Gulyás György♦

A kritikus infrastruktúrák és a kritikus információs infrastruktúrák védelmének jelentősége a beszállítók sikeres művelettámogatásában

DOI 10.17047/HADTUD.2025.35.E.46

A sikeres katonai műveletek egyik alapvető feltétele a beszállítók által nyújtott, többféle szerződéseken keresztül megvalósuló támogatás. Ez kiterjedhet a különböző alágazatokban történő fuvarozásra, az élelmezésre, hajtóanyagra, tábori elhelyezésre és a kapcsolódó egyéb szolgáltatásokra, de a logisztikai szolgáltatásokon túl egyéb támogatási területekre is. Mindezek többféleképpen beszerezhetők. Például egy helyi beszerzés alkalmával egyedi szerződés, keretszerződések, keretmegállapodások útján vagy például ún. szerződés integrátor bevonásával. Ami viszont sok esetben elkerüli a parancsnokok és logisztikai szakemberek figyelmét az az, hogy a beszállítók bizonyos infrastruktúrái, azok egyes elemei szintén beletartozhatnak a védendő kritikus infrastruktúrába, sőt a működésük során használt infokommunikációs rendszerek is. A szerző ezen kérdéskör fontosságára szeretné felhívni a figyelmet jelen cikkében.
KULCSSZAVAK: művelettámogatás, kritikus infrastruktúra védelme, információ biztonság, beszállítók művelettámogatása

The Importance of Protecting Critical Infrastructure and Critical Information Infrastructure in Supporting the Successful Operations of Contractors

One of the basic conditions for successful military operations is the support provided by contractors through various contracts. This may cover transport in various sub-sectors, food, fuel, camp accommodation, and other related services, but also other support areas in addition to logistics services. All of these can be purchased in several ways. For example, in the case of a local procurement, through individual contracts, framework contracts, framework agreements, or with the involvement of a contract integrator. What often escapes the attention of commanders and logistics specialists is the fact that certain infrastructures of contractors and their individual elements can also be part of the critical infrastructure to be protected, or even of the info-communication systems used during their operation. The author's intention is to draw attention to the importance of this issue through this article.
KEYWORDS: operational support, critical infrastructure protection, information security, contractor support to operations

Bevezetés

A North Atlantic Treaty Organization (NATO) vagy az Európai Unió (EU) katonai műveleteinek logisztikai támogatására több lehetőség is kialakult az elmúlt évtizedek során,

♦ Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék – *University of Public Service, Faculty of Military Science and Officer Training, Department of Supply, Finance and Military Transportation;* gulyas.gyorgy@uni-nke.hu; https://orcid.org/0000-0002-5334-470X

ezek egyike a beszállítókon keresztül megvalósuló logisztikai vagy egyéb támogatás. Elmondható, hogy ennek hiányában nagyon nehéz lenne a haderők organikus képességei és a befogadó nemzeti támogatás által le nem fedett katonai logisztikai igényeket kielégíteni. A különböző katonai alakulatoknak hazai bázisaikról kellene kiszállítaniuk az ellátásukhoz szükséges anyagok igen jelentős részét a hadműveleti területre az expedíciós műveleteik során, ami teljesen elképzelhetetlen és logisztikailag még a hatalmas szállítási kapacitásokkal rendelkező nemzetek számára is nehézséget okozna. Habár a szükségletek többnemzeti logisztikai megoldásokon keresztül történő kielégítésére több lehetőség is ismert (mint például a logisztikai vezető nemzeti támogatás), de igazából a legtöbb esetben ott vannak a beszállítók a háttérben, akik a mondjuk a logisztikai vezető nemzeten keresztül a kívánt készleteket vagy szolgáltatásokat nyújtják. A történelem során minden háború alkalmával igénybe vették a hadviselő felek a polgári gazdasági szereplőket, vállalatokat a fentebb említett anyagok vagy szolgáltatások megszerzése céljából. Azonban napjainkban – az első Öböl-háború óta – a polgári cégek szerepe a műveletek logisztikai támogatásában jóval nagyobb, mint valaha. A 2003-ban indult iraki koalíciós (*Operation Iraqi Freedom* – OIF) és a kicsivel később kezdődött NATO (*NATO Training Mission Iraq* – NTM-I) műveletekben a katonák és beszállítók aránya 1:1, viszont a 2001-ben Afganisztánban kezdődöttekben már 1:1,43 volt[1]. A nemzeti vagy szövetséges haderők több okból is igénybe veszik ezeket a polgári cégeket a gyakorlataik vagy műveleteik logisztikai támogatásához. Egyrészt a nem kifejezetten katonai, vagyis nem ún. core competence feladatok kiszervezése civil cégek számára anyagi megtakarításokat eredményezhet a fegyveres erők számára, amellett a katonaállomány más tevékenységekre is felhasználható lehet (megvalósítva a beszállítók művelettámogatási tevékenységének „force multiplier" funkcióját). De valószínűleg politikailag is fontos szempont, ha az említetteknek köszönhetően kevesebb veszteséget szenved el a haderő egy konfliktusban. Mikor beszállítókról írok, ide értendők a „műveleti kontraktor logisztika" [2] kategóriába tartozó expedíciós katonai missziókat támogató vállalkozások, a NATO különféle logisztikai és egyéb szolgáltatásokat nyújtó ügynökségei, de azok az Európában található (például olaj- vagy közlekedési) vállalatok is, amelyek mondjuk hadtáp anyagokkal és tevékenységeiken keresztül látják el a nemzeti erőket, a NATO parancsnokságait és alakulatait. Utóbbiaknak különösen jelentős szerepük van az Ukrajnát 2014-ben ért orosz agresszió óta, amikor is a műveleti fókusz ismét visszakerült Európába.

Mivel ezen vállalkozások művelettámogatásban betöltött szerepét az ellenség is felismerte, ezért gyakran támadják az ellátási útvonalakat, a kontraktorok konvojait, a közlekedési infrastruktúra elemeket, valamint a telephelyeket, az elosztó vagy raktárbázisokat is. Ezek fokozott védelme ezért létfontosságú.

[1] EU Concept for Contractor Support to EU-led military operations. Council of the European Union. Brussels, 2014.
[2] Nyitrai 2023.

Milyen szempontok figyelembe vétele szükséges a beszállítók műveletámogatásra történő alkalmazásához?

