NEMZETI KÖZSZOLGÁLATI EGYETEM
VÉDELMI-BIZTONSÁGI SZABÁLYOZÁSI ÉS KORMÁNYZÁSTANI KUTATÓMŰHELY

VÉDELMI-BIZTONSÁGI SZABÁLYOZÁSI ÉS KORMÁNYZÁSTANI MŰHELYTANULMÁNYOK

2021/14.

DR. VIKMAN LÁSZLÓ

A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra

ISSN 2786-2283

Rólunk

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

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

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

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

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

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

Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/14.

Szerző(k):

dr. Vikman László

Szerkesztő:

Dr. Kádár Pál PhD dandártábornok

Kiadja

Nemzeti Közszolgálati Egyetem

Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely

Kiadó képviselője

Dr. Kádár Pál PhD dandártábornok

A kézirat lezárva: 2021. november 2.

ISSN 2786-2283

Elérhetőség:

Nemzeti Közszolgálati Egyetem

Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely

1441 Budapest, Pf.: 60

Cím: 1083 Bp., Ludovika tér 2.

Központi szám: 36 (1) 432-9000

Vikman László[1]

A KÖZMŰSZOLGÁLTATÁSOK ÉS A REZILIENCIA EGYES KÉRDÉSEI, KÜLÖNÖS TEKINTETTEL A KIBERBIZTONSÁGRA

A szerző munkájában áttekintést ad a nemzeti ellenálló képesség és a közműszolgáltatások folytonosságának összefüggéseiről, a kiberbiztonság kapcsolódó kérdéseiről. A műhelytanulmány bemutatja azon dokumentumokat, amelyek a hazai, a szövetségi és az európai uniós szabályozásban stratégiai szinten jelennek meg e vonatkozásban, majd részjavaslatokat fogalmaz meg a reziliencia fejlesztése kapcsán a jövő kihívásainak kezelésére.

1. Bevezető

A címben szereplő három kulcsszó az elmúlt években a biztonság- és védelempolitikai szakirodalom legnépszerűbb témái közé tartozik, az egyébként szintén említésre kerülő hibrid kontextussal kiegészítve már lehetetlen lenne elkerülni a hatásvadászat vádját. Ennek ellenére jelentőségük és aktualitásuk nehezen eltúlozható, hiszen csak a közelmúlt nagy publicitású közszolgáltatási ellátási zavarait áttekintve nyilvánvaló, hogy micsoda társadalmi feszültségeket és frusztrációt képesek gerjeszteni az egyes országokban a hétköznapokban megszokott fogyasztási rendet érintő – akár csak átmeneti – fennakadások. Az Európát (és a világot) jelenleg is sújtó földgáz-ellátási krízis[2], vagy a nyilvánvalóan célzott és szándékos, energetikai infrastruktúrákat bénító kibertámadások[3] további terjedelmes bizonyítást nem igénylően jelzik, hogy a mára szinte főszabállyá váló[4], a nemzeti és nemzetközi jog

[1] Dr. Vikman László főhadnagy, jogász, Magyar Honvédség

[2] Az európai földgázellátási zavarokról: https://www.bbc.com/news/world-europe-58896847
Moldova arra kényszerült, hogy Lengyelország segítse ki, mivel az orosz szállító partnerrel nem tudott megállapodásra jutni: https://www.euronews.com/2021/10/27/moldova-receives-first-non-russian-gas-delivery-as-it-grapples-with-severe-energy-crisis

[3] Colonial Pipeline ransomware támadás: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/
Amerikai villamos-energia hálózat elleni támadás: https://www.secureworld.io/industry-news/first-u.s.-power-grid-attack-details

[4] A hibrid hadviselés és a 21. századi biztonságpolitikai kihívások kapcsán lásd pl. Farkas Ádám (szerk.): Az állam katonai védelme az új típusú biztonsági kihívások tükrében, 2018, NKE Budapest, vagy Farkas Ádám: Komplex biztonság, hibrid konfliktusok, összetett válaszok, Honvédségi Szemle 2020/4. 11-23. o.; Farkas Ádám: A totalitás kora? Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018., Farkas Ádám: Az állam fegyveres védelmének alapvonalai. Budapest, Katonai Nemzetbiztonsági Szolgálat, 2020.
A különleges jogrendi szabályok áttekintés és szükséges reformja kapcsán lásd pl. Farkas Ádám, Kelemen Roland (szerk.): Szkülla és Kharübdisz között - Tanulmányok a különleges jogrend elméleti és pragmatikus kérdéseiről, valamint nemzetközi megoldásairól, 2020, Magyar Katonai Jogi és Hadijogi Társaság; Hódos László: A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai, Honvédségi Szemle 148. Évf. 4(2020), https://doi.org/10.35926/HSZ.2020.4.4, Kelemen Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható

legfontosabb vörös vonalait nem átlépő hibrid konfliktusok egyik elsődleges hadszínterévé váltak a közszolgáltatások.

A clausewitz-i maxima értelmezése, miszerint a háború a politika folytatása más eszközökkel, mára katonai körökben is jócskán megváltozott. Két vagy több állami – sőt nem-állami – aktor közötti relációkban már régen nem csak ez a két fokozat képzelhető el egy konfliktusban. Talán közelebb van az igazsághoz, hogy az ellenérdekeltek közt a politika eszköztárában az ultima rationak tekintett háború mellett a korábban sem ismeretlen diplomáciai lépéseken túl a gazdasági nyomásgyakorlás[5,] vagy a különböző adminisztratív és igazgatási korlátozások széles eszköztára mellé csak gazdagodtak a választható érdekérvényesítő lehetőségek a hibrid konfliktusok újításaival, amelyek lehetnek hagyományos eszközök „új csomagolásban" (mint a lawfare[6], avagy a jogi sérülékenységek kihasználása) vagy teljesen újak is (mint a kiberműveletek). Ezt a képet pedig csak bonyolítja az a tény, hogy a glóbusz különféle részein ezen eszközöket használni törekvő állami és nem állami szereplők egyre kevéssé kívánják a Nyugat által diktált szabályok szerint folytatni a hatalmi társasjátékot[7], miközben a Nyugaton belül is vannak sajátutas törekvések (mint a drónhadviselés[8]), illetve rendszerszintű változások.[9]

Nagyrészt a kibertér sajátosságainak köszönhetően még bőven a háború szintje előtt mára lehetségessé vált hagyományos fegyveres erők alkalmazása nélkül olyan infrastrukturális zavarok és rombolás előidézése, amelyekhez akár csak néhány évtizede elszánt és jól informált, felszerelt és kiképzett szabotőrökre vagy részletes haditervek fegyelmezett végrehajtására volt szükség, ezzel kockáztatva, vagy akár nyíltan felvállalva az attribúciót, (amely a kiberműveletek kapcsán mindig központi kérdés jogi szempontból) és amelyek kapcsán jogosan mérlegelhető lehet egyes esetekben, hogy az okozott kár elérte-e a

fejlődése, Honvédségi Szemle 148. Évf. 4(2020), https://doi.org/10.35926/HSZ.2020.4.5; Resperger István: Az aszimmetrikus hadviselésre adható válaszok, Honvédségi Szemle Évf. 145. szám 1(2017) 24-43. o.; Porkoláb Imre: Aszimmetrikus konfliktusok tapasztalatai a nemzetbiztonsági tanácsadó szemszögéből, Honvédségi Szemle Évf. 145. szám 4(2017) 3-15. o.

[5] Lásd pl. Michael Taillard: Economics and Modern Warfare - The Invisible Fist of the Market, 2012, Palgrave MacMillan

[6] Átfogó és rendszerező igényű feldolgozások: Orde F. Kittrie: Lawfare, Law as a Weapon of War, 2016, Oxford University Press; Cristiano Zanin, Valeska Martins, Rafael Valim: Lawfare: Waging War through Law, 2021, Routledge; Petruska Ferenc: A lawfare fogalma, Katonai Jogi és Hadijogi Szemle, 9. évfolyam, 2021/3. szám, 97-106. o.

[7] A téma kapcsán lásd: Farkas Ádám: Gondolatok a védelmi és biztonsági szabályozást és kormányzást meghatározó egyes eurázsiai trendekről. In: Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/10. (letöltve: 2021.10.29., https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK%20M%C5%B1helytanulm%C3%A1nyok%202021_10_%20Farkas%20%C3%81d%C3%A1m_Gondolatok%20a%20v%C3%A9delmi%20%C3%A9s%20biztons%C3%A1gi%20szab%C3%A1lyoz%C3%A1st%20%C3%A9s%20korm%C3%A1nyz%C3%A1st%20meghat%C3%A1roz%C3%B3%20egyes%20eur%C3%A1zsiai%20trendekr%C5%91l.pdf)

[8] Lásd Spitzer Jenő: A dróntámadások nemzetközi joggal való összeegyeztethetőségének egyes kérdései, kitekintéssel a drónok védelmi célú alkalmazásának perspektíváira, In. Farkas Ádám (szerk.): Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében, 101-146. o.; Magyar Katonai és Hadijogi Társaság, Budapest 2018.; Kis Kelemen Bence: Drónok háborúja (1.), Honvédségi Szemle, Évf. 146. szám 1(2018), 70-82 o.

[9] Lásd Magyar Sándor, Simon László: A terrorizmus és indirekt hadviselése az EU kiberterében, SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA 2017: (4) pp. 57-68.; Vikman László: Az amerikai titkosszolgálati rendszer áttekintése, Katonai Jogi és Hadijogi Szemle 2020/4. szám, 35-68. o.; Spitzer Jenő: A nemzetbiztonsági szolgálatok helye, szerepe Franciaország védelmi és biztonsági rendszerében, Katonai Jogi és Hadijogi Szemle 2020/4. szám, 69-94. o.;

nemzetközi jogi értelemben vett fegyveres támadás szintjét (ami az ENSZ Alapokmány 51. cikkelye, vagy a Washingtoni szerződés 5. cikkelye szempontjából vizsgálandó).

