nemzetbiztonsági Szakszolgálat szervezetén belül 2015. október 1-jével hozták létre a Nemzeti Kibervédelmi Intézetet, amelynek tevékenysége három pillérre épül:

- hatósági feladatok ellátása: a Nemzeti Elektronikus Információbiztonsági Hatóság az Ibtv.-ben, valamint a 187/2015 (VII. 13.) Korm. rendeletben meghatározott feladat- és hatáskörben a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozik;
- incidenskezelési tevékenység: az eseménykezelő központ a kibertérből érkező támadásokkal és fenyegetettségekkel kapcsolatos eseménykezelési feladatokat látja el;
- sérülékenységvizsgálat: az informatikai rendszerek gyenge pontjainak feltárására, a rendszer védelmi képességeinek tesztelésére irányul.

Biztonsági események kezelése során az NBSZ NKI:

- az Ibtv. 2. §-ában meghatározott szervek – a honvédelmi célú elektronikus információs rendszerek kivételével – nyílt,
- az alapvető szolgáltatást nyújtó szolgáltatók és a bejelentésköteles szolgáltatók,
- a honvédelmi létfontosságú rendszerelemek kivételével az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők,
- a központosított informatikai és elektronikus hírközlési szolgáltató, valamint
- a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat

elektronikus információs rendszereit érintő biztonsági eseményeket és fenyegetéseket kezeli.[9]

Az incidensek kezelésének alapszabályait az Ibtv. felhatalmazása alapján az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet fekteti le, amely rendelkezik az intézmények és az eseménykezelő központ jogairól és kötelességeiről, valamint egyéb lehetőségekről is.

---

7 Lásd: https://kifu.gov.hu/
8 Lásd: www.cert.hu/
9 Ibtv. 19–20. §, 271/2018. (XII. 20.) Korm. rendelet 3. § (1).

Az NKI által kezelt incidensek statisztikai adatai

Az NBSZ NKI által detektált és gyűjtött, incidensekre vonatkozó statisztikai mutatókat az alábbi kategorizálás szerint tagolva bocsátotta kutatási célból a rendelkezésemre 2022. februárban:

- évenkénti bontás (havi bontásban is),
- szektorális bontás,
- incidensek típusai szerinti bontás.

- Évenkénti bontás: 2019, 2020, 2021 évenként, hónaponkénti bontásban.
- Szektorális bontás
  - állami és önkormányzati szervek: Az Ibtv. 2. §-ában meghatározott szervek;
  - nemzeti létfontosságú rendszerelemek: 2012. évi CLXVI. törvény (Lrtv.)[10] alapján kijelölt létfontosságú rendszerelem, amelynek kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt elsősorban Magyarországon lenne jelentős hatással (energia, közlekedés, agrárgazdaság, egészségügy, TB, pénzügy, infokommunikációs technológia, víz, honvédelem, közbiztonság-védelem);
  - alapvető szolgáltatásokat nyújtó szereplők:[11] Lrtv. alapján alapvető szolgáltatásokat nyújtó szereplőnek azon szervezet vagy gazdasági szereplő intézmény jelölhető ki, amely:
    - alapvető szolgáltatást nyújt (kritikus társadalmi vagy gazdasági tevékenységek fenntartásához szükséges, elektronikus információs rendszertől függő, az alapvető szolgáltatások jegyzékében feltüntetett szolgáltatás),
    - az általa nyújtott alapvető szolgáltatás elektronikus információs rendszerektől függ,
    - az általa nyújtott alapvető szolgáltatást érintő biztonsági esemény – kormányrendeletben meghatározott – jelentős zavart okozna szolgáltatás nyújtásában és
    - az erre irányuló eljárásban alapvető szolgáltatást nyújtó szereplőként került azonosításra.
  - bejelentésköteles szolgáltatók: 2001. évi CVIII. törvény (Ekertv.) alapján bejelentésköteles szolgáltatást nyújtónak minősül a magyarországi székhelyű gazdasági társaság, amely a következő információs társadalommal összefüggő szolgáltatások valamelyikét nyújtja:
    - aki online piacteret működtet, vagy egy elérhető online piactér igénybevételével online adásvételi és szolgáltatási szerződések megkötését teszi lehetővé fogyasztók és kereskedők/ kereskedő és kereskedő között,
    - keresőszolgáltatást,
    - felhőalapú számítástechnikai szolgáltatást nyújt.[12]

[10] 2012. évi CLXVI. törvény (Lrtv.) 1. § *k)*.
[11] 2012. évi CLXVI. törvény (Lrtv.) 1. § *d)*.
[12] 2001. évi CVIII. törvény (Ekertv.) 2. § *j)*.

  - közvetítő szolgáltatók: Az Ekertv. alapján az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amely
    - az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, vagy a távközlő hálózathoz hozzáférést biztosít (egyszerű adatátvitel és hozzáférés-biztosítás);
    - az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, és az alapvetően a más igénybe vevők kezdeményezésére történő információtovábbítás hatékonyabbá tételét szolgálja (gyorsítótárolás);
    - az igénybe vevő által biztosított információt tárolja (tárhelyszolgáltatás);
    - információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (keresőszolgáltatás);
    - alkalmazásszolgáltató;
    - videómegosztóplatform-szolgáltató.[13]
  - nemzetbiztonsági védelem alá eső szervezetek: A nemzetbiztonsági védelem alá eső szervek és létesítmények köréről szóló 2009/2015. (XII. 29.) Korm. határozat 1. mellékletében felsorolt szervek (például NAIH, AB, ÁSZ, KEH, OBH);
  - oktatási intézmények;
  - egyéb szervezetek:
    - a honvédelmi létfontosságú rendszerelemek kivételével az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők[14],
    - a központosított informatikai és elektronikus hírközlési szolgáltató[15],
    - a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat[16],
    - egyéb bejelentések alapján.
- Incidensek típusai szerinti bontás
  Az NBSZ NKI az incidenstípusok meghatározásánál az Európai Unió Hálózat- és Információbiztonsági Ügynöksége (ENISA) által kidolgozott rendszer módosított változatát használja, ugyanis a magyar gyakorlat nem sorol be minden incidenst biztonsági eseménynek, amelyet az ENISA annak tekint.[17] Az eseménykezelő központ által a 2019–2021. években detektált eseményeket az alábbi incidenstípusok szerint határozták meg:
  - adminisztrátorfiók kompromittálódása *(privileged account compromise);*
  - behatolás *(intrusions):* ez jelentheti egy rendszer vagy alkalmazás (szolgáltatás) sikeres kompromittálását is, amely történhet távolról egy ismert vagy új sebezhetőség révén, de akár jogosulatlan helyi hozzáférés is okozhatja. Ide tartozik a botnet is;[18]
  - behatolási kísérlet *(intrusion attempts):* egy rendszer veszélyeztetésére vagy bármely szolgáltatás megzavarására irányuló kísérlet, például ismert vagy

13 Ekertv. 2. § (l).
14 271/2018. (XII. 20.) Korm. Rendelet 3. § (1).
15 271/2018. (XII. 20.) Korm. Rendelet 3. § (1).
16 Ibtv. 20. § (3).
17 Marsi 2018: 58.
18 ENISA 2018.

ismeretlen sérülékenység kihasználása révén, vagy többszöri bejelentkezési kísérlettel (jelszavak kitalálása/feltörése, *brute force*);[19]
- bejelentkezési kísérlet *(login attempts):* többszöri bejelentkezési kísérlet például jelszavak kitalálása/feltörése, brute force segítségével;[20]
- C&C szerver: a parancs- és vezérlőkiszolgáló (C&C) egy támadó vagy kiberbűnöző által vezérelt számítógép, amelyet arra használnak, hogy parancsokat küldjenek a rosszindulatú programok által feltört rendszereknek, és fogadjanak ellopott adatokat a célhálózatról. Számos kampányban felhőalapú szolgáltatásokat, például webmail- és fájlmegosztó szolgáltatásokat használnak C&C-kiszolgálóként, hogy elvegyüljenek a normál forgalomban és elkerüljék a felderítést;[21]
- DDoS: Distributed Denial of Service – elosztott szolgáltatásmegtagadással járó támadás, olyan logikai támadás, amely az informatikai rendszer egy (vagy több) kiszolgálóját tömeges szolgáltatásigénnyel túlterheli, ami a felhasználók hozzáférését nehezíti, vagy akár a kiszolgáló teljes leállásához is vezethet;[22]
- defacement research: weboldal rongálása;
- DoS: Denial of Service – szolgáltatásmegtagadással járó támadás;[23]
- elemzés;
- elérhetőség *(availability):* az elektronikus információs rendszer vagy annak elemének tulajdonsága, amely arra vonatkozik, hogy az (ideértve az abban vagy az által kezelt adatot is) a szükséges időben és időtartamban használható;[24]
- erőforrások illetéktelen használata *(unauthorized use of resources):* az erőforrások jogosulatlan célokra való felhasználása, beleértve a nyereségszerzést is (például az e-mail használata illegális profitszerző láncelevelekben való részvételre vagy piramisjátékokban);[25]
- féreg *(worm):* olyan program, amely a számítógép-hálózaton keresztül, a hálózati funkciók kihasználásával terjed számítógéptől számítógépig, és károkozó hatását önmaga – a számítógép összeomlásáig tartó – reprodukálásával, továbbításával éri el;[26]
- illicit/sértő tartalom *(abusive content):* például spam, harmful speech, azaz valakinek a lejáratása vagy diszkriminációja (például internetes zaklatás, rasszizmus, fenyegetések egy vagy több személy ellen), illetve ide tartozik a gyermekpornográfia és az erőszak magasztalásával kapcsolatos tartalmak is;[27]

19 ENISA 2018.
20 ENISA 2018.
21 Lásd: www.trendmicro.com/vinfo/us/security/definition/command-and-control-server
22 Muha–Krasznay 2014: 115.
23 Berzsenyi et al. 2018: 392.
24 Ibtv. 1.§ (1) 38. pont
25 ENISA 2018.
26 Muha–Krasznay 2014: 116.
27 ENISA 2018.

- információbiztonság (Information Security): Az adatokkal és rendszerekkel való helyi visszaélés mellett az információbiztonságot veszélyeztetheti egy fiók vagy alkalmazás sikeres kompromittálása, valamint olyan támadások, amelyek révén információkat hallgatnak le és férnek hozzá átvitel közben (lehallgatás, hamisítás vagy eltérítés). Ugyanakkor az emberi/konfigurációs/szoftverhiba is veszélyeztetheti az információbiztonságot;[28]
- információgyűjtés *(information gathering):* például szkennelés *(scanning)* útján, amelynek során mintegy a tesztelési folyamat részeként olyan kéréseket küldenek egy rendszerhez a gyenge pontok felderítése érdekében, amely információt gyűjt a hosztokról, szolgáltatásokról és fiókokról (például DNS-lekérdezés, portellenőrzés). Információ gyűjthető lehallgatás *(sniffing)* útján is, amely a hálózati forgalom megfigyelése és rögzítése. A social engineering technikák is alkalmasak információgyűjtésre;[29]
- információk illetéktelen hozzáférése *(unauthorised access to information);*
- információk illetéktelen módosítása *(unauthorised modification of information);*
- ismeretlen típusú káros kód: ismeretlen rosszindulatú számítógépes program (például vírus, féreg, logikai bomba, kémprogram stb.);
- ismert sérülékenység kihasználása *(exploiting known vulnerabilities):* a sérülékenység az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;[30]
- IT-biztonsági szaktanácsadás *(IT security consulting)* vagy szaktanácsadás;
- káros tevékenység: káros kód, fertőzött rendszer, C&C server, káros kód konfiguráció.
- letapogatás *(scanning):* szkennelés során mintegy a tesztelési folyamat részeként olyan kéréseket küldenek egy rendszerhez a gyenge pontok felderítése érdekében, amely információt gyűjt a hosztokról, szolgáltatásokról és fiókokról (például DNS-lekérdezés, portellenőrzés);[31]
- logelemzés: például a vállalati informatikai rendszerek, tűzfalak, behatolásgátló és vírusirtó rendszerek naplóbejegyzéseinek, elemzése;
- megszemélyesítés *(masquerade):* a social engineering egy esete, amikor egy entitás (személy, program, folyamat stb.) magát más entitásnak tünteti fel;[32]
- nem adminisztrátor fiók kompromittálódása *(unprivileged account compromise);*
- nyitott port *(open port):* „nyitott kapuk", amelyeken elérhetők a hálózat szolgáltatásai, így például a vírusok ezen a porton keresztül is bejuthatnak a szerveztek informatikai rendszereibe és gépeibe, ezáltal megbénítva a működést;
- pszichológiai manipuláció *(social engineering):* a social engineering az emberi hiszékenységre, együttműködésre építő támadási forma. Bár ezt az élet sok