Megfigyelhető, hogy a nemzeti haderők honi bázisaikon, illetve a NATO vagy az EU parancsnokságai és különböző missziókban működő katonai szervezetei is igénybe veszik a beszállítók által nyújtott anyagokat vagy szolgáltatásokat. Ehhez azonban mindig szükséges megvizsgálni a műveletek logisztikai tervező szakembereinek, hogy mely esetekben érdemes a logisztikai támogatás ezen lehetőségét is igénybe venni. Az alapvető szempontok a következők:

- amennyiben, politikai döntés révén, egy művelet során a szükséges katonai erő a hadműveleti területen csak korlátozott létszámban érhető el;
- egy adott képesség nem érhető el katonai forrásokból;
- a szükséges képesség egyáltalán nem érhető el egy adott műveletben;
- a meglévő katonai képesség nem elérhető a kívánt mértékben, hogy fenntartsa vagy támogatni tudja az adott műveletet;
- létezik ugyan a kívánt katonai képesség, de egy másik műveletben van rá szükség épp az adott időszakban;
- a helyi beszállítók alkalmazása támogatja a kívánt civil-katonai együttműködési (CIMIC) tervet;
- a beszállítók alkalmazása bizonyos szakterületeken és időszakban, költséghatékonyabb lehet, mint a katonai erők alkalmazása;
- a műveleti érdek megkövetel bizonyos fokú folytonosságot és tapasztalatot, amit a katonai erők alkalmazása azok rotációja (missziós váltásai) nem tesznek lehetővé.[3]

Akár tervezetten, akár ad-hoc módon szerződik egy haderő a beszállítókkal, a polgári cégekkel kötött szerződések képesek kiegészíteni a katonai képességekben jelentkező hiányokat és megjelenik ezen kereskedelmi megoldások ún. „force multiplayer” hatása.

A szerződések az adott szakterülettől, anyagnemtől vagy művelettől függően, lehetnek:

- műszaki, technikai szolgáltatásokra vonatkozók;
- fegyverrendszerekre vonatkozó rendszertámogató szerződések;
- lízing szerződések adott eszközökre;
- partnerségi megállapodások fővállalkozókkal hosszútávú szolgáltatások biztosítására;
- egy bizonyos időszakra vonatkozó ún. „alvó szerződések”, amelyek csak akkor kerülnek aktiválásra, ha szükség van rájuk;
- nagy fontosságú és a piacon csak korlátozottan elérhető képességekhez garantált hozzáférést biztosító szerződések;
- keretszerződések, mint a NATO-nál alkalmazott Basic Ordering Agreement – amikor egyetlen beszállítóval kötött szerződéshez több ügyfél is csatlakozhat vagy
- keretmegállapodások, amikor több potenciális beszállító is biztosíthatja a kívánt

[3] AJP- 4.9 Allied Joint Doctrine for Modes of Multinational Logistic Support. NATO Standardization Agency. 2013 Február.

szolgáltatást egy megállapodás keretében, illetve

– az ún. „spot market-ről” könnyen elérhető szolgáltatások megvásárlása.

Ki kell hangsúlyozni azt is, hogy a művelettervezésnek szerves eleme a logisztikai tervezés. Ennek részeként történik az anyagok és szolgáltatások forrásainak azonosítása, így a beszállítók alkalmazási lehetőségének megvizsgálása is ekkor kell, hogy megvalósuljon, méghozzá ennek a folyamatnak a lehető legkorábbi szakaszában. Mindennek részét képezheti, különösen a NATO-nál, a szerződés integrátor bevonása is a tervezésbe. Ez egy olyan szervezet, amely mintegy kapuként funkcionál a nemzeti haderők és a NATO részére a piaci szereplők szolgáltatásai felé. Ilyen entitások lehetnek a nemzetek honvédelmi minisztériumai tulajdonában lévő vállalkozások is (mint pl. a HM EI Zrt.) vagy a NATO esetében, a NATO Support and Procurement Agency. Ezen vállalatok, ügynökségek bevonása a szolgáltatások és anyagok beszerzésének megkönnyítésén túl már egy biztonsági szempontú garanciát is jelent arra, hogy a tervezés során megjelenő minősített információk megfelelően kezelésre kerülnek és nem kerülnek illetéktelenekhez.

A beszállítók igénybevétele ugyanis egy hadműveleti és egy harcászati szintű biztonsági kockázattal is jár. Hadműveleti szinten ez alapvetően a tervek és a katonai szándék beszállítók általi megismeréséből fakad. A harcászati szinten jelentkező kockázat pedig a hadműveleti területre átcsoportosítandó vagy a már ott jelen lévő alakulatok képességeinek, harcértékének vagy tevékenységének megtudásából ered. Az előbbi esetén, a már említett szerződés integrátorok bevonása, utóbbi esetében pedig az alapos biztonsági bevizsgálás jelentheti a megoldást a vonatkozó kockázatok csökkentésére. A szerződés integrátor már a beszerzési eljárás során előírhatja, hogy a jövőbeni beszállító és annak alvállalkozói milyen szintű nemzetbiztonsági vagy NATO/EU bevizsgálással rendelkezzenek. Továbbá az ad-hoc szerződések beszállítóinak műveleti területen megvalósuló kiválasztása történhet a helyi hatóságok vagy a NATO/EU biztonsági szakembereinek bevonásával.

A kritikus infrastruktúra védelmének közösségi és hazai jogi háttere

Általánosságban érvényesnek találom azt a kijelentést, hogy a különböző biztonsági jellegű kockázatokat akkor vagyunk képesek elemezni és értékelni, ha már sikerült azokat beazonosítani. A hazai kutatók a kritikus infrastruktúra védelmével kapcsolatban alapvetően két módszert alkalmaznak. Az első szerint négy-hat rendező elv szerint csoportosítva a lehetséges kockázati tényezőket (mint például természeti, civilizációs eredetű vagy egyéb forrásúakra).[4] A másik módszer alapja, hogy a korábban tapasztalt rendkívüli események és szóba jöhető fenyegetési tényezők elemzését követően számba veszik azokat a kockázat típusokat, amelyek veszélyeztethetik a kritikus infrastruktúrák biztonságát vagy esetleg azok kieséséért felelhetnek. Az ezredfordulót követően az Amerikai Egyesült Államokban kialakult gyakorlat szerint viszont a szakemberek a biztonságot fenyegető tényezőket komplexen, együtt vizsgálják a várható káros hatásokkal. Ennek alapján fizikai- (mint például természeti katasztrófák); kiber- és humán kockázatokat (amelyek lehetnek szándékosságból vagy

[4] Bonnyai 2012.

gondatlanságból fakadók is) különböztetnek meg. A kockázati tényezők meghatározásakor pedig figyelembe kell venni a fenyegetés jellegét, a az adott rendszer vagy rendszerelem sérülékenységét, illetve a várhatóan bekövetkező események valószínű hatásait is.[5]