Az energia-ellátás, és az ivóvízhálózat zavartalan működése a nyugati demokratikus társadalmak egyik súlyponti eleme – akár katonai művelettervezési szempontból is értelmezhető módon[10]. Ezek minden formája a jóléti szolgáltatások alapfeltétele, nélkülük többek közt a távközlés, az egészségügyi szolgáltatások, a közlekedés és szállítás, és a magas hozzáadott értékű gazdasági tevékenység sem végezhető. Így triviális módon a közszolgáltatások zavartalan működése és működtetése minden tartósabb politikai stabilitást célzó vezető elit prioritásai közt magasan értékelt. A klímaváltozás fokozatosan[11], a COVID-pandémia viszont sokk-szerűen ébresztette rá a társadalmakat, hogy az egyébként kényelmes életmódunk, fogyasztási szokásaink, ingatlanjaink, az ellátási láncaink és készletfelhalmozási szokásaink a 21. század eleji Európában nincsenek felkészülve még néhány hetes alapszolgáltatási zavarokra sem. Nem szükséges túl élénk fantázia ahhoz sem ezek után, hogy egy kifejezetten az ezeket a szolgáltatásokat, vagy akár csak fontos részfolyamataikat, kulcsfontosságú logisztikai mozzanataikat célzó, több irányból és fázisban érkező támadás mekkora káoszt lehet képes előidézni. Egy ilyen „doomsday scenario" részelemeire számtalan demonstratív példát lehet felsorolni úgy a valóságban[12], mint a biztonságpolitikai tárgyú fikciós irodalomban[13].

Természetes módon ezeket a kockázatokat és fenyegetéseket felismerve a döntéshozók nemzeti, EU-s és NATO-szövetségi szinten is tettek megelőző lépéseket vonatkozó stratégiák elfogadásával, keret- és specifikus szabályozások alkotásával, a döntéshozatali eljárásaik „áramvonalasításával", meglévő szervezetek új hatáskörökkel való felruházásával, vagy teljesen új szervezetek létrehozásával.

Ebben a rövid tanulmányban – nem feltétlenül a teljesség igényével, sokkal inkább az aktualitásokra és a várható fejleményekre koncentrálva – kifejezetten a közműszolgáltatók előtt álló kihívásokra kitérve szeretnék felvetni néhány gondolatot. Majd a nemzeti stratégiáink jelenlegi állapotának „leltározása" után kissé rövidebben a NATO, és részletesebben az EU új és tervezett lépéseit és vízióját áttekintve szeretnék egy képet adni arról, hogy milyen irányokban várható elmozdulás a nemzeti szabályozást is nagyban determináló szupranacionális regulatív közegben, végül rövid kitekintést adok arról, hogy a közösségi és nemzeti fejlesztéspolitika hogyan kívánja ösztönözni az ellenállóképesség és különösen a kiberbiztonság szintjének emelését az uniós tagállamokban.

[10] Lásd pl. Vikman László: A művelettervezés jogi feladatai, Honvédségi Szemle 149. szám (2) 2021. 44-56. o. https://doi.org/10.35926/HSZ.2021.2.4

[11] Vö. Nagy Rudolf: A klímaváltozás hatása a kritikus infrastruktúrák védelmére, Nemzet és Biztonság, 2010/2., 35-44.o. http://www.nemzetesbiztonsag.hu/letoltes.php?letolt=126 (letöltve: 2021.10.30.)
Georgios Marios Karagiannis et al.: Climate change and critical infrastructure – floods, 2019, EU Joint Research Centre, https://publications.jrc.ec.europa.eu/repository/handle/JRC109015 (letöltve: 2021.10.30.)

[12] Simona R. Soare, Joe Burton: Smart Cities, Cyber Warfare and Social Disorder, in. A. Ertan et al. (ed): Cyber Threats and NATO 2030: Horizon Scanning and Analysis, 106-124. o., 2020, NATO CCDCOE, https://ccdcoe.org/library/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis/ (letöltve: 2021.10.31.)

[13] P.W. Singer, August Cole: Ghost Fleet: A Novel of the Next World War, 2015. Eamon Dolan/Houghton Mifflin Harcourt

2. Reziliencia és kiberfenyegetések a közműszolgáltatások területén

A reziliencia definíciójára már ezerféle megközelítés található, részemről a praktikusabbakat preferálva az alábbi kettőt tekintem leginkább irányadónak.

„A reziliencia egy rendszer képessége arra, hogy külső sokkok ellenére képes legyen fenntartani struktúráját és funkcióit."[14]

Egy másik megközelítésben egy közösség rezilienciája a forrásbiztonság és az adaptív képesség eredője.[15] Elképzelhetők tehát csekély erőforrásokkal rendelkező, de magas adaptív képességű közösségek, amelyek képesek reziliensek lenni, de a viszonylagos erőforrás-bőség is pótolhatja az alkalmazkodási képesség terén tapasztalható hiányosságokat.

Közösségi reziliencia	
Forrásbiztonság	Források teljesítménye
	Források redundanciája
	Források diverzitása
Alkalmazkodóképesség	Szervezeti emlékezet
	Innovatív tanulás
	Összekapcsoltság

A gazdálkodó szervezetek kultúrájába, különösen az összetett tervezési folyamatokkal működő multinacionális cégeknél az ellenállóképesség, a termelés, a működés folyamatosságának megőrzése és fenntartása már régen bevéződött. Nem az informatikai technológiák fejlődésének robbanásszerű fejlődése, nem is a 20. század elején megjelenő modern gyártósorok, vagy a klasszikus szénporos ipari forradalom kényszerítette ezt ki, hanem a kapitalizmus belső logikája. Az informatikai katasztrófa-elhárítási, vagy helyreállítási tervek ezen eszközök bevezetésével szinte egyidőben jelentek meg, hiszen az üzletmenet folytonosságát ezek vonatkozásában is garantálni kellett, és a jelentős üzemeket irányító mérnökökhöz hasonloan az üzleti menedzsmentet végző közgazdászok számára is teljesen magától értetődő ezeknek az elővigyázatossági intézkedéseknek a jelentősége.

A gazdasági működés fenntartását mára már szinte tudományos igényességgel művelik, és részévé vált a nemzetközi üzleti tanácsadó cégek szolgáltatási portfóliójának is:

„Az üzletmenet-folytonosság szervezése magában foglalja az infrastruktúrával, információ-biztonsággal, alkalmazottakkal, működéssel és kommunikációval kapcsolatos kockázatokkezelését azzal a céllal, hogy felkészítse a vállalatot az új kihívásokra, amelyekkel szembe kell néznie, és biztosítsa a működés és a termelés folyamatosságát.

Az üzletmenet-folytonosság menedzsment stratégiai és operatív keretet határoz meg a vállalat ellenállóképességének növelésére a megszokott működés biztosítása, és a működést

[14] Kuslits Béla: Reziliencia: változás és állandóság társadalmi-ökológiai rendszerekben, Magyar Tudomány 181 (2020) 12, 1648-165, https://mersz.hu/dokumentum/matud202012__13 (letöltve: 2021.10.31.)
[15] Longstaff, Patricia H. et al. "Building Resilient Communities: A Preliminary Framework for Assessment." Homeland Security Affairs 6, Article 6 (September 2010). https://www.hsaj.org/articles/81

zavaró események (pl. üzemleállás) megfelelő kezelése érdekében. A cél egyértelmű: megakadályozni a folyamatok vagy szolgáltatások fennakadását."[16]

A Deloitte például kifejezetten a COVID hatásaival kapcsolatban állított össze egy intézkedéscsomagot[17]:

- Kezdeti intézkedések
    - Alapvető biztonsági intézkedések bevezetése
    - A WHO, CDC stb. ajánlásainak bevezetése
    - Az iparágon belül bevezetett intézkedések összegyűjtése
    - Utazási korlátozás vagy tiltás a munkavállalók számára
    - Üzletmenet-folytonosság menedzsment tanácsadás
- Infrastrukturális kockázatok
    - Az infrastuktúra és más szolgáltatások (SaaS stb.) ellenőrzése, készek-e a távolról történő munkavégzés következtében megnövekvő terhelés fogadására
    - A vállalati rendszerek távolról működtethetők-e az informatikai alkalmazottak fizikai jelenléte nélkül (üzemeltetés, támogatás stb.)
    - A távoli működtetés esetén a lehetséges meghibásodási pontok feltérképezése az infrastruktúrán belül, az ellenintézkedések megtervezése
    - A szállítók felelősségének meghatározása vészhelyzet esetén, szükséges szerződésmódosítások előkészítése
    - Elegendő informatikai támogatás kialakítása a távolról dolgozó munkavállalók számára
    - Prioritások kialakítása a vállalati rendszerekhez való hozzáférésre (menedzsment, felső vezetés prioritása stb.)
    - A távoli elérést biztosító alkalmazások licenszeinek áttekintése
- Kiberbiztonsági kockázatok
    - A rendszerek biztonsága és monitorozása megfelelő-e távoli hozzáférés esetén
    - A távoli elérésű alkalmazások (VPN stb.), továbbá azok patch szintjének és hardening beállításainak tesztelése
    - A válsághoz kapcsolódó adathalász, social engineering támadásokkal kapcsolatostudatossági képzések szervezése
- Munkavállalói kockázatok
    - A kulcsfontosságú szerepek (amelyek megkövetelik a helyszíni hozzáférést) elemzése, helyettesítési terv készítése ezen szereplők hiánya esetére
    - Intézkedések megtervezése, amelyek segítik a munkavállalókat a stressz és a stresszes helyzetek kezelésében
    - A munkavállalók elosztásának megszervezése a csökkentett tevékenységek különböző szintjein
    - Mobilitási lehetőségek biztosítása a munkavállalóknak (műszakok megosztása, szállítás stb.)
- Üzleti és működési kockázatok
    - A szervezeten belüli lehetséges meghibásodási pontok (folyamatok, alkalmazottak, technológiák) feltérképezése, ellenintézkedések készítése

[16] https://www2.deloitte.com/hu/hu/pages/deloitterol/articles/covid19/uzletmenet-folytonossag-menedzsment-tanacsadas.html (letöltve: 2021.10.31.)
[17] Uo.