28 ENISA 2018.
29 ENISA 2018.
30 Muha–Krasznay 2014: 121.
31 ENISA 2018.
32 Muha–Krasznay 2014: 119.

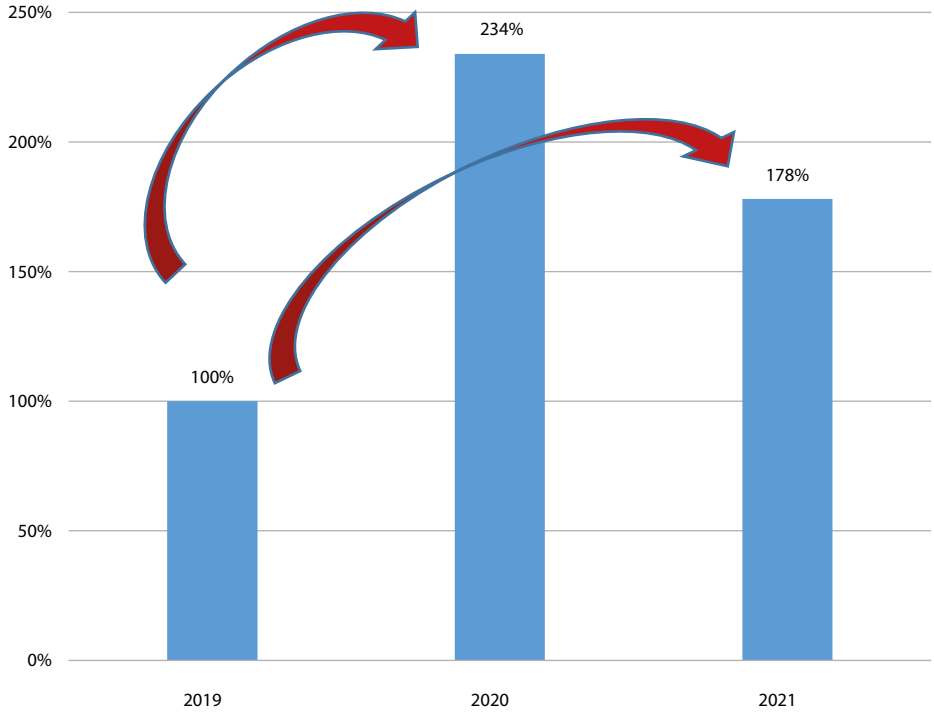
más területén is kihasználják, a social engineering kimondottan az információ megszerzésére irányul, ezen belül is elsősorban az informatikai eszközökön tárolt adatokra fókuszálva;[33]
- *ransomware:* zsarolóvírus;
- *spam:* levélszemét minden olyan kéretlen üzenet, amelyet tömegesen küldenek (kéretlen tömeges e-mail vagy UBE);[34]
- SPAM IP: egy botnetfertőződésből fakadóan, spamelés miatt a használt IP-cím feketelistákra kerülhet, és bizonyos levelezőszerverek nem fogják befogadni az innen érkező, küldött leveleket;[35]
- trójai *(trojan):* olyan kártékony program, amelyet alkalmazás, játék, szolgáltatás vagy más egyéb tevékenység mögé rejtenek, álcáznak. Futtatásakor fejti ki károkozó hatását;[36]
- visszaélés *(fraud):* például erőforrások illetéktelen használata, megszemélyesítés, adathalászat, vagy licenc nélküli kereskedelmi szoftverek vagy egyéb szerzői jogi védelem alatt álló másolatok felajánlása vagy telepítése;[37]
- zaklatás *(harassment):* bántó, valótlan üzenetek küldözgetése online;[38]
- egyéb.

Az NKI által detektált incidensek összehasonlítása évenként és incidenstípusokként

Az NKI az incidensekre vonatkozó átadott adatokat számszerűen – hónaponként, szektoronként és incidenstípusonként – bocsátotta a rendelkezésemre. Tekintettel arra, hogy az Ibtv. 22. § (4) bekezdése szerint az NBSZ NKI eljárásai során keletkezett adatok nem nyilvánosak, továbbá a konkrét számadatok tükrében olyan – a kapacitásaikra és képességeikre vonatkozó – következtetések is levonhatók, amelyek megnehezíthetnék a szolgáltatások ellátását, a konkrét számadatok nem publikálhatók. Az adatok feldolgozása során kizárólag a számadatokból levont következtetéseket, a számadatokban való változás százalékos mértékét vagy egymáshoz viszonyított arányát lehet bemutatni. A tanulmány az adatok elemzése során a fenti követelmények figyelembevételével mutatja be a hazai incidenstrendeket.

Az NKI által kezelt incidensek százalékos eloszlását évenkénti összehasonlításban az 1. ábra mutatja be:

[33] Muha–Krasznay 2014: 53.
[34] Lásd: www.eset.com/hu/levelszemet/
[35] Lásd: https://nki.gov.hu/it-biztonsag/tudastar/keretlen-level-feketelista-spam-blacklist/
[36] Muha–Krasznay 2014: 122.
[37] ENISA 2018.
[38] Monori 2016: 247.



1. ábra: Kezelt incidensek százalékos eloszlása évenkénti összehasonlításban
Forrás: a szerző szerkesztése

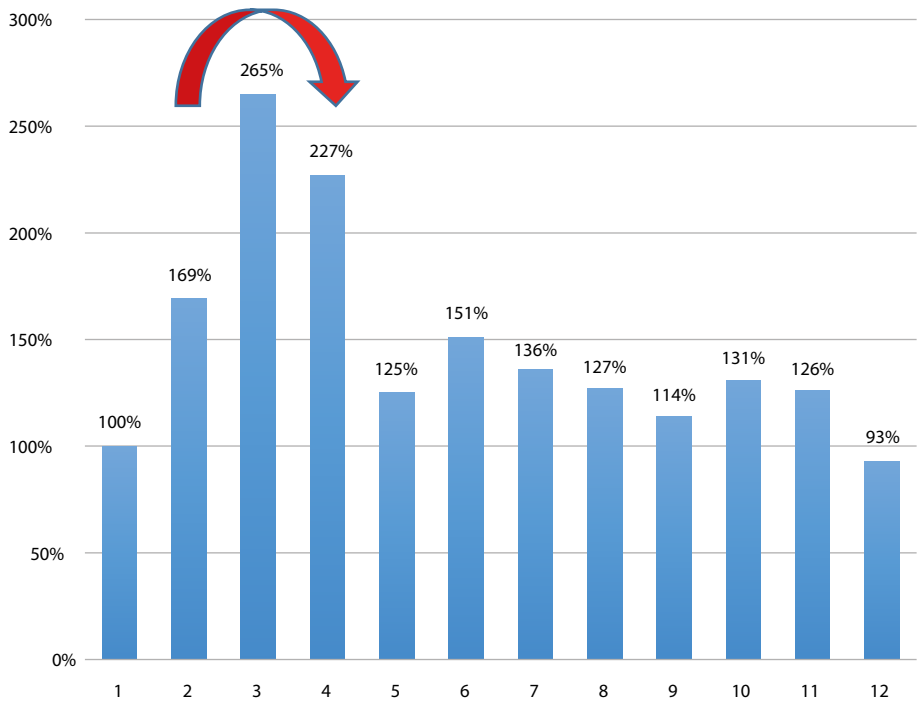
A grafikon segítségével egyértelműen kimutatható, hogy amennyiben a 2019-es évben, az összes kezelt incidens számát tekintjük 100%-nak, akkor a 2020-ban kezelt összes incidensek száma közel két és félszeres emelkedést mutat, és bár arányait tekintve csökkenés tapasztalható a 2021-es évben, ugyanakkor 2019-hez viszonyítva a kezelt incidensek aránya még mindig meredeken emelkedett. A tapasztalható emelkedés lehetséges okai a következők lehetnek:

- Early Warning System (EWS): 2020. május 30-án hatályba lépett az elektronikus információbiztonsági korai figyelmeztető rendszerről szóló 214/2020. (V. 18.) kormányrendelet, amelynek értelmében a korai figyelmeztető szolgáltatás nyújtására a NBSZ NKI-t jelölték ki. Az EWS egy szignatúra alapú illetéktelen hálózati behatolást jelző rendszer (*network based intrusion detection system,* nIDS), amely kifejezetten nyílt internetről elérhető rendszerek (például web-oldalak) elleni támadásokat képes felismerni és jelezni;
- koronavírushoz kapcsolódó világjárvány és az ezzel összefüggésbe hozható megtévesztő levelek, álhírek, közösségimédia-üzenetek, valamint az új koronavírussal kapcsolatos, Covid–19 témájú káros tartalmú mobilalkalmazások és weboldalak;
- távmunka, otthoni munkavégzés kockázatai.

A Deloitte által készített, a Covid–19-járvány hatásait vizsgáló tanulmány szerint a felhasználók 47%-át érte adathalász támadás otthoni munkavégzés során. 2020. február és május között a videókonferencia-szolgáltatásokat igénybe vevő, több mint félmillió felhasználó adatait szerezték meg a támadók, és adták el a dark weben. Azon kibertámadások száma, amelyek korábban még nem ismert rosszindulatú programokat vagy módszereket alkalmaztak a korábbi 20%-ról a pandémia alatt 35%-ra emelkedtek.[39] Az Interpol a Covid–19-hez kapcsolódó kiberfenyegetések kapcsán az adathalászatra, a különböző csalásokra, a rosszindulatú domainnevek, a malware-ek, a ransomware-ek valamint az álhírek gyorsan emelkedő terjedésére figyelmeztetett.[40]

2020. év vizsgálata

Ahhoz, hogy hazai viszonylatban is megvizsgáljam a világjárvány hatásait, elemezni szükséges a 2020. év emelkedő tendenciát mutató hónapjaiban azonosított incidenstípusokat. A 2020-ban kezelt incidensek havi eloszlását a 2. ábra részletezi.

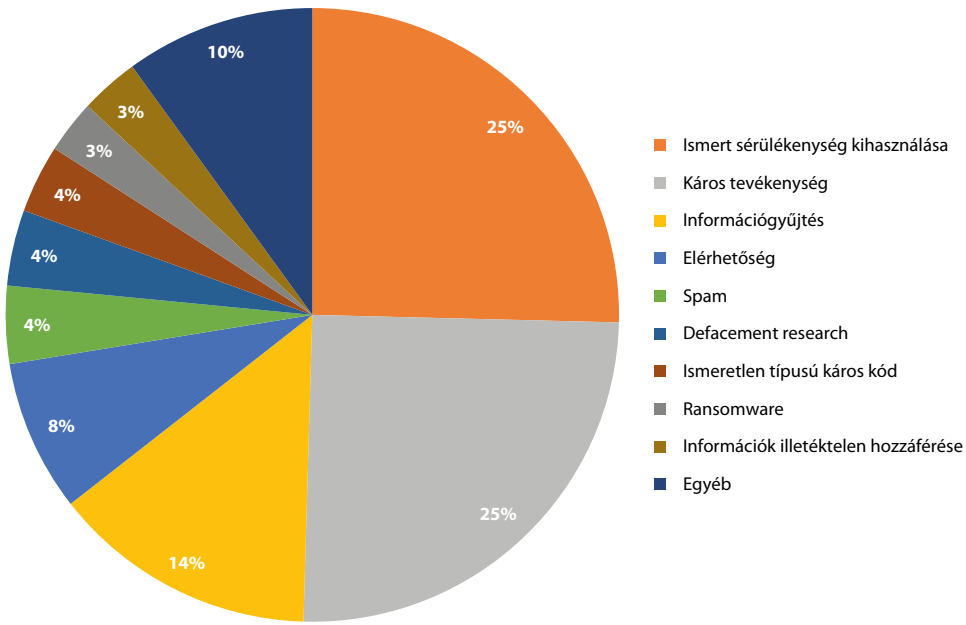


2. ábra: A 2020-ban kezelt incidensek havi eloszlása
Forrás: a szerző szerkesztése

[39] Nabe (é. n.).
[40] Interpol (é. n.).

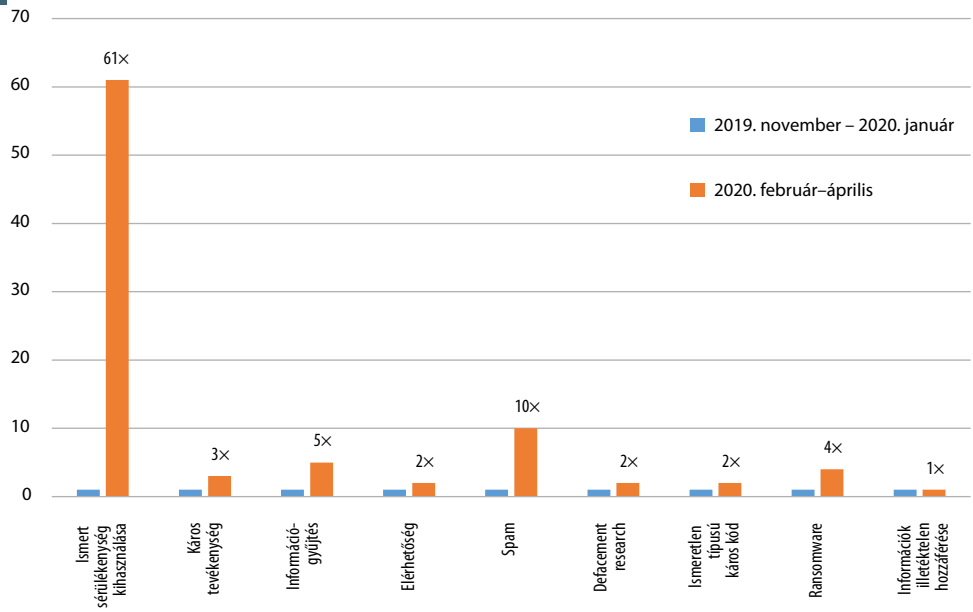
A havi eloszlásokból egyértelműen megállapítható, hogy az incidensek száma a Covid–19 első hullámában indult meredek emelkedésnek. A márciusban kezelt incidensek – a 2020-ban kezelt incidensek összesített számához viszonyított – százalékos aránya több mint két és félszeres emelkedést mutat a januári eredménnyel összehasonlítva.

A 2020. február–április közötti időszakban az NKI által kezelt incidensek típusait a következő, 3. ábra szemlélteti.



3. ábra: az NKI által kezelt incidenstípusok 2020. február–április
Forrás: a szerző szerkesztése

Az incidensek képzeletbeli dobogóján az első három helyen az alábbi incidensek szerepelnek: első helyen megosztottan az ismert sérülékenység kihasználása (25%) és a káros tevékenység (25%), második helyen az információgyűjtés (14%), a harmadik helyen pedig az elérhetőség (8%) szerepel. Amennyiben összehasonlítjuk a 2020. február és április közti, valamint az azt megelőző három hónapot (2019. november és 2020. február között), az egyes incidenstípusok esetén a 4. ábrán leolvasható emelkedést tapasztalhatjuk.



4. ábra: 2020. február–április és 2019. november – 2020. január összehasonlító vizsgálata
Forrás: a szerző szerkesztése

A grafikon alapján megállapítható, hogy az ismert sérülékenység kihasználása mutatja a legnagyobb emelkedést (61-szeres), de a spamek (10x), az információgyűjtés (5x), a ransomware (4x), valamint a káros tevékenység is (3x) többszörös növekedést mutat. Az ismert sérülékenység kihasználása tekintetében, amennyiben megvizsgáljuk a jelzett időszakban az NKI által kiadott riasztásokat, tájékoztatásokat, híreket, megállapíthatjuk, hogy az emelkedés hátterében több olyan konkrét fenyegetés is azonosítható, amelyek egyenként is okozhatták a kiemelkedő statisztikai eredményt. Ilyen fenyegetések többek között: Microsoft Windows 0. napi sérülékenysége,[41] az Exchange mail szerverek ellen detektált támadások,[42] a HP Support Assistant segédprogramjának kritikus sérülékenysége, az Adobe és Oracle szoftverek,[43] valamint a VMware vCenter Server[44] sérülékenységei.

A megnövekedett káros tevékenység és az információgyűjtéshez kapcsolódó incidensek hátterében a koronavírushoz, valamint az otthoni munkavégzéshez kapcsolódó fenyegetések állnak. A NKI 2020. márciusban tájékoztatást[45] adott ki az új koronavírus témájú kiberfenyegetésekről, amelyeket az 5. ábra mutat be.

41 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/microsoft-windows-0-napi-serulekenysegek/
42 Lásd: https://nki.gov.hu/it-biztonsag/hirek/exchange-szerverek-veszelyben/
43 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-adobe-szoftverek-serulekenysegeirol-4/ https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztato-oracle-szoftverek-serulekenysegeirol/
44 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-vmware-vcenter-server-serulekenysegerol/
45 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/az-nki-tajekoztatoja-az-uj-koronavirus-temaju-kiberfenyegetesekrol/

5. ábra: Koronavírus témájú kiberfenyegetések
Forrás: a szerző szerkesztése

A vizsgált időszak további kiemelt fenyegetései közé tartozik az Emotet vírus, amelyet az Europol a világ legveszélyesebb rosszindulatú programjaként tart számon.[46] A 2014-ben felfedezett Emotet egy fejlett, moduláris banki trójai, amely a kormányzati és magánszektort egyaránt célozza. Alapképességeit tekintve elsősorban banki adatok lopására szakosodott, ugyanakkor az évek során megjelenő újabb változatai szinte bármilyen más káros tevékenységre alkalmasak (például személyes adatok ellopása vagy zsarolóvírus telepítése), nem véletlen tartják az egyik legköltségesebb és legpusztítóbb vírusnak.[47] Jellemző a kártevőre, hogy aktívan kihasználja az aktuális tendenciákat, híreket, így a vizsgált időszakban jellemzően a Covid–19 témájához kapcsolódva terjedt a gyanútlan áldozatok között.

46 Europol 2021.
47 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-egeszsegugyi-intezmenyeket-erinto-emotet-terjesztesi-kampannyal-kapcsolatban/

Elsősorban az otthoni munkavégzéshez kapcsoló fenyegetésként jelentek meg a zsarolólevelek és a zsarolóvírusok. A Phobos ransomware például nyitott vagy nem biztonságos távoli asztali kapcsolaton keresztül, RDP hitelesítő adatok brute force támadásával, kiszivárgott vagy megszerzett RDP hitelesítő adatok segítségével, valamint klasszikus és jól bevált adathalász technika segítségével terjedt.[48]

Az ENISA minden évben kiadja a kiberbiztonsági fenyegetettség helyzetéről szóló éves jelentését. Az ENISA Threat Landscape 2020, a 2019. január és 2020. április közötti időszakra vonatkozóan határozza meg a legfőbb fenyegetéseket[49], amelynek részeként külön foglalkozik a 2020-ban kezdődő pandémiás időszakkal.

Az összesített jelentés a 2018-as fenyegetettségi helyzethez képest a legnagyobb változásként a digitális környezet Covid–19 által vezetett átalakulását említi. A világjárvány során a kiberbűnözők képességeiket továbbfejlesztették, gyorsan alkalmazkodtak és hatékonyabban célozták meg a releváns áldozati csoportokat.

Az ENISA a Covid–19 során detektált fenyegetettségi térképe alapján, a hazai detektált incidensekkel egybehangzó módon megállapítható, hogy az Európai Unióban is megnőtt a távmunkához kapcsolódó infrastruktúrákhoz köthető támadások, a csaló, koronavírussal kapcsolatos domainek, az sms-es és az e-mailes adathalászat, a hamis tesztelési alkalmazások, valamint a támadások száma az egészségügyi szervezetek ellen. A támadások eredményeként szignifikánsan emelkedett a személyes adatok, információk és jelszavak eltulajdonítása, a pénzügyi csalások, a zsarolóvírusokhoz kapcsolódó váltságdíjfizetések és egyéb, a szervezetek működését befolyásoló zavaró tényezők száma.[50]

A 2020. évet tovább vizsgálva a következő kiugrást a júniusi hónapban láthatjuk, amelynek hátterében a Covid–19-hez kapcsolódó, újra erőre kapó, több esetben rosszindulatú csatolmányokat tartalmazó adathalász-kísérletek, koronavírusra hivatkozó csaló honlapok, valamint a mobiltelefonokat veszélyeztető zsarolóvírusok állnak. Ebben az időszakban az NKI riasztást adott ki,[51] az ORFK[52] pedig arra figyelmeztetett, hogy az országos tisztifőorvos, valamint a Nemzeti Népegészségügyi Központ nevében elektronikus leveleket küldtek elsősorban egészségügyi, állami intézményekbe és cégekhez, amelyek csatolmánya feltehetően rosszindulatú programot tartalmaz. A csaló levél példáját a 6. ábra szemlélteti.

48 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-phobos-zsarolovirus-terjedeserol/

49 ENISA Threat Landscape 2020, lásd: www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020

50 Lásd: www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/threat-landscape-mapping-infographic-2020

51 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-a-nemzeti-nepegeszsegugyi-kozpont-neveben-kuldott-karos-csatolmanyt-tartalmazo-levellel-kapcsolatban/; https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-nemzeti-nepegeszsegugyi-kozpont-arculati-elemeit-felhasznalo-adathalasz-levelekkel-kapcsolatban/

52 Lásd: https://koronavirus.gov.hu/cikkek/operativ-torzs-visszaeltek-az-orszagos-tisztifoorvos-es-az-nnk-nevevel

P 2020. 06. 12. 9:12

Nemzeti Egészségügyi Központ Magyarország <Muller.Cecilia@nnk.gov.hu>

Message has been disinfected :A Covid-19 védőfelszerelés ingyenes forgalmazása (Nemzeti Egészségügyi Központ Magyarország)

Címzett undisclosed-recipients:

NEMZETI NÉPEGÉSZSÉGÜGYI KÖZPONT

Állami Népegészségügyi és Tisztiorvosi Szolgálat

Kedves mindenkinek,
A magyar kormány által kiadott covid-19 válaszadási utasítások szerint mi, a Magyar Nemzeti Egészségügyi Központ a covid-19 védőeszközöket ingyenesen kívánjuk eljuttatni a magyarországi összes regisztrált vállalathoz és iparághoz. Kérjük, töltse ki egyértelműen a mellékelt űrlapot. győződjön meg arról, hogy az alkalmazottak száma és a cég címe egyértelműen meg van írva ebben a formában.

Töltse ki a mellékelt űrlapot, és a mai bezárás előtt küldje vissza nekünk a másolatot, várva a gyors választ.

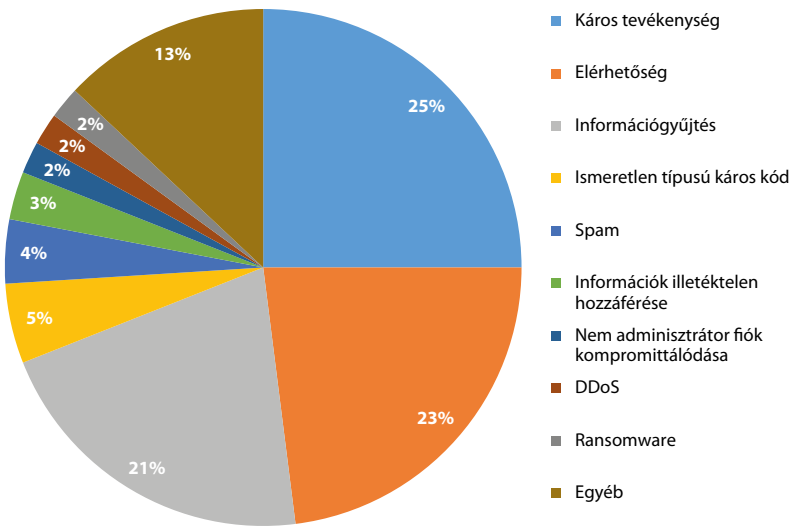
Az összes kitöltött nyomtatványt erre az e-mailre kell küldeni: Müller.Cecília@nnk.gov.hu

Szia

- Dr. Müller Cecília
- osztályvezető
- Országos Tisztifőorvos
- NEMZETI NÉPEGÉSZSÉGÜGYI KÖZPONT
- 1097 Budapest, Albert Flórián út 2-6.
- Müller.Cecília@nnk.gov.hu

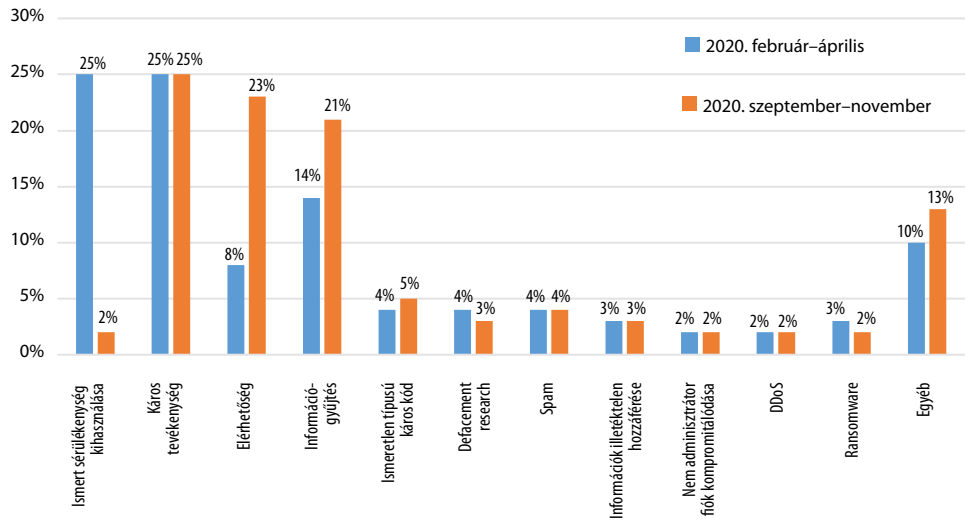
6. ábra: Riasztás a Nemzeti Népegészségügyi Központ nevében küldött, káros csatolmányt tartalmazó levéllel kapcsolatban
Forrás: https://bit.ly/3nAuAFl

A 2020-ban a detektált incidensek száma tekintetében a következő emelkedés az őszi, szeptember és november közötti időszakra, tehát a Covid–19 második hullámára tehető. Ezen időszakban az alábbi, 7. ábra által bemutatott incidenstípusokat azonosították.



7. ábra: Az NKI által detektált incidensek eloszlása 2020. szeptember–november
Forrás: a szerző szerkesztése

A dobogó legfelső fokán elhelyezkedő káros tevékenység hátterében a megnövekedett Emotet-aktivitás áll, amely jellemzően egészségügyi intézmények nevében kiküldött, káros csatolmányt tartalmazó csaló levelekkel,[53] valamint fertőzött e-mail-fiókok kapcsolati listája útján terjed.[54] Emellett a jelzett időszakban közüzemi szolgáltatók nevével visszaélő,[55] valamint Covid–19 témájú adathalász/káros tartalmú levelek okoztak incidenseket, a kormányzati és a pénzügyi szektorokat érintő DDoS-támadások[56] mellett. Ez utóbbinak köszönhető, hogy az őszi időszakban az elérhetőség a dobogó második helyén végzett. A következő, 8. ábrán látható grafikon a Covid–19 első és második hulláma során azonosított incidensek típusait hasonlítja össze.



8. ábra: A Covid 1. és 2. hulláma alatti incidenstípusok összehasonlítása
Forrás: a szerző szerkesztése

Az elemzésből egyértelműen megállapítható, hogy míg az első hullám során az ismert sérülékenység kihasználása, illetve a káros tevékenység voltak a domináló incidenstípusok, addig a második hullámban a káros tevékenység mellett már az elérhetőség és az információgyűjtés voltak a legmeghatározóbbak. Egyéb típusok tekintetében, mint az ismeretlen típusú káros kód, defacement, spam, információk illetéktelen hozzáférése, nem adminisztrátor fiók kompromittálódása, valamint a DDoS és a ransomware, kiegyenlített volt az összes incidenshez viszonyított arányuk mindkét időszakban.

53 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-egeszsegugyi-intezmenyeket-erinto-emotet-terjesztesi-kampannyal-kapcsolatban/
54 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-megnovekedett-emotet-aktivitas-kapcsan/
55 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-kozuzemi-szolgaltatok-nevevel-visszaelo-adathalasz-uzenetekrol/
56 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-kormanyzati-es-penzugyi-szektorokat-erinto-ddos-tamadasokkal-kapcsolatban/

Amennyiben a kapott eredményeket összevetjük az ENISA által, a Threat Landscape 2020 keretében bemutatott Covid–19-hez kapcsolódó elemzésével,[57] illetve az Interpol által összeállított jelentéssel, amely a kibertámadások riasztó arányát mutatja a Covid–19 idején,[58] megállapíthatjuk, hogy az elemzés eredményeként a Covid 2020-as időszakában azonosított hazai incidenstrendek megfelelnek az európai trendeknek. Az összehasonlítást az 1. táblázat mutatja be részletesen.

1. táblázat: A Covid–19 idején, az NKI által detektált hazai incidensek összehasonlítása az európai incidenstrendekkel

ENISA Threat Landscape 2020 – Covid–19 Incidenstrendek	NKI, 2020 (1. és 2. hullám) Incidenstrendek	Interpol – Covid–19 Incidenstrendek	NKI, 2020 (1. és 2. hullám) Incidenstrendek
Távmunkához kapcsolódó infrastruktúrákhoz köthető támadások	✓	Adathalászat/Átverés/Csalás	✓
Koronavírussal kapcsolatos domainek	✓	Malware/Ransomware	✓
Sms-es adathalászat	✓	Rosszindulatú domainek	✓
E-mailes adathalászat	✓	Álhírek	✓
Hamis tesztelési alkalmazások			
Támadások egészségügyi szervezetek ellen	✓		

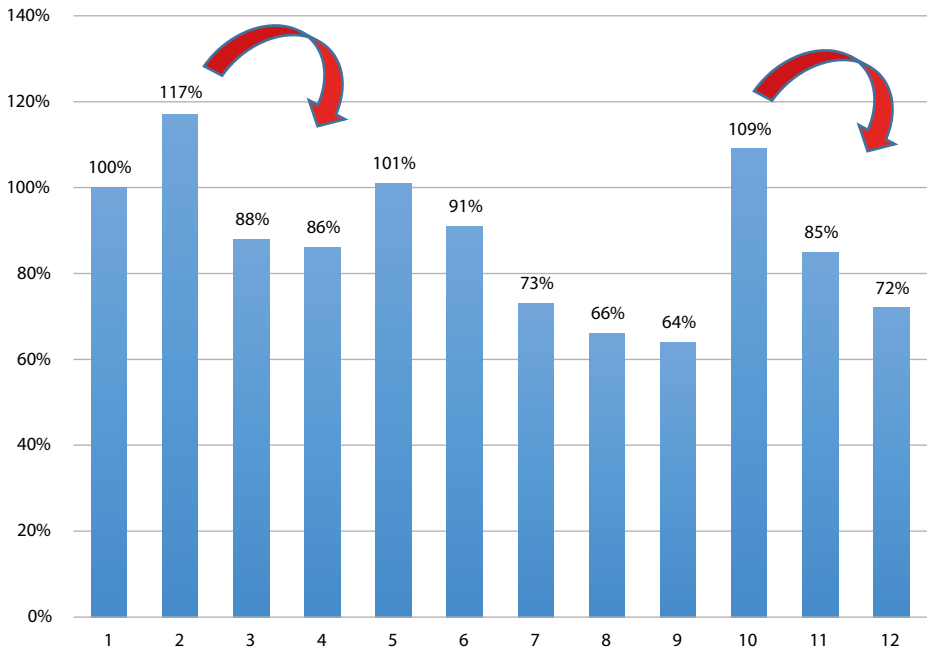
Forrás: a szerző szerkesztése

2021. év vizsgálata

A 2021. évben, az NKI által azonosított incidensek havi eloszlása tekintetében – a 2020. évhez hasonlóan – megállapítható a Covid tavaszi (harmadik) és őszi (negyedik) hulláma során történő százalékos emelkedés. (A 9. ábrán látható elemzés során – az előző két évhez hasonlóan – a januári hónapban azonosított incidenseket tekintem 100%-nak, és az ehhez képest való elmozdulást vizsgálom havonkénti viszonylatban.)

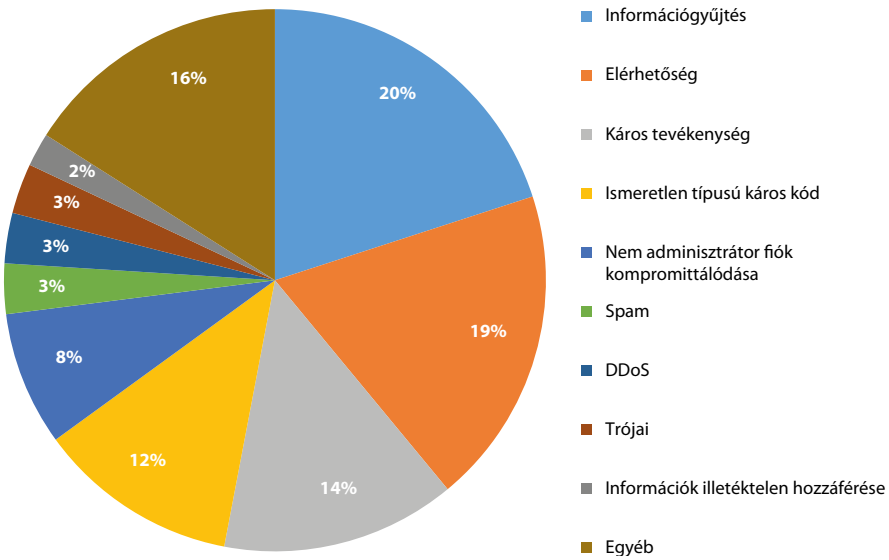
[57] Threat Landscape Mapping Infographic 2020, lásd: www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/threat-landscape-mapping-infographic-2020

[58] Interpol 2020.



9. ábra: 2021. évi vizsgálat – Az incidensek havi eloszlása
Forrás: a szerző szerkesztése

A 2021-ben kezelt incidensek típusai szerinti eloszlást az alábbi, 10. ábra mutatja be:



10. ábra: A 2021. év NKI által kezelt incidensei
Forrás: a szerző szerkesztése

Az incidensek típus szerinti eloszlása tekintetében az előző évhez képest nem történt jelentős változás, az arányok tekintetében csupán néhány százalék eltérés mutatható ki. A három leggyakoribb incidenstípus az információgyűjtés (20%), az elérhetőség (19%), valamint a káros tevékenység (14%), de jelentős százalékban fordul elő az ismeretlen típusú káros kód (12%), valamint a nem adminisztrátor fiókok kompromittálódása (8%) is.

A statisztikai eredmények hátterében a következő tendenciák azonosíthatók:

- a Covid–19-járványhoz kapcsolható kiberfenyegetések és incidensek száma csökkent;
- az Emotet vírus a Covid harmadik hullámának elején (2021. február),[59] valamint az őszi következő hullámban (2021. november)[60] ismét fokozott aktivitást mutatott;
- 2021. márciusban a Microsoft Exchange szerverek esetében négy nulladik napi, tehát a fejlesztők által még fel nem fedezett sérülékenységet (ProxyLogon, illetve a ProxyShell) azonosítottak, amelyek kihasználásával a támadók teljes irányítást szerezhettek a levelezőrendszer felett;[61]
- 2021. márciusban megjelent, majd októberben[62] újra erőre kapott a Flubot malware, amely csomagküldő szolgáltatók nevével visszaélő, káros kód terjesztésével összefüggő sms-üzenetek útján terjedt;[63]
- 2021. októberben a Pécsi Tudományegyetem,[64] valamint a Magyar Posta nevével és arculati elemeivel visszaélő[65] káros csatolmányt tartalmazó levelek terjedtek el a magán- és a közszférában egyaránt;
- 2021. októberben nagy mennyiségű kéretlen, adathalász tartalmú, káros csatolmánnyal rendelkező e-mail-üzenetek terjedése volt megfigyelhető;[66]
- 2021. novemberben a Microsoft Exchange szervereket érintő újabb 0. napi sérülékenységet (ProxyNotShell) azonosítottak. Sikeres kihasználás esetén a megfelelő jogosultsággal rendelkező támadó távoli kódfuttatást hajthatott végre az érintett szerveren;[67]

59 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-emotet-malware-kapcsan/

60 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-emotet-malware-ismetelt-felbukkanasaval-osszefuggesben/

61 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-microsoft-exchange-szerverek-serulekenysegeivel-kapcsolatban/

62 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/rendkivuli-tajekoztato-flubot-malware-rel-kapcsolatban/

63 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-csomagkuldo-szolgaltatok-nevevel-visszaelo-malware-terjesztessel-osszefuggo-sms-uzenetekkel-kapcsolatban/

64 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-a-pecsi-tudomanyegyetem-nevevel-visszaelo-karos-csatolmanyt-tartalmazo-levelekkel-kapcsolatban/

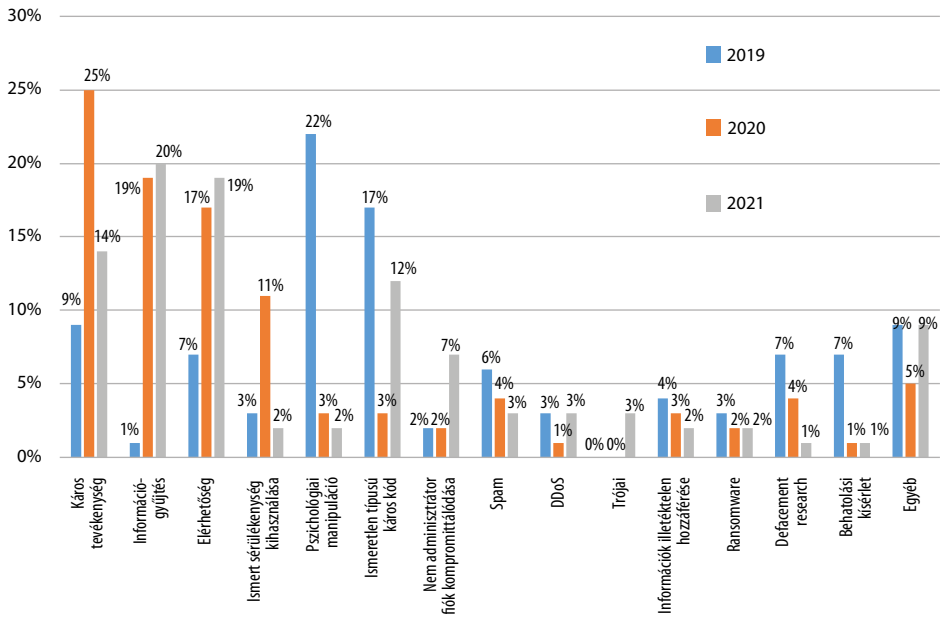
65 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-a-magyar-posta-nevet-es-arculati-elemeit-felhasznalo-adathalasz-uzenetekkel-kapcsolatban/

66 Lásd: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/rendkivuli-tajekoztato-keretlen-adathalasz-tartalmu-e-mail-uzenetek-kapcsan/

67 Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-microsoft-exchange-szervereket-erinto-0-napi-serulekenysegrol/

- 2021. decemberben az azonosított Log4shell sérülékenység kihasználásával kapcsolatban ransomware-/malware-terjesztés volt megfigyelhető. A sérülékenység hitelesítés nélküli, tetszőleges, távoli kódfuttatást tett lehetővé a támadók számára, amelynek sikeres kihasználása estén teljes, rendszerszintű hozzáféréssel rendelkezhettek.[68]

A 11. ábra, a 2019–2021 közötti időszak évenként azonosított, leggyakoribb tíz incidenstípusának összehasonlítását mutatja be (az egyes évek tekintetében, az adott incidenshez kapcsolódó százalékos arány az adott évben detektált valamennyi incidenshez viszonyított aránya).



11. ábra: 2019–2021 TOP 10 incidenstípusai
Forrás: a szerző szerkesztése

A vizsgált három év viszonylatában megállapítható, hogy az egyes incidenstípusok tekintetében – néhány kivételtől eltekintve – a 2019. évhez viszonyítva 2020-ban és 2021-ben százalékos emelkedés figyelhető meg, amely hangsúlyosan a dobogó első három helyét elfoglaló incidenstípusok, a káros tevékenység, az információgyűjtés és az elérhetőség esetén jelenik meg. Hasonló tendencia mutatkozik meg a nem adminisztrátor fiók kompromittálódása, valamint a trójai vírus esetében is. Az ismert sérülékenység kihasználásának 2020-ban tapasztalható kiugróan magas aránya a Microsoft Exchange mailszervereket érintő támadásnak volt köszönhető.

[68] Lásd: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-apache-log4j-konyvtart-erinto-kritikus-serulekenyseggel-kapcsolatban/

A pszichológiai manipuláció esetében a 2019-es évhez viszonyítva jelentős visszaesés tapasztalható a 2020–2021-es években. Szakmai tapasztalatom és megfigyelésem alapján ez nem jelenti a social engineering típusú támadások tényleges csökkenését, valójában egy kategorizálásból eredő eltérés állhat a hátterében. Ugyanis, ha jobban megvizsgáljuk a grafikont, akkor látható, hogy a pszichológiai manipuláció csökkenésével párhuzamosan emelkedik az információgyűjtés százalékos aránya. Az ENISA referenciaincidens-taxonómiája[69] szerint a pszichológiai manipuláció az információgyűjtés fő kategóriájához tartozik, annak egyik alkategóriája, így feltételezhetően az incidensek osztályozása során a pszichológiai manipulációval megvalósuló információgyűjtés esetén az utóbbi típust, tehát az információgyűjtést jelölte meg a 2020. és 2021. években.

Az ismeretlen típusú káros kód, a spam, az információk illetéktelen hozzáférése, a ransomware, a defacement és a behatolási kísérlet százalékos arányában, az adott évben detektált incidensek összesített számához képest, a 2020. és 2021. évben csökkenés figyelhető meg. Természetesen ez nem jelenti feltétlenül az adott típushoz tartozó incidensek számszerű csökkenését, ez csupán arra a tendenciára utal, amely az adott incidenstípus esetében, az adott évben bekövetkező összes incidenshez viszonyított arányában való változást szemlélteti.

Szektorális összehasonlítás

A tanulmány jelen részében, az NKI által detektált, az írás elején részletesen bemutatott alábbi szektorok tekintetében azonosított incidenseket elemezzük:

- állami és önkormányzati szervek,
- nemzeti létfontosságú rendszerelemek,
- alapvető szolgáltatásokat nyújtó szereplők,
- bejelentésköteles szolgáltatók,
- közvetítő szolgáltatók,
- nemzetbiztonsági védelem alá eső szervezetek,
- oktatási intézmények,
- egyéb szervezetek.

A 2019 és 2021 közötti időszakban az NKI az egyes vizsgált szektorokat érintően az állami és önkormányzati szervek tekintetében detektálta a legtöbb eseményt – a vizsgált három évben az összes incidens 47%-a –, míg a nemzetbiztonsági védelem alá eső szervezetek esetében ez az arány 8%, a közvetítő szolgáltatók és az oktatási intézmények tekintetében pedig 7%.

A 2. táblázat összefoglalja a 2019–2021 közötti időszakban az egyes szektorokat érő incidenseknek az összes detektált incidenshez viszonyított százalékos arányát.

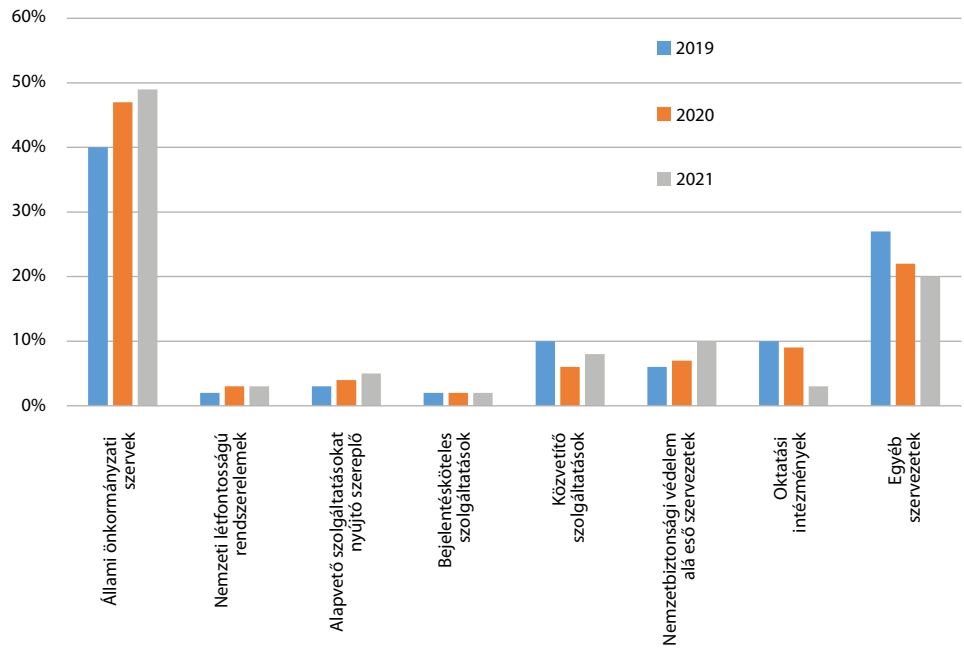
[69] ENISA 2018.

2. táblázat: Az egyes szektorokban kezelt incidensek százalékos eloszlása a 2019–2021. évek összesített eredményeinek tükrében

Az incidensben érintett szektor	Incidensek összesített százalékos aránya 2019–2021
Állami és önkormányzati szervek	47%
Nemzetbiztonsági védelem alá eső szervezetek	8%
Közvetítő szolgáltatók	7%
Oktatási intézmények	7%
Alapvető szolgáltatásokat nyújtó szereplő	4%
Nemzeti létfontosságú rendszerelemek	3%
Bejelentésköteles szolgáltatók	2%
Egyéb szervezetek	22%

Forrás: a szerző szerkesztése

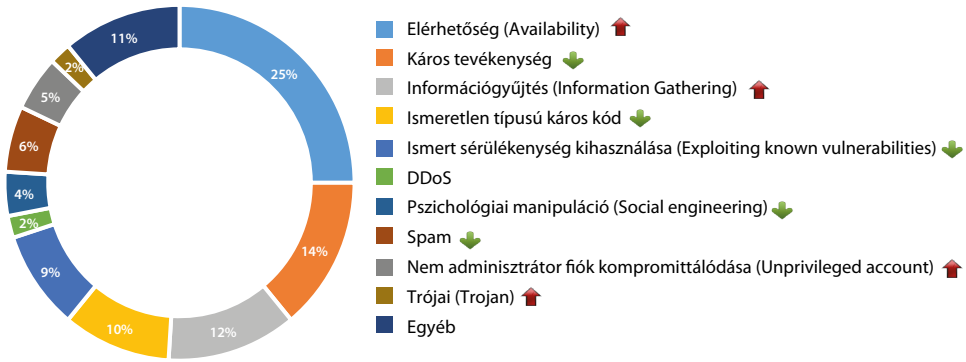
Ahhoz, hogy az egyes szektorokat érintő trendek is kimutathatók legyenek, meg kell vizsgálni, hogy az egyes szektorokat évenkénti bontásban milyen arányban érte incidens, amit a 12. ábra szemléltet.



12. ábra: Szektorális bontás 2019–2021 közötti időszakban, évenkénti bontásban
Forrás: a szerző szerkesztése

A grafikon alapján megállapítható, hogy a leginkább támadott állami és önkormányzati szervek esetében az egyes években, az eseményeknek az összes detektált incidenshez viszonyított aránya nő, így e szektor részéről fokozott védelmi intézkedések szükségesek a további emelkedés megakadályozása érdekében. Hasonló emelkedő tendencia mutatható ki a második legtámadottabb szektor, a nemzetbiztonsági védelem alá eső szervek tekintetében is, valamint az alapvető szolgáltatásokat nyújtó szereplők és a nemzeti létfontosságú rendszerelemek esetében is. A bejelentésköteles szolgáltatók esetében stagnálás, míg a közvetítő szolgáltatók és az oktatási intézmények tekintetében csökkenés figyelhető meg. Az állami és az önkormányzati szervek – mint a legtámadottabb szektor – különálló, incidenstípusok szerinti vizsgálata is indokolt annak érdekében, hogy azonosíthatók legyenek a leginkább fenyegető támadási vektorok.

A 2019 és 2021 közötti időszakban, az állami és önkormányzati szerveket érő incidensek eloszlását a 13. ábra mutatja be.



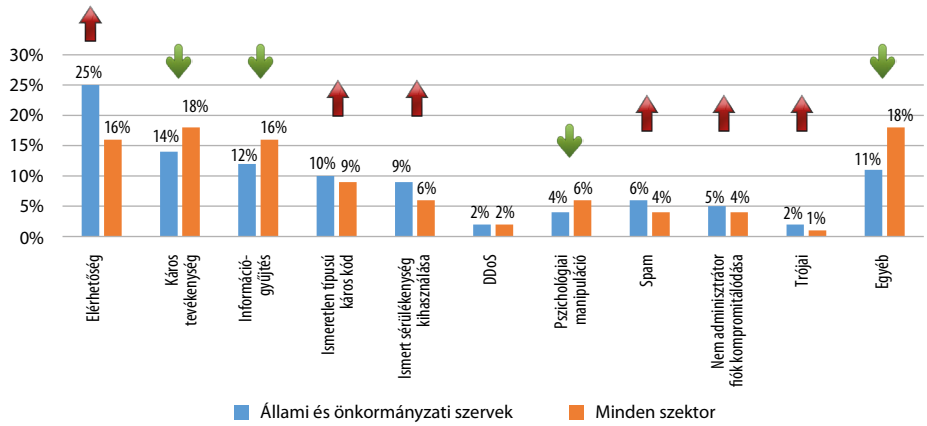
13. ábra: Az állami és önkormányzati szervek incidensei, 2019–2021
Forrás: a szerző szerkesztése

A vizsgált időszakban az elérhetőség volt a legkritikusabb incidenstípus, minden negyedik incidens eredményezte a rendelkezésre állás problémáját az állami és önkormányzati szerveknél (az összes detektált incidenshez viszonyított aránya 25%). Káros tevékenység az incidensek 8%-ában, információgyűjtés 12%-ban, míg ismeretlen típusú káros kód, illetve ismert sérülékenység kihasználása 10, illetve 9%-ban fordultak elő. Az összincidensekhez viszonyítva 10% alatti az aránya a spameknek, a nem adminisztrátor fiók kompromittálódásának, a pszichológiai manipulációnak, valamint a DDoS- és a trójaivírus-támadásoknak.

Amennyiben összehasonlítjuk az állami és önkormányzati szerveket érő leggyakoribb tíz incidenstípus százalékos arányát az egyes incidenstípusoknak az összes szektoron belüli arányával, az alábbi összefüggéseket állapíthatjuk meg a 14. ábra segítségével:

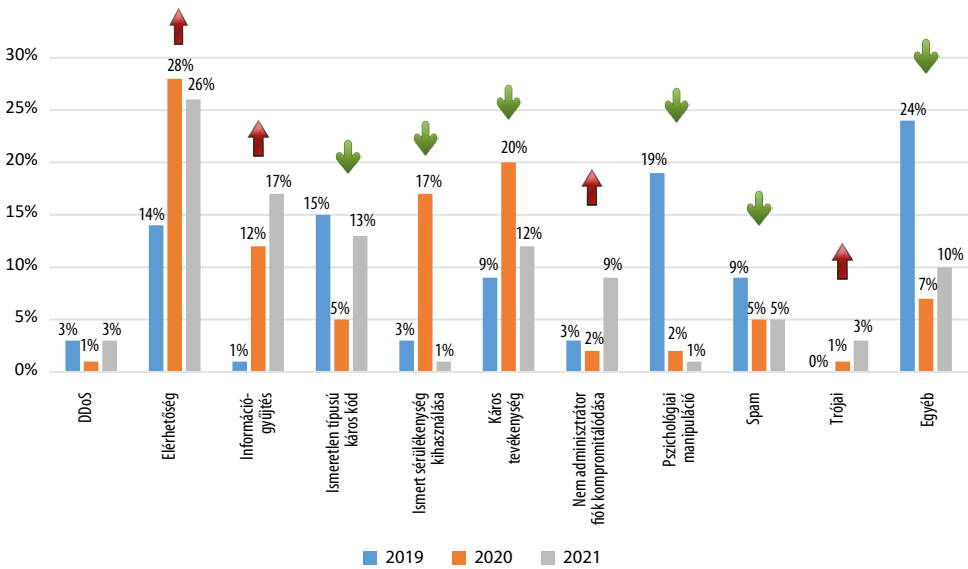
Az elérhetőség, az ismeretlen típusú káros kód, az ismert sérülékenység kihasználása, a spam, a nem adminisztráror fiók kompromittálódása, valamint a trójai vírus incidenstípusok nagyobb arányban fordulnak elő az állami és önkormányzati szervek esetében (az összes szektort érintő átlaghoz viszonyítva), ugyanakkor a káros

tevékenység, az információgyűjtés és a pszichológiai manipuláció kisebb százalékban mutatható ki.



14. ábra: Összehasonlító statisztika az állami és önkormányzati szervek és az összes szektor tekintetében, incidenstípusok alapján
Forrás: a szerző szerkesztése

A 15. ábra segítségével meghatározhatók az állami és önkormányzati szerveket érintő leggyakoribb incidenstípusokhoz kapcsolódó trendek is.



15. ábra: Az állami és önkormányzati szervek incidenstípusai évenkénti összehasonlításban
Forrás: a szerző szerkesztése

A grafikon alapján az elérhetőség, az információgyűjtés, a nem adminisztrátor fiók kompromittálódása, valamint a trójai vírus esetében emelkedő trend azonosítható, míg az ismeretlen típusú káros kód, az ismert sérülékenység kihasználása, a káros tevékenység, a pszichológiai manipuláció, illetve a spamek esetében csökkenő tendencia látható. A DDoS esetében a 2020-ban történő csökkenést követően 2021-ben az arányszám ismét a 2019-es szintre emelkedett.

Pszichológiai manipuláció *(social engineering)*

A pszichológiai manipuláció (social engineering) az emberi hiszékenységre és együttműködésre építő támadási forma. Bár ezt az élet sok más területén is kihasználják, a social engineering kimondottan az információ megszerzésére irányul, ezen belül is elsősorban az informatikai eszközökön tárolt adatokra fókuszálva.[70]

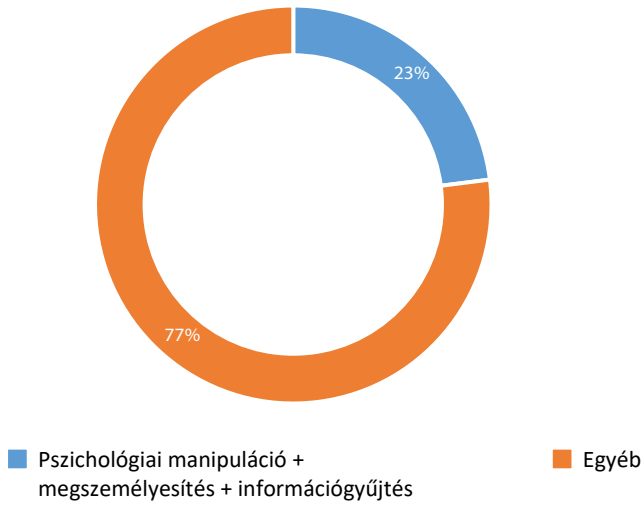
A NKI adatait évenkénti bontásban vizsgálva már megállapítottuk, hogy a pszichológiai manipuláció esetében a 2019-es évhez viszonyítva jelentős visszaesés tapasztalható a 2020–2021-es években, ami azonban nem jelenti a social engineering típusú támadások tényleges csökkenését, valójában egy kategorizálásból eredő eltérés állhat a hátterében. Az elemzett adatok alapján megállapítottuk, hogy a pszichológiai manipuláció csökkenésével párhuzamosan emelkedik az információgyűjtés százalékos aránya, aminek hátterében az ENISA referenciaincidens-taxonómiája állhat, amely szerint a pszichológiai manipuláció az információgyűjtés alkategóriáját képezi. Így feltehetően az incidensek osztályozása során a pszichológiai manipulációval megvalósuló információgyűjtés esetén az utóbbi típust, tehát az információgyűjtést jelölték meg a 2020. és 2021. években.

E jelenségből adódó statisztikai eltérések kiküszöbölése érdekében a pszichológiai manipuláció vizsgálatánál az incidenstípusok alábbi három kategóriájának összesített százalékos eloszlását vizsgáltam a 2019–2021. időszakban:

- pszichológiai manipuláció,
- megszemélyesítés (amely a pszichológiai manipuláció egyik támadási formája) és
- információgyűjtés.

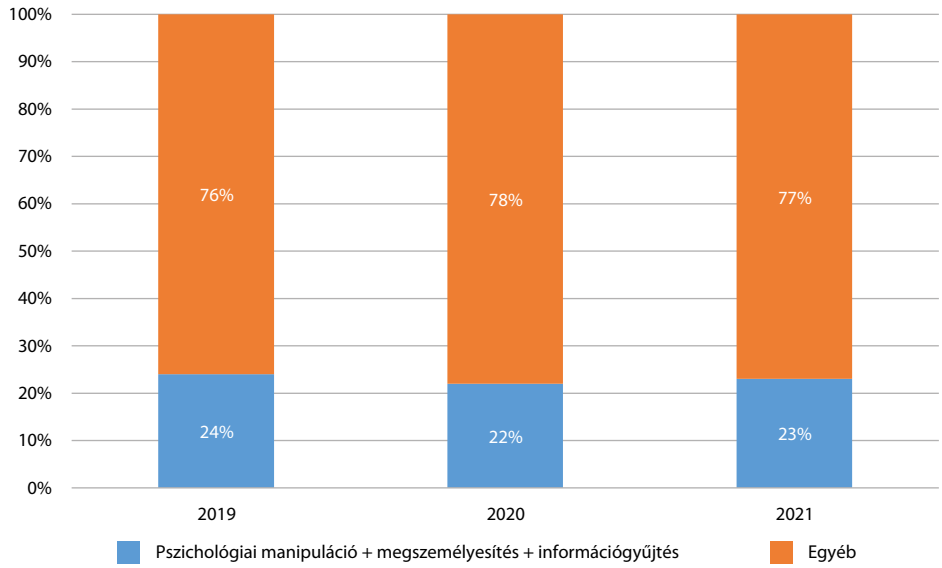
A 16. ábra alapján megállapítható, hogy a három incidenstípus összesített aránya a 2019–2021. években detektált összes incidenshez képest 23%.

[70] Muha–Krasznay 2014: 53.



16. ábra: A pszichológiai manipuláció, a megszemélyesítés és az információgyűjtés összesített aránya, 2019–2021
Forrás: a szerző szerkesztése

A tágabb értelemben vett pszichológiai manipulációt jellemző trend meghatározása érdekében összehasonlítottam az egyes években kimutatható arányukat az összes incidensen belül, amit a 17. ábra szemléltet.



17. ábra: A pszichológiai manipuláció, a megszemélyesítés és az információgyűjtés együttes, egyéb incidenstípusokhoz viszonyított aránya, 2019–2021
Forrás: a szerző szerkesztése

Az elemzés segítségével megállapítható, hogy a pszichológiai manipuláció, a megszemélyesítés és az információgyűjtés együttes aránya kiegyensúlyozott az egyes években, az egyéb incidenstípusokhoz viszonyított arányuk 22% és 24% között mozog. Ugyanakkor meg kell jegyezni, hogy még ha százalékos arányban a detektált incidensek majd egynegyedénél mutatható csupán ki tágabb értelemben vett pszichológiai manipuláció, sikerességük esetén jelentősen nagyobb és komolyabb károk következhetnek be, legyen szó akár információk jogosulatlan megszerzéséről, adatok titkosításáról vagy egyéb káros tevékenységről.

Összegzés és következtetések

A digitalizáció robbanásszerű terjedésének köszönhetően a kibertérben megjelenő, különböző forrásból származó fenyegetések száma és volumene, valamint a támadások következményei is jelentősen megnövekedtek. A kiberbiztonság megfelelő szinten tartása és folyamatos fejlesztése, a kockázatok kezelése, a hatékony védelmi intézkedések alkalmazása az állam elsőrendű feladata. A biztonsági események típusainak és az azonosítható trendeknek az ismerete nagyban elősegíti e kibervédelmi feladatok ellátását és Magyarország szuverenitásának védelmét a magyar kibertérben.

A 2019 és 2021 közötti évek incidenstrendjei azonosítása érdekében e tanulmány keretében elemeztem a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet által detektált incidensekre vonatkozó statisztikai adatokat évenkénti és szektorális bontásban. Az egyes évek vizsgálata során bemutattam a Covid–19-pandémia kiberbiztonságra gyakorolt hatását is. Az ágazati elemzés során kiemelten vizsgáltam a leginkább támadott szektort, az állami és önkormányzati szerveket érő incidenseket, az eredményeket összevetettem az NKI által kezelt egyéb ágazatokban kimutatható események típusaival és az azokhoz köthető trendekkel. Külön fejezetben tértem ki az emberi hiszékenységen és együttműködési készségen alapuló pszichológiai manipuláció, azaz social engineering típusú támadási forma vizsgálatára.

Elemzésem során néhány kiemelkedő tendenciát összevetettem a nemzetközi incidenstrendekkel, aminek segítségével megállapítottam, hogy a hazai incidenstrendek a vizsgált években jelentős eltérést nem mutattak a nemzetközi trendekhez képest. Ennek hátterében elsősorban az áll, hogy a magyar kibertér nem határolható le a klasszikus fizikai országhatárokhoz hasonlóan. A Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat értelmében

> „Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett".

E megfogalmazásból is jól látható, hogy a magyar kibertérben zajló események egyáltalán nem függetleníthetők a globális kibertértől, ez utóbbinak részei, így a globális

hatások hazánkban is kimutathatók, a világszerte tapasztalható incidensek valamilyen formában itt is megjelennek.

A 2020-ban megjelenő világjárvány tökéletesen megmutatta a határokon, sőt kontinenseken átívelő tendenciákat. A 2020. évre vonatkozó elemzésből kiderül, hogy a koronavírus egyes hullámaihoz kapcsolódóan szignifikánsan megemelkedett az NKI által detektált incidensek száma, a tavaszi (2020. február–április) és az őszi hullám (2020. szeptember–november) incidenseinek összesített aránya eléri az összes éves incidens közel 60%-át. 2021-re is igaz, hogy az incidensek százalékos aránya a tavaszi (2021. február–április) és az őszi (2021. szeptember–november) hullám során jelentősen megemelkedett. Mind a számszerű emelkedés, mind pedig az incidenstípusok tekintetében jelentős átfedés tapasztalható a nemzetközi trendekkel, amelyeket a kibertámadók praktikusan alakítottak át, sok esetben a magyar viszonyoknak megfelelően.

Az azonosított trendek egyértelműen bizonyítják a kibertámadók rendkívül gyors alkalmazkodóképességét a világ megváltozott körülményeihez. A Covid–19-világjárvány egyedülálló lehetőségeket teremtett a fenyegetettségi szereplők számára, hogy hasznot húzzanak a bizonytalanságból, a korlátozásokból és az egyes termékek iránti kereslet fellendüléséből. A pandémia alatt a támadók a kiberbűnözés már létező formáit úgy alakították át, hogy azok megfeleljenek a világjárvány narratívájának, kihasználva a helyzet bizonytalanságát és a lakosság megbízható információ iránti igényét. A csalók előszeretettel alkalmaztak social engineering technikákat az emberi viselkedés manipulálására és a gyenge pontok kihasználására az információk megszerzése érdekében.

Az elemzés egyértelműen rávilág arra a tényre, hogy a kiberbiztonsági fenyegetések, a bekövetkezett biztonsági események típusainak, számszerűségének és következményeinek ismerete, valamint az incidenstrendek vizsgálata és figyelemmel kísérése jelentősen hozzájárul a hatékony védelmi intézkedések meghatározásához, végső soron a magyar kibertér megfelelő védelméhez.

Irodalomjegyzék

Berzsenyi Dániel et al. (2018): *Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest: Dialóg Campus.

ENISA (2018): *Reference Incident Classification Taxonomy.* Online: www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Europol (2021): *World's Most Dangerous Malware EMOTET Disrupted through Global Action.* 2021. január 27. Online: www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

Interpol (é. n.): *COVID-19 Cyberthreats.* Online: www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats

Interpol (2020): *Interpol Report Shows Alarming Rate of Cyberattacks during COVID-19.* 2020. augusztus 4. Online: www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Krasznay Csaba – Dobos László – Palla Gergely – Pollner Péter (2019): Információbiztonsági incidensek a közigazgatásban. In Auer Ádám – Joó Tamás (szerk.): *Hálózatok a közszolgálatban.* Budapest: Dialóg Campus, 135–154.

Marsi Tamás (2018): A Nemzeti Kibervédelmi Intézet szerepe az eseménykezelésben. In Berzsenyi Dániel et al.: *Incidensmenedzsment.* Budapest: Nemzeti Közszolgálati Egyetem, 49–84. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/6848/Incidensmenedzsment.pdf?sequence=1

Monori Zsuzsanna Éva (2016): Zaklatás-e a cyberbullying? Az internetes zaklató magatartások büntetőjogi szankcionálásának dilemmái. *In Medias Res,* 5(2), 246–261.

Muha Lajos – Krasznay Csaba (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem.

Miniszterelnöki Kabinetiroda (2021): *Nemzeti Digitalizációs Stratégia 2022–2030.* Online: https://cdn.kormany.hu/uploads/document/6/60/602/60242669c9f12756a2b104f8295b866a8bb8f684.pdf

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

Jogi források

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól

NEMZETBIZTONSÁGI SZEMLE
11. évfolyam (2023) 1. szám 108–112. • DOI: 10.32561/nsz.2023.1.7

Bandi István[1]

Kém az örökkévalóságnak: Frank Wisner – Szomorú kémtörténet egy emberről, aki azt hitte, megváltoztathatja a világot

Szerkesztette: George Cristian Maior, Bukarest, RAO Kiadó, 2014, 272 oldal

Frank Gardiner Wisner 1909-ben született Laurelben (Mississippi állam). A CIA egyik alapító hírszerző vezetőjeként kétségtelenül a hidegháború egyik jelentős szereplője, és – ami ugyanilyen fontos – olyan tevékeny kortanú, akit az áruló Kim Philby ellentéteként emlegetnek. Az ő életrajza ihlette ezt a kötetet, amely George Maior,[2] a román kémelhárítás volt vezetője irányításával, a Nyílt Források Központ munkatársainak – Cristina Posaştiuc, Cristian Lazăr, Cristian Iancu és Monica Bălan – gondozásában jelent meg 2014-ben Bukarestben, a RAO Kiadónál román nyelven.

A könyv megszületésében megkerülhetetlen szerepe volt Frank Gardiner Wisner fiának, akivel George Maior 2002-ben került közvetlen kapcsolatba. Maior rögtön felismerte az ifjabb Frank Wisnerben, aki szintén diplomata, sőt, a védelmi miniszter helyettese volt, hogy segítségével apját, a fedett műveletek irányításával megbízott hírszerzővezetőt tevékenysége árnyékából a nyilvánosság elé állíthatja. A köteten végigvonul az a szerkesztői szimpátia – akár családi barátságból, az ifjabb Wisner visszaemlékezéseinek hatására, akár szakmai elfogultságból fakadt –, amellyel Maior az amerikai hírszerzés egyik atyjának életrajzát az ismeretterjesztő irodalom lazább keretei felé tolja.[3]

[1] Tudományos főmunkatárs, Állambiztonsági Szolgálatok Történeti Levéltára, doktori hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola. E-mail: istvanbandi@gmail.com

[2] George Cristian Maior (1967) román diplomata és szociáldemokrata politikus, szenátor. 2006 és 2015 között a román kémelhárítás (SRI) igazgatójaként dolgozott, 2015–2021-ben Románia amerikai egyesült államokbeli nagykövete volt. 2021 őszétől Romániának a Jordán Királyságba delegált nagykövete.

[3] Maior szerk. 2014: 7–8.

Frank Wisner az ügyvédi pályát elhagyva kezdte meg hírszerzői karrierjét némi kitérővel, hiszen 1941 júliusában az amerikai haditengerészet cenzori irodájában, a District Intelligence Office hadnagyaként dolgozott. Feltehetően a Pearl Harbor-i incidens hatására, 1943 októberében sikerült áthelyeztetnie magát az akkor létrehozott Office of Strategic Serviceshez (OSS, Stratégiai Szolgálatok Hivatala), ahol komoly karriert futott be. A kezdeti szervezeti nehézségeket Hugh Wilford így írja le: „Volt némi szervezeti káosz és rosszul kialakított elképzelések, de az OSS többnyire jó eredményeket ért el a háborúban. Különleges hadműveleti ága a megszállt területeken a gerillatevékenységet irányította, amely helyi ellenállási mozgalmakat inspirált, és elterelte az ellenség figyelmét."[4] Wisner ebbe a szervezetbe érkezett Franklin Delano Roosevelt amerikai elnök egyik tanácsadója segítségével. Első komoly kiküldetésekor, 1942-ben az OSS kairói állomására került, amely akkor az amerikai hírszerzés és kémelhárítás egyik kiemelt központja volt. Kairó után, 1944 júniusában áthelyezték Isztambulba, abba a metropoliszba, amely szinte az összes Balkánnal kapcsolatos intrika és műveleti „játék" központjává vált a második világháború alatt. 1944. augusztus 10-én nevezték ki az OSS isztambuli állomásának vezetőjévé.

A plausible deniability (elhihető/valószerű tagadhatóság) doktrínája[5] idején az OSS kairói központjából induló Wisner haditengerészeti hadnagy életének harmadik állomása Románia volt. Ottani tevékenysége már 1945 januárjában véget is ért, de annál intenzívebb volt hírszerzői pályája szempontjából. Igazi feladata a megállíthatatlan szovjethatalom szándékainak szisztematikus kifürkészése volt, és ebben a tevékenységében úttörőnek számított. Románia 1944. augusztus 23-i kiugrása Wisner számára ideális lehetőséget biztosított arra, hogy közelebb kerüljön az új ellenséghez, a szovjetekhez. Így 1944. szeptember elején Bukarestbe érkezett, ahol egy elég nagy csapatot vezetett, amely a Hammerhead nevű műveletben vett részt, és ezen keresztül, a hivatalos álláspont szerint, az országban korábban elfogott amerikai hadifoglyok hazajuttatását segítették. Valójában azonban információkat gyűjtött, többek között az előrenyomuló szovjethatalom megerősödéséről is.

Bill Colby, a későbbi CIA-igazgató azt állította, hogy Wisnernek nem kevesebbet sikerült kialakítania, mint „egy templomos lovagrendéhez hasonló légkört, melyben az volt a feladatuk, hogy megmentsék a Nyugatot a kommunista sötétségtől".[6]

A kötet – mindamellett, hogy beszámol a korábban említett titkos művelet keretében ledobott ejtőernyősök kimenekítéséről – empatikus leírást ad a német ajkú polgárok 1945. januári deportálásáról, és reflektál a román béketapogatózás kapcsán a magyar katonai hírszerzők tevékenységére is, többek között Hatz Ottó[7]

---

4 Wilford 2019: 8.

5 Az Amerikai Egyesült Államok hivatalosan tagadta bármilyen titkos akcióban való részvételét, ha esetleg az ellenfél kiderítette volna.

6 Colby 1978: 73.

7 Hatz Ottó (1902–1977) hivatásos tiszt, diplomata, hírszerző, vívó. 1932-ben végzett a Magyar Királyi Honvéd Ludovika Akadémián. 1934-től a Honvéd Vezérkar munkatársa. 1941-től 1944-ig Szófiában és Ankarában katonai attasé. Mindeközben a magyar kormány megbízásából tárgyalásokat folytatott angol és amerikai megbízottakkal a fegyverszünet megkötéséről. 1944 májusában a Gestapo letartóztatta. 1944. július 1-jétől október 15-ig Csatay Lajos honvédelmi miniszter szárnysegédje, és részt vett a titkos moszkvai fegyverszüneti delegáció útjának előkészítésében. 1944. november 7-én átszökött a szovjet hadsereghez. 1944 decemberében az Ideiglenes Nemzetgyűlés alapító tagja, illetve Debrecenben a Honvédelmi Minisztérium hivatásos állományában tevékenykedett. 1945. április elején a szovjet államvédelmi szervek letartóztatták, és 1952-ig

balkáni tevékenységére, akit árulónak minősített. Ezzel szemben Kádár Gyulát[8] és Szombathelyi Ferencet,[9] akik a Dogwood[10] műveletben közvetve szerepeltek, az USA védelmére méltónak találta. A korábban említett szerkesztői elv tükröződik abban, ahogyan a 160 oldalas törzsszöveg megoszlik a Wisner és Románia kapcsolatát taglaló fejezetek és a hírszerzői életút későbbi állomásait bemutató részek között, az előbbiek javára. Wisner további karrierjének állomásait kilenc fejezetben mutatta be a Maior irányította munkaközösség.

Rövid, a civil életbe tett kitérő után az amerikai külügyben fedett műveletekért felelős vezetőként az OPC (Office of Policy Coordination, Szakpolitikai Koordinációs Hivatal) szervezetét irányítja 1948-ban. Ez maradt a vadászterülete egészen az ötvenes évek végéig, amikor is betegsége miatt a CIA vezetője, Allen Dulles kivonta a különleges műveletek vezetéséből. 1965-ben saját farmján lett öngyilkos. Wisner irányítása alatt az OPC rejtett akciói növekvő „iparággá" váltak a CIA számára. 1949 és 1952 között az OPC 300-ról több mint 5000 főre növelte állományát, míg költségvetése 4,7 millióról 82 millió dollárra emelkedett, jelenléte a tengerentúli CIA-állomások számát illetően 7-ről 47-re növekedett.[11]

Számos fedett művelet kiötlője és vezetője volt: a kelet-európai országokból származó menekültek soraiban végzett tippkutatástól a beszervezésig, majd a vasfüggöny államaiba (Albániába, Lengyelországba, Ukrajnába) való beszivárogtatásig. A titkos műveleteket személyesen vezette végig. A kommunista rendszereket nem sikerült megdönteni, de a világ más tájain hatékony tevékenységet fejtett ki, így Mohammad Mosaddegh iráni elnök megdöntése vagy a guatemalai antikommunista beavatkozás növelte szakmai elismertségét.

Moszkvában vizsgálati fogságban tartották. 1952-ben a Szovjetunió elleni tevékenység vádjával 15 évi börtönbüntetésre ítélték, 1955-ben a vádak alól felmentették, és hazatérhetett Magyarországra.

8 Kádár Gyula (1898–1982) katonatiszt, hírszerző. 1918-ban avatták gyalogos hadnaggyá a Magyar Királyi Honvéd Ludovika Akadémián. 1933-tól tanított a Ludovikán. Az 1933–34-es tanévtől a Ludovika Akadémia tanára. 1937-ben vezérkari őrnaggyá léptették elő. 1942 májusától a 6. vkf. (nemzetvédelmi és propaganda) osztályának a vezetője. 1943 augusztusától a 2. vkf. (hírszerző és kémelhárító) osztályát vezette. Szombathelyi Ferenc a Honvéd Vezérkar főnöke utasítására ő készítette elő az angolszász ejtőernyős egységek és égi úton szállított csapattestek magyarországi fogadását a kiugrás esetére, valamint a magyar honvédség csatlakozását az angolszász expedíciós hadsereghez. A német megszállás után előbb a Gestapo tartóztatta le, majd szabadulása után német nyomásra a magyar hatóságok, végül a bíróság a hűtlenség vádja alól felmentette. A nyilasok újból letartóztatták, és a front közeledtével Németországba szállították. Hazatérésekor a Katonapolitikai Osztály tartóztatta le, majd átadták a szovjeteknek. A Szovjetunióban a szovjet katonai bíróság 15 évi kényszermunkára ítélte. 1955-ben szabadult és tért haza.

9 Szombathelyi Ferenc (1887–1946) hivatásos katonatiszt, Honvéd Vezérkar főnöke. A bécsi hadiiskolán (Kriegsschule) végzett. Hírszerző, kémelhárító pályáját 1920-ban Szegeden kezdte. 1926-tól 1931-ig a Magyar Királyi Honvéd Ludovika Akadémián a szabályzatismertető tanfolyamot, majd 1936-tól 1938-ig az Akadémia parancsnoka. 1941-től 1944 áprilisáig a Honvéd Vezérkar főnöke. 1944 októberében a nyilasok letartóztatták és Sopronkőhidára szállították. 1946-ban a Népbíróságok Országos Tanácsa (NOT) életfogytiglani börtönbüntetésre ítélte. Később mint elítéltet kiadták Jugoszláviának, ahol az újvidéki eseményekért felelős vezetőként kivégezték.

10 Dogwood művelet: az OSS által a második világháború alatt Törökországban felépített hírszerzőhálózatot Dogwoodnak hívták, és Lanning Macfarland vezette. A Dogwoodot valójában Macfarland alakította ki, fedőfoglalkozásként pedig az isztambuli Western Electric Company alkalmazottjaként tevékenykedett. Eredetileg Dogwood egy Alfred Schwarz nevű csehszlovák mérnök fedőneve, akinek az volt a feladata, hogy vegyék fel és tartsák a kapcsolatot a náciellenes csoportokkal Ausztriában, Németországban és Magyarországon.

11 Pisani 1991: 68.

A kötet nem kerüli meg a hírszerző Wisner személyesebb, mentális összeomlásának kényes témáját sem, ami a túlzott alkoholfogyasztásban és dohányzásban, de ingerlékenységben is megnyilvánult, és egyre inkább hátrányosan hatott a munkájára. Az 1956-os magyar forradalom kudarca felerősítette depresszív hajlamait, megerősítve benne azt a fokozódó meggyőződést, hogy az Amerikai Egyesült Államok el fogja veszíteni a hidegháborút. A kötetben második Gomulkaként emlegetett Nagy Imre fémjelezte budapesti forradalom amiatt is különösen fontos, mert a CIA nem hivatalos szerepvállalását vizsgáló bizottság azzal vádolta a hírszerzést, hogy „a Red Sox/Red Cap csapatok irreális ígéreteket tettek a magyar tüntetők vezetőinek, melyek szerint az USA támogatni fogja a megmozdulást, ami a tüntetés felesleges felizzásához és ebből következően keményebb megtorlásokhoz vezetett a szovjetek részéről". Wisnernek élete végéig kétségei voltak a magyar forradalommal kapcsolatban kifejtett tevékenységéről.

Tartalmi szempontból tovább emelte volna a kötet hitelességét, ha a szerkesztő és munkatársai hivatkoztak volna a CNSAS, illetve az SRI archívumában fellelhető dokumentumokra. A „Különleges Hírszerző Szolgálat (SSI) román irattárakban megtalálható, a minősítés alól feloldott dokumentumok kutatásából származó eddig nem ismert információk" említése a szerzői bevezetőben azt a benyomást keltheti az olvasóban, hogy a kötetben használtak ilyen iratokat, azonban a törzsszövegben és a mellékletekben is kizárólag Frank Gardiner Wisner személyes irataiból válogattak dokumentumokat, amelyeket a fia bocsátott a szerkesztői csapat rendelkezésére.

Mindent egybevetve a könyv leképezi egy hírszerző életének rendkívüli bonyolultságát. Egy igazi hírszerzőét, aki már a második világháború alatt felfogta a szovjetek stratégiáját, és ez ellen harcolt élete végéig. Olyan tiszt volt, aki sokáig titkos műveletek tervezésében és ellenőrzésében remekelt. A műveletek sikertelensége (például Philby árulása) nem Wisner hibája volt, aki – bármilyen kompetens és kitartó is lett volna – egymaga nem változtathatta meg a világot. Ha egy picit is azonosulunk a narratív szállal, akkor el tudunk képzelni egy fiatal tisztet és a harcait, és „élőben" asszisztálhatunk a kommunista világ elleni harchoz.

A mű szerzői 70 oldalon keresztül gazdag, eredeti fényképanyaggal és korabeli dokumentumokkal teszik hitelesebbé a hírszerző tiszt életútját. Külön név- és tárgymutató, illetve kronológia segíti az olvasót a szövevényes narratívában és a szakkifejezések rengetegében.

A kötet jól illeszkedik ahhoz a dinamikus és önálló arculatátalakításhoz, amely a szakmai külkapcsolatok szerves részét képezte, ezekkel segítették Románia politikai diplomáciai építkezését. Így érdemes a George Maior, az SRI volt vezetője szerkesztette kötetre tekinteni mindamellett, hogy a könyv az amerikai hírszerzés egyik alapítójáról egyedi dokumentumokat, továbbá magyar vonatkozású adatokat is tartalmaz, amelyek a korszakkal foglalkozók számára is az újdonság erejével hathatnak.

Irodalomjegyzék

Colby, William (1978): *Honorable Men: My Life in the CIA*. New York: Simon & Schuster.

Maior, George Cristian szerk. (2014): *Spion pentru eternitate: Frank Wisner. O poveste tristă de spoinaj despre un om care a crezut că poate schimba lumea*. București: Editura RAO.

Pisani, Sallie (1991): *The CIA and the Marshall Plan.* Lawrence: University Press of Kansas.

Wilford, Hugh (2019): *A History of the CIA.* Course Guidebook. Long Beach: California State University. Online: www.library.pima.gov/wp-content/uploads/sites/6/2020/09/Agency-a-History-of-the-CIA-8000.pdf

Tartalom