Ahogyan azt Horváth Attila írja egyik munkájában, a kritikus infrastruktúrák sérülékenységére egyáltalán nem tekinthetünk úgy, mint újkeletű problémára, hiszen ez már az ókor óta fenyegette az emberiség által létrehozott létesítményeket és rendszereket háborúk vagy például természeti katasztrófák által. Eme infrastruktúrák védelme, mint fogalom megjelenése csupán az 1990-es évek második felére tehető az Amerikai Egyesült Államokban[6], de a 2001. szeptemberi támadássorozat után a kérdés világszerte nagyobb hangsúlyt kapott. Az Európai Bizottság 2005 novemberében közreadta a „*Zöld Könyv a kritikus infrastruktúra védelem európai programjáról*" című anyagát, amelybe ajánlásokat fogalmaz meg, itt olvasható először a kritikus információs infrastruktúra fogalma: „A kritikus információs infrastruktúra azokat az infokommunikációs rendszereket jelenti, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából (távközlés, számítógépek és szoftver, internet, műholdak stb.)." védelme pedig a „tulajdonosok, üzemeltetők, gyártók és használók, valamint a hatóságok programjai és tevékenységei, melyek célja fenntartani a kritikus információs infrastruktúra teljesítményét meghibásodás, támadás vagy baleset esetén a meghatározott minimális szolgáltatási szint felett, illetve minimálisra csökkenteni a helyreállításhoz szükséges időt, valamint a károkat."[7] Megállapítja, hogy a kritikus információs infrastruktúrák védelme egy ágazatközi jelenség és nem korlátozódik konkrétan egyes ágazatokra. Ezek védelmét pedig szorosan koordinálni szükséges a kritikus infrastruktúrák védelmével. Az uniós szinten elsőként létrehozott szabályzó „az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről" szóló 2008. december 8-i „2008/114/EK tanácsi irányelv, amelynek honi végrehajtására pedig" a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről" szóló 2012. évi CLXVI törvény (Lrtv.) készült. Az EU-s és a hazai szabályozás célja a létfontosságú rendszerelemek azonosítása volt, valamint ezek teljeskörű védelme és üzemfolytonos működésük biztosítása. A törvény meghatározta a fogalmakat, rendelkezett a nemzeti és az európai szintű létfontosságú rendszerelemek kijelöléséről, előírta az üzemeltetők részére biztonsági terv elkészítését, olyan szakember meghatározását, aki biztonsági összekötőként funkcionál, taglalta a nyilvántartással és ellenőrzéssel kapcsolatos előírásokat, illetve a szankcionálás módjait. Fentiekből is kitűnik, hogy a kritikus infrastruktúra elemeinek kijelölése többszintű tevékenység: nemzeti, valamint európai uniós. A követelmények megállapítása ezeken a szinteken valósult meg, ezért léteznek az ágazati kritériumok is ebben a két kategóriában. A különbség jól érzékelhető, ha rávilágítunk arra, hogy amíg egy uniós létfontosságú infrastruktúra vagy ennek elemének kimaradása, esetleg

[5] Horváth 2016.
[6] Horváth 2010.
[7] Európai Bizottság: Zöld Könyv egy Kritikus Infrastruktúra Védelmi Európai Programról, COM(2005) 576, 2005. november 17. (Commission of the European Communities: Green Paper on a European Programme for Critical Infrastructure Protection, Brussels, 17.11.2005 COM(2005) 576 final)

működésének leállása számos országban jelentkező hatást válthat ki, addig a nemzeti létfontosságú infrastruktúrában megjelenő ilyen probléma csupán a szóban forgó országra van befolyással.

Ezt követően 2016. július 19-én az EU elfogadta az Európai Parlament és a Tanács 2016/1148 irányelvét „A hálózat és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelvet” (röviden: NIS [8] Irányelv). Ez lett az első széleskörű közösségi szabályzó az információbiztonsági kérdéskört tekintve, amely a hálózati- és információs rendszerek megfelelő biztonsági szintjét akarta garantálni az unióban. Az említett irányelv hatálya alá esik azon szolgáltatók csoportja, amelyek az alapvető-, és a digitális szolgáltatásokat nyújtják.Az irányelv három fő pilléren nyugszik:

1. A felkészültség elérése érdekében a NIS-irányelv előírja a tagállamok számára, hogy fogadjanak el nemzeti stratégiát a hálózati és információs rendszerek biztonságára vonatkozóan. A tagállamok kötelesek kijelölni a kockázatok és incidensek kezeléséért felelős nemzeti számítógépes biztonsági eseményekre reagáló csoportokat (CSIRT)[9], egy illetékes nemzeti NIS-hatóságot és egyetlen kapcsolattartó pontot (SPOC).[10] Az SPOC-nak kapcsolattartó funkciót kell ellátnia, hogy biztosítsa a határokon átnyúló együttműködést a tagállamok illetékes hatóságaival és a NIS Együttműködési Csoporttal.
2. A NIS-irányelv létrehozza a NIS-Együttműködési Csoportot a tagállamok közötti stratégiai együttműködés és információcsere támogatására és elősegítésére, valamint a CSIRT-hálózatot, amely elősegíti a nemzeti CSIRT-ek közötti gyors és hatékony operatív együttműködést.
3. Az említett irányelv biztosítja a kiberbiztonsági intézkedések meghozatalát hét olyan ágazatban, amelyek létfontosságúak gazdaságunk és társadalmunk számára (az energia, a közlekedés, a bankszektor, a pénzügyi piaci infrastruktúra, az ivóvíz, az egészségügy és a digitális infrastruktúra).

Mindezek mellett szükségessé vált az infrastruktúrák nemzeti létfontosságú rendszerelemmé történő kijelölési folyamatának meghatározása is. Azon üzemeltetők, amelyek az Lrtv. 1. melléklete szerinti ágazatokban kínálnak szolgáltatást ún. azonosítási vizsgálatot kell, hogy végrehajtsanak. Ez ki kell terjedjen többek között azon tényezők felmérésére és elemzésére, amelyek a rendszerelemek szolgáltatásainak folytonosságát veszélyeztethetik, valamint arra, hogyan teljesülnek mind az ágazati mind pedig a horizontális kritériumok.

A vizsgálat végén egy „azonosítási jelentés” készül, amely tartalmazza a vizsgálat eredményét és a rendszerelemmé történő kijelölésre vonatkozó javaslatot (nemzeti, illetve európai szinten). Az üzemeltető által elkészített azonosítási jelentés horizontális és ágazati kritériumoknak való megfelelését az ágazati kijelölő hatóság vizsgálja szakhatóság

[8] NIS: Security of Network and Information Systems.
[9] CSIRT: Computer Security Incident Response Teams.
[10] SPOC: Single Point of Contact.

bevonásával. Legalább egy ágazati és legalább egy horizontális követelmény megvalósulása esetén a létfontosságú rendszerelemet az említett hatóság nyilvántartásba veszi, és intézkedik az üzemeltető entitás alapvető szolgáltatást nyújtók jegyzékébe történő felvételére. A szakhatóság a horizontális kritériumok teljesülését ún. vélemény nyilvánító szervek bevonásával (például NAV, Alkotmányvédelmi Hivatal) vizsgálja meg. „A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról" szóló 65/2013. (III. 8.) Kormányrendelet meghatározásai szerint a horizontális kritériumok a következők: a gazdasági hatás; a politikai hatás; a társadalmi hatás; a környezeti hatás; a veszteségek; és a védelem kritériuma.

Az alapvető szolgáltatást nyújtó szereplők meghatározás szerint „olyan szervezetek vagy gazdasági szereplők, amelyek létfontosságú társadalmi és/vagy gazdasági folyamatok és funkciók ellátásának biztosítása céljából alapvető szolgáltatást nyújtanak, szolgáltatásuk elektronikus információs rendszerektől függ és a szolgáltatásukat érintő biztonsági esemény jelentős zavart okozna a szolgáltatásban, valamint az erre irányuló eljárásban alapvető szolgáltatást nyújtó szereplőként kerül azonosításra."[11]

Hazánkban a 2013. évi L. törvény szabályozza a létfontosságú rendszerek és létesítmények információbiztonságra vonatkozó keretrendszerét. Ennek hatósági felügyeletével a Nemzetbiztonsági Szakszolgálat foglalkozik. A katasztrófavédelmi hatóság központi szerve (a BM OKF) a kijelölt nemzeti létfontosságú rendszerelemet 5 évenként komplex ellenőrzés során ellenőrzi.