    - Vészhelyzeti intézkedések és szervezeti utasítások kidolgozása a működés folyamatosságának biztosítása érdekében, a kockázati szinteknek megfelelően
    - Reagálási tervek felállítása (eljárások, munkavállalók elosztása, eszközök és egyéb erőforrások)
    - Felkészülés az ellátási láncban keletkező problémákra
    - Intézkedések és megállapodások bevezetése a távolról nem végezhető munkákkal kapcsolatban
    - Felkészülés az iroda vagy üzleti egységek bezárásának szükségességére
    - A szervezet stabilizálása a jelentős piaci hatással bíró gazdasági események hatására (költségek, folyamatok és portfóliók optimalizálásának tervezése)
    - Forgatókönyvek, tervek és intézkedések készítése az üzleti műveletek helyreállításához (katasztrófa helyreállítási tervek)
- Kommunikációs kockázatok
    - Kommunikációs eljárásrend kialakítása a munkavállalókkal (pozitív), az üzletipartnerekkel, beszállítókkal, hatóságokkal és a nyilvánossággal

A COVID által okozott stressz mértékét jól jelzi, hogy nem csak az alapvetően közép- és nagyvállalati szférára célzó tanácsadói szektor, de a Magyar Kereskedelmi és Iparkamara is igyekezett tanácsokkal előállni, és Üzleti Túlélőcsomag[18] címmel egy folyamatosan frissített tájékoztató dokumentumot készített, amelyben szintén vannak javaslatok az üzletmenetfolytonosság biztosítására, kitérve pl. a beszállítókkal való folyamatos egyeztetés, a távmunka, vagy a céges válságstáb kijelölésének fontosságára.

A KPMG 2018-ig készített a hazai üzletmenetfolytonosság-menedzsment helyzetéről éves körképet[19], kifejezetten az informatikai kockázatkezelési szolgáltatások irányából értékelve ki a felmérésben kitöltött kérdőíveket. A felmérésben túlsúllyal szerepeltek a pénzügyi szféra szolgáltatók (60%), de voltak válaszolók IT szektorból, távközlésből, hulladékgazdálkodásból és a közigazgatásból is. Ezek mellett is némileg meglepő, hogy a válaszadók 20%-a egyáltalán nem rendelkezett üzletfolytonosság-menedzsment programmal és csak egyharmaduknál létezett, mint kiforrott rendszer. Arra a kérdésre, hogy az IT-költségvetés hány százalékát költik a katasztrófa utáni helyreállítási képességekre a válaszadók a pénzügyi szolgáltatók közül 4-10%-os, az egyéb szektorok szereplői kevesebb, mint 1%-os értéket jelöltek meg. A pénzügyi szolgáltatóknál arra is volt adat, hogy a folytonossági tervet 11%-uknál kellett már kibertámadás miatt alkalmazni, de a leggyakoribb okok a telekommunikációs kiesések, a hardver/szoftver problémák és az áramszünet voltak. Érdekes lenne ezeket az adatokat szélesebb válaszadó rétegen, és különösen a pandémia 4. hulláma környékén, a ransomware-támadások mindennapossá válása tükrében 2021-re is megkutatni.

Fentiek alapján is könnyen belátható, hogy a meglehetősen széles üzleti kulturális horizonton elhelyezkedő közszolgáltatók (a multinacionális nagyvállalati módszerekkel működő regionális energetikai cégektől az alig száz fős önkormányzati tulajdonú távhőszolgáltatókig) gazdasági teljesítőképességüktől, fejlesztési kapacitásaiktól, a tulajdonosi elvárásoktól és a menedzsment szofisztikáltságától, valamint alapvetően az üzemeltetendő infrastruktúra által megkövetelt szinttől függően vezetnek be intézkedéseket ellenállóképességük növelésére, és igazítják ehhez informatikai rendszereiket is.

[18] https://mkik.hu/hirek/uzleti-tulelocsomag-friss-20200513 (letöltve: 2021.10.31.)
[19] https://home.kpmg/hu/hu/home/tanulmanyok/2018/11/bcm-korkep-2018.html (letöltve: 2021.10.31.)

Az is egyértelmű, hogy az IT csak az egyik aspektus a sok reziliencia-összetevő közül, a menedzsmentnek biztosítania kell az adott társaság fő profilja érdekében a működés technikai és infrastrukturális, adminisztratív, és HR-oldalát is a rendelkezésre álló pénzügyi források, támogatási és pályázati lehetőségek segítségével. A teljesség igénye nélkül:

- beszerzési források és beszállítók oldaláról – minden körülmények között a tevékenységhez szükséges alapenergiahordozók, anyagok beszerzése biztosított kell legyen, rendelkezni kell a saját erőforrásokat meghaladó karbantartási/helyreállítási feladatokhoz külső vállalkozókkal. A hosszú távú, így elkötelezettséget jelentő szerződések mellett késznek kell lenni az esetleg szükségessé váló diverzifikációra;
- infrastruktúra oldaláról – megbízhatóan működő, jó műszaki állapotú hálózatok, ritka üzemzavarokkal, jó és gyors elhárítási mechanizmusokkal, rendszeres és folyamatos karbantartások és fejlesztések, ezekhez megfelelő források biztosítása tulajdonosi/állami oldalról;
- környezeti hatások és különösen klímaváltozás hatásai – rendkívüli üzemzavar elhárító tevékenység, de ide értendő a hálózati tervezési tűréshatárok feletti stresszhatások kezelése is, fogyasztási csúcsok kezelése, katasztrofális szolgáltatáskiesések gyors felszámolása;
- üzemeltető személyzet és szakemberek oldaláról – gyakran problémát jelent már a megfelelő szakember és mérnök utánpótlás, emiatt is terjednek az egyre kevesebb manuális beavatkozást igénylő távfelügyeleti informatikai megoldások, amelyek bevezetésével adott esetben egy szakmai sebezhetőséget informatikai sebezhetőségre cserélnek;
- adminisztratív és szabályozási oldalról – vállalati szinten az üzletmenet-folytonosságot biztosító, racionális és forrásokkal megtámogatott terveket[20] jelenti elsősorban, hatósági szinten a Magyar Energia- és Közműszabályozási Hivatal, a katasztrófavédelem, és a kiberbiztonsági hatóságok támogató munkáját, szabályozási szinten pedig a szaktárcák és a törvényalkotás jövőbemutató tevékenységét;
- IT oldalról – az egyes közműszolgáltatók fő tevékenységét kiszolgáló IT eszköz- és szoftvereszköz állománya is meglehetősen sokszínű, nem ritkák az egyedi fejlesztések, bizonyos esetekben már elavult, gyártói támogatással már nem rendelkező háttérrel működtetve. Mindezek mellé társulnak az utóbbi időben szinte mindenhol valamilyen formában bevezetett vállalatirányítási rendszerek, munkaerő-nyilvántartó rendszerek, ügyfélnyilvántartó-rendszerek, amelyek gyakran egyedi fejlesztések (ebben az értelemben a szállító irányában függést jelentenek), külső erőforrásokon (privát-felhőben, bérelt szerveren) üzemeltetettek, miközben rengeteg személyes adatot tartalmaznak és a cég alapfolyamataihoz (könyvvitel, számlázás, bérszámfejtés) elengedhetetlenek.
- tulajdonosi háttér oldaláról – a közműszolgáltatások ebből a szempontból sem homogének, míg a víz- és távhőszolgáltatások jelentős – de nem teljes köre – önkormányzati érdekkörben van, a földgázszolgáltatás és a villamos áram jellemzően nagyvállalati vagy multinacionális hátterű, de szektoron belül is hatalmas különbségek lehetnek pl. a budapesti Főtáv és egy vidéki kisváros távhőszolgáltatója közt. Ez azt is eredményezheti, hogy két vállalat menedzsmentje egy szektoron belül sem ugyanazon

[20] Lásd az üzemeltetői biztonsági terv részletes szabályait: a létfontosságú rendszerek és létesítmények azonosításáról és védelméről szóló 2012. évi CLXVI. törvény 6. §, és a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet 7. §

elvárások mentén végzi tevékenységét, lehetnek a működésből fakadó kihívásaik közel azonosak, mégis egyéb determinációk miatt juthatnak teljesen diverz eredményekre, nem minden helyzetben csak a szakmaiság szempontjait szem előtt tartva.

Ahhoz, hogy a közműszolgáltatások rezilienciája és ehhez kapcsolódva a kiberbiztonság területén bárhol érdemi előrelépések történjenek, az elsősorban biztonsági és energetikai vagy más közműszektorális kérdésekkel foglalkozó szakembereknek együtt kell működnie a fejlesztéspolitika képviselőivel, legyen szó városfejlesztési, urbanisztikai szintről vagy nemzeti, akár regionális szinteket is érintő támogatáspolitikai, forrásallokációs döntéseket előkészítő kollégákról. A kooperációnak pedig ki kell terjednie a tervezett fejlesztések és forrásaik előteremtése mellett az egyes szolgáltatások közötti kölcsönhatásokra, az ellátási láncokra és diverzifikálásukra, a szükséges szaktudás folyamatos biztosítására és nyilvánvalóan az üzemfolytonossági és biztonsági jellegű kérdésekre, megvizsgálva adott esetben a kölcsönös támogatásnyújtás lehetőségeit is. Ez a komplex megközelítés nagyon jól látható a témát általában multidiszciplináris megközelítéssel feldolgozó nemzeti[21] és nemzetközi szakirodalomból[22], de szerencsére mára már a nemzeti, NATO és EU stratégiai dokumentumokból, keretszabályozásokból is, ezek lényegi elemeivel folytatjuk.

3. Magyar nemzeti stratégiai keretek

A hatályos magyar részletszabályozás feldolgozása jócskán túlterjedne e cikk keretein[23], viszont a kritikus infrastruktúrákra (így a közműszolgáltatásokra) és a kiberbiztonságra vonatkozó nemzeti stratégiai keretek áttekintése mindenképpen hasznos. Elsősorban azért, mert ezek közül néhány a jelenleg hatályos szabályozási keretek[24] hatályba lépése után, viszont az új uniós stratégiák és témánkat érintő irányelvtervezetek várható elfogadása előtt készültek, ezért fontos, hova helyezik a hangsúlyaikat, esetleg később hol igényelhetnek majd korrekciót a közösségi törekvések, fejlesztéspolitikai célkitűzések ismeretében.

- Magyarország Nemzeti Biztonsági Stratégiája[25]

A biztonság- és védelempolitika szempontjából vezérdokumentumnak számító Nemzeti Biztonsági Stratégiát (a továbbiakban: NBS) 2020. áprilisában fogadta el a Kormány. 8. pontja központi érdekként az ország szuverenitásának megőrzését jelöli meg, a gazdasági, társadalmi (kritikus infrastruktúra) mellett az információs és a kibertérbeli biztonságot is kiemelt

[21] Pl. SeConSys: Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve, https://www.seconsys.eu

[22] Pl. Gian Paolo Cimellaro: Urban Resilience for Emergency Response and Recovery - Fundamental Concepts and Applications, 2016, Springer, DOI 10.1007/978-3-319-30656-8; Alexander Fekete, Frank Friedrich ed.: Urban Disaster Resilience and Security - Adressing Risks in Societies, 2018, Springer, https://doi.org/10.1007/978-3-319-68606-6 ;
Thomas A. Johnson ed.: Cybersecurity - Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, 2015, CRC Press; Jon Coaffee: Terrorism, Risk and the Global City - Towards Urban Resilience, 2009, Ashgate

[23] Szerencsére erre nincs is szükség, lásd: Bognár Balázs, Bonnyai Tünde (szerk.): Kritikus infrastruktúrák védelme I., Dialóg Campus Kiadó, Budapest 2019.

[24] Elsősorban itt központinak a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, és az állami és önkormányzati szervek elektronikus információbiztonságáról 2013. évi L. törvény tekintendő, melyek a jelenleg hatályos EU-s irányelvek által adott keretek szerint készültek.

[25] 1163/2020. (IV. 21.) Korm. határozat, Magyarország Nemzeti Biztonsági Stratégiájáról

értékként kezeli. Irányadónak nevezi nemzeti érdekeink mellett a NATO és az EU stratégiai dokumentumaiban foglaltakat.

Célként jelöli ki a hibrid fenyegetésekre hivatkozva az információs és kiberhadviselés elleni védekezés rendszerének fejlesztését és nemzetközi jogi értelemben is fontos deklarációt tesz, amikor kimondja, hogy Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges, valamint, hogy a kiberműveletek sokszor nehezen bizonyítható attribúciójára, az elkövető azonosítására, megnevezésére való tekintettel a válaszlépések különösen körültekintő, eseti elbírálást igényelnek az érintett kormányzati szervezek bevonásával.

Közműszolgáltatások szempontjából fontos, hogy a földgáz-ellátás vonatkozásában ellátási kockázatként jelöli meg az importfüggőséget (így implicite kritikus fontosságot tulajdoníthatunk a szállító-infrastruktúrának is), számol az energiapiacon a villamos áram erősödő térnyerésével (ismét ideérthető ezzel az áramhálózat jelentőségének növekedése), illetve a földrajzi elhelyezkedésünkből fakadó kitettségünkre is felhívja a figyelmet az ivóvízkészletek vonatkozásában.

A biztonsági környezet elemzésénél külön is kitér a források és szállítókapacitások korlátozott számából fakadó kockázatokra, és diverzifikáció szükségességére, ami egyúttal az ország ellenállóképességének növeléséhez is hozzájárul. A hazai vízbázis védelme stratégiai fontosságú, nagy jelentősége van a jelentős folyóink vízgyűjtő területén fekvő országokkal történő szoros vízbiztonsági együttműködésnek.

A kiemelt biztonsági kockázatok közt azonosítja a jelentős károkat okozó kibertámadásokat a kormányzati informatikai rendszerek, az E-közigazgatás, a közműszolgáltatók, a stratégiai vállalatok, a létfontosságú infrastruktúra egyéb elemei és más, a társadalom működésében fontos szervezetek számítógépes hálózatai ellen, és a közműszolgáltatások vonatkozásában jelentős, az energiaimportból fakadó ellátási válsághelyzetek, jelentős ipari baleseteket és katasztrófákat, nagyobb természeti katasztrófákat (ár-, belvíz, aszály, tüzek) és a globális felmelegedés káros hatásait is.

A feladatok meghatározásánál külön hangsúlyt kap a kiberképességek összkormányzati fejlesztése, a kiberbiztonság megfelelő szintjének garantálása, és megjelenik a katonai kiberképességek fejlesztése is. Feladat a K+F tevékenységek, az állam és a magánszektor közötti és nemzetközi partnerségek építése is, mi több a mesterséges intelligencia[26] szerepének várható erősödése is említésre kerül.

A környezeti biztonság megteremtésében az alapvető életfeltételek, így az ivóvíz védelme, a környezetvédelem és klímacélok is megjelennek. A 173. pont pedig egyértelműen fogalmaz a kritikus infrastruktúrák vonatkozásában:

„Hazánk kiemelten kezeli az ország mindennapi életkörülményeinek fenntartásához, a gazdaság és az államszervezet működéséhez szükséges létfontosságú infrastruktúra hatékony védelmét. Biztosítani kell, hogy ezen infrastruktúra működésének esetleges megzavarása vagy manipulálása megelőzhető, kivédhető, illetve a lehetséges mértékben rövid, kivételes és kezelhető legyen."

[26] 1573/2020. (IX. 9.) Korm. határozat, Magyarország Mesterséges Intelligencia Stratégiájáról, valamint a végrehajtásához szükséges egyes intézkedésekről
https://ai-hungary.com/api/v1/companies/15/files/137203/view (letöltve: 2021.10.30.)

Képességépítés szempontjából kiemeli a katasztrófavédelmet, illetve a tömegpusztító fegyverek, a terrorizmus, a kibertámadások, a hibrid műveletek és a katasztrófák elleni védelmet hazánk nemzeti ellenálló képességének fokozása érdekében.

- Magyarország Nemzeti Katonai Stratégiája[27]

A Nemzeti Katonai Stratégia (a továbbiakban: NKS) a legfrissebb a témához kapcsolódó dokumentumok közül, idén júniusban fogadta el a Kormány az erre vonatkozó előterjesztést, ennek megfelelően a helyzetértékelése is a leginkább aktuális fenyegetettségi helyzetnek megfelelő, hangsúlyozza a reziliencia jelentőségét és az NBS-ben már hangsúlyosan megjelenő katonai kibervédelem is még inkább részletezett módon, konkretizált feladatokat kap.

Az NKS a kockázatokat nem titkolva leszögezi, hogy egy potenciális európai hadszíntéren vívott háború során szerepet kaphatnak, illetve célponttá is válhatnak Magyarország kommunikációs és közlekedési infrastruktúrái, valamint más létfontosságú rendszerelemei, emiatt az ország teljes területe, légtere és kibertere katonai műveletek színtere lehet.

Tisztázza, hogy *a modern konfliktusoknak a legtöbb esetben kiberbiztonsági összetevője is van, amelyek irányulhatnak akár a kormányzati informatikai rendszerek, az e-közigazgatás, a közműszolgáltatók, a stratégiai jelentőségű vállalatok, a közlekedési ágazat és más, a gazdaság működése szempontjából fontos ágazat létfontosságú rendszerelemeinek, a társadalom működéséhez nélkülözhetetlen szervezetek digitális hálózatainak megzavarására***,** illetve az azokon tárolt adatok és információk manipulálására, megszerzésére vagy hozzáférhetetlenné tételére.

Az NKS 4.3. pontja a Nemzeti Ellenállóképesség (Reziliencia) címet kapta és jelenleg a fogalom kormányzati szabályozási szinten legrészletesebb meghatározását adja meg:

„A komplex, nehezen kiszámítható biztonsági környezetben fel kell készülni a hazánkat, illetve a magyar állampolgárokat veszélyeztető kinetikus és nem-kinetikus támadásokra, hibrid fenyegetésekre, valamint más válsághelyzetekre. Ennek érdekében tovább kell fejleszteni a csapásokat elviselő, azok hatásait elhárítani, enyhíteni és felszámolni, a kritikus fontosságú képességek működését fenntartani képes nemzeti ellenállóképességet. A magyar nemzetgazdaság teljesítményének és ezzel együtt a nemzeti védelmi ipari kapacitásoknak a fokozása jelentős mértékben hozzájárul a biztonság és a nemzeti ellenállóképesség erősítéséhez.

A magas szintű nemzeti ellenállóképesség kialakítása csökkenti a potenciális támadás kockázatát, hozzájárulva ezzel az elrettentési képességekhez. Emellett erősíti az országvédelmi képességet, valamint javítható általa a társadalom azon képessége is, hogy a katonai, rendvédelmi és civil tevékenységek kombinált alkalmazásával el tudja hárítani a veszélyeket, fenyegetéseket és támadásokat, kezelni tudja azok következményeit és gyorsan helyre tudja állítani működőképességét. A Magyar Honvédségnek ezért képesnek kell lennie a hagyományos és a hibrid fenyegetések elleni fellépésre, a nemzeti ellenállóképesség katonai képességekkel történő növelésére, a honvédelmi ágazathoz tartozó létfontosságú rendszerelemek és egyes, a honvédelem szempontjából fokozott védelmet igénylő létesítmények őrzésére és védelmére, valamint a civil és rendvédelmi szervek feladatellátásának támogatására, a velük történő együttműködésre."

[27] 1393/2021. (VI. 24.) Korm. határozat, Magyarország Nemzeti Katonai Stratégiájáról

- Magyarország Nemzeti Kiberbiztonsági Stratégiája[28]

A Nemzeti Kiberbiztonsági Stratégiát (a továbbiakban: NKibS) elfogadó Kormányhatározat jelentőségét úttörő jellegén kívül az is alátámasztja, hogy ennek alapján jött létre a Nemzeti Kiberbiztonsági Koordinációs Tanács[29] is. A testület feladata a NKibS által meghatározott cselekvési területeken a kormányzati tevékenység koordinációjának elősegítése és a végrehajtás figyelemmel kísérése, és ezen keresztül az NKibS rendszeres felülvizsgálatához kapcsolódó háttérmunka elvégzése, ami a 2013-as hatályba lépésre és az EU-s keretszabályozások változására tekintettel aktuálisnak is tekinthető.