A kritikus infrastruktúra védelmével az egyes ágazati kormányrendeletek foglalkoznak, például a honvédelem esetében *„a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről359/2015. (XII. 2.) Korm. rend."* De témánkat érintően szintén nagyon fontos „a közlekedési létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről" szóló 161/2019. (VII. 4.) Kormányrendelet is, amely ezen a területen felsorolja az uniós és nemzeti ágazati kritériumokat.

Az információbiztonsági követelmények kiterjednek a létfontosságú rendszerelemek üzemeltetői által működtetett létesítményekre is. A területet alapvetően szabályozó kiemelten jelentős jogszabályok:

- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.);
- az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet;
- 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;
- az Ibtv-ben meghatározott technológiai biztonsági, valamint a biztonságos információs

[11] https://www.katasztrofavedelem.hu/109/kritikus-infrastrukturak-vedelmevel-osszefuggo-hatosagi-feladatok-jogszabalyok

eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet.

A terület szabályozását illetően meg kell még említeni mindenképpen:

– a 2023. január 16-án hatályba lépett „az Európai Parlament és Tanács (EU) 2022/2555 irányelvét („az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről” vagy röviden: NIS2 irányelv);
– illetve a szintén 2023 óta hatályos, az Európai Parlament és Tanács (EU) 2022/2557 irányelvét („a kritikus entitások ellenálló képességéről” vagy másképpen: CER[12] irányelv).

A NIS2 célja a korábbi hálózat- és információbiztonsági irányelv hiányosságainak orvoslása, a jelenlegi igényekhez való igazítása és jövőbiztossá tétele. Kiterjeszti a korábbi NIS-irányelv hatályát új ágazatokkal a gazdaság és társadalom szempontjából kulcsfontosságú szerepük alapján, valamint egyértelművé teszi, hogy a kiválasztott ágazatokban valamennyi közép- és nagyvállalat a hatálya alá tartozik. Ezeken túlmenően megerősíti és egyszerűsíti a vállalatokra vonatkozó biztonsági és jelentéstételi követelményeket egy kockázatkezelési megközelítés előírásával, amely megadja az alkalmazandó alapvető biztonsági elemek minimális listáját. Ezen kívül a Bizottság javasolja az ellátási láncok és a beszállítói kapcsolatok biztonságának kezelését azáltal, hogy megköveteli az egyes vállalatoktól, hogy foglalkozzanak az ellátási láncokban és a beszállítói kapcsolatokban felmerülő kiberbiztonsági kockázatokkal. A tagállamok a Bizottsággal és az EU Kiberbiztonsági Ügynökséggel (ENISA) együttműködve összehangolt kockázatértékelést végezhetnek a kritikus ellátási láncokkal kapcsolatban, illetve az irányelv fokozni kívánja a tagállami hatóságok közötti információmegosztást és együttműködést.

A CER irányelv kötelezettségeket ír elő az EU-tagállamok számára, hogy tegyenek konkrét intézkedéseket annak biztosítására, hogy a létfontosságú társadalmi funkciók vagy gazdasági tevékenységek fenntartásához nélkülözhetetlen szolgáltatásokat akadálytalanul biztosítsák a belső piacon. Az említett piac megfelelő működése szempontjából kritikus fontosságú jogalanyok ellenálló képességének széles körű kezelése érdekében az irányelv átfogó keretet hoz létre, amely a kritikus entitások ellenálló képességével foglalkozik minden veszély tekintetében, legyen az akár természetes, akár ember alkotta, véletlen vagy szándékos. A kritikus gazdálkodó egységeknek komplex ismeretekkel kell rendelkezniük azokról a releváns kockázatokról, amelyeknek ki vannak téve, és kötelességük ezeket elemezni. E célból kockázatértékelést kell végezniük sajátos körülményeikre és e kockázatok alakulására tekintettel.

A Bizottság 2023. július 25-i rendelete kiegészíti a CER irányelvet az alapvető szolgáltatások listájának létrehozásával, amely tartalmazza a katonai műveletek támogatásához nélkülözhetetlen szolgáltatásokat, tevékenységeket és szakmai kategóriákat, mint például az olajágazaton belül az olajszállító csővezetékek üzemeltetőit, közlekedési

[12] CER: Critical Entities Resilience.

ágazatban a légi fuvarozókat és a vasúti vállalkozásokat is.

Fentieket figyelembe véve a hazai szabályozás megalkotta „a kritikus szervezetek ellenálló képességéről” szóló 2024. évi LXXXIV. törvényt, amelynek 1. melléklete ágazatokra és alágazatokra lebontva tartalmazza az alapvető szolgáltatásokat.[13] Így például, az energia ágazat, kőolaj alágazatába tartozó kőolajvezeték üzemeltetés, kőolajtermelés és –finomítás, biztonsági készletezés alapvető szolgáltatásokat vagy a közlekedés ágazat, vasúti közlekedés alágazatán belül a vasúti szállítást és kiszolgáló létesítmények üzemeltetését. Ezek ugyan csak kiragadott példák, de az Európában esetlegesen bekövetkező katonai műveletek támogatásához ezek a zömében polgári vállalatok által nyújtott anyagok és szolgáltatások is nélkülözhetetlenek lesznek. Így a biztosításukról történő megfelelő gondoskodás, beleértve az ezeket szolgáltató kritikus szervezetek [14] rezilienciájának felépítése a sikeres művelettámogatás alapvető feltétele.

A témához kapcsolódik még, hogy 2024. július 12-én megjelent „a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról” szóló (EU) 2024/1689 rendelet, amely követelményeket és kötelezettségeket ír elő a mesterséges intelligencia (MI) fejlesztői és alkalmazói számára, annak konkrét felhasználásai tekintetében. Mivel az MI felhasználása lényeges kihívásokat is magában hordozhat a fenti két irányelvet végrehajtó szervezetek számára (például az ún.: adatmérgezés alkalmazásával),[15] az MI rendszereket használó NIS 2 és CER által lefedett szektorokban működő entitásoknak meg kell felelniük a fenti irányelvek és az MI rendelet előírásainak is.