A stratégia magát a nemzeti vagyon részét képező nemzeti adatvagyon, valamint a kapcsolódó létfontosságú rendszerek és létesítmények kiberbiztonságának alapdokumentumaként határozza meg. Megvalósítandó célként rögzíti, hogy az ország nemzeti adatvagyona megfelelő szintű védelemben részesüljön, létfontosságú rendszereinek és létesítményeinek kibertérhez kapcsolódó működése üzembiztos legyen, valamint rendelkezésre álljon kompromittálódás esetén a megfelelően gyors, hatékony és a veszteséget minimalizáló, különleges jogrend idején is alkalmazható helyreállítási képesség.

A célok eléréséhez szükséges feladatok közt kitér a gazdasági szereplők motivációjára, ami alapján leszögezi, hogy az informatikai és hírközlési közbeszerzések kiberbiztonsági követelményeinek meghatározása során Magyarország abban érdekelt, hogy azok a lehető legmagasabb szintű kiberbiztonsági védelem kialakítására ösztönözzék a közbeszerzéseken résztvevő informatikai és hírközlési eszközgyártókat és szolgáltatókat, kiemelt hangsúlyt fektetve a nemzetközi biztonsági tanúsítási szabványoknak való megfelelésre. Magyarország törekszik egyben arra, hogy a gazdasági élet szereplőivel közösen dolgozzon ki olyan ösztönző intézkedéseket a gazdaság szereplői számára, amelyek a kiberbiztonság fokozását célozzák.

- Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiája[30]

2018. év végén fogadta el a Kormány a hálózati és információs rendszerek biztonságára vonatkozó stratégiát, ami a tanulmány szempontjából a leginkább specifikus „programdokumentum". A stratégia szerint fontos veszélyforrást jelentenek a rendkívül szofisztikált támadások, amelynek keretében a támadók hosszú időn át elrejtve tudják végezni a károkozó tevékenységüket. Hangsúlyozza, hogy *a hálózati és információs rendszerek, mint kritikus információs infrastruktúrák elleni támadások egyre gyakoribbá, komplexebbé és kifinomultabbá válnak, jellemző rájuk a társadalom működésének fenntartásához szükséges alapfunkciók akadályozása, és hogy a társadalom belső kohézióját próbálják gyengíteni.*

Az alapvető szolgáltatások, valamint a létfontosságú infrastruktúrák és szolgáltatásaik védelme vonatkozásában leírja, hogy *az egyes létfontosságú infrastruktúrák védelme komplex feladat, amelynek végrehajtásában a különböző állami szerveken túlmenően a gazdasági élet szereplőinek is részt kell vállalniuk.*

[28] 1139/2013. (III. 21.) Korm. határozat, Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

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

[30] 1838/2018. (XII. 28.) Korm. határozat, Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiája

A kijelölt létfontosságú rendszerek és létesítmények üzemeltetőinek nagyobb hangsúlyt kell fektetniük rendszereik kockázatokkal arányos, teljes körű védelmének megteremtésére. A kockázatok azonosítását lehetővé tevő, mérőszámokat tartalmazó kockázatértékelési módszertant kell kialakítaniuk, és azonosítaniuk kell azokat az intézkedéseket, amelyekkel a fenyegetésekre való felkészülés kellő időben megkezdhető, a kiváltott hatásuk mielőbb minimalizálható.

A stratégiában megfogalmazott legfontosabb intézkedések:

- ágazati szintű kockázatértékelés, kockázat-elemzési módszertan kidolgozása

- ágazatközi, illetve ágazat-specifikus konszenzust képviselő ajánlások és jó gyakorlatok elérhetővé tétele a biztonsági célok elérésére vonatkozóan

- az állami intézmények és a magánszektor szereplőinek kölcsönös bizalmon alapuló együttműködése

- a kritikus infrastruktúrák üzemeltetői részére, a védelmet kiegészíteni képes egységes szolgáltatáscsomag rendelkezésre állása

- célzott pályázati lehetőségek biztosítása szükséges az üzemeltetők, a szolgáltatást nyújtók, az érintett hatóságok és az eseménykezelő központok működésének fejlesztésére a létfontosságú rendszerek, létesítmények és szolgáltatások fizikai és kiberbiztonsága területén a hatékony megelőzés és gyors reagáló képesség fejlesztésére

- információbiztonsági tudatosítási tevékenység fokozása

- létfontosságú infrastruktúrák üzemeltetőinek bevonása a nemzeti és nemzetközi védelmi gyakorlatokba

4. NATO

Bár már a 2014-es wales-i csúcson komoly hangsúlyt kapott a szövetségi kibervédelem, az egyik legfontosabb szövetségi alapdokumentum a kibervédelem tárgyában jelenleg a 2016. július 8-án kiadott Cyber Defence Pledge[31]. Ebben az állam- és kormányfők célként tűzték ki, hogy lépést tartanak az erősödő kibertéri fenyegetésekkel. Megerősítették a nemzeti felelősségvállalásaikat, összhangban a washingtoni szerződés 3. cikkelyével, amely egyébként rögzíti a tagállami reziliencia elvét is, illetve a kifejezték szándékukat erős partnerségek építésére (pl. az EU-val), valamint támogatták a vonatkozó nemzetközi jogi intézmények és normák tiszteletben tartását, alkalmazását a kibertérben is. Konkrét kötelezettségvállalásként rögzítették:

- a nemzeti infrastruktúra és képességek fejlesztését,

- az ehhez szükséges nemzeti források biztosítását,

- a felelős nemzeti kibervédelmi szereplők közti kooperáció erősítését,

- a kiberfenyegetések vizsgálatának elmélyítését, a szerzett információk és értékelések megosztását,

[31] Cyber Defence Pledge, Press Release (2016) 124 Issued on 08 Jul. 2016 https://www.nato.int/cps/en/natohq/official_texts_133177.htm

- nemzeti szinten minden szereplő körében a készségek és a tudatosság szintjének emelését az alapvető kiberhigiénétől a szofisztikált és robusztus kibervédelmi rendszerekig,

- az oktatás támogatását kiberkészségek terén, az erők képzését és gyakorlatoztatását, az oktatási intézmények megerősítését, a bizalom- és a tudás építését szövetségi szinten,

- a meghatározott kibervédelmi vállalások végrehajtását, különösen azon nemzeti rendszerek esetében, amelyekre a NATO is támaszkodik.

Végül rögzítették, hogy a kötelezettségvállalások megvalósulásának ellenőrzését évente végrehajtják[32].

Nagyrészt a COVID-pandémia alatt elharapózó kibertéri támadások, zsarolóvírusok kártételei miatt került kiadásra 2020. június 3-án egy Észak-atlanti Tanács által jegyzett nyilatkozat[33], amely megerősítette a Cyber Defence Pledge vállalásait, és leszögezte, hogy a tagállamok elszántak a kritikus infrastruktúráik védelmében, az ellenállóképességük építésében. A 2018-as brüsszeli csúcsra visszautalva a kibertér védelmét a NATO egyik kulcsfeladatának nevezte, megerősítve a szövetség védelmi mandátumát a teljes képesség-készlet alkalmazására kibertéri támadások esetében is, és ismét felhívta a figyelmet a nemzetközi jog hatályára és tiszteletben tartására a kibertérben.

2021. márciusában publikálták a NATO főtitkár 2020-as évre vonatkozó éves jelentését[34], amely természetesen mind a kibervédelem, mind a reziliencia témájával részletesen foglalkozott. Ebben ismét szerepel, hogy a szövetség többször kifejezte az 5. cikkely felhívhatóságát súlyos kibertámadás esetén, és ezirányú felkészültségét a 2020-ban kiadott NATO kiberdoktrínával[35] is alátámasztja, ami a szövetségi kiberműveletek alapvető szabályait rögzíti. Az információk megosztásának javítására több fórumot is kialakítottak a tagállamok közt (NATO Intelligence on Cyberspace Community of Interest, NATO Communications and Information Agency - Cyber Collaboration Network) és a magánszektor felé is (NATO Industry Cyber Partnership).

A reziliens szövetségesek és tagállamok kulcsfontosságúak a NATO kollektív biztonsága szempontjából, mivel ezek ellenállóképessége az első védelmi vonal. A 3. cikkely szerint ez minden tagállam részéről kötelezettségvállalás is egymás és a szövetség irányába. Mindennek fontosságára komoly figyelmeztetést adott a COVID-járvány, ahol a katonai képességek is jelentős szerepet kaptak. A 2016-os varsói csúcson meghatározott alapvető ellenállóképességi követelmények változatlanok:

- a kormányzás és a kritikus kormányzati szolgáltatások folytonossága

- reziliens energiaellátás

- reziliens víz- és élelmiszerforrások

- ellenálló polgári kommunikációs rendszerek

- ellenálló közlekedési rendszerek

[32] Legutóbb lásd a 2021-es konferencia Észtországban: https://kaitseministeerium.ee/en/CyberPledge2021

[33] Statement by the North Atlantic Council concerning malicious cyber activities (2020), Press Release (2020) 049 Issued on 03 Jun. 2020: https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en

[34] The Secretary General's Annual Report 2020, 16 March 2021, https://www.nato.int/cps/en/natohq/opinions_182236.htm

[35] AJP-3.20 ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS, Edition A Version 1 JANUARY 2020

- képesség nagyobb embertömegek mozgásának ellenőrzésére

- képesség a tömeges sérülések/megbetegedések kezelésére

A rezilienciáról 2021 júniusában kiadásra került egy a varsói csúcson elfogadottakat megerősítő közös elköteleződést tartalmazó újabb nyilatkozat[36]. A nemzeti felelősség elvét fenntartva megegyeztek a nemzeti reziliencia-törekvések koordinációjában és folyamatos nyomon követésében. Hangsúlyt kap az ellátási láncok diverzifikálása, a kritikus infrastruktúrának ellenállóképességének biztosítása – ideértve a káros gazdasági befolyásokat is. Szerephez jutnak ebben az új technológiák, a biztonságos kommunikációs megoldások és szellemi alkotások védelme. Növelni kívánják az energiaellátás biztonságát, és a klímaváltozás által okozott természeti kihívásainak kezelésére tett erőfeszítéseket. A reziliencia növelését szolgálja a robusztus, rugalmas és interoperábilis katonai képességek fejlesztése is. Mindezt a szövetségi döntéshozatal gyorsabbá tételével kívánják alátámasztani.

5. A területet meghatározó új EU dokumentumok

A kiberbiztonság és a reziliencia uniós szabályozásának területén szintén látványos a technológia exponenciális fejlődése által kiváltott „amortizáció". A hatályos stratégiai és jogi keretek az aktuális, és várható kihívások és fenyegetések tükrében nem lesznek elegendőek, ezért az EU szervek – jelentős részben a COVID-pandémia tapasztalatai alapján is – úgy döntöttek, hogy új, szélesebb körű és mélyebb együttműködésekre építő regulációs környezetet alkot. A közelmúlt fontosabb stratégiai dokumentumai[37] mellett két kiemelten fontos irányelvtervezetet, és a teljes kép biztosítása érdekében egy fejlesztéspolitikai eszközt is szeretnék röviden érinteni.

5.1. Jelentős új EU-stratégiák

A biztonsági unióra vonatkozó uniós stratégiát[38] 2020 júliusában bocsátotta ki a Bizottság, és a 2020-2025 közötti időszakra vonatkozik. Elsődleges célja az időtálló biztonsági környezet biztosításához szükséges képességek és kapacitások kiépítése. A stratégia a következő közös célkitűzésekre épül:

- A válságok korai felismeréséhez, megelőzéséhez és gyors kezeléséhez szükséges képességek és kapacitások kiépítése
- Eredményközpontúság
- Az állami és a magánszektor valamennyi szereplőjének bevonása a közös erőfeszítésbe

Négy, egymástól kölcsönösen függő uniós szintű stratégiai prioritást határoz meg: időtálló biztonsági környezet, a változó fenyegetések kezelése, az európaiak védelme a terrorizmussal és a szervezett bűnözéssel szemben, valamint erős európai biztonsági ökoszisztéma.

[36] Strengthened Resilience Commitment, 15 Jun. 2021, https://www.nato.int/cps/en/natohq/official_texts_185340.htm

[37] Mivel a témához nem közvetlenül kapcsolódik, ezért csak említjük: A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK, Digitális iránytű 2030-ig: a digitális évtized megvalósításának európai módja, Brüsszel, 2021.3.9., COM(2021) 118 final

[38] A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, AZ EURÓPAI TANÁCSNAK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK, A biztonsági unióra vonatkozó uniós stratégia, Brüsszel, 2020.7.24. COM(2020) 605 final

Az EU kiberbiztonsági stratégiája[39] úgy kívánja biztosítani a globális és nyílt internetet, hogy erős biztosítékok álljanak rendelkezésre az európaiak biztonságát, illetve alapvető jogait és szabadságait veszélyeztető kockázatok kezelésére. Három fő (szabályozási, beruházási és szakpolitikai) eszköz alkalmazására tesz javaslatokat az uniós fellépés alábbi három területén: 1. reziliencia, technológiai szuverenitás és vezető szerep, 2. operatív kapacitásépítés a megelőzés, elrettentés és reagálás érdekében, és 3. a globális és nyílt kibertér előmozdítása.

Az első terület jelentős stratégiai kezdeményezései:

- az átdolgozott kiberbiztonsági irányelv elfogadása,
- a biztonságos dolgok internetére vonatkozó szabályozási intézkedések,
- a kiberbiztonsági CCCN beruházások (mindenekelőtt a Digitális Európa program, a Horizont Európa és a helyreállítási eszköz) révén akár 4,5 milliárd EUR összegű állami és magánberuházás 2021–2027 között,
- a mesterséges intelligenciát használó biztonsági műveleti központok uniós hálózata és a kvantumtechnológiákon alapuló ultrabiztonságos kommunikációs infrastruktúra,
- a kiberbiztonsági technológiák széles körű elfogadása a kkv-knak nyújtott támogatás révén a digitális innovációs központok keretében,
- az uniós DNS címfeloldási szolgáltatás kifejlesztése, amely biztonságos és nyílt alternatívát kínál az uniós polgároknak, vállalkozásoknak és közigazgatásoknak az internet-hozzáférésre.

Az operatív kapacitásépítés gyakorlati lépései:

- létre kell hozni az európai kiberbiztonsági válságreagálási keretet, és ki kell dolgozni a közös kiberbiztonsági egység létrehozásának folyamatát a kapcsolódó mérföldkövekkel és határidőkkel,
- folytatni kell a kiberbűnözéssel kapcsolatos menetrend végrehajtását a biztonsági unióra vonatkozó stratégia keretében,
- elő kell mozdítani és segíteni az EU INTCEN-en belül a tagállamok kiberhírszerzési munkacsoportjának létrehozását,
- elő kell mozdítani a kibertevékenységektől való elrettentésre vonatkozó uniós megközelítést[40], hogy megakadályozza és visszaszorítsa a rosszindulatú kibertevékenységeket, elrettentsen tőlük, és reagáljon rájuk,
- felül kell vizsgálni a kibervédelmi szakpolitikai keretet,
- elő kell segíteni „A kibertérre mint műveleti területre vonatkozó katonai jövőkép és stratégia” című uniós dokumentum kidolgozását a KBVP katonai missziói és műveletei vonatkozásában,
- támogatni kell a polgári, védelmi és űripar közötti szinergiákat,
- meg kell erősíteni az űrprogram keretében a kritikus űrinfrastruktúrák kiberbiztonságát.

Végül a globális és nyílt kibertér előmozdítása érdekében:

- meg kell határoznia a nemzetközi szabványosítási folyamatok célkitűzéseit, és elő kell mozdítani őket nemzetközi szinten;

[39] KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK, Az EU kiberbiztonsági stratégiája a digitális évtizedre, Brüsszel, 2020.12.16., JOIN(2020) 18 final

[40] Lásd pl. az EU kiberdiplomáciai eszköztárát: A TANÁCS (EU) 2019/796 RENDELETE (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről

- elő kell mozdítani a kibertérben való nemzetközi biztonságot és stabilitást, mindenekelőtt az EU és a tagállamai által az ENSZ-nél a kibertérben gyakorolt felelős állami magatartás előmozdítására irányuló cselekvési programra vonatkozóan benyújtott javaslat révén;
- gyakorlati iránymutatást kell nyújtani az emberi jogok és az alapvető szabadságok kibertérben való alkalmazásához,
- hatékonyabb védelmet kell biztosítani a gyermekek szexuális zaklatása és kizsákmányolása ellen, illetve gyermekjogi stratégiát kell előterjesztenie,
- meg kell erősíteni és elő kell mozdítani a számítástechnikai bűnözésről szóló budapesti egyezményt, többek között a budapesti egyezmény második kiegészítő jegyzőkönyvével kapcsolatos munka révén,
- ki kell terjeszteni a harmadik országokkal, valamint a regionális és nemzetközi szervezetekkel folytatott uniós kiberbiztonsági párbeszédet, többek között egy informális uniós kiberdiplomáciai hálózat révén,
- meg kell erősíteni a több érdekelt felet tömörítő közösséggel való információcserét, mindenekelőtt a magánszektorral, a tudományos közösséggel és a polgári társadalommal folytatott rendszeres és strukturált információcserével,
- javaslatot kell tenni egy uniós külső kiberkapacitás-építési menetrendre és egy uniós kiberkapacitás-építési testületre.

5.2. Fontos új irányelv-javaslatok

A címben is szereplő témákban irányadó (kritikus infrastruktúrák és kiberbiztonság) alapvető uniós irányelveket váltó új irányelv-tervezetek kerültek kiadásra 2020. decemberében[41].

A kritikus fontosságú szervezetek rezilienciájáról szóló irányelv-javaslat[42] a 2008-asnál szélesebb szkóppal, tíz szektort kíván lefedni: energia, közlekedés, bank, pénzpiaci infrastruktúra, egészségügy, ivóvíz, szennyvíz, digitális infrastruktúra, közigazgatás és űrkutatás. A javaslat fogalom-meghatározása szerint a reziliencia képesség a kritikus fontosságú szervezetek működését megzavaró vagy annak megzavarására alkalmas biztonsági események bekövetkezésének megelőzésére, azokkal szembeni ellenállásra, hatásaik enyhítésére és elnyelésére, azokhoz való alkalmazkodásra, majd a szervezet működésének helyreállítására. A tagállamok a kritikus fontosságú szervezetek rezilienciájának megerősítésére irányuló nemzeti stratégiát fogadnak el, meghatározott elemekkel. A kritikus fontosságú szervezetek azonosítása céljából az illetékes hatóságoknak össze kell állítaniuk az alapvető szolgáltatások jegyzékét, és rendszeresen értékelniük kell minden olyan releváns kockázatot, amely hatással lehet ezen alapvető szolgáltatások nyújtására. A tagállamok gondoskodnak arról, hogy a kockázatértékelés lényeges elemeit elérhetővé tegyék a kritikus fontosságú szervezetek számára, valamint, hogy rendszeresen a Bizottság rendelkezésére bocsássák az azonosított kockázatok típusaira és kockázatértékeléseik eredményeire vonatkozó adatokat.

[41] Fontos szerepe van, de a közműszolgáltatásokhoz közvetlenül nem kapcsolódik a pénzügyi ágazatra vonatkozó tervezett módosításnak is: Brüsszel, 2020.9.24., COM(2020) 595 final, 2020/0266 (COD), Javaslat AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK rendelet, a 648/2012/EU rendelet, a 600/2014/EU rendelet, valamint a 909/2014/EU rendelet módosításáról

[42] Javaslat AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE, a kritikus fontosságú szervezetek rezilienciájáról, Brüsszel, 2020.12.16., COM(2020) 829 final, 2020/0365 (COD)

A kritikus fontosságú szervezetek nemzeti kockázatértékelések és más releváns információforrások alapján rendszeresen értékelik a vonatkozó kockázatokat. Az ilyen szervezeteknek megfelelő és arányos technikai és szervezeti intézkedéseket kell foganatosítaniuk rezilienciájuk biztosítása érdekében, továbbá gondoskodniuk kell arról, hogy egy rezilienciafejlesztési tervben vagy azzal egyenértékű dokumentumban vagy dokumentumokban leírják ezeket az intézkedéseket.