Kritikus infrastruktúra és információs struktúra védelme

Nem elhanyagolható kérdés az sem, hogy a kritikus fontosságú infrastruktúrák kinek a tulajdonában vannak. Elmondható, hogy ez a tulajdonosi megoszlás nagyon eltérő lehet. A központi állami irányítás, minisztériumok, honvédelmi vagy rendvédelmi szervek, állami tulajdonú vállalatok (például repterek) tulajdonában lévő számítógépes és távközlési hálózatok rendszerei általában állami, önkormányzati tulajdonban vannak. De a magánszektorhoz is tartozhat több kritikus infrastruktúra és ezek között is megtalálhatók a távközlési és helyi áramszolgáltatók. Azonban előfordul, hogy a tulajdonos infrastruktúráját más cég üzemelteti, de megeshet, hogy a saját infokommunikációs hálózattal rendelkező cég nagymértékben függ a különböző eszközök beszállítóitól. Továbbá fontos tényező a szolgáltatók gazdasági érdeke is, hiszen a versenyszférában egy vállalat lehet, hogy inkább bevállalja a rendszerhibákból időnként bekövetkező leállásokat, megspórolva a karbantartásra

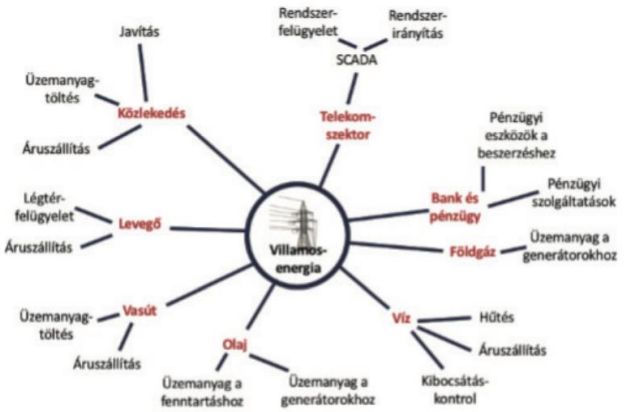
[13] Alapvető szolgáltatás: a kritikus szervezet által nyújtott, az 1. mellékletben foglalt táblázat „C” oszlopában meghatározott szolgáltatás, amely elengedhetetlen Magyarország társadalmi, gazdasági stabilitásához, és a biztonság, a környezet, a közegészségügy, a védelmi képességek és a nemzeti ellenálló képességi rendszer fenntartásához.

[14] Kritikus szervezet: olyan alapvető szolgáltatást nyújtó szervezet, amelyet a kijelölő hatóság a III. Fejezetben meghatározottak szerint kijelölt és elengedhetetlen Magyarország társadalmi, gazdasági stabilitásához és a biztonság, a környezet, a közegészségügy, a védelmi képességek és a nemzeti ellenálló képességi rendszer fenntartásához.

[15] Adatmérgezés: egy formája a gépi tanulási rendszerek elleni támadásnak, ahol a támadók a képzési adatokat manipulálják szándékosan, annak érdekében, hogy a modell viselkedését befolyásolni tudják.

vagy a meglévő infrastruktúra fejlesztésére, illetve annak biztosítására szánt költségeket, hogy a szolgáltatásait folyamatosan legyen képes nyújtani. Helyette inkább olyan területeket fejleszt, amelyek nagyobb nyereséggel kecsegtetik Ez jellemző lehet például a monopolhelyzetben lévő áramszolgáltató vállalatokra, amelyeket nem fenyegetnek a versenytársak azzal, hogy jobb teljesítményükkel megszerzik az ő piaci részesedésüket is. Ezért fontos a tulajdoni viszonyok vizsgálata, hiszen az infrastruktúra védelmekor eltérő eljárás és kezelés szükséges a magánszektor és az állam kezében lévő vagyon, ingatlan esetében. Lényeges a felelősségi határok megállapítása is, vagyis pontos törvényi előírások megalkotásával leszögezni, hogy az adott infrastruktúra tulajdonosai mely pontig kezeljék a kockázatokat és mikor kapcsolódjon be ezek kezelésébe az állam szerepvállalása. Persze mindemellett rendkívül fontos a közös érdekek keresése, valamint az ebből kiinduló magán- és állami szféra együttműködésének kialakítása is.[16]

Az is egyértelmű, hogy az infrastruktúrák vagy ezek elemeinek működése nem izolált módon történik, hanem kevésbé vagy kimondottan közeli kapcsolatban állnak egymással, vagyis interdependencia alakult ki közöttük, amelyet az alábbi ábra is illusztrál (1. ábra), bemutatva a villamosenergia ellátás kapcsolatait és hatásait.



1. ábra

A villamosenergia ellátás kapcsolatai és hatásai

(Forrás: Bonnyai Tünde, Danyek Miklós, Görgey Péter, Kriskó Edina, Molnár Anna, Tikos Anita: *Kritikus információs infrastruktúrák védelme.* Nemzeti Közszolgálati Egyetem. Budapest, 2019.)

A csatlakozó infrastruktúrák révén a megjelenő problémák felhalmozódva, sokkal meglepetésszerűbb és komolyabb zavarokat hozhatnak létre egy adott ország létfontosságú szolgáltatásaiban. Vagyis a különböző összekapcsolódó infrastruktúrák sérülékenyebbé teszik az egész rendszert. Például elmondható, hogy a szállítástól függ az energiatermelés, a szállítás viszont függ az energiától, és mindketten függnek az infokommunkációs rendszerektől, ám az infokommunikációs rendszer is függ az energiától.[17] Ezt jól példázza az az eset, amikor 2003. szeptember 28-án Olaszországban és Svájcban egy áramellátási zavar keletkezett, amely

[16] Muha 2015.
[17] Muha 2015.

Ausztriát, Franciaországot és Szlovéniát is érintette. A más szektorokat érintő következmények mellett a nyílt vonalakon megálló vasúti szerelvényekben ragadt több mint 30.000 ember, ezenkívül több száz embert kellett kimenteni a különböző városok metró alagútjaiból is. Csak a közekedési rendszerben nagyobb erőfeszítéssel lehetett a következményeket felszámolni, mint magát az áramszolgáltatás folyamatosságát visszaállítani. Az esemény befolyással volt az egészségügyi-, üzemanyag-, víz- és gázszolgáltatásra, továbbá a közúti és légi közlekedésre is.[18]

Műveletek a kibertérben

Egy ország stabilitásának létfeltétele, hogy a kritikus infrastruktúrák zökkenőmentesen működjenek, ideértve az interdependenciák folyamatos és stabil üzemét is. Vagyis, a működésük zavarai szinte biztosan gazdasági és belpolitikai instabilitást fognak eredményezni. Ezért, ezeknek az infrastruktúráknak az értéke, az elkövető szempontjából szemlélve különösen magas. Ezen rendszerek, létesítmények károkozási célú kiberműveletek fő célpontjaivá válhatnak. Ezek módszerei különbözőek lehetnek:

- „a fizikai károkozás, amely valamilyen kinetikus (be)hatás segítségével jöhet létre;
- az adott infrastruktúrán belüli – egymással interdependenciában lévő – alrendszerek közötti kommunikáció manipulálása vagy blokkolása;
- egy vagy több alrendszerben történő belső, fizikai károkozás."[19]

Mindhárom módszer kivitelezhető kiberműveleteken keresztül, amelyek előnyei, hogy a végrehajthatók távolról, tehát nincs szükség helyszíni jelenlétre, így olcsóbb, kockázatmentesebb és nehezebben bizonyítható a tett az elkövetőre. A kibertérben zajló műveletek okai gazdasági hátterűek, alapvetően politikai célok elérése érdekében, de nem kívánnak nyílt összeütközést a támadó és megtámadott között. Mivel ezek a módszerek és eljárások a történelemben korábban nem léteztek, így használatuk mértéke, amely eddig a bevett szokásjogon alapul, nem állapítható meg könnyen. Ezért meglehetősen nagy az a homályos zóna, amelyen belül a kiberműveletek jól használhatók. Így nem igazán határozható meg az a választóvonal, ahol egy olyan ország, amelyet kiber eszközökkel támadtak meg már nyílt támadásként értelmez egy incidenst. Annak kimondása, egy ország részéről, hogy azt kibertámadás érte alapvetően politikai döntés kérdése.

Kiberműveletek során, ha az állam rendeli meg vagy ő maga hajtja végre, állami érdekérvényesítést említünk. Ennek pedig végrehajtója az állam rendvédelmi, honvédelmi vagy nemzetbiztonsági szerve lehet, esetleg ezek valamelyik szakszolgálata és/vagy az azzal kapcsolatban lévő más gazdasági vagy polgári aktor, fedett műveletekben.

Azonban a kiberakciókkal véghezvihető pusztítás is lehet akkora, mint a más hadviselési módszerekkel végrehajtottak. Ennek egyik példája, amely szerencsére meghiúsult, a 2017-ben indított kibertámadás a szaúd-arábiai Petro Rabigh kőolajfinomító ellen. A kibertérben indított támadás célja az volt, hogy robbanást idézzenek elő a finomítóban, megsemmisítve ezzel a

[18] Union for the Coordination of Transmission of Electricity 2004. FINAL REPORT of the Investigation Committee on the 28 September 2003 Blackout in Italy.
[19] Kralovánszky 2021.

gyár minél nagyobb részét és termelés kiesést okozzanak.[20] Ezzel szemben, egy más módszerrel, mondjuk rakétával indított támadás nyílt háborút jelenthetett volna a támadóval, mivel egy rakéta indítójának azonosítása jóval egyszerűbb és nyíltabb akció. A finomító elleni akció azonban ezen kívül rávilágít az interdependenciák fontosságára. A gyár támadásával a másodlagos hatás – az infrastruktúra által kiszolgált gazdasági szereplők korlátozása és ezáltal a megtámadott ország működésében zavart okozni – nagyobb lett volna, mint az elsődleges. Egy jelentős kibertámadási képességekkel rendelkező ország lehetséges, hogy sokkal jobban ismeri ezeket a másodlagos hatásokat, mint a csapást elszenvedő ország. Ugyanígy, sokkal nagyobb lenne az említett szekunder hatás hazánkban az energetikai beszállítók, mint a MOL, főbb telephelyei, finomítója vagy a vasúti szállítás biztonságában létfontosságú szerepet játszó Egységes Európai Vasúti Közlekedésirányítási Rendszer vagy az Egységes Európai Vonatbefolyásoló Rendszer ellen indított támadás esetében is, mint az elsődleges hatás. Az üzemanyag szolgáltatás megbénulása vagy akadozása rengeteg zavart tudna okozni az egész ország működtetésében, az említett vasúti rendszerek leállása pedig a vasúti közlekedést lenne képes bénítani, ami szintén hatalmas szereppel bír a kereskedelemben, a lakossági ellátásban és az ország fenntartásában, de a katonai műveletek támogatásában is. Végül pedig megemlíthető az orosz-ukrán konfliktus kapcsán 2023 júniusában több holland kikötő ellen orosz hekkercsoport által végrehajtott ún. túlterheléses kibertámadás, válaszul a holland kormány terveire, hogy az harckocsikat vásárolna Svájctól. Az incidens több mint egy órára elérhetetlenné tette az amszterdami kikötő honlapját, míg a grönöngeni kikötői létesítményben két napon keresztül zavarokat lehetett tapasztalni.[21] A hollandiai tengeri ki- és berakóhelyek kulcsszerepet játszanak a NATO jelenlegi védelmi terveiben. Egy ilyen rendkívüli esemény összezavarhatja és késleltetheti a szövetséges erők műveleti területre történő átcsoportosítását, a hadtápanyagok és felszerelések hadszíntérre való beérkezését. Az említett nehézségek pedig alapvetően képesek hátráltatni a tervezett katonai műveletek végrehajtását. Mindezeken felül a hajóforgalom akadályozása, az áruk kirakásának és tovább szállításának megnehezítése a polgári lakosság ellátását is negatívan befolyásolhatja.

EU–NATO együttműködés a kibervédelem terén

A kiberterület fontosságát felismerve az EU és a NATO már 2012-től magasszintű együttműködésbe kezdett. Ez 2016-ban a varsói NATO-csúcson, az Európai Tanács elnöke, az Európai Bizottság Elnöke és a NATO főtitkára által aláírt EU és NATO közötti együttműködésről szóló nyilatkozat megalkotásával újabb lendületet kapott. Ez a kooperáció lefedi a hibrid fenyegetések leküzdésének kérdését, továbbá a kiberbiztonság és -védelem területét is. Konkrét célként fogalmazódott meg a kibervédelmi interoperabilitás megerősítése a katonai műveletek és egyéb missziós tevékenységek során, a kooperáció növelése gyakorlatokon és képzéseken, együttműködés a kibervédelmi kutatásokban és technológiai innovációban, illetve a kibernetikus szempontok beépítése a válságkezelésbe. Szintén 2016-ban jött létre egy technikai megállapodás az EU Computer Emergency Response Teams

[20] Kralovánszky 2021.
[21] https://www.vg.hu/kozelet/2023/06/orosz-kibertamadas-erte-rotterdam-kikotojet

(CERT) és a NATO's Computer Incident Response Capability (NCIRC) között. Mindkét szervezet alapvető célja volt, elősegíteni a technikai adatok és információk megosztását a kibereseményekelkerülése és megelőzése végett, valamint az említett események, incidensek feltárása, illetve az ezekre történő reakció erősítése. Finn kezdeményezésre 2017-ben a NATO és az EU támogatásával létrejött a Hibrid Tevékenységek Elleni Kiválósági Központ (*European Centre of Excellence for Countering Hybrid Threats*) Helsinkiben, amelynek elsődleges feladata pedig az Oroszországtól bejövő kiberbiztonsági veszélyek (mint, például a dezinformációs akciók) elemzése, illetve az ezekre reagáló megfelelő és összehangolt válaszok kimunkálása volt. A központ munkájába az évek során Ausztria, Kanada, Ciprus, a Cseh Köztársaság, Dánia, Észtország, Finnország, Franciaország, Olaszország, Németország, Lettország, Litvánia, Hollandia, Norvégia Lengyelország, Románia, Spanyolország, Svédország az Egyesült Királyság és az USA is bekapcsolódott.[22] Az EU mind nagyobb energiákat és forrásokat összpontosít a kiberbiztonság kapacitásépítésébe, ideértve a különböző pályázatokat és kutatásokat is. Csupán 2013-ban és az azt követő öt évben nagyjából 80 millió eurót invesztált ebbe.[23] Mindez persze nem jelenti azt, hogy az együttműködés a NATO tagállamok és az EU között tökéletes lenne. Erre hívta fel a figyelmet a Center for European Policy Analysis nevű think tank egyik tanulmányában.[24] Ebből kiderül például, hogy jelentős egyensúlyhiány mutatkozik a kiberbiztonsági jelentési követelmények és a későbbi kiberfenyegetettség-értékelési kapacitás EU és Egyesült Államokbeli normatív keretei között. Hogyan lehetne a kiberincidens-jelentésekre építeni, ha az Egyesült Államok kiberkockázati paraméterei eltérhetnek az EU-n belül elterjedtektől. Ez különböző szinteket eredményez a NIS-irányelv és a NIST[25] keretrendszer által bevezetett kiberbiztonsági szabványok terén a jövőben, amelyek közvetlenül befolyásolják a kiberkockázatok kezelésének képességét az Egyesült Államokban és az EU tagállamaiban.

Kibertámadás előjelzése

A kiber kapacitásépítés és -kutatások megkezdéséhez a saját nemzeti, valamint a szomszédos és a régióban található országok kritikus infrastruktúrájának megismerése az első lépések egyike. A kritikus infrastruktúrák elleni támadások, beleértve a kibertámadásokat is, nagyon sok esetben hatással lehetnek a szomszédos országok infrastrukturális rendszereire és létfontosságú szolgáltatásaira is. Az energiaszektor és a közlekedési hálózat épp ilyen rendszerek. Ezért alapvető fontosságú, hogy ismerjük a (kritikus) nemzeti és a kapcsolódó szomszédos kritikus infrastruktúra rendszerek sajátosságait, illetve a köztük lévő interdependenciákat annak érdekében, hogy minél inkább kiszáíthassuk a támadások mely elemek ellen irányulnak majd és milyen elsődleges és másodlagos célt kívánnak elérni. Tehát a védekezés egyik sarokköve a kibertámadások előjelzése. A kiberhadviselés esetében ennek

[22] Bonnyai 2019.
[23] Bonnyai 2019, 8.
[24] Selga 2021.
[25] NIST: National Institute of Standards and Technology, az USA első fizikai kísérleti laboratóriuma, 1901-ben jött létre National Bureau of Standards néven. Az USA Kereskedelmi Minisztériumának felügyelete alatt működik.

két fő módszere van. Az első mód a hatékony hírszerzés. Elmondható, hogy egy stratégiai szintű kiber csapásméréshez nagyon komoly előkészületeket kell tennie a támadónak, amelyek bizonyos adatait és részleteit bonyolult és nehézkes lehet titokban tartani. Egy megfelelően funkcionáló hírszerzési rendszer – főként, amely mondjuk a NATO keretében, nemzetek közötti együttműködésben üzemel – egyes elemeit ennek képes felfedni. Különösen igaz ez abban az esetben, ha a támadó ország több kormányzati szervét is be kell vonnia a csapásméréshez. Alapvetően igaz, hogy az összes akciónak, csapásnak és támadásnak van konkrét indoka, elérendő célja, illetve, ha indoka van, akkor nagy valószínűséggel van valamiféle előtörténete is. Egy bonyolult nemzetközi közegben az indokok igen különfélék, ezért nincs is rá garancia, hogy ezek a kellő időkeretben beazonosíthatók. De amennyiben tevőleges szándék is kapcsolódik az okokhoz, akkor ezek fenyegetéssé válnak, és ezek megfelelő előjelzési eszköze a hírszerzés.[26]

A másik módszer, ha a saját infokommunikációs rendszereinket figyeljük és vizsgáljuk, továbbá elemezzük és értékeljük. A normálisan működő hálózatokban jól megfigyelhető és feltérképezhetővé válik az átlagos működés a felhasználói szokások alapján. Amennyiben az ettől való eltérést vizsgáljuk, valószínűleg megállapítható lesz, hogy az kockázatokat, fenyegetést jelez-e vagy csupán valamiféle normál üzemi használatból származó, de megmagyarázható devianciával állunk szemben. Ez az elemzéssel és értékeléssel végzett módszer ugyanúgy alkalmazható egy csupán néhány eszközből álló vagy pedig egy többezer hálózati végponttal bíró nagyvállalati rendszeren vagy az egész kormányzathoz tartozó infokommunikációs hálózaton is. Ez a fajta folyamatos figyelési és elemzési tevékenység jó alapot nyújthat a szükséges értékelések elvégzéséhez, de nem biztos, hogy képes felfedni a támadást indító személy kilétét. Azonban az elkövetési módok és a felhasznált eszközök, kártevők jellemzőek lehetnek a rossz szándékú akciót tervező csoportra. Egyébként hasonló elemzésekre lenne szükség a már megtörtént támadásokat követően is, amikor a cél szintén a végrehajtó személyének azonosítása. Ebben az esetben viszont már sokkal világosabb, hogy milyen tényezőket kell keresni, mint a támadást megelőzően.[27]

Összegzés

Alapvető igazság, hogy az államok akaratuk érvényesítéséhez, valamint céljaik eléréséhez gyakran a hadviselést választják eszközül, amelyben napjainkra új tartományként a kibertér szerepe és súlya folyamatosan nő. A kritikus infrastruktúrák védelme kiemelt jelentőséggel bír a jövőben már békeidőben is. Napjainkban nem szükséges, hogy egy olajfinomítót vagy egy vasúti biztosító berendezés hálózatát egy hadüzenetet követően kinetikus eszközökkel rombolja le az ellenség, hiszen a hibrid hadviselés módszerei és a kibertérben induló támadások éppen megfelelő fegyvert adnak a támadó kezébe ahhoz, hogy az adott megtámadott rendszeren túl hatalmas károk keletkezzenek az interdependenciák által összekötött egyéb kiemelten fontos területeken is. Az szintén megfigyelhető, hogy az elmúlt 20 évben a kiberműveletek egy ismeretlen és szinte inkább csak egzotikus minőségből a

[26] Kralovánszky 2021.
[27] Kralovánszky 2021.

modern hadviselés fontos és megkerülhetetlen részévé fejlődtek, amelyeket számításba kell venni stratégiai, hadműveleti és harcászati szinteken is. Ezen támadások esetleges megvalósulását, hatásait jó előre, a bekövetkezést megelőzően elemezni és értékelni kell, továbbá megvizsgálni a csapások valószínűségét. Emellett, az ezekkel kapcsolatos kockázatelemzést, előkészületeket széleskörűen, körültekintően, szakértő szakmai alapon kell elvégezni akár nagyvállalati, akár nemzeti szinten, polgári és katonai tekintetben egyaránt, sőt mondhatjuk, hogy szövetségi együttműködés szintjén is. Mivel pedig a különböző kritikus infrastruktúrák határokon átívelő rendszereket is képezhetnek és az interdependenciák több ágazatra kiterjednek, ennek a kooperációnak működnie kell bilaterális, multilaterális és regionális alapon. A kibertér gyors felértékelődésének alapjai az információs társadalom váratlan és rohamos térnyerésében keresendők, illetve az e mögött álló technológiai fejlődésnek az eredményei. Így nem csoda, hogy napjainkra a világpolitikában az egyes nemzetek kiberképességei és az ezekkel való akarat érvényesítésének szándéka egyre nagyobb súlyt nyom a latban. Ezért a fejlett országok ma már a kiberteret és a benne végzett műveleteket azonos szintre sorolják a többi hadműveleti tartomány képességi elvárásaival. Az államnak meg kell teremtenie, üzemeltetnie és folyamatosan rendelkezésre állónak tartania mindazt a tudást és technológiát, amelynek segítségével felkészültsége a kibertérben nagyságrendileg megegyező lehet a vele nagyjából azonos méretű vagy geopolitikai státuszú más államok hasonló képességeivel.[28] A hatékony kibervédelmi eszközökkel és módszerekkel megóvott kritikus infrastruktúrák biztosíthatják a szolgáltatásokat a gazdasági szereplők, az európai katonai műveletek, illetve a lakossági ellátás részére. A kőolajból származó hajtóanyag előállítása, tárolása, szállítása – ideértve a különböző szállítási módokat és a közlekedési infrastruktúrát is – kiemelten fontos szerepet játszanak a katonai műveletek támogatásában. Az említett szektorban működő cégek, mint beszállítók jelennek meg a piac oldaláról, akiknek képességeit és kapacitásait a védelmi erők nem tudják nélkülözni. Mindezekért, ezeknek a szolgáltatóknak a kulcsfontosságú eszközeit, infrastruktúráját, valamint az ezekkel kapcsolatos kritikus információt a megfelelő nemzetközi együttműködés eszközeivel, a hatékony előjelzés és kockázatelemzés módszereivel védeni kell. Ebbe a munkába a fenti szektorok vállalatait is be kell vonni, megkeresve az ösztönzés lehetőségeit a civil és katonai kooperáció kialakítására, egymás érdekeinek kölcsönös figyelembe vételével.

Az említetteket ösztönzik az Európai Bizottság különböző kutatásokra irányuló kezdeményezései is, mint például az évente kiírásra kerülő HORIZON Programme keretében induló projektek. Ezek kutatóműhelyeknek, nemzetközi együttműködésben szerveződő egyetemi konzorciumoknak is lehetőséget adnak a kritikus infrastruktúrák beazonosításával, kockázatok elemzésével és a kibervédelemmel kapcsolatos kutatásoknak. Az ilyen nemzetközi szinten megvalósuló tanulmányokat, vizsgálatokat, elemzéseket a kritikus infrastruktúrákat működtető polgári vállalatok, valamint az illetékes kormányzati szervek és hatóságok is támogatják, mintegy validálva a kutatások eredményeit.

Azt hiszem, a döntéshozók és piaci szereplők együttműködését remekül bemutatja a

[28] Kralovánszky 2021, 14.

Bombardier Transportation [29] mozdonyokat, vasúti személykocsikat, motorvonatokat és villamosokat is gyártó német vállalat 2020. augusztus 07-i „feedback” levele,[30] amelyet az Európai Bizottságnak küldött meg az EU kritikus infrastruktúra védelemmel összefüggő erőfeszítéseivel kapcsolatban. Ebben a vállalkozás kiemeli a vasúti kritikus infrastruktúra védelmének fontosságát, a természeti katasztrófák vagy rosszindulatú, ember általi támadásokkal szemben, valamint felhívja a figyelmet a „barátságtalan idegen tulajdon vagy idegen közvetlen befektetés” veszélyeire, amellyel nem európai államok egyre nagyobb befolyást tudnak szerezni és később gyakorolni kritikus közlekedési infrastruktúrák vagy ezek elemei felett. A Bombardier Transportation további koordinációt szorgalmaz a döntéshozók és piaci szereplők között, a vonatkozó szabályzók összevetésére más jelenleg működő kezdeményezésekkel és további konzultációt „a Bizottság az egységes piacon belüli külföldi támogatásokról” szóló fehér könyvvel kapcsolatban. Mindennek eredményeként született meg többek között „a belső piacot torzító külföldi támogatásokról” szóló (EU) 2022/2560 rendelet, amely lehetővé teszi, hogy az Európai Bizottság megvizsgálja azokat a támogatásokat, amelyeket nem európai uniós országok adnak az EU-ban működő vállalatoknak, illetve orvosolja ezen pénzek uniós piacon jelentkező negatív hatásait is, amellyel a biztonsági mellett a versenyképességi kihívásokat is igyekszik kezelni.

FELHASZNÁLT IRODALOM

AJP-4.9 Allied Joint Doctrine for Modes of Multinational Logistic Support. NATO Standardization Agency. 2013 Február

Bombardier Transportation. Feedback from: Bombardier Transportation. Berlin. 2022. augusztus 7. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Protecting-critical-infrastructure-in-the-EU-new-rules/F541603_en (Letöltés ideje: 2024. december 30.)

Bonnyai Tünde 2012. Úton a kritikus információs infrastruktúrák azonosítása és védelmük kialakítása felé. *Hadmérnök,* 7 (2): 90–105.

Bonnyai Tünde, Danyek Miklós, Görgey Péter, Kriskó Edina, Molnár Anna, Tikos Anita 2019. *Kritikus információs infrastruktúrák védelme*. Budapest: Nemzeti Közszolgálati Egyetem.

Európai Bizottság: Zöld Könyv egy Kritikus Infrastruktúra Védelmi Európai Programról, COM(2005) 576, 2005. november 17.

EU Concept for Contractor Support to EU-led military operations. Council of the European Union. Brussels, 2014.

[29] A vállalat többek között a TRAXX mozdonycsalád gyártója, amely típusokat Európa-szerte használnak vasúttársaságok, mint például a DB Cargo éa a MÁV is.

[30] Bombardier Transportation. Feedback from: Bombardier Transportation. Berlin. 2022. augusztus 7. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Protecting-critical-infrastructure-in-the-EU-new-rules/F541603_en

Horváth Attila 2010. Hogyan értessük meg a kritikus infrastruktúra komplex értelmezésének szükségességét és védelmének fontosságát? *Hadmérnök,* 5 (1): 377–386.

Horváth Attila 2016. A létfontosságú rendszerelemek és a technológiai fejlődés új kockázatai. I. rész (A biztonság változó értelmezése). *Hadtudomány,* 26. (E): 189–201.
https://doi.org/10.17047/HADTUD.2016.26.E.189

Kralovánszky Kristóf 2021. A kibertér fejlődése (második rész) – Kiberműveletek és kritikus infrastruktúrák egyes kapcsolatai. *Hadmérnök,* 16 (1): 145–160.
https://doi.org/ 10.32567/hm.2021.1.9

Muha Lajos 2015. *A kritikus információs infrastruktúrák védelme.* Budapest: RelNet Technológia Kft.

Nyitrai Mihály 2023. *A NATO műveleti logisztikai támogatás vizsgálata többszempontú döntéselőkészítési módszerrel.* Doktori értekezés. Budapest: Nemzeti Közszolgálati Egyetem.

Selga, Eriks K. 2021. *Building common ground in transatlantic cybersecurity – A Baltic approach.* Washington, DC.: Center for European Policy Analysis.

Union for the Coordination of Transmission of Electricity 2004. FINAL REPORT of the Investigation Committee on the 28 September 2003 Blackout in Italy

https://www.katasztrofavedelem.hu/109/kritikus-infrastrukturak-vedelmevel-osszefuggo-hatosagi-feladatok-jogszabalyok (Letöltés ideje: 2024. november 20.)

https://www.vg.hu/kozelet/2023/06/orosz-kibertamadas-erte-rotterdam-kikotojet (Letöltés ideje: 2024. december 14.)