A tagállamok gondoskodnak arról, hogy a kritikus fontosságú szervezetek bejelentsék az illetékes hatóságnak azokat a biztonsági eseményeket, amelyek jelentősen megzavarják a működésüket, vagy alkalmasak lehetnek annak jelentős megzavarására. Az illetékes hatóságok pedig a bejelentő kritikus fontosságú szervezet rendelkezésére bocsátják a megfelelő nyomonkövetési információkat. Az illetékes hatóságok az egyedüli kapcsolattartó ponton keresztül a többi érintett tagállam egyedüli kapcsolattartó pontjait is tájékoztatják abban az esetben, ha a biztonsági esemény határokon átnyúló hatásokat okoz vagy okozhat egy vagy több másik tagállamban.

A kiemelt európai jelentőségű, kritikus fontosságú szervezetek azok, amelyeket kritikus fontosságú szervezetként azonosítottak, és amelyek a tagállamok legalább egyharmadában vagy legalább egyharmada számára nyújtanak alapvető szolgáltatásokat, ehhez a státuszhoz többletkötelezettségek és külön felügyeleti intézkedések kapcsolódnak.

Az eredeti NIS irányelvet 2016-ban fogadták el, a NIS 2.0-nak[43] is nevezett javaslat az eredeti kereteket több ponton tovább kívánja fejleszteni, ezzel növelve az EU teljes területén a kibervédelem színvonalát.

Kritikus kérdés kibertér kapcsán a joghatóság, ebben tisztázó lépést tesz a tervezet. Bizonyos típusú szervezetek (DNS-szolgáltatók, legfelső szintű doménnév-nyilvántartók, felhőszolgáltatók, adatközpont-szolgáltatók és tartalomszolgáltató hálózati szolgáltatók, valamint bizonyos digitális szolgáltatók) annak a tagállamnak a joghatósága alá tartoznak majd, amelyben az üzleti tevékenység fő helye az Unióban van, egyéb esetben továbbra is a szolgáltatás nyújtásának helye az irányadó. Ennek célja annak biztosítása, hogy az említett szervezetek ne szembesüljenek eltérő jogszabályi követelményekkel, mivel különösen nagy mértékben nyújtanak határokon átnyúlóan szolgáltatásokat. Az ENISA-nak[44] kell létrehoznia és vezetnie az utóbbi típusú szervezetek nyilvántartását.

Az irányelv az I. mellékletben felsorolt ágazatokban (energia; szállítás; banki szolgáltatások; pénzügyi piaci infrastruktúrák; egészségügy, ivóvíz; szennyvíz; digitális infrastruktúra; közigazgatás és űrkutatás) működő egyes *alapvető* állami és magánszervezetekre, valamint a II. mellékletben felsorolt ágazatokban (postai és futárszolgálatok; hulladékgazdálkodás; vegyi anyagok gyártása, előállítása és forgalmazása; élelmiszer-előállítás, -feldolgozás és -forgalmazás; gyártás és digitális szolgáltatók) ágazatokban tevékenykedő, egyes *fontos* állami és magánszervezetekre vonatkozik, mikro- és kisvállalkozásokra csak az elektronikus hírközlő hálózatok vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatások szolgáltatói, a megbízható szolgáltatók, a legfelső szintű doménnév-nyilvántartók és közhiteles nyilvántartását vezetők, valamint bizonyos egyéb szervezetek, például egy tagállamban a szolgáltatás egyedüli szolgáltatója esetében.

[43] Javaslat AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE, az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről, Brüsszel, 2020.12.16., COM(2020) 823 final, 2020/0359 (COD)

[44] European Union Agency for Cybersecurity, https://www.enisa.europa.eu/

A tagállamoknak biztosítaniuk kell, hogy az irányelv hatálya alá tartozó szervezetek megfelelő és arányos technikai és szervezési intézkedéseket hozzanak a hálózati és információs rendszerek biztonsága által keltett kiberbiztonsági kockázatok kezelésére. Arról is gondoskodniuk kell, hogy a szervezetek értesítsék az illetékes nemzeti hatóságokat vagy a CSIRT-eket minden olyan kiberbiztonsági eseményről, amely jelentős hatással van az általuk nyújtott szolgáltatás biztosítására.

A tagállamok olyan szabályokat határoznak meg, amelyek lehetővé teszik a szervezetek számára, hogy konkrét kiberbiztonsági információmegosztási megállapodások keretében vegyenek részt a kiberbiztonsággal kapcsolatos információk megosztásában. Ezenkívül a tagállamok lehetővé teszik az irányelv hatályán kívül eső szervezetek számára, hogy önkéntes alapon jelentést tegyenek jelentős eseményekről, kiberfenyegetésekről vagy majdnem bekövetkezett eseményekről.

Az illetékes hatóságok kötelesek felügyelni az irányelv hatálya alá tartozó szervezeteket, különös tekintettel annak biztosítására, hogy megfeleljenek a biztonsági és eseménybejelentési követelményeknek. Az irányelv megkülönbözteti az alapvető szervezetekre vonatkozó előzetes felügyeleti rendszert és a fontos szervezetekre vonatkozó utólagos felügyeleti rendszert, amely utóbbi azt igényli az illetékes hatóságoktól, hogy tegyenek lépéseket, ha bizonyítékokat vagy jelzést kapnak arról, hogy egy fontos szervezet nem felel meg a biztonsági és eseménybejelentési követelményeknek. Bírságolási szabályokat is meghatároz az irányelv.

A tagállamoknak szükség szerint együtt kell működniük és segíteniük kell egymást, ha a szervezetek több tagállamban nyújtanak szolgáltatást, vagy ha a szervezet üzleti tevékenységének fő helye vagy képviselője egy adott tagállamban található, de hálózata és információs rendszerei egy vagy több más tagállamban találhatók.

5.3. A Helyreállítási és Rezilienciaépítési Eszköz

Elsősorban a COVID-járvány által okozott gazdasági recesszió megfordítására, de az Unió politikáit meghatározó fő irányok mentén született meg egy rendkívüli fejlesztési alap[45] 2021 elején.

A Helyreállítási és Rezilienciaépítési Eszköz hat pillérre tagolt: a) zöld átállás; b) digitális transzformáció; c) intelligens, fenntartható és inkluzív növekedés, beleértve a gazdasági kohéziót, a foglalkoztatást, a termelékenységet, a versenyképességet, a kutatást, a fejlesztést és az innovációt, valamint az erős kkv-kat magában foglaló, jól működő belső piacot; d) társadalmi és területi kohézió; e) egészségügy, valamint gazdasági, társadalmi és intézményi reziliencia, többek között a válsághelyzetekre való felkészültség és a válsághelyzetekre való reagálási képesség növelése céljából; és f) a következő generációra, a gyermekekre és a fiatalokra – így például az oktatásra és a készségekre – vonatkozó szakpolitikák.

Az eszköz általános célkitűzései közt a témának szempontjából legfontosabb az Unió gazdasági, társadalmi és területi kohéziójának előmozdítása a tagállamok rezilienciájának, válsághelyzetekre való felkészültségének, alkalmazkodóképességének és növekedési potenciáljának javítása, támogatva a zöld átállást, hozzájárulva a 2030-ra vonatkozó uniós

[45] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2021/241 RENDELETE (2021. február 12.) a Helyreállítási és Rezilienciaépítési Eszköz létrehozásáról

éghajlat-politikai célok eléréséhez, valamint megfelelve a 2050-ig teljesítendő uniós klímasemlegességi célkitűzésnek és a digitális átállási célkitűzésnek, továbbá hozzájárulva az Unió stratégiai autonómiájához egy nyitott gazdaság mentén, és európai hozzáadott értéket teremtve. Az említett általános célkitűzés megvalósítása érdekében az eszköz egyedi célkitűzése az, hogy pénzügyi támogatást nyújtson a tagállamoknak a helyreállítási és rezilienciaépítési tervükben a reformokra és beruházásokra vonatkozóan meghatározott mérföldkövek és célok megvalósítása céljából. Ezen egyedi célkitűzést az érintett tagállamokkal szoros és átlátható együttműködésben kell megvalósítani.

Magyarország Helyreállítási és Ellenállóképességi Terve[46] 2021. május 21-én került benyújtásra. Célja a koronavírus járvány gazdasági és társadalmi hatásainak ellensúlyozása, illetve a gazdaság ellenálló-képességének, fenntarthatóságának és a zöld és a digitális átmenettel kapcsolatos kihívásokra és lehetőségekre való felkészültségének a növelése. A terv több ponton tartalmaz olyan fejlesztési programokat, forrásokat, amelyek – különösen az új EU-s irányelv javaslatok fényében – jelentős vagy fontos infrastruktúrákhoz, valamint informatikai és IT témákhoz kapcsolódnak, ezért remélhetőleg a terv elfogadása és végrehajtása esetén pozitív változást hoznak a nemzeti ellenállóképesség és kiberbiztonság területén.

6. Összegzés

A tanulmányban egy meglehetősen széles területről szerettem volna egy átfogó képet adni a szabályozott területtől a nemzeti stratégiák megközelítésén át a NATO, majd az EU fontos dokumentumainak áttekintésével. Nagyon fontos, hogy az egyébként is egyre inkább jelentőséggel bíró hálózatosság ezeken a területeken és a szabályozásukban is tetten érhető, ezért a lényeges egymásra hatások és függőségek ismerete nélkül esélye sem lehet egy tartós és jövőbemutató megközelítésnek. Különös figyelmet érdemelnek az EU elfogadás előtt álló irányelv-tervezetei, amelyek a következő évtizedre várhatóan meghatározzák majd úgy a reziliencia, mint a kiberbiztonság közösségi szabályozását, és új emelt szintű standardeket adva remélhetőleg egy magasabb biztonsági szintet, emelt biztonsági tudatosságot eredményeznek.

Érzékelhető tendencia, hogy az irányelvi javaslatokban megjelenő új elemek, azaz a reziliencia témájában a kockázatértékelés, a rezilienciafejlesztési terv, valamint a kiberbiztonsági tervezetben is jelentős emelt szintű hatósági nyomonkövetés, információcsere és együttműködés mind azt szolgálják, hogy a magasabb színvonalú biztonság érdekében tett intézkedések visszamérhetően, ténylegesen előrelépést hozva meg is valósítsák a kitűzött célokat. Elfogadásuk esetén ezt a hazai stratégiai és szabályozási környezeten is át kell majd vezetni, és nemzeti sajátosságainkhoz kell igazítani. Az esetleg hiányzó technikai-műszaki képességek mellett a szabályozásban, hatósági tevékenységben és oktatás-képzésben is minőségi ugrást jelentő változások megvalósításához újító szemléletre és multidiszciplinárisan gondolkodni és együttműködni tudó szakemberekre és együttműködést biztosító fórumokra lesz szükség.

A Helyreállítási és Rezilienciaépítési Eszközre azért tartottam érdemesnek kitérni, mivel mind a létfontosságú rendszerelemek berendezéseire és alapfunkcióit biztosító eszközeire, mind a szervezeti szintű kiberbiztonságra igaz, hogy komoly pénzügyi források nélkül a korszerűsítésük nem megoldható. Aktív fejlesztési- és támogatáspolitikai lépések szükségesek

[46] https://www.palyazat.gov.hu/helyreallitasi-es-ellenallokepessegi-eszkoz-rrf

ahhoz, hogy az érintett szervezetek lehetőséget kapjanak a szükséges technológiaváltások végrehajtására.

Fontos caveatként végül azért el kell mondani azt is, hogy a sokáig halogatott, elavult eszközöket lecserélő üzemeltetési célú fejlesztések önmagukban még nem feltétlenül a reziliencia érdekében tett lépések. A rendes – akár gazdaságosabb – üzemmenet nem tekinthető emelt szintű ellenállóképességnek, még akkor sem, ha egy korábbi alacsonyabb műszaki színvonalat egy magasabb szinten automatizált és takarékos új műszaki tartalom halad meg. Kell, hogy legyen hozzáadott érték biztonsági szempontból is – különösen a fejlett informatikai megoldásokkal vezérelt következő generációs berendezéseknél –, amelyet remélhetőleg az irányelv-tervezetben megjelenő új kockázatértékelési rendszer kimutathatóvá és kikényszeríthetővé is tesz majd. Nem érdemes bujtatott fejlesztéspolitikai beruházásokkal magasabb biztonsági színvonalról beszélni. Ugyanúgy ahogy a zöld beruházások kapcsán problémát okozhat a „greenwashing”[47], ellenőrizni kell, hogy ne épülhessenek illúziók reziliencia és a kiberbiztonság vonatkozásában sem.

[47] Azaz környezetbarát, vagy fenntartható beruházásként feltüntetni valamit, ami nem az. A pénzügy szolgáltatók vonatkozásában már tett ellenlépéseket az EU: AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/2088 RENDELETE (2019. november 27.) a pénzügyi szolgáltatási ágazatban a fenntarthatósággal kapcsolatos közzétételekről

Irodalom- és jogforrás jegyzék

BOGNÁR Balázs, BONNYAI Tünde (szerk.): Kritikus infrastruktúrák védelme I., Dialóg Campus Kiadó, Budapest 2019.

CIMELLARO, Gian Paolo: Urban Resilience for Emergency Response and Recovery - Fundamental Concepts and Applications, 2016, Springer

FARKAS Ádám (szerk.): Az állam katonai védelme az új típusú biztonsági kihívások tükrében, 2018, NKE Budapest,

FARKAS Ádám: Komplex biztonság, hibrid konfliktusok, összetett válaszok, Honvédségi Szemle 2020/4. 11-23. o.;

FARKAS Ádám: A totalitás kora? Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.,

FARKAS Ádám: Az állam fegyveres védelmének alapvonalai. Budapest, Katonai Nemzetbiztonsági Szolgálat, 2020.

FARKAS Ádám: Gondolatok a védelmi és biztonsági szabályozást és kormányzást meghatározó egyes eurázsiai trendekről. In: Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/10.

FARKAS Ádám, Kelemen Roland (szerk.): Szkülla és Kharübdisz között - Tanulmányok a különleges jogrend elméleti és pragmatikus kérdéseiről, valamint nemzetközi megoldásairól, 2020, Magyar Katonai Jogi és Hadijogi Társaság;

FEKETE, Alexander, FRIEDRICH Frank ed.: Urban Disaster Resilience and Security - Adressing Risks in Societies, 2018, Springer, https://doi.org/10.1007/978-3-319-68606-6

HÓDOS László: A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai, Honvédségi Szemle 148. Évf. 4(2020),

JOHNSON, Thomas A. ed.: Cybersecurity - Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, 2015, CRC Press; Jon Coaffee: Terrorism, Risk and the Global City - Towards Urban Resilience, 2009, Ashgate

KARAGIANNIS, Georgios Marios et al.: Climate change and critical infrastructure – floods, 2019, EU Joint Research Centre, https://publications.jrc.ec.europa.eu/repository/handle/JRC109015

KELEMEN Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése, Honvédségi Szemle 148. Évf. 4(2020)

KIS Kelemen Bence: Drónok háborúja (1.), Honvédségi Szemle, Évf. 146. szám 1(2018), 70-82 o.

KITTRIE, Orde F.: Lawfare, Law as a Weapon of War, 2016, Oxford University Press

KUSLITS Béla: Reziliencia: változás és állandóság társadalmi-ökológiai rendszerekben, Magyar Tudomány 181 (2020) 12, 164-165. o.

LONGSTAFF, Patricia H. et al. "Building Resilient Communities: A Preliminary Framework for Assessment." Homeland Security Affairs 6, Article 6 (September 2010)

MAGYAR Sándor, SIMON László: A terrorizmus és indirekt hadviselése az EU kiberterében, Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata 2017: (4) pp. 57-68.;

NAGY Rudolf: A klímaváltozás hatása a kritikus infrastruktúrák védelmére, Nemzet és Biztonság, 2010/2., 35-44.o.

PETRUSKA Ferenc: A lawfare fogalma, Katonai Jogi és Hadijogi Szemle, 9. évfolyam, 2021/3. szám, 97-106. o.

PORKOLÁB Imre: Aszimmetrikus konfliktusok tapasztalatai a nemzetbiztonsági tanácsadó szemszögéből, Honvédségi Szemle Évf. 145. szám 4(2017) 3-15. o.

RESPERGER István: Az aszimmetrikus hadviselésre adható válaszok, Honvédségi Szemle Évf. 145. szám 1(2017) 24-43. o.;

SeConSys: Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve, https://www.seconsys.eu

SINGER, P.W., COLE, August: Ghost Fleet: A Novel of the Next World War, 2015. Eamon Dolan/Houghton Mifflin Harcourt

SOARE, Simona R., BURTON, Joe: Smart Cities, Cyber Warfare and Social Disorder, in. A. Ertan et al. (ed): Cyber Threats and NATO 2030: Horizon Scanning and Analysis, 106-124. o., 2020, NATO CCDCOE,

SPITZER Jenő: A nemzetbiztonsági szolgálatok helye, szerepe Franciaország védelmi és biztonsági rendszerében, Katonai Jogi és Hadijogi Szemle 2020/4. szám, 69-94. o.;

SPITZER Jenő: A dróntámadások nemzetközi joggal való összeegyeztethetőségének egyes kérdései, kitekintéssel a drónok védelmi célú alkalmazásának perspektíváira, In. FARKAS Ádám (szerk.): Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében, 101-146. o.; Magyar Katonai és Hadijogi Társaság, Budapest 2018.;

TAILLARD, Michael: Economics and Modern Warfare - The Invisible Fist of the Market, 2012, Palgrave MacMillan

VIKMAN László: Az amerikai titkosszolgálati rendszer áttekintése, Katonai Jogi és Hadijogi Szemle 2020/4. szám, 35-68. o.;

VIKMAN László: A műveléttervezés jogi feladatai, Honvédségi Szemle 149. szám (2) 2021, 44-56. o.

ZANIN, Cristiano, MARTINS, Valeska, VALIM Rafael: Lawfare: Waging War through Law, 2021, Routledge;

Cyber Defence Pledge, Press Release (2016) 124 Issued on 08 Jul. 2016 https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Statement by the North Atlantic Council concerning malicious cyber activities (2020), Press Release (2020) 049 Issued on 03 Jun. 2020: https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en

The Secretary General's Annual Report 2020, 16 March 2021, https://www.nato.int/cps/en/natohq/opinions_182236.htm

AJP-3.20 ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS, Edition A Version 1 JANUARY 2020

Strengthened Resilience Commitment, 15 Jun. 2021, https://www.nato.int/cps/en/natohq/official_texts_185340.htm

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK, Digitális iránytű 2030-ig: a digitális évtized megvalósításának európai módja, Brüsszel, 2021.3.9., COM(2021) 118 final

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, AZ EURÓPAI TANÁCSNAK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK, A biztonsági unióra vonatkozó uniós stratégia, Brüsszel, 2020.7.24. COM(2020) 605 final

KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK, Az EU kiberbiztonsági stratégiája a digitális évtizedre, Brüsszel, 2020.12.16., JOIN(2020) 18 final

A TANÁCS (EU) 2019/796 RENDELETE (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről

Javaslat AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE, a kritikus fontosságú szervezetek rezilienciájáról, Brüsszel, 2020.12.16., COM(2020) 829 final, 2020/0365 (COD)

Javaslat AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE, az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről, Brüsszel, 2020.12.16., COM(2020) 823 final, 2020/0359 (COD)

European Union Agency for Cybersecurity, https://www.enisa.europa.eu/

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2021/241 RENDELETE (2021. február 12.) a Helyreállítási és Rezilienciaépítési Eszköz létrehozásáról

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/2088 RENDELETE (2019. november 27.) a pénzügyi szolgáltatási ágazatban a fenntarthatósággal kapcsolatos közzétételekről

1163/2020. (IV. 21.) Korm. határozat, Magyarország Nemzeti Biztonsági Stratégiájáról

1573/2020. (IX. 9.) Korm. határozat, Magyarország Mesterséges Intelligencia Stratégiájáról, valamint a végrehajtásához szükséges egyes intézkedésekről

1393/2021. (VI. 24.) Korm. határozat, Magyarország Nemzeti Katonai Stratégiájáról

1139/2013. (III. 21.) Korm. határozat, Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

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

1838/2018. (XII. 28.) Korm. határozat, Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiája