ISSN 2676-9042

Vol 1, No 1-2, 2019.

2019, I. évf. 1-2. szám

Safety and Security Sciences Review

international, peer-reviewed, professional and scientific journal of safety and security sciences

Biztonságtudományi Szemle

a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

COLUMNS	ROVATOK
Material security	Anyagbiztonság
Philosophy and history of security	Biztonságfilozófia és -történet
Security policy	Biztonságpolitika
Security systems	Biztonságtechnika
Security awareness	Biztonságtudatosság
Food safety	Élelmiszerbiztonság
Economic security	Gazdasági biztonság
Military security and defense	Hadbiztonság és rendvédelem
Information security	Információbiztonság
Industrial and operational safety	Ipar- és üzembiztonság
Legal and social security	Jog- és társadalombiztonság
Book review	Könyvismertetés
Security environment	Környezetbiztonság
Traffic safety	Közlekedésbiztonság
Workplace safety	Munkabiztonság
Technical safety	Műszaki biztonság

https://biztonsagtudomanyi.szemle.uni-obuda.hu

Biztonságtudományi Szemle
Safety and Security Sciences Review
2019, I. évf. 1-2. szám
ISSN 2676-9042

Az Óbudai Egyetem Biztonságtudományi Doktori Iskola lektorált folyóirata
Peer-reviewed journal of the Óbuda University Doctoral School for Safety and Security Sciences

Rovatok	Columns
Anyagbiztonság	Material security
Biztonságfilozófia és -történet	Philosophy and history of security
Biztonságpolitika	Security policy
Biztonságtechnika	Security systems
Biztonságtudatosság	Security awareness
Élelmiszerbiztonság	Food safety
Gazdasági biztonság	Economic security
Hadbiztonsági és rendvédelem	Military security and defense
Információbiztonság	Information Security
Ipar- és üzembiztonság	Industrial and operational safety
Jog- és társadalombiztonság	Legal and social security
Könyvismertetés	Book review
Környezetbiztonság	Security environment
Közlekedésbiztonság	Traffic Safety
Munkabiztonság	Workplace safety
Műszaki biztonság	Technical safety

E számunk szerzői/authors of this issue

Beláz Annamária, Berek László, Berek Tamás,
Kollár Csaba, Rajnai Zoltán, Szakali Miklós

Biztonságtudományi Szemle – Safety and Security Sciences Review
Az Óbudai Egyetem Biztonságtudományi Doktori Iskola lektorált folyóirata

ISSN 2676-9042

http://biztonsagtudomanyi.szemle.uni-obuda.hu

A **folyóirat célja** a biztonságtudomány területén, vagy ahhoz kapcsolódó területeken dolgozó szakemberek és a téma iránt érdeklődők számára a biztonságtudomány tágan értelmezett diszciplináris keretébe tartozó tanulmányok, kutatási jelentések, beszámolók, könyvismertetők megjelentetése, s ennek révén a biztonságtudatosság és a biztonsági kultúra fejlesztése.

Megjelenés negyedévente, jellemzően magyar, eseti jelleggel idegen nyelven. Konferenciákhoz és témákhoz kapcsolódóan különszámok, tematikus számok alkalmi jelleggel magyar, vagy idegen nyelven jelennek meg.

Szerkesztőség	Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Biztonságtudományi Doktori Iskola 1081 Budapest, Népszínház utca 8. kollar.csaba@phd.uni-obuda.hu
Arculatterv	**Keserűné Balázs Tímea**
Kiadó	Óbudai Egyetem
A kiadó székhelye	1034 Budapest, Bécsi út 96/B.
A kiadásért felel	**Prof. Dr. Réger Mihály**, az Óbudai Egyetem rektora

A Biztonságtudományi Szemle folyóiratban csak két független lektor által lektorált és megjelentetésre alkalmasnak tartott tanulmányok jelenhetnek meg. A beküldött kéziratoknak formai és tartalmi szempontból egyaránt meg kell felelnie a Folyóirat weboldalán közölt elvárásoknak. El nem fogadott kéziratokat nem áll módunkban visszaküldeni.

A Biztonságtudományi Szemle folyóiratban megjelenő cikkek az Óbudai Egyetem Digitális Archívumában (ÓDA) archiválásra kerülnek.
Az Óbudai Egyetem munkatársainak és hallgatóinak a Folyóiratban megjelent tanulmányait az Egyetemi Könyvtár munkatársai rögzítik a Magyar Tudományos Művek Tárában (MTMT).

Tartalom

E számunk szerzői

BELÁZ ANNAMÁRIA (1993) okleveles közigazgatási szakértő, alapdiplomáját 2015-ben, mesterfokozatát 2017-ben szerezte közigazgatás-tudományi szakirányon a Nemzeti Közszolgálati Egyetemen. Elnyerte a Hétpecsét Információbiztonsági Egyesület által adományozott, „Az év információbiztonsági szak-és diplomadolgozata 2017" díjat diplomadolgozat kategóriában. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusza, az Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Kar jogász szakos hallgatója. 2017-ben és 2018-ban a „Nemzeti Kiberverseny" felsőoktatási szimulációs verseny főszervezője volt. 2017 óta a Bánki Közlemények című szakmai folyóirat szerkesztője. Az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán az infokommunikációs rendszerek, az információbiztonság szabályozása mellett projektmenedzsment témájú tárgyakat oktat. Kutatási területe az információbiztonsági szemléletmód kialakítása, a közigazgatás információbiztonságának fejlesztése jogi és műszaki szempontokból, a kiberbiztonság európai- és nemzetközijogi szabályozása.

BEREK LÁSZLÓ (1981) okleveles informatikus-könyvtáros, rendszerinformatikus, web fejlesztő, az Óbudai Egyetem Egyetemi Könyvtárának igazgatója. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD hallgatójaként kutatási területe az online tudományos kommunikáció biztonsága, predátor/parazita kiadók és folyóiratok veszélyei, valamint a közgyűjteményi és könyvtári biztonság optimalizálása. A Magyar Tudományos Művek Tára (MTMT) Informatikai Szakbizottságának tagja.

BEREK TAMÁS (1973) okleveles biztonságtechnikai mérnök, okleveles védelmi igazgatási menedzser, a hadtudományok habilitált doktora (PhD). Kutatási területe az objektumvédelem elmélete és gyakorlata, az objektumvédelem komplex rendszereinek alkalmazhatósága, az ABV védelmi támogatás kihívásai a 21. században, az ivóvíz-, és élelmiszer-gazdálkodás környezetbiztonsági kockázatai. A Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, a Katonai Műszaki Doktori Iskola, Hadtudományi Doktori Iskola, valamint az Óbudai Egyetem Biztonságtudományi Doktori Iskola oktatója, témavezetője. A Magyar Hadtudományi Társaság elnökségi tagja, a Vegyivédelmi és Környezetbiztonsági Szakosztály elnöke.

KOLLÁR CSABA (1971) kommunikációtechnikai mérnök, okleveles kommunikációs szakember, elektronikus információbiztonsági vezető, a közgazdaságtudományok doktora (PhD), tanácsadó, coach, mediátor. Kutatási területe a digitális kor társadalmi vetületei és gazdasági hatásai, kiemelten az információbiztonság humán aspektusa, az információbiztonság-tudatosság fejlesztése, az ember-robot interakció, az okosváros, a mesterséges intelligencia, a társadalmi kredit rendszere. A Szent István Egyetem Gazdaság- és Társadalomtudományi Kar Vezetéstudományi Tanszék, valamint a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola oktatója, témavezetője. Az Igazságügyi Minisztérium regisztrált közvetítője (mediátora), elnök a szakmai képesítő vizsgákon (OKJ). A PREMA Consulting vezető tanácsadója, mediátora és coacha, a Magyar Hadtudományi Társaság és a Humán Szakemberek Országos Szövetsége szakértője. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában gyarapítja ismereteit. 2018. negyedik negyedévétől a Mesterséges Intelligencia Konzorcium tagja.

RAJNAI ZOLTÁN (1962) mérnök ezredes, az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar dékánja, az Egyetem Biztonságtudományi Doktori Iskolája operatív vezetője, Magyarország kiberkoordinátora. Katonai tanulmányait a Zalka Máté Katonai Műszaki Főiskolán, majd a Zrínyi Miklós Katonai Akadémián végezte. 1993-tól a Zrínyi Miklós Katonai Akadémián, illetve a Zrínyi Miklós Nemzetvédelmi Egyetemen, a Nemzeti Közszolgálati Egyetem jogelőd intézményeiben dolgozott egyetemi oktatóként. A vezetésével alakult meg 2008-ban a Bolyai János Katonai Műszaki Kar és a Nemzetvédelmi Egyetem Híradó tanszékeinek összevonásával az NKE-n ma is működő híradó tanszék. 2001-ben doktori fokozatot, 2006-ban habilitációt szerzett. Elnyerte a Magyar Tudományos Akadémia Bolyai Jánosról elnevezett kutatási ösztöndíját. 2007 és 2011 között a COMMIT francia-magyar nemzetközi tudományos (K+F+I) projekt magyarországi programigazgatója volt, ezzel párhuzamosan vendégoktató Franciaországban a Rennes-i Katonai Műszaki Főiskolán. 2012-től a Puskás Tivadar Híradó Bajtársi Egyesület elnöke. Kutatási területei: minősített időszakok kommunikációs hálózatainak biztonsága, kritikus infrastruktúra védelme, információbiztonság.

SZAKALI MIKLÓS (1963) alezredes, hivatásos katona, jelenleg a NATO Nemzetközi Katonai Törzs, Védelmi Tervezési és Képességek osztályán teljesít szolgálatot. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában gyarapítja ismereteit, mint a másodéves doktorandusz hallgató. Kutatási területe a biztonság és a védelmi tervezés kölcsönhatásainak vizsgálata. A napjainkban megjelenő biztonsági kihívások új, komplex formáit és azok megelőzésének és kezelésének lehetőségeit vizsgálja. Vizsgálja a NATO védelmi tervezési rendszerének (és általában a védelmi tervezési rendszerek) alkalmazhatóságát az új típusú kihívások kezelésére.

Biztonságtudományi Szemle

http://biztonsagtudomanyi.szemle.uni-obuda.hu

OKOS RENDSZEREK LEHETŐSÉGEI ÉS BIZTONSÁGI KIHÍVÁSAI

OPPORTUNITIES AND SECURITY CALLANGES OF SMART SYSTEMS

BEREK TAMÁS[1]

ABSZTRAKT

A jövőben a populációnk meghatározó hányada városi környezetben fog élni. A nagy népsűrűség, a szűkülő élettér, a klímaváltozás számos olyan nehézséget fog támasztani, melyek megoldására intelligens rendszereket kell megalkotni a fokozódó hatások enyhítése érdekében. Ezek az okos megoldások könnyebbé teszik életünket, azonban számos biztonsági kihívást is generálnak, amelyre fel kell készülnünk.

Kulcsszavak: fenntartható fejlődés, okos megoldások, intelligens rendszerek, biztonsági kihívások

ABSTRACT

In the future, the majority of our population will live in an urban environment. The high population density, the shrinking living space, and climate change will cause many difficulties that need to be addressed by intelligent systems to mitigate the increasing impact. These smart solutions make our lives easier, but they also generate a number of security calls to be prepared for.

Keywords: sustaniable development, smart solutions, intelligent systems, security challanges

[1] berek.tamas@uni-nke.hu | ORCID: 0000-0001-8358-6139 | egyetemi docens, Nemzeti Közszolgálati Egyetem

BEVEZETÉS

A nagyvárosok lakosságának egyre nagyobb léptékű növekedése a jövőben is folytatódik egyebek mellett gazdasági versenyképességük révén. Ezzel egyidőben egyre növekvő a társadalmi igény az élhető környezet megteremtésére és fenntartására. Az antropogén eredetű környezeti tényezők mellett a klímaváltozás olyan hatásaival is számolni kell az előttünk álló évtizedekben, amelyek a városi környezetben fokozottan jelentkeznek és kedvezőtlenül befolyásolják életminőségünket. A különböző autonóm intelligens városi rendszerek fejlesztésével és azok térhódításával sorra alkalmazásba kerülnek a mindennapi életünket jobbító innovatív megoldások, melyek azonban közvetlen és közvetett hatással bírnak más rendszerekre, folyamatokra. Több más mellett ez is szükségessé tette azok összehangolását, valamint az okos város koncepció kidolgozását. A fenntartható városi mobilitás, az épületek energiahatékonyságának növelése és az életminőség javítása érdekében kifejlesztett intelligens rendszerek hozzá járulnak egyben a társadalmi ellenállóképességhez a klímaváltozás hatásaival szemben. Ezeknek az intelligens városi rendszereknek kiépítése és üzemeltetése azonban kihívásokat hív életre a biztonságtechnika területén.

Már jelenleg is többen élnek a városokban, mint vidéken, s ez az állapot az elkövetkező időszakban sem fog változni. A technikai fejlődésnek, s azon belül elsősorban a felhő alapú számítástechnikának, a big data elemzésnek, a mesterséges intelligenciának köszönhetően a városokban és a vidéken is egyre több okos megoldással lehet találkozni, a döntéshozatal megkönnyítése, a kényelem, a biztonság érdekében. Az intelligens települések koncepcióinak kidolgozása során vizsgálni szükséges a növekvő urbanizáció, az infrastruktúrák fejlesztésével, növekvő társadalmi és gazdasági elvárásokkal kapcsolatos problémaköröket a növekvő környezeti kihívások tükrében akkor is, ha technológiai képességek dinamikus fejlődése, illetve a csökkenő technológiai költségek egyre nagyobb mértékben képesek támogatni jobbító törekvéseket. (Kollár 2019)

Városi környezetben azzal a növekvő problémával kell szembe nézni, hogy az egészséget veszélyeztető mértékben növekszik a levegő szennyezettsége. Az emberi tevékenység következményeként levegőben lévő szennyező anyagoknak való kitettség egészségre gyakorolt hatása főleg tüdőt érintő súlyos rákos megbetegedések és az asztma gyakoriságának növekedését eredményezi. (Cohen et al 2004)

Ez széles skálán kihat a társadalom egészére és tekintettel arra a prognózisra, hogy a városok lakossága a jövőben növekedni fog az élhetőbb urbanizált környezet feltételeit megteremtő okos város koncepciók kialakítása kezdődött el.

Az intelligens rendszerek kialakítása jelentősen csökkentheti a környezeti ártalmakat és javíthatja életminőségünket, azonban számos olyan újabb biztonsági aspektusát mutatják meg jövőbeli környezetünknek, melyekre választ kell adnia a biztonságtechnikának is.

AUTONÓM RENDSZEREK ÉS BIZTONSÁGI KIHÍVÁSAIK

A jelenlegi világ népességi kilátások adatai alapján az urbanizáció hosszú távú hatásai már most is kitapinthatók. A városi területek népességnövekedése olyan társadalmi, technológiai és politikai feszültségeket okoz, amely a jövőben egyre nagyobb hatással bíró tényező

lesz. Az intelligens városi rendszerek kiépítésekor elengedhetetlen volt a globális megközelítés, hiszen a város fejlesztése során nyilvánvaló kölcsönhatások lépnek fel a különböző városi rendszerek között. A kiber-fizikai rendszerek már jelentős mértékben jelen vannak mindennapjainkban. A fizikai környezetet kiegészítő virtuális elemek folyamatos fejlesztése tapasztalható és ennek fényében számos, a biztonsággal összefüggő kérdés merül fel. A komplex számítógépes világ önmagában is új kihívásokat jelent a városi rendszerek számára, különösen az intelligens városi megvalósításokban. (Tokody-Schuster 2016)
Az információtechnológiában bekövetkező forradalmi változások lehetővé teszik a városi ellátási rendszerek nagy ütemű fejlesztését. Ezen a rendszerfejlesztések eredményeképp az alkalmazó szervezetek környezeti adatigénye jelentős.
A különböző ellátási szervezetek alkalmaznak olyan rendszereket, melyek a meghatározott mérőpontokról származó adatok gyors kiértése és feldolgozása révén azonnal be tudnak avatkozni raktározási, szállítmányozási vagy szolgáltatási folyamatokba az optimalizáció jegyében. Az adatok egyre nagyobb szerepet kapnak sikeres és biztos működés érdekében, így egyre nagyobb értéket is képviselnek. Ezeknél a folyamatoknál a biztonság mellett az információ-és adatbiztonságot támogató környezet megteremtése alapvető követelmény. A jelentős értéket képviselő adat és információ nem csak jogszabályok révén, hanem a szervezeti belső szabályzatokban foglaltak segítségével is védelmet kell, hogy kapjon. Ezek ki kell hogy térjenek a munkavállaló tudomására jutott bizalmas és titkos vállalati információk továbbadásának a tilalmára, a munkavállaló által használt informatikai és számítástechnikai eszközök használatára, a vállalati adatok tárolásának módjára, továbbá hozzáférés jogosultságaira is. (Kollár 2018)
A tapasztalatok azt mutatják, hogy a pontosan felépített, a felelősség- és jogköröket egyértelműen meghatározó szabályozók alkalmazása csak részben teremtik meg az érzékeny adatok védelmének feltételeit. Az alkalmazottak biztonságtudatos magatartása hatékonyan hozzájárul az emberi tényező, mint hibafaktor kockázatának csökkentéséhez. Tekintettel arra, hogy manapság az adatok gyűjtése, tárolása, feldolgozása és továbbítása informatikai eszközök segítségével történik, ezeknek az informatikai rendszerek védelme kiemelten fontos. A digitális kompetencia egyre nagyobb társadalmi fontossággal bír. Napjainkban a digitális eszközök és az internet elterjedése miatt elengedhetetlen alapszintű információbiztonsági ismeret. A kiber korszak csak néhány évtizedre nyúlik vissza. A kibertérben megjelenő támadások veszélyességét gyakran nem tudják felmérni helyesen. Hazai kutatás (Nyikes 2019) egyes eredményei is azt mutatják, hogy a Közép-Kelet európai lakosság biztonságtudatossági- és digitális kompetencia szintje szerteágazó. A lakóhely és az életkor alapján elkészített korrelációk segítségével meg lehet határozni azokat a gyenge pontokat, amelyek alapján akár kormányzati, vagy akár társadalmi összefogással szükséges segítséget nyújtani a felhasználók számára. Az informatikai rendszerek felhasználóinak jó biztonságtudatossági szintje elengedhetetlen az ipari termelés optimalizálása, valamint az intelligens ellátási rendszerek alkalmazásának kedvező hatásainak kiaknázásához.(Nyikes 2019)
A szenzitív adatokhoz történő jogosulatlan hozzáférést megakadályozó biztonsági eljárások fejlődése folyamatos. A biometrikus azonosítási módszerek alkalmazását lehetővé tevő technikai újítások azonban óriási mértékben gyorsították fel megbízhatóságuk fokozásával azok elterjedését.
A biztonságtechnika rohamosan fejlődő területe lett az ember biometrikus azonosítása. A biometrikus azonosítás eszközeinek használata életünk szerves részévé válhat a jövőben. Előnyös tulajdonságai révén olyan azonosítási módszert biztosít, amely esetében a modern

eszközöket tekintve nehéz biztonsági rést találni. A birtok, vagy a tudás alapú azonosítási módszerekkel szemben nagy előnye, hogy biometriai jegyeink folyamatosan rendelkezésünkre állnak. A modern technikai háttér fejlődése lehetővé teszi olyan biztonsági kockázatú területeken történő alkalmazását ahol a proxy kártyás, kód alapú rendszer nem alkalmazható. A kényelemhez és a megfelelő biztonsági szinthez mérten az élet minden területén alkalmazható a biometrikus azonosítás dinamikus terjedésére lehet számítani tehát a jövőben. (Kovács et al 2012)

Ezen a területen is kézelfoghatóan jelentkezik az egyének egyes biometriai jellemzőivel kapcsolatos adatainak biztonságos tárolása, melyre kiemelt figyelmet kell fordítani. A biometrikus azonosítási rendszerek térnyerésével egyre több pontos adat fog leképeződni az egyének mindennapi szokásairól, útvonalaikról stb,, melyek szenzibilitása okán további biztonsági kérdések merülnek fel. Megjegyzendő, a probléma nem újkeletű, évtizedekkel ezelőtt a térfigyelő kamerák terjedése hasonló problémákat vetett fel.

Az emberek magánéletének védettségét fenyegető újonnan megjelenő tényezők között számolnunk kell a különböző rendeltetésű pilóta nélküli repülőeszközök terjedésével is, továbbá a drónok bűnös célú használatának lehetősége a személy és vagyonvédelem területén már meglévő és a jövőben létesítendő fizikai védelmi rendszerek tervezése során is új gondolkodásmódot igényel.

A pilóta nélküli repülőeszközök polgári célú alkalmazása kezdetekben lehetővé tette elsősorban különböző rendezvények dokumentálását, katasztrófa sújtotta területek felmérését, különböző kutatási feladatok, térinformatikai alkalmazások támogatását. A fejlesztések és tapasztalatok feldolgozása lehetővé teszi a drónok alkalmazását a nagyvárosok által teremtett környezet különböző vizsgálati szempontok mentén történő feltérképezésében. A településrendezési tervezés támogatásával fel lehet mérni és módosítani a településszerkezetet, vagy akár a városi környezetben kialakuló hősziget jelenség és a hőhullámok idején megnövekvő hűtési kapacitás hatékonyságának elősegítésének érdekében épületenergetikai felméréseket lehet segítségükkel végezni.

A személy- és vagyonvédelem területén, különösen az objektumvédelem ágazatban kedvező lehetőségekkel kecsegtet a pilóta nélküli repülőeszközök alkalmazása, melyek térnyerése a mind a gazdasági, mind pedig a játékipar területén óriási léptékű volt az elmúlt évtizedben. A katonai és más egyéb célú alkalmazás mellett ezeknek az eszközöknek, különösen az alkalmazásorientált kialakítású és felszerelésű specializációinak a fejlesztését követően a magánbiztonsági célú alkalmazása várható már a közeljövőben. Az intelligens megoldások alkalmazásával, megfelelő algoritmusok révén sokoldalúan alkalmazható mobil ezközévé válhat a vagyonvédelemnek.

A pilóta nélküli repülőeszközök elterjedésével azonban a védelmi rendszereink képességeinek bővítése mellett is számolnunk kell annak biztonsági kihívásaival is a jövőben. Ezek a berendezések ugyanis eszközként jelenhetnek meg a bűnös célú elkövetők tárházában is.

A technológiai fejlődés következtében megjelenő új típusú veszélyforrások között kell számon tartani tehát drónokkal elkövetett cselekményeket. Első körben a kiemelten fontos objektumoknál szükség lehet észlelő és elfogó berendezések telepítésére. Ehhez azonban a jelenlegi technológiák fejlesztésére van szükség, elsősorban azok hatótávolságának növelése érdekében. Az előbbi mellett kihívásként jelentkezik az objektumvédelemben alkalmazott eszközök kibertámadással szembeni sérülékenysége is. Egyre több olyan berendezés kerül alkalmazásra amely önálló intelligenciával és döntési képességgel van felruházva és

emellett valamilyen felügyeleti szoftverrel folyamatosan kommunikálnak. Ez olyan támadási felületet eredményez, amely védelme érdekében a pontosabb tervezés, precízebb kivitelezés mellett gondosabb üzemeltetési magatartást kell megkövetelni a felhasználóktól. Megfelelő informatikai tudás birtokában egy külső behatoló akár mesterszintű felhasználói jogosultságokkal felülvezérelheti a komplex védelmi rendszert. Ezért a komplex objektumvédelemnek ki kell terjednie megfelelő szintű informatikai védelemre is. Figyelemmel kell tehát lenni arra, hogy az objektumvédelemben alkalmazott korszerű alrendszerek kényelmi szolgáltatásai mellett újabb támadási felület jelenhet meg, így az objektumvédelem komplexitása további aspektusokkal egészül ki. (Tóth 2018)

Az objektumvédelem, különösen egy stacioner jellegű létesítménycsoport esetében egy jól körülhatárolható terület köré szerveződik, a védelmi eszközrendszer olyan arányban történő szervezésével, amely a várható támadási irányoknak megfelelően kiépítve a veszély nagyságával arányos védelmet képes biztosítani. A jogosulatlan behatolás elleni védelemnek az utóbbi időkig néhány speciális (főleg a kritikus infrastruktúrákhoz köthető) eset kivételével elsősorban a perimétervédelmet ellátó fizikai védelmi rendszer túloldaláról indított, annak megbontásával, vagy más úton történő leküzdésével végrehajtott behatolásokra kellett felkészülnie. A pilóta nélküli repülőeszközök magánszférában történő rohamos terjedése azonban további lehetőséget nyújt a jogosulatlan behatolást elkövetők számára, ami az objektumvédelem fejlesztésének új dimenzióját nyitja meg egyben.

A drónok használata az elmúlt évtizedben jelentősen megnőtt. Különböző területeken történő felhasználásuk egyre jobban bővült. A filmipar, a térképészet, távérzékelés, és a védelmi szektor (határőrség, katasztrófavédelem) mellett a hobbi célú alkalmazása is megjelent napjainkra. A személy-és vagyonvédelem egyik legnagyobb területe az objektumvédelem. Az objektumok védelmére kiépített komplex rendszerek alkalmasak a földfelszíni és felszín alatti eredetű támadások elhárítására. A légtérből érkező támadások elhárítását nem minden szervezet tudja magának biztosítani. Ez a veszélyforrás napjainkra egyre kézelfoghatóbb a megfizethető drónok megjelenésével. A növekvő drónhasználat szükségessé teszi az objektumvédelem területén új technológiák kidolgozását és bevezetését, melyek a nem kívánatos repülőeszköz használat elhárítását szolgálják. (Heller 2017)

A pilóta nélküli légijárművek, mint a védelmet segítő mobil eszközök használata a biztonságtechnikában előirányoz néhány alapvető feltételt. Az ezen a területen alkalmazandó pilóta nélküli légijárművekkel szemben támasztott speciális követelmény az irányításhoz való hozzáférés valamint az adatok védelme, azaz, hogy az irányítópult és a drón közötti kapcsolatot úgy kell kialakítani, hogy az ne legyen zavarható, továbbá lehallgatás védett legyen. (Kovács- Viplak 2017)

A fenti és minden olyan programozható biztonságkritikus rendszer tervezése és kialakítása során a funkcionalitás elvét szem előtt tartva kiberbiztonsági szempontokat is figyelembe kell venni tehát a jövőben.

Ez a biztonsági kihívás fokozottan jelenik meg a közlekedésbiztonság területén tekintettel arra, hogy a járműiparban az autonóm, önvezető járművek fejlesztése intelligens közlekedési rendszerek kialakítása mellett viharos gyorsasággal zajlik.

Az okos város koncepciója mentén kutatások folynak az intelligens közlekedési infrastruktúra feltételeinek vizsgálata terén is. Az okos közlekedési rendszerek, mint innovatív üzleti megoldás hozzájárulnak fenntartható fejlődéshez és azon túl kényelmi funkciókkal is szolgálnak.

Az intelligens járművek, járműrendszerek elterjedésének feltétele az intelligens közlekedési infrastruktúra. Az intelligens közlekedési rendszerek alkalmazásának egyik célja lehet a gazdaságosság a szállítási kapacitás növelése révén, a kevesebb baleset elérése, és a károsanyag-kibocsátás csökkentése. Az autonóm intelligens járművek terjedésének össztársadalmi az előnyösségük. A járművek közötti kommunikáción kívül a V2X (Vehicle-to-everything) kommunikáció hozzájárul az okos város koncepcióhoz. A járművek fizikai rendszerei mellett egyre hangsúlyosabb szerep jut a kiber-fizikai komplex rendszereknek. Az autóipari fejlesztések kiberbiztonság szempontú megközelítése új és fejlődő terület. A járművek és járműrendszerek biztonságorientált alkalmazása nem csak a tervező feladata. Ahogy a hagyományos járművek is esetében is, az autonóm járműrendszerek üzemeltetői is felelősek járművük biztonságáért, így a járművek és járműrendszerek kiberbiztonságára is figyelemmel kell lenniük a jövőben. (Tokody et al 2018)

Az okos város koncepció intelligens autonóm rendszereivel számos területen a városközösség számára kedvező és hasznos kényelmi megoldásokat kínál, azonban fel kell készülnünk annak biztonsági kihívásaira is. Az egyes függetlenül, eseménvezérelten működő rendszerek, alrendszerek – akár egy objektumfelügyeleti rendszer esetében - egymásra hatással vannak mely hatásokat vizsgálni és tanulmányozni szükséges. A rendszerek védelméért felelős biztonsági vezetőknek a jövőben olyan kihívásokkal kell szembe nézniük, melyekre tudatosan fel kell készülni.

A felhasználók biztonságtudatos magatartása kialakítása mellett hangsúlyos szerepet kell, hogy kapjon a biztonságtechnikai szakembergárda felkészítése. A biztonsági vezetőnek ki kell terjesztenie az adott objektumra szakosodott biztonsági ismereteit új irányokba képzések során. Széleskörű ismeretek ugyanis elengedhetetlenek ezen a területen. (Szabó-Rajnai 2017)

A fenntartható fejlődést is szolgáló intelligens, energiahatékonyságot is szolgáló megoldások mellett is nagy bizonyossággal prognosztizálható az, hogy a társadalom energiaigénye növekedni fog. A folyamatos és üzembiztos energiaellátás kulcseleme az okos város koncepciónak. Az energetikai rendszerek - ide értve az elosztóhálózatot is – védelme fontos marad a jövőben is. Az energiaszektor sérülékenységének csökkentése és az energiahatékonyság növelése mellett jelentős erőfeszítéseket kell tenni a hálózatbiztonság területén is, ugyanis egy energetikai kollapszus bekövetkezése rendkívüli mértékű szerteágazó kihatással bír akár regionális szinten is.

Számos, az elmúlt évtizedben bekövetkezett áramkimaradást a kánikula, valamint az ebből adódó, a légkondicionálók ellátásához szükséges energiaigény váltotta ki. A rendszer gyenge pontjait gyakran az elavult technológiával felszerelt rendszerelemek jelentették és emberi mulasztások sorozata vezetett az összeomláshoz. Ezek az események több tízmillió embert érintettek. Az anyagi károk általában jelentősek voltak, repülőtereket kellett lezárni, forgalomirányító rendszerek maradtak felügyelet, valamint irányítás nélkül. A vasúti közlekedés is összeomlott. A kórházakban jelentősen megnövekedett az egészségügyi krízisesetek száma, ami elsősorban a légzőszervi megbetegedésben szenvedőket érintette. Számos haláleset is történt az idős emberek körében a létfenntartó gépek hiánya miatt. Az ivóvízrendszer szinte teljesen megbénult, a szivattyútelepek nem működtek. Ezért a víztisztító rendszerek sem voltak képesek ellátni feladatukat. (Vass et al 2015)

Az energetikai rendszer összekapcsolása a folyamatos fejlesztéseknek köszönhetően az 1880-as évektől kezdve zajlik. Az európai hálózat növekedése is a két világháború időszakától eltekintve folyamatos. Azonban annak végével és a vasfüggöny megszűnésével a rendszer elérte jelenlegi állapotát. A következő nagy lépés az Európát Észak-Afrikával valamint az Arab-félszigettel összekötő interkontinentális hálózat elkészítése jelentené. Jelen koncepció alapján ez a megvalósulás 2020-ra valósulhat meg. Az így megépülő architektúra jóval rugalmasabb, stabilabb több tartalékot tartalmazna, mint a korábbi hálózaté. Az Észak-Afrikai területek jóval magasabb lefedettséggel rendelkeznének, mint jelenleg ami részben növelné az ellátás biztonságát és olcsóbbá tenné a villamos energiát is. Azonban a nagyobb kiterjedés potenciálisan nagyobb támadási felületet is jelentene az Európán kívüli területek felől. Ezért egy olyan szigetekre bontás szükséges mely megvalósulása esetén a hálózat nem áll le teljesen, hanem adott területekre válik szét. Az így kialakult kisebb mikrogridek önműködően tartják fenn magukat egészen az újbóli szinkronizációig.(Berek et al 2018)
Az energiabiztonság jegyében kiemelt szerepe van energiahatékony megoldások fejlesztésének és alkalmazásának a jövőben. Az épületenergetikai hatékonyságot nagymértékben támogathatják a létesítményekben kiépített és üzemeltetett biztonságtechnikai rendszerek valamint épületfelügyeleti rendszerek integrált alkalmazása, mely során a vagyonvédelmi komplexum elektronikai alrendszerének érzékelői segítségével az épülethasználatra vonatkozó adatok kinyerésével és feldolgozásával közvetlenül lehet módosításokat végrehajtani épületüzemeltetési alrendszerek működésében és energiafelhasználásukban.

A társadalom fejlődését biztosító és a kutatások egyik jelentős hátterét jelentő tudásbázis megőrzése és védelme mindig is fontos feladatot jelentett. Napjainkra a világban zajló tudományos kutatások eredményei óriási számban látnak napvilágot, így ez a tudásbázis rohamos gyorsasággal bővül, amelynek gondozását hivatott, a közhiteles adatbázisokat üzemeltető könyvtárak feladata napról napra bővül különös tekintettel arra, hogy az azok által szolgáltatott adatmennyiség jó része elektronikusan tárolt és hálózati elérésű.
Az elektronikus információs rendszerek, és a könyvtári infokommunikáció jelentősége fokozódik, hiszen egyre fontosabb elemeivé válnak a 21. század könyvtárainak. Már a jelenkorban is, de a jövőben a könyvtárakban szolgáltatott állomány egyre nagyobb része lesz elérhető elektronikus, hálózaton keresztül, így a biztonsági kérdések és megoldások súlya is egyre növekszik. A könyvtári infokommunikáció biztonsága annak rendeltetésszerű működését veszélyeztető cselekmények, események és a velük szemben támasztott intézkedések együtthatása. A könyvtár által archivált és szolgáltatott elektronikus dokumentumok mennyisége már ma is meghaladja a hagyományos, fizikai hordozón megjelent állományrészt, ami a biztonságos szolgáltatás és a hosszú távú megőrzés feltételrendszerének kialakítását, biztosítását követeli meg. Sorra kell venni a fenyegetettségre adandó válaszokat, tehát a könyvtári infokommunikációs biztonság fenntartása érdekében tett intézkedéseket és eszközöket. (Berek Rajnai 2015)

ÖSSZEFOGLALÁS

A jövőben az okos-, mobil eszközök térhódítása az infokommunikációs technológiában egyértelműen megmutatkozik. Környezetünkben olyan szenzorok érzékelik folyamatosan különböző folyamatok állapotait, melyek képesek kommunikálni egymással az interneten keresztül. A technológia fejlődésének köszönhetően az internetre csatlakozó eszközök száma folyamatosan emelkedik az IoT terjedése révén, ami lehetővé teszi, hogy a mindennapos használati tárgyaink is az internetre kapcsolódjanak. Az IoT megjelenik az okosváros koncepciókban de a kritikus infrastruktúrában, is. (Haig 2018)
Az okos rendszerek a jövőben számos, a mindennapi életünket meghatározó és hatással bíró folyamatot fognak felügyelni hozzájárulva egyebek mellett kényelmünkhöz, az élhető környezetünkhöz, a fenntartható fejlődéshez, valamint a biztonsághoz. A biztonságosabb életet lehetővé tevő megoldások azonban újabb és újabb biztonsági kihívásokat keltenek, melyekre a biztonságtechnika területén is fel kell készülnünk.

FELHASZNÁLT IRODALOM

Berek László - Rajnai Zoltán (2015): A könyvtári infokommunikáció biztonsága HADMÉRNÖK 10 : 2 pp. 199-208.
Berek Lajos - Szabolcsi Róbert - Vass, Attila (2018) The Splitting of an Energy System HADMÉRNÖK (XII) I 1/2018 pp. 9-19.
Aaron J. Cohen - H. Ross Anderson – Bart Ostro - Kiran Dev Pandey - Michal Krzyzanowski – Nino Künzli - Kersten Gutschmidt - C. Arden Pope III, Isabelle Romieru - Jonathat M. Samet – Kirk R. Smith (2004): Urban air pollution in Comparative Quantification of Health Risks Global and Regional Burden of Disease Attributable to Selected Major Risk Factors Volume 1 Edited by: Majid Ezzati, Alan D. Lopez, Anthony Rodgers and Christopher J.L. Murray World Health Organization Geneva
Haig Zsolt (2018): Információs műveletek a kibertérben Budapest, Magyarország : Dialóg Campus Kiadó ISBN: 9786155945052 ISBN: 9786155945045
Hell Péter (2017): Drónelhárító rendszerek az objektumvédelemben HADMÉRNÖK 12 : 3 pp. 37-47.
Kollár Csaba (2018): A vezető személyes márkaépítésének információbiztonsági problémái JEL-KÉP: KOMMUNIKÁCIÓ KÖZVÉLEMÉNY MÉDIA 2018/I. pp. 97-108.
Kollár Csaba (2019): Az okos város és az okos vidék szimbiózisa: Utópia, fikció, vagy realitás? In: Kőszegi, Irén Rita (szerk.) III. Gazdálkodás és Menedzsment Tudományos Konferencia : Versenyképesség és innováció Kecskemét, Magyarország : Neumann János Egyetem, pp. 29-35.
Kovács Tibor - Otti Csaba (2012): A biztonságtudomány biometriai aspektusai In: Hautzinger, Zoltán (szerk.) A biztonság rendészettudományi dimenziói : Változások és hatások Pécs, Magyarország : Magyar Rendészettudományi Társaság, pp. 1-10.
Kovács Tibor -Viplak Armand Máté (2017) Drónok a biztonságtechnikában HADMÉRNÖK XII : 2 pp. 7-13.

Szabó Anikó – Rajnai Zoltán (2017) The review of the external risk factors during the operation training plan of the security guards In: Szakál, Anikó (szerk.) IEEE 15th International Symposium on Intelligent Systems and Informatics : SISY 2017
New York, Amerikai Egyesült Államok : IEEE, (2017) pp. 359-364.

Tokody Dániel - Rajnai Zoltán – Albini Attila - Ady László - Temesvári Zsolt Marcell (2018): Kiberbiztonság az autóiparban BÁNKI KÖZLEMÉNYEK 1 : 3 pp. 71-77.
Tokody Dániel - Schuster György (2016):Driving Forces Behind Smart City Implementations-The Next Smart Revolution., Journal of Emerging Research and Solutions in ICT 1.2, pp. 1-16., http://eprints.fikt.edu.mk/171/, (letöltés ideje: 2019.02.23.)
Tóth Levente (2018): A komplex objektumvédelem kihívásai napjainkban BOLYAI SZEMLE 27 : 1 p. 35
Nyikes Zoltán (2017): A Közép-Kelet Európai Generációk Digitális Kompetencia és Biztonságtudatosság Vizsgálatának Eredményei = Results of Digital Competency and Safety Awareness Assesement in Middle East Europe HADMÉRNÖK XII : 4 pp. 159-172.
Vass Attila – Berek Lajos (2015): Napenergia és az elektronikai jelzőrendszer, villamos energia hálózattól távol lévő objektumok védelmének lehetőségei Hadmérnök 24:(2) pp. 41-57. http://www.hadmernok.hu/152_04_vassa_bl.pdf

THE CHANGING ROLE OF THE EU IN CYBERSECURITY

AZ EURÓPAI UNIÓ VÁLTOZÓ KIBERBIZTONSÁG KONCEPCIÓJA

BELÁZ ANNAMÁRIA[1]

ABSTRACT

Cyberspace poses a great challenge to the traditional governance, that is mainly state-centric – it challenges the traditional concepts like security, borders, privacy and sovereignty. Legal discussions about cyberspace governance often focus on international cybercrime arrangements, international standards and national sovereignty. Due to the globalisation and the interconnected nature of cyberspace and the cross-border impacts of attacks, it has been made impossible for any organisation to manage cyberspace and cyber threats without an adequate level of cooperation with various partners and allies. This is especially relevant in certain areas of national security, as well as in the Common Foreign and Security Policy (CFSP) of the European Union.
But what does cybersecurity mean for the European Union and how its viewpoint changed through the past decades? This paper analyses the EU acquis to provide an overview on EU cybersecurity policy and to understand the challenges EU currently facing as a cyber-actor.

Keywords: European Union, cybersecurity, Common Foreign and Security Policy (CFSP), governance

ABSZTRAKT

A kibertér megjelenése kihívást elé állítja a biztonság, határok, magánélet és szuverenitás hagyományos értelmezésén alapuló klasszikus kormányzati modellt. A kibertér kormányzásával kapcsolatos jogi viták és értekezések középpontjában túlnyomórészt a nemzetközi számítógépes bűnözés, nemzetközi jogi

[1] belaz.annamaria@phd.uni-obuda.hu | ORCID: 0000-0002-8222-5283 | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

normák és a nemzeti szuverenitás kérdései állnak. Azonban a globalizáció, valamint a kibertámadások határokon átnyúló jellegének köszönhetően egyes országok vagy szervezetek önállóan, más szervezetekkel vagy nemzetekkel való együttműködés nélkül képtelenek leküzdeni a kiberbiztonsági fenyegetéseket. Az együttműködés kérdése kiemelkedően fontos a nemzetbiztonság egyes területein, valamint az Európai Unió közös kül- és biztonságpolitikájában. De mit jelent a kiberbiztonság az Európai Unió számára és hogyan változott a nézőpontja az elmúlt évtizedekben? Jelen tanulmány áttekintést nyújt az uniós jog fejlődéséről, valamint azonosítja az Európai Unió kibertérből fakadó kihívásait

Kulcsszavak: Európai Unió, kiberbiztonság, Közös Kül- és Biztonságpolitika, irányítás

INTRODUCITION

Since the first appearance of personal computers, the development of new technologies and the global digitalization poses a difficult challenge for policymaking experts since the innovative solutions not only appear at the individual but at the governmental level. This challenge requires both regulatory and defence (precisely cyber security and cyber defence) actions. International experiences show that electronic information systems, in particular, governmental and public administration systems, are a constant target of organized cyber-attacks, therefore cybercrime, information warfare, and cyber terrorism are a constant threat to public systems.

In order for the European Union to provide the highest level of security for its citizens, it is essential to tackle down the regulatory and defence challenges. The network and information systems play a crucial role in the cross-border movement of goods, services, and people. The disruption of these systems, regardless of where they occur, can affect the Member States individually, a region or the Union as a whole, therefore, the protection of these systems is vital for the EU.

Based on the EU *acquis communautaire* this paper aims to examine what cybersecurity mean for the EU, how its' viewpoint changed on cyber-related issues in the past decades, and how the current institutional and legal framework support the Union's vision to became a leading actor in the cyber domain.

THE CHANGING ROLE OF THE EU IN THE CYBERSECURITY ARENA

Due to the high level of global cybercrime and the increasing number of threats from cyberspace, cybersecurity became a top-level policy in the many states, regions, international organisations and in the European Union. (Carrapico & Barrinha 2018) The policy and debate focus on political measures and behaviour in cyberspace, they searching for an answer how to govern and control the global cyberspace. At the heart of this discussion lie the ***fundamental questions of power and control***. "But how does this play out in the specific

case of the European Union, who is claiming influence as an actor in matters of European and even global cyberspace?" (Cavelty 2018:304) Analysing the relationship between power and governance of the cyberspace is an important step towards understanding that EU's emerging role in the in virtual realm also supports its aspiration to become a leading international security actor. Existing texts and research including those specifically addressing European cyber-power (Klimburg & Tirmaa-Klaar, 2011; Dewar 2017; Christou 2017), are of a primarily policy-oriented nature, there also is a clear dominance of military or strategic voices (Carrapico & Barrinha 2017; Bendiek, 2017b).

In the past few years the idea of ***building a stronger and more resilient internal security by strengthening cyber security policy and institutions*** appeared within the EU. On 19-20 October 2017, the European Council asked for the adoption of a common approach to EU cybersecurity following the proposed ***reform package***[2], calling for 'a common approach to cybersecurity: the digital world requires trust, and trust can only be achieved if we ensure more proactive security by design in all digital policies, provide adequate security certification of products and services, and increase our capacity to prevent, deter, detect and respond to cyberattacks'.[3] But what were the antecedent actions which led to this reform?

Based on previous the research conducted by R. S. Deward (2017) and Molnár (2017) together with the latest legislative reforms, the following part of this paper will examine - in chronological order - the turning points in the EU's existence which led to the development of the current institutional structure. It is not the aim of this section to enter into a lengthy analysis of the EU's history. Such discussions have been conducted in many academic books. However, it is beneficial to briefly consider the key landmarks in the path of cyber policy development.

The beginnings 1985— 2001

In this time-period four events established particular institutional dynamics which affected the later development of cyber security policy. ***1985 Single Market***: ICT and the Internet itself, were viewed as a great opportunity for social and economic growth - thanks to the free movement of goods, services and people-, and this viewpoint led to the ***commercialisation of the cyber policy***. The economic maximalisation climaxed in the publication of the ***Bangemann Report*** in 1994. The document it contained the conceptual seeds for all elements of the EU's later discourse and "cyber" policy.[4]

After the Union's commercial interest in the ICT sector were articulated, its competences solidified in the Treaty-based codification. The ***Single European Act*** of 1987 and the ***Maastricht Treaty*** of 1992 formalised EU's role in cybersecurity by restricting its competences to "political and economic aspects"[5]. These decisions limited the Union's competence on the "soft" powers, leaving out the "hard" capabilities (meaning a militarized and centralised

[2] Joint Communication to The European Parliament tnd The Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final

[3] European Council Conclusions of 19 October 2017.

[4] The Report makes clear that economic factors such as market forces, and the creation of jobs underpin the Union's interest and strategic outlook in ICT. The protection of fundamental rights such as privacy, security and safety are core elements both in the Bangemann Report and later in the European Union Cyber Security Strategy.

[5] European Union, 1987. Single European Act., p. 1049

security governance).[6] Thus, cyber security policy took a non-military, strategic, socio-economic approach.
Under the Treaty of Maastricht, and due to the importance of the internal market info-communication technologies, and so cyber issues fell into the First Pillar. This, in one hand, enabled the EU to initiate legislation and engage proactively in the decision-making process, on the other hand, it strengthened the economical nature of the cyber policy and in the meantime separated it from the cybercriminal issues.
This focus of cyber security initiated the Commission's ***proposal for an information and network security strategy*** in 2001,[7] this is the first document representing an identifiable cyber security policy in the European Union. The document is a milestone in the cybersecurity policy, because it contained a detailed topology of cyber threats, recommended specific technical measures to improve security, defined the network and information systems (this definition was used until 2013), and highlighted the need for reliable warning and information sharing system across Europe.

The facilitating role 2002— 2006

The 2001 Proposal laid out the economic dominance of cybersecurity, and highlighted the importance of criminal justice. As a result, two new agencies were established to carry out the policy operations. Within the Europol[8] a new department was established in 2002, called ***"high-tech crime" centre*** (HTCC). The dedicated aim of this centre was tackling computer related criminal activities and online child exploitation, and serve as an intelligence hub for the EU. In this period ***ENISA*** began its operations in 2004 on Heraklion on the island of Crete[9] as a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. The Agency:

- assists the Member States in implementing relevant EU legislation,
- works to improve the resilience of EU's critical information infrastructure and networks,
- supports the development of cross-border communities,
- collates information necessary for risk analysis,
- develops joint methods to prevent security problems whilst following the development of security standards,
- creates its own recommendations, and
- acts as a counsellor for the European Commission.

[6] This viewpoint was also represented in the Petersberg Tasks of 1992, which specified, that any military action under an EU banner would be restricted to peace-making, peacekeeping and rescue. In that day this restriction seemed logical and acceptable, however, this attitude limited the EU from developing a holistic approach of cybersecurity including offensive cyber-attack capabilities.
[7] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach /* COM/2001/0298 final */
[8] The organisation responsible for coordinating Member States' police forces with the goal to combat international crime, terrorism, drug and human trafficking. It became operational in 1999.
[9] The European Network and Information Security Agency was established following a regulation passed on 10 March 2004 by the European Parliament and the Council (460/2004/EC). This was modified in 2008 and again in 2011. In 2013, the new basic regulation of 526/2013 references the agency as European Union Agency for Network and Information Security (ENISA).

During this period ***EU started to shape its role*** in the cyber domain ***by becoming a facilitator*** rather than a policy leader. It was visible from the language the EU documents used. For example, the Member States instead of being *instructed* to do something, in the new documents they were *encouraged* or *invited* to take certain actions. Above all, detailed technological measures and best practices disappeared from the *acquis*. With the publication of the Strategy for a Secure Information Society[10], this new role was made official.

The awakening 2007— mid-2016

Due to the complexity, influence, and the high level of risks these major cyber-attacks beginning with those targeted at Estonia in 2007 caused, the Union interest in cybersecurity significantly transformed. As the consequence between 2007 and 2013, ***73 of the total 143 legal documents accepted relates to cybersecurity in some extent***. The attacks against Estonia were considered as a threat to the internal market, hence EU was able to initiate legislation and undertake the fortification of digital security measures.[11]
The European Union started cybersecurity regulations in the area of ***critical infrastructure protection*** in March 2009.[12] The CIIP action plan was based on five pillars:

1. preparedness and prevention,
2. detection and response,
3. mitigation and recovery,
4. international cooperation and
5. criteria for European Critical Infrastructures in the field of ICT.

The Commission decided to follow the CIIP plan, and [13]strengthen its intention to build a ***coherent approach to cybersecurity***, although it put the ***national interests and practices into the first place***. In the same year, the Council of the European Union highlighted the need for the development of resilient and secure ICT systems and the necessity to upgrade Europe's ***technical competences***. Two Ministerial Conferences were held (Tallinn, 2009 and Balatonfüred, 2011) which led to the adoption of the European Parliament Resolution on Critical Information Infrastructure Protection,[14] the establishment of the European Forum for Member States and of the European Public-Private Partnership for Resilience; two pan-European exercise (Cyber Europe 2010 and 2012); policy recommendation by ENISA

[10] Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society - "Dialogue, partnership and empowerment" {SEC(2006) 656} /* COM/2006/0251 final */
[11] As Deward (2017:171) argues: "Economic threats are issues where the EU can act. Direct threats to national security, by contrast, are sectors where Union action is severely restricted… It needed to address, or at least acknowledge, the threat of state-sponsored aggression against national communications infrastructures and the potential impact of such incidents on the EU's financial and economic viability."
[12] Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe From Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience" {Sec(2009) 399} {Sec(2009) 400}
[13] European Commission, Brussels, 31.3.2011 COM(2011) 163 final
[14] European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security (2011/2284(INI))

on a minimum set of baseline capabilities and services; and recommendations on the functioning of national CERTs (Computer Emergency Response Teams).[15]

As Deward (2017:181) points out, as a response for ***2008's financial crisis***: "certain industrial sectors were identified where stimuli would be established to increase economic growth and employment. In a move of striking similarity to that of 1985, the digital domain was specifically earmarked for attention. As a result, a ***"Digital Agenda for Europe"*** was initiated. This was a programme intended to increase uptake of digital technology in all sectors of society – political, social and economic – and transform the EU into a knowledge-based economy." The ***Treaty of Lisbon***, which entered into force in 2009[16] codified the effects of the Estonian cyber-attacks and the financial crisis. The Treaty's core was, to improve the coherence and effectiveness of the policy-making, and policy implementing structure, with the abolition of the pillar structure, and the codification of the exclusive, shared and supporting competences of the Union. In the fields of foreign affairs and security, the role of the High Representative of the Union for Foreign Affairs and Security Policy was extended. The High Representative was to be assisted in the fulfilment of the Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP), by the new European External Action Service (EEAS) and the European Defence Agency (EDA).
The Lisbon Treaty shows the importance of cybersecurity, by specifically mentioning (Article 69 (b)) as an ***area requiring cooperation*** to support the stability of the internal market. Thanks to the abolition of the pillar structure a more holistic approach to cybersecurity became possible. Activities related to policies and jurisdiction of cyber-crime where joined up, thus the Commission gained the ability to officially support the ***Europol EC3*** (previously established high-tech centre which later transformed to the European Cybercrime Centre) and supervise the implementation of cyber-crime related regulations.
The policy-making and changing processes started in the beginning of 2007, strengthened by the Lisbon Treaty culminated in the development of the ***European Union Cyber Security Strategy*** (EUCSS) -following a long controversial negotiation process[17]-, published in 2013[18]. The vision of the EUCSS was, to build a resilient cybersecurity to maintain the global status quo, and in the same time being adaptive to new challenges. The strategy emphasises the unity of public authorities and the private sector, and the development of cyber capacities, resources and efficiency (Kovács 2018).
To achieve this goal EU level prevention, detection and management system was needed. The following actions were taken:

- ENISA's task to fortify European cyber resilience by
  - establishing minimum requirements and
  - creation of ***CERT network***

[15] For more information on CIIP policy, read: https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip
[16] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, (2007/C 306/01)
[17] The proposal for the strategy was published in two parts from which the first part is the Communication from the European Commission and the High Representative for Foreign Affairs and Security Policy on the EU Cyber Security Strategy. The second part is the European Commission's proposal for a directive on network and information security, which has later become known as a package for the NIS Directive.
[18] EU cybersecurity strategy: an open, safe and secure cyberspace - European Parliament resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP))

- the Member States adopted national cybersecurity strategies
- Launch of the ***European Cyber Security Month*** (ECSM) series in 2013
- Establishment of the ***Safer Internet Programme*** (SIP),
- Initial cybersecurity training started for public servants.

Finally, the EUCSS calls for an ***international policy,*** the 46th point reads "there is no need at present for the creation of new legal instruments at international level; welcomes, however, international cooperation to develop norms of behaviour for cyberspace, supporting the rule of law in cyberspace; considers that the updating of existing legal instruments to reflect advancements in technology should be considered and holds the view that jurisdictional issues require a thorough discussion on the subject of judicial cooperation and prosecution in transnational criminal cases." This objective includes the EUs intention to make cyberspace issues the part of its CFSP.
Although the multitude of adopted regulation during this period, the modus operandi of the EU in cyberspace remained the same: high-level information sharing and political cooperation platform. As Swilinski (2014:13) reasons "behind this state of affairs is the lack of a truly pan-European vision of the role of the EU as an agent of cyber-security on the part of particular member states as well as the whole institution. What limits the European Union most in cyber-security is its inter-governmental character and the corresponding lack of collective vision on the part of member states." But this role was about to change. How?

Repositioning EU in the cyber sector mid2016—nowadays

On the 6th of July 2016 the first piece of EU-wide cyber legislation was adopted by the Parliament. The proposal on the ***Directive on security of network and information systems*** (NIS Directive)[19] was introduced. Yet three more years were needed to finalise the document, and further shape EU's role in the cyberspace. The NIS Directive set up a new legal and institutional framework to boost the overall level of cybersecurity in the EU. It includes the following criterions:

- The Member States are required to appoint a national NIS authority and a CERT (or Computer Security Incident Response Team -CSIRT)
- Setting up an information exchange network between the Member States, and the network of national CSIRTs, to promote swift and effective operational cooperation
- Building a culture of security across every sector which are vital for the economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure
    - Businesses in these sectors that are identified by the Member States as operators of essential services (OES) will have to take appropriate security measures and to notify serious incidents to the relevant national authority.
    - Key digital service providers (DSPs -search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.

[19] Directive (EU) 2016/1148 of The European Parliament and of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

The NIS Directive is a cornerstone of the EU's response to the growing cyber threats and challenges which accompany the digitalisation of the economic and societal life. To support the implementation of the NIS Directive, the Commission released a Communication[20] which urged the Member States to harmonise their national legislations and policy with the NIS Directive as quickly as possible[21].

During 2016 other significant communications were released, like: launch of public-private partnership on cybersecurity, strengthening cyber resilience system and innovative cyber-security industry.[22] Furthermore, the Commission announced that it would bring forward the evaluation and review of Regulation (EU) No 526/2013 of the European Parliament and of the Council concerning ENISA and repealing Regulation (EC) No 460/2004 ("ENISA Regulation"). The goal of the evaluation is the reform of the ENISA by enhancing its capabilities and capacities to support Member States, and strengthening its central, operational role in the cyber field.

According to the NIS Directive a cooperation group ("***NIS Cooperation Group***") has been established, to promote cooperation and exchange of information. The Cooperation Group is supported by the work of the network of Computer Security Incident Response Teams (***the CSIRT s Network***). Its' members are the representatives of the Member States, the Commission and the ENISA.

On 13 September 2017, Jean-Claude Juncker, President of the European Commission, stated in his regular annual report on the Union: "in the past three years, we have made progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber- attacks. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks". The Commission and the EU High Representative proposed a reform package, which envisions EU's new, leading position in the cyberspace.[23]The ***reform package*** includes the following six proposal as shown in Fig. 1.

- Establishing a stronger ***European Union Cybersecurity Agency*** built on the Agency for Network and Information Security (ENISA), to assist Member States in dealing with cyber-attacks. (Proposal of the ***Cybersecurity Act***)
- Creating an EU-wide ***cybersecurity certification scheme*** that will increase the cybersecurity of products and services in the digital world.
- A Blueprint for how to respond quickly, operationally and in unison when a large-scale cyber-attack strikes.
- A network of competence centres in the Member States and a ***European Cybersecurity Research and Competence Centre*** that will help develop and roll out the tools and technology needed to keep up with an ever-changing threat and make sure our defence is as strong as possible.

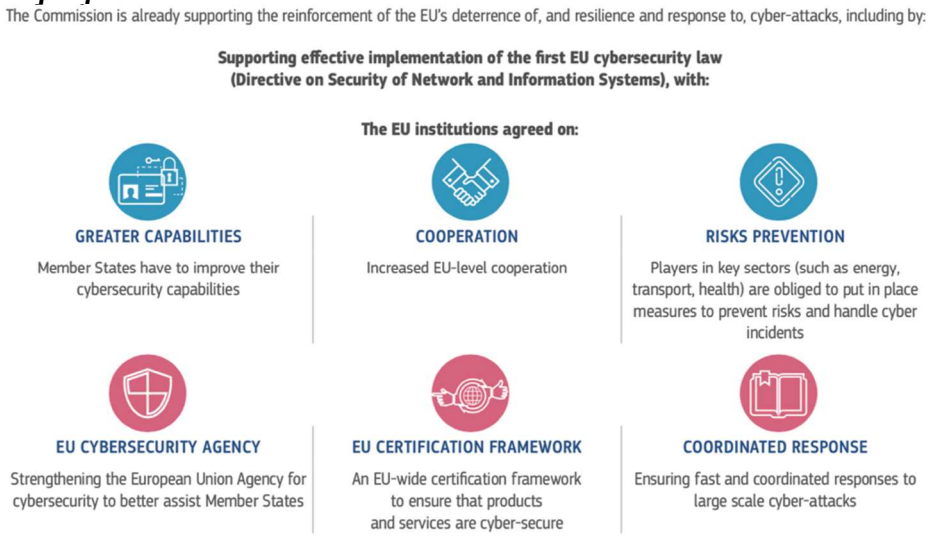
[20] Communication from The Commission to The European Parliament and the Council Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. COM/2017/0476 final

[21] Although the NIS Directive should have been implemented by May 9th 2018 in every Member State, most of them failed to succeed by the given deadline.

[22] Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final. -15 November 2016.

[23] Joint Communication to The European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU JOIN/2017/0450 final

- A Framework for a ***Joint EU Diplomatic Response to Malicious Cyber Activities*** and measures to strengthen international cooperation on cybersecurity, including deepening of the cooperation between the EU and NATO.
- Skills development for civilian and military professionals through providing solutions for national efforts and the set-up of a ***cyber defence training and education platform.***



1. Figure The cybersecurity reform package recommendations (source EU Commission)

The European Economic and Social Committee stated the following in its opinion on the "Cybersecurity Act": "So far, ***no legal framework has been able to cope with the pace of digital innovation,*** and a number of legal texts are contributing item by item to establishing an appropriate framework: the revision of the Telecoms Code, the GDPR, the NIS Directive, the e-IDAS Regulation, the EU-US Privacy Shield, the Directive on non-cash payment frauds, and so on." This means that ***the reform package is "…the recognition of the fact that the European Union is not fully prepared to handle cyber-attacks and cyber incidents,*** such as the events of 2016 ransomware attacks." (Kovács (2018)

Obviously, the Union's previous vision on its role in the cyber field as an information sharing platform, and the perception of cyber and ICT development in general as an economic issue failed. In order to reach the full spectrum of cybersecurity the Union has to adopt several new regulations, and it has to scrutinise the implementation in every Member State. The EU took a major step towards stabilisation of its new role on the 10th December 2018, when the European Parliament, the Council of the European Union, and the European Commission have reached a political agreement on the "Cybersecurity Act" [24]. ENISA's new Regulation requires a formal approval by the European Parliament and the Council of the European Union. The approval is expected in the following weeks, and after its publication in the EU Official Journal, the "Cybersecurity Act" will immediately enter into force.

The Act will replace ENISA's limited mandate to a permanent mandate and provides more resources to the agency. It establishes an EU framework for cybersecurity certification,

[24] Agreement on the „Cybersecurity Act" – European Commission Press release http://europa.eu/rapid/press-release_IP-18-6759_en.htm

boosting the cybersecurity of online services and consumer devices. This new approach is clearly a paradigm shift towards a more centralised policy-making and governance. (Bendiek 2017a)

Cooperation with the Member States

In the previous part of this paper we examined how EU's viewpoint on cybersecurity policy changed through the past few decades. In this part, we will examine the cooperation between centralised EU level and the Member States.

The Treaty of Lisbon specifically mentions the area of cybersecurity whereas cooperation between EU and Member States is needed. Though the EU's explicit goal is, to strengthen its cyber-power, the perception on cybersecurity remains economic and not security based as it should be. It is generally accepted, that cybersecurity is a multilateral field, therefore the origin of the policy initiation is irrespective, until it promotes resilience and high level of preparedness. EU's main focus in the coherent cybersecurity policy is directed to cybercrime, critical information infrastructure protection and cyber defence. Regarding to the security approach institutional cooperation and mutual understanding of security are the most important "pillars". Institutional co-operation is understood as being particularly important given that ***the European governance of cybersecurity is rather decentralized***, with relevant bodies to be found in the public and private sectors and national and international levels.

As Carrapico & Barrinha (2017:1264) highlights: "***There are co-ordination problems*** between, but also within institutions, which are related to the historical evolution of the different cybersecurity areas, as well as the perception that each area still experiences different separate challenges. It is not unusual to find projects whose objectives clash with those of other institutions. Furthermore, states, via the Council, seem to be more reluctant than other institutions (such as the European Parliament) to enhance EU powers in this area…as a consequence, ***the allocated resources are often extremely low when compared with other security areas and other parts of the world***."

The following table summarize the EU institutions currently appointed to certain particular cybersecurity related tasks:

1. Table: EU institutions dealing with cybersecurity issues

Organisation	Missions, tasks
ENISA	Issues of cybersecurity, cybercrime, network and information security
DG HOME	Development of policies, trainings and fostering cross border investigations in the area of organised cybercrime, encryption.
Europol EC3	Central hub for criminal information and intelligence; supports operations and investigations, provides highly specialised technical and digital forensic capabilities, and offers strategic analysis and training. Focuses on: cyber-dependent crime; online child sexual exploitation; payment fraud
CERT-EU	The team is made up of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, Economic and Social Committee). It cooperates closely with other CERTs in the Member States and beyond as well as with specialised IT security companies.
EU INTCEN (Intelligence and Situation Centre)	Cybercrime, cyber defence - providing intelligence analysis, early warning and situational awareness to the High Representative and to the European External Action Service
eu-LISA (European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice)	The Agency is currently managing Eurodac, the second-generation Schengen Information System (SIS II) and the Visa Information System (VIS). The agency's core mission is to be dedicated to continuously add value to Member States, supporting through technology their efforts for a safer Europe.
ECSO (the European Cyber Security Organisation) A self-financed non-for-profit organisation under the Belgian law, established in June 2016.	Collaborate with the Commission to promote (R&I) in cybersecurity; foster market development and investments. Support the widest and best market uptake of innovative cybersecurity technologies and services Promote and assist in the definition and implementation of a European cybersecurity industrial policy and support the development and the interests of the entire cybersecurity and ICT security ecosystem.
EDA (the EU Defence Agency)	Supporting the development of defence capabilities and military cooperation among the European Union Member States; stimulating defence R&T and strengthening the European defence industry; acting as a military interface to EU policies.

The ***adequate level of cooperation between national and EU level is hard to determine***. Although mandatory institutional regulations have been set up by the NIS Directive, cybersecurity in many countries still considered a sensitive issue, where sharing of information does not come naturally. Meanwhile some Member States (like France, the Netherlands and Germany) promote deeper cooperation throughout the EU, others foster cooperation on a

more regional, sub-regional level.[25] Furthermore, all EU Member States differ in their institutional systems, political preferences, cybersecurity governance models and ideologies and cyber-defence capabilities.

The Member States must establish and provide for (financial, technical, human resources) the national institutions determined by the NIS Directive. These are the:

- Competent Authority (CA): Every Member State appoint one at least, with the role to monitor the application of the Directive at a national level. The CA is to be notified in case of an incident.[26]
- Single Point of Contact (SPC): This institution exercises a liaison function to ensure cross-border cooperation. (in case of an incident, SPC is responsible to notify the other affected Member States)
- CSIRT: Institution which reside inside the CA, responsible for monitoring incidents, providing early threat warnings, responding to incidents, and cooperating with the private sector. Concrete tasks of CSIRTs have to be clearly defined and supported by national policy.

Despite the centralisation efforts, and EU's vision, that cybersecurity is a complex and transnational issue, where cooperation is crucial, the ***policy remains mostly an exclusive national prerogative*** (Renard 2014:13). Carrapico & Barrinha (2017:1266) summarises the EU and Member State level cooperation on cybersecurity with the following remarks: "Brussels often has difficulty convincing Member States of the importance of furthering integration in this area, often resorting to projects 'á la carte' where national participation is voluntary as is the case of EDA projects. The problem, however, does not stem only from the national level. The NIS Directive is a specific example which could lead to co-ordination problems and a lack of coherence, particularly regarding the division between network information infrastructure bodies and law enforcement ones, as EC3 plays a very limited role in the directive."

CONCLUSIONS

Cybersecurity is an activity, ability or capability to protect information and communications systems and the data/information contained therein. Based on this paper, in contrary with nation-states where cybersecurity is a crucial part of the national security policy, for the European Union, cybersecurity has always had an economic perception as the part of the digital single market. Cyber-related questions arise in the Common Foreign and Security Policy as well in the Common Security and Defence Policy – main areas of action are: cybercrime, critical information infrastructure protection and cyber defence

The cyber domain is a multilateral field where institutional cooperation and mutual understanding of security are the most important "pillars". Institutional co-operation is understood as being vital given that the European governance of cybersecurity is rather decentralized, with relevant bodies to be found in the public and private sectors and national and international levels.

[25] As an example the Visegrad Group + Austria founded the Central European Cyber Security Platform in 2013 to promote the cooperation and sharing of information between their CERTs/CSIRTs

[26] Article 8, par. 6 NIS-Directive.

There are several bodies and agencies in the EU at the central level, national bodies and organisations at every Member State and transnational, international organisations at the global level.
The new "Europe of security" concept is clearly a conflicting idea with the vision of multilateralism. The cybersecurity reform package proposals prefer civilian police and military defensive instruments to protect information technology infrastructures, it fosters the secure development of digital market and supports the interoperability of systems, procedures, technologies. Though, the proposals package and especially the Cybersecurity Act was accepted by the main EU bodies, the effectiveness of this reform requires a deeper engagement from the Member States. The Union as a whole, can be conceptualised as an emerging soft power in cybersecurity, underpinned with the aim to secure cyberspace through development of resilience and preparedness for large-scale cyber-attacks. Hence, it is still a question whether the Member States are willing to engage, and if yes to what extent in the new cybersecurity ecosystem. That is why the greatest challenge is the trusting relationship between all participants.

BIBLIOGRAPHY

Bendiek, A. (2017a) *A Paradigm Shift in the EU's Common Foreign and Security Policy: From Transformation to Resilience*. SWP Research Paper 2017/RP 11, October, p. 1-30

Bendiek, A. Bossong, R. and Schulze M. (2017b) *The EU's Revised Cybersecurity Strategy, Half-Hearted Progress on Far-Reaching Challenges.* SWP Comments 47, November, p. 1-7

Carrapico, H., Barrinha, A. (2017) *The EU as a Coherent (Cyber)Security Actor?* Journal of Common Market Studies 2017 Vol. 55., No. 6. p. 1254–1272.

Cavelty, M. D. (2018) *Europe's cyber-power*. European Politics And Society, Vol. 19, No. 3, p. 304–320

Christou, G. (2017) *The EU's Approach to Cybersecurity*. University of Essex Online paper series, Spring/Summer 2017

Dewar, R. S. (2017) The European Union and Cybersecurity: A Historiography of an Emerging Actor's Response to a Global Security Concern. In: O'Neill, M. Swinton, K. Eds*.: Challenges and Critiques of the EU Internal Security Strategy*. Cambridge Scholars Publishing, p. 113 - 148

Feliks Sliwinski, K. (2014): *Moving beyond the European Union's Weakness as a Cyber-Security Agent*, Contemporary Security Policy, p. 1-19.

Klimburg, A., Tiirmaa-Klaar, H. (2011) '*Cyber war and Cyber security: challenges faced by the EU and its Member States*', DG for External Policies, Policy Department, European Parliament, April.

Kovács L. (2018) *Cyber security policy and strategy in the European Union and NATO*. Land Forces Academy Review Vol. XXIII, No 1(89)

Molnár D. (2017) *Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése*. Hadmérnök. vol. 12, no. 1, p. 255-267.

Renard, T. (2014) '*The Rise of Cyber-Diplomacy: The EU, Its Strategic Partners and Cyber- Security*', ESPO Working Paper No. 7, European Strategic Partnership Observatory.

Sliwinski, Krzysztof Feliks (2014): *Moving beyond the European Union's Weakness as a Cyber-Security Agent*, Contemporary Security Policy

A MÉDIA MÉRŐSZÁMAI ÉS A DIGITÁLIS KOMMUNIKÁCIÓ BIZTONSÁGÁNAK MUTATÓSZÁMAI

INDICATORS OF MEDIA MEASUREMENTS AND KPI'S OF THE DIGITAL COMMUNICATION SECURITY

KOLLÁR CSABA[1]

ABSZTRAKT

Tanulmányomban a bevezetést követően a médiatervezés módszertani alapjait tekintem át, majd a média mutatószámainak kategóriáit ismertetem. Az online/digitális média vonatkozásában több olyan utalást is teszek a mutatószámok ismérveire, amelyek az információbiztonság mutatószámainál is megjelennek. A digitális kommunikációról szóló részt követően az információ biztonságával és sebezhetőségével foglalkozom, megnevezve az információgyűjtés, az információtovábbítás, az információ feldolgozása, az információ tárolása, valamint a humán erőforrás ellen indított támadásokat. A digitális kommunikáció biztonságának mérésénél kisebb részben az intuitív, nagyobb részben az egzakt mérésről értekezem. Kitérek a teljesítménymutatók és teljesítménymutató indexek meghatározásainak a lépéseire. Írásművemet a kommunikáció és az információbiztonság egymással párhuzamosan futó folyamatainak közös területe fejlesztési lehetőségeire tett javaslataimmal zárom.

Kulcsszavak: információbiztonság, teljesítménymutató, mutatószám, KPI, KPX

ABSTRACT

In my study, following the introduction, I will review the methodological basis of media planning, afterwards I will present the categories of the media index numbers. Regarding the online/digital media, I will give several references to the indexes' criteria, which also appear in the index numbers of information security. After the part which deals with digital communication, I will continue

[1] kollar.csaba@phd.uni-obuda.hu | ORCID: 0000-0002-0981-2385 | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

with the security and vulnerability of information, indicating the gathering, the transmission, the processing and the conservation of information, as well as the attacks launched against the human resources. Regarding the measurement of the security of digital communication, on a lesser extent I will confer about intuitive measurement, while on a larger extent I will confer about exact measurement. I will also deal with the steps of determining performance indicators and the indexes of performance indication. I will conclude my study with recommendations concerning the possibilities for development of the joint areas of the parallel processes, which are present within communication and information security.

Keywords: information security, performance indicators, performance index, KPI, KPX

BEVEZETÉS

Az adatok korában a szervezeti működést a szervezet által „termelt" megannyi adattal és információval lehet jellemezni, s a belőlük képzett szervezeti tudás, tapasztalat és bölcsesség a garancia a hosszú távú, átlátható és tervezhető üzletvitelre. A szervezeti biztonság komplex értelmezésében helyet kap a munka- és termelésbiztonság mellett többek között a gazdasági, az informatikai és információ, valamint a kommunikáció biztonsága is. A szervezeteknek érdeke, hogy a róluk szóló, általuk létrehozott és gerjesztett kommunikációs folyamatokat kézben tartsák, mivel a hibás működés közvetlen és komoly hatással lehet a gazdasági és pénzügyi teljesítményre is. Olyan megoldásokat kell kínálni a szervezeteknek, munkavállalóiknak és partnereiknek, amelyek révén minden üzenet (vagy legalábbis azok közel 100%-a) célba ér, nem veszik el, s miközben a címzett felé száguld, nem módosítja harmadik fél, illetve a tartalmát sem ismerik meg idegenek. Az online médiafelületeken biztosítani kell a hírfogyasztó biztonságát is azzal, hogy csak a számára releváns tartalmakhoz fér hozzá, illetve, hogy a releváns tartalmak valós tények, nem pedig álhírek alapján születnek. A szervezetek számára nem ismeretlenek az olyan fogalmak, melyek az adatvagyonnal, az adatok védelmével kapcsolatosak. Ez azt jelenti, hogy az adatokat csak az arra illetékes személyek ismerhetik meg, azokat csak a megfelelő jogosultsággal rendelkező emberek módosíthatják, illetve törölhetik. A (digitális) kommunikáció és az adatok és információk biztonságával kapcsolatos folyamatok és aktivitások futnak párhuzamosan a szervezetek életében, tanulmányomban arra keresem a választ, hogy lehet-e a két terület mérésének módszertanában olyan közös pontokat találni, amelyek a szervezet számára előnyöket jelentenek.

A MÉDIATERVEZÉS MÓDSZERTANI ALAPJAI

A médiatervezéssel kapcsolatban Fazekas és Harsányi (2004:315) úgy fogalmaz, hogy „a kampánytervezés azon része, melyben meghatározásra kerülnek a (média)célok, a (média)stratégia, s ez alapján a felhasználandó médiumok köre, valamint a konkrét ütemezés egy adott kampányban". Incze és Pénzes (2002:166) egy praktikusabb definíciót ismertet,

miszerint „a médiatervezés nem más, mint válaszadás néhány kérdésre: kinek, hol, mikor, milyen médiumban, milyen erősen, mennyi ideig és mennyiért hirdessünk".
Szabó D. Tamás (1999:29) a médiatervezési munka kiindulópontjának az ügynökség és a megbízó közötti szerződés mellett a briefet tartja, amelyik „rövid tömör megfogalmazásában rögzíti a főbb pontokat", s segítségével „tisztázódnak és találnak egymásra a két fél elképzelései". Nevezett a MaRS[2] ajánlására hivatkozva ismerteti a médiatervezési briefet[3], melynek tanulmányom szempontjából lényeges elemei a következők (zárójelben saját és nevezett szerző megjegyzései):

- ügyfél (akitől az üzenet származik, aki, vagy akinek a megbízásából valaki az üzenetet elkészítette)
- kampány időzítése (mikor indul, meddig tart a kampány, szezonalitás fontossága)
- háttér (piaci helyzet)
- főbb versenytársak (konkurencia tevékenységének és aktivitásainak értékelése)
- célok (mi lehet a cél? ismertség, eladás, stb…)
- célcsoport(ok) (üzenet címzettjei)
- preferált média (az üzenet mely médiában jelenik meg)
- a kommunikáció tartalma, stílusa, hangvitele
- költségek
- előírt/elvárt mutatószámok

A következőkben a média mutatószámaival foglalkozom.

A (média)mutatószámok kategóriái

Balassa és Klausz (2015), Fazekas és Harsányi(2004), Hamburger (1995), Incze és Pénzes (2002), Kollár (2004), Szabó (1999), Virányi (s.a.) többféle elv szerint foglalja csoportokba az egyes mutatószámokat, s rendszerint az adott médiumra jellemző mutatószámok/mérőszámok kerülnek egy kategóriába.
A ***nyomtatott médiánál*** többek között az elérésenkénti megjelenést (reach per issue), illetve a legnagyobb olvasottságot célszerű meghatározni. Az előbbi azt jelenti, hogy kik azok, akik rendszeresen olvassák az adott sajtóterméket. Ehhez képest magasabb értéket mutat a legnagyobb olvasottság (broadest readership), mivel itt a rendszeres olvasók és az alkalmankénti (lapszámonkénti) olvasók számának összege szerepel.
A ***klasszikus televíziónál és rádiónál*** beszélhetünk elérésről (reach), azt mutatja, hogy „egy adott műsor/csatorna a teljes nézettség milyen arányát érte el a vizsgált időszakban" (Hamburger, 1995:11). Egy másik gyakori mérőszám a nézettség (rating), amelyik azt jelentette, hogy a célcsoportba tartozó összes emberből hány százalék nézte/hallgatta az adott műsort meghatározott időben. Az affinitás (affinity) az mutatja számszerűen, hogy a célcsoport hogyan viszonyul egy adott műsorhoz, csatornához, napszakhoz (Incze – Pénzes, 2002), vagy másképp fogalmazva a médiának az a tulajdonsága, hogy „a teljes fogyasztói közül hány

[2] MaRS: „A MAKSZ Magyarországi Reklámügynökségek Szövetségeként 1995 májusában jött létre. A kommunikációs ügynökségek szövetségévé (MAKSZ) történő átalakulást elsősorban a kommunikációs szakmában dolgozó ügynökségek közös gondjai és problémái, és az ezek megoldását szolgáló együttgondolkodás és együttes cselekvés indokolta". http://maksz.com (letöltés ideje: 2018.02.10.).
[3] Mivel a MaRS átalakult MAKSZ-ra, így a brief ismertetésénél nevezett szerző, valamint a Szövetség érvényben levő Briefing Útmutatóját összevontan mutatom be. Tartalmuk gyakorlatilag azonos, a különbség nevezett szerző munkájának tartalmi tagolásában van.

százalék tartozik a célcsoportba" (Szabó, 1999). Az átlagos nézettségi idő (average time spent) azt határozza meg, hogy az adott programot, műsort átlagosan meddig nézték/hallgatták a megadott időben.
A digitális átállást követően már lehetőség van a közel 100%-os mintavételre is, mivel a digitális műsorszolgáltatást igénybe vevők csatornaválasztása, illetve az ott töltött idő adatai rendelkezésre állnak, így adatbányászat segítségével a rejtett összefüggések is felfedhetők.
Az ***online/digitális média*** vonatkozásában (internetes mérőszámok) részint az általános (weblap, klasszikus online hirdetés), részint a közösségi médiát tudjuk megkülönböztetni. Az általánosnál érdemes megnevezni a webszerverre történő kapcsolatok számát adott időben (hit), az oldalletöltések számát (page impression, vagy page view), ami a Magyar Reklámszövetség Internetes Tagozatának ajánlása alapján (idézi Incze és Pénzes, 2002:155) azt fejezi ki, hogy „hány teljes oldalt töltöttek le. Egy teljesen letöltött oldal tehát egy page impression-t eredményez, függetlenül az oldalon szereplő adatfájlok számától". Látható, hogy ez a mutató ugyan hasonlít a nézettséghez, mivel a médiahasználat mértékét méri, de az oldalletöltés nem foglalkozik a célcsoporttal. A látogatás (visit) Balassa és Klausz (2015:52) szerint az oldalra látogatások számát jelenti egy nap. Ha valaki „kétszer kattint az oldalra, az (már) két látogatásnak számít". A nevezett mérőszámok mellett az online hirdetéseknél a reklámmegjelenést (ad view), az átkattintást (click through), illetve az átkattintási rátát (click through rate) célszerű megkülönböztetni. Az első a weboldalon megjelenő adott hirdető reklámbannereit számolja, a kattintás pedig azt, hogy hányszor kattintottak a hirdetésre, illetve, hogy az oldalra látogatók, s a hirdetést látók hány százaléka kattintott a hirdetésre.
Balassa és Klausz (2015) a közösségi média típusainál a blogot, a wikit, a videomegosztást, a social networking-et, az aukciós oldalakat, a geolokációs alkalmazásokat, valamint a kiterjesztett valóság platformokat különbözteti meg.
A ***blogoknál*** a megtekintés száma (page view) alapján meghatározható, hogy adott időszak alatt hányan látogatták meg az oldalt. A blogbejegyzések többségénél vannak linkek, amelyek különböző weboldalakra mutatnak. A honlaplátogatások (website visit) azt méri, hogy a blog olvasói közül hányan kattintanak a linkre. Az oldallátogatások (pages per visit) mutató azt méri, hogy a felhasználó egy-egy látogatás alkalmával hány oldalt nyit meg, de mérni lehet vele az adott oldalon való tartózkodás idejét is. A blognál érdemes még mérni a blogra mutató linkek számát (backlinks), a feliratkozók számát (subscribers), a bejegyzések számát adott időszak alatt (number of posts published), a bejegyzések megosztását (social shares per post) is.
A ***Facebook*** vonatkozásában az elkötelezettségnek négy típusa jelenik meg Balassa és Klausz (2015) értelmezésében. A (1) hozzászólások (comments) azt méri, hogy egy adott bejegyzéshez hányan fűztek megjegyzést, a (2) like és egyéb érzelmek ikonikus jelzése azt mutatja, hogy az adott bejegyzésre hányan reagáltak érzelmi ikonokkal, a (3) megosztások (shares) száma azt méri, hogy egy bejegyzést hányan osztottak meg, (4) kattintások, mely mutató az elkötelezettség mérésénél nagyon fontos. Az elköteleződési rátát (engagement rate) a lájkok, a hozzászólások és a megosztások összege adja.
A ***Youtube***-nál mérhető többek között a megtekintések száma (views), a megtekintési idő (watched time), a feliratkozók száma (subscribers), az elköteleződés (engagement), a ***Twitternél*** az elköteleződési ráta. A ***Linkedin*** mérőszámai között fontos a kapcsolatok/ismerősök száma (total connections), a megtekintések száma (profile views), az ajánlások száma (recommendation), mely azt méri, hogy más felhasználók hányszor írtak ajánlást az adott

fiókhoz, az elérés (reach), a bejegyzések száma (posts), a kedvelések (likes) száma, illetve a hozzászólások (comments) száma.

Az utóbbi időben egyre nagyobb hangsúlyt kap az egyén mobileszközökön (elsősorban okostelefon) történő médiafogyasztása, így a média mutatószámainál egy új kategóriát lehet megkülönböztetni: a ***mobil eszközöket***. A tartalmak egy része egyaránt megjelenthet számítógépen és mobiltelefonon, a megtekintések, látogatások, letöltések, kattintások arányából következtetni lehet a felhasználók szokásaira, attitűdjeire, s lehetőség van összehasonlító elemzések elvégzésére is.
A mutatószámok médiatípus szerinti felosztása mellett léteznek a költségekhez, valamint a tartalomhoz kapcsolódó mutatószámok is.

A ***költség típusú, költséghatékonyságot kifejező mutatószámok*** azt vizsgálják, hogy bizonyos számú ember elérése mennyibe kerül, valamint, hogy mennyi egy kampány médiumonkénti költsége, illetve összköltsége. Az ezer kontaktusra eső költséget (cost per thousand) a hirdetések elhelyezési költségének és a hirdetéssel várhatóan elért személyek számának hányadosa alapján képzik. A CPP-vel (cost per point) a célcsoport 1%-ának elérési költségét mérik. Ha az online médium bevételt is termel, akkor esetében számolni lehet a felületén elhelyezett valamennyi reklámból (banner, PR-cikk, stb.) származó bevétellel (revenue), a látogatásokra jutó bevétellel (revenue per visits), illetve az oldalra jutó bevétellel (revenue per page) is, ez utóbbi a hirdetés teljes bevétele és az oldalletöltések számának a hányadosa alapján kerül kiszámításra.

A ***tartalomhoz kapcsolódó mutatószámoknál*** alapvetően nem önmagában a megtekintés, hanem annak értékelése, véleményezése kerül a fókuszba. A Facebooknál a like (tetszik) mellett az imádom, a vicces, a hűha, a szomorú és a dühítő lehetőségek közül is választani lehet, s a választott lehetőségek egymáshoz viszonyított aránya révén a tartalom fogadására, a vele való azonosulásra is következtetni lehet. Ugyancsak következtetni lehet az azonosulásra, illetve az érzelmi érintettségre a tartalmak megosztásának számai, illetve a megtekintés és a megosztás hányadosa alapján, valamint az adott tartalomhoz fűzött megjegyzések száma alapján is. Önmagában az adott oldalt követők, illetve az adott személyt ismerők száma, illetve e szám időbeli változása (progresszív, degresszív), s e változás dinamikája is enged következtetni az üzenetek tartalmának fogadtatására.

GONDOLATOK A DIGITÁLIS KOMMUNIKÁCIÓRÓL

A digitális kommunikáció meghatározásakor a definíciók két aspektusból közelítik a témát. Egyfelől digitális kommunikáció révén valósul meg minden olyan üzenet, amely digitális eszközökön keresztül történik, másfelől digitális kommunikációnak tekintjük a digitális formában küldött bármilyen típusú információt. Jelen tanulmánynak nem célja, hogy állást foglaljon a kétféle megközelítés egyike mellett, vagy, hogy megadja a két fogalom szinergikus summázatát.
Az üzenet gyűjtőkategória, melynek részét képezi a weboldalon olvasható írott tartalom, az e-mail, az SMS, az MMS, a(z okos)telefonon keresztül megvalósított beszélgetés, a számí-

tógép közvetítésével létrejött szöveges-, hang- és videochat, a blog, a wikitartalom, a közösségi média felületein folytatott diskurzusok, az online multimédiás tartalmak, s ide sorolom a tartalmakra adott válaszreakciókat is (pl.: kedvelés).
A digitális kommunikációra írásművemben úgy tekintek, mint a hagyományos világ digitális leképezése során keletkezett digitális világban, illetve a virtuális valóságra és egyéb kevert valóságokra épülő platformokon megvalósuló kommunikáció/eszmecsere, ahol az előbbi esetben a tartalmakat előbb digitális formába kell átalakítani (analóg-digitális átalakító, pl.: scanner, digitális fényképezőgép), míg utóbbinál a programozók fantáziájára van bízva, hogy milyen elvek mentén alakítsák ki a képzeletbeli világokat. Értelmezésemben a digitális kommunikáció másik sajátossága az, hogy az analóg-digitális átalakítást követően, vagy amikor az egyén belép az online világba, akkor az egy labirintushoz hasonlít, melynek komolyabb és részletesebb technikai, informatikai működését rendszerint nem kell megértenie ahhoz, az üzenetét eljuttassa a címzetthez. A shannon-waeveri modellben (1949) értelmezett küldő üzenetét kódolja (értve ezalatt, hogy leírja, elmondja, felveszi, rögzíti, stb.), majd ez a küldő által kódolt üzenet a rendszer sajátosságai szerint műszaki-informatikai értelemben is kódolódik (pl.: csomagokra bontják, címkézik, stb.) annak érdekében, hogy a vezetékes és/vagy vezeték nélküli hálózatokon keresztül eljusson a címzetthez, akinél az aktuális informatikai eszköz (pl.: számítógép, laptop, okostelefon, okostévé) előbb műszaki-informatikai értelemben dekódolja azt (pl.: összekapcsolja a csomagokat), majd a címzett dekódolja a tartalmat. A csatorna zaj, a környezeti zaj, a szemantikai és szintaktikai zaj, a fiziológiai zaj, a pszichológiai zaj és a kulturális zaj mellett a digitális környezetben számolni lehet az információ (és így az üzenet) biztonságos célba juttatását, vagy az üzenet (tartalom) elérhetőségét veszélyeztető tényezőkkel is, melyeket részint informatikai-technikai, részint humán/támadó zajnak definiálok írásomban. A következő részben az információ biztonságával foglalkozok részletesebben.

Az információ biztonsága és sebezhetősége

Az információbiztonság az MSZ ISO/IEC 27001:2006 szabvány szerint „az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá egyéb tulajdonságok, mint a hitelesség, a számonkérhetőség, a letagadhatatlanság és a megbízhatóság szintén ide tartoznak”. A bizalmasság, titkosság olyan tulajdonság, amely „biztosítja, hogy az információt jogosulatlan egyének, entitások vagy folyamatok számára nem teszik hozzáférhetővé, és nem hozzák azok tudomására”. Sértetlenség alatt a „vagyontárgyak pontosságának és teljességének védelmét biztosító”, rendelkezésre álláson pedig olyan tulajdonságot értünk, amely lehetővé teszi, hogy „az adott objektum – feljogosított entitás által támasztott igény alapján – hozzáférhető és igénybe vehető legyen”. A szabvány által leírt definíciók és azok tartalmi elemzése felveti annak szükségességét, hogy az adatokat és az információkat a szükséges mértékben védjük annak érdekében, hogy azok felhasználásával az egyén és a szervezet számára tudást, tapasztalatot és bölcsességet tudjunk képezni, vagy saját maguk tudjanak képezni. Ezt a folyamatot veszélyezteti egyfelől az adatok és információk manipulálása, módosítása, törlése, illetéktelen személyekhez kerülése, másfelől az adatokat és információkat tároló, illetve azokat közvetítő rendszerek sebezhetősége – összességében a kritikus infrastruktúrák gyenge pontjai és az ellenük indított támadások.

Munk (2008) a kritikus infrastruktúra általános fogalmát úgy értelmezi, hogy „mindazon infrastruktúrák (működtető személyzet, folyamatok, rendszerek, szolgáltatások, létesítmények, és eszközök összessége), amelyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése egy adott felhasználói kör létére, lét- és működési feltételeire jelentős negatív hatással jár". Haig (2015) a kritikus infrastruktúra elleni fenyegetések forrásánál az egyes személyeket, a jogosulatlan felhasználókat, a terroristákat, a különböző nemzeti szervezeteket, a külföldi hírszerző szolgálatokat, illetve a katonai szervezeteket azonosítja, akik a komplex információs támadást a fizikai, az információs (ezeket összefoglaló névvel technikai jellegűnek is hívjuk) és a kognitív (vagy más névvel humán) dimenziók mentén követik el. A fizikai dimenzióhoz sorolható az elektromos berendezések megrongálása, az elektromos hálózat kiiktatása például robbantással, kábelek elvágásával, fizikai rombolóerő alkalmazásával. Az informatikai dimenzió részét képezik az informatikai folyamatok elleni támadások, az adatszerzés és –manipulálás, valamint végleges törlés többek között vírusok, kémprogramok, adathalász e-mail-ek, DoS és DDoS[4] támadások révén. A kognitív dimenzióban megvalósuló támadásoknál a támadóknak nem kell komoly informatikai tudással rendelkezniük, hiszen elsősorban kommunikációs és pszichológiai ismereteik és tapasztalataik alapján gyakorolnak hatást áldozataikra, például humán típusú social engineering módszerekkel, hamis, csúsztatott, manipulált üzenetekkel, valós, a címzettek viselkedését szándékosan befolyásolni akaró hírekkel. Ezek a technikák részint a fizikai világban beszéd formájában, részint a nyomtatott és az elektronikus média segítségével jutnak célba. A támadók Haig (2015:102-103) szerint öt, egymástól jól elkülöníthető felületen támadnak:

1. Az ***információgyűjtés*** humán, vagy szenzor alapon történik, az előbbinél gyakran a nyilvánosan, legális eszközökkel megszerezhető adatok és információk (OSINT) gyűjtése zajlik. A támadás során a cél az adatok és információk gyűjtésének megakadályozása, vagy késleltetése, hamis adatok közlése, az adatok manipulálása.
2. ***Információtovábbítás*** alatt a különféle, információ továbbítására alkalmas vezetékes és vezeték nélküli hírközlési hálózatok funkcióját, részint a szóbeli közlést értjük. A támadók az adatokat és az információkat eltéríthetik, a továbbítását akadályozhatják, vagy késleltethetik, illetve jogosulatlanul férhetnek hozzá.
3. Az ***információ feldolgozása*** történhet manuális és számítógépes módon is, az utóbbinál különböző hardverek és szoftverek (programok, alkalmazások) szolgáltatják azt a környezetet, amiben a feldolgozás megtörténik. Támadás során részint a rendszerek fizikai működését szabotálhatják (pl.: áramkimaradás, rongálás), vagy rosszindulatú programokkal (pl.: vírus) férnek hozzá, vagy késleltetik az adat- és információfeldolgozást.
4. Az ***információtárolás és az adattárolás*** a feldolgozott adatok és információk tárolását jelenti részint papír alapon, részint elektronikus úton. Ez utóbbinál a támadók hamis adatokat tudnak bevinni, a meglevő adatokat törölhetik (megsemmisítés) és módosíthatják, illetve azzal, hogy az adatokhoz hozzáférhetnek, ellophatják azokat.
5. A ***humán erőforrás*** a fenti négy terület működtetésében, fejlesztésében, üzemeltetésében, az adatok és információk gyűjtésében, továbbításában, elemzésében, tárolásában vesz részt. A támadás célja, hogy a social engineering (pszichológiai és

[4] DoS és DDoS támadás: (elosztott) szolgáltatásmegtagadással járó támadás, vagy más néven túlterheléses támadás, amelynek során a támadók célja, hogy a rendszert nagyon lelassítsák, illetve megbénítsák, így a rendszer szolgáltatásai (pl.: weblap) nem érhetők el a felhasználók számára.

kommunikációs manipuláció) módszereivel kihasználják hiszékenységüket, segítőkészségüket, naivitásukat, s hozzáférést szerezzenek az adatokhoz, információkhoz, s így megszerezzék, módosítsák, töröljék azokat.

A DIGITÁLIS KOMMUNIKÁCIÓ (BIZTONSÁGÁNAK) MÉRÉSE

A fentiek alapján látható, hogy az adatok és az információk, valamint a velük kapcsolatban levő műszaki-informatikai és humán tényezők mennyire sebezhetők. Bár az ideális az lenne, ha valamennyi támadást meg lehetne akadályozni, a gyakorlatban inkább a támadások számának minimalizálására, illetve arra törekednek, hogy támadások esetén minél kisebb legyen az okozott kár, végleges adat- és információvesztés ne következzen be, s minél hamarabb vissza lehessen állítani a támadás előtti állapotot. Az info-kommunikációs rendszerek működésének leírására, illetve monitorozására kidolgozott mutató- és mérőszámok, valamint ezek feldolgozása, elemzése, a köztük levő kapcsolatok megismerése és vizuális bemutatása (adatvizualizáció) hatékonyan képes támogatni (1) a vezetőket a biztonságosabb környezet kialakításához szükséges döntések meghozatalában, illetve (2) a szakembereket abban, hogy az informatikai támadásokat minél nagyobb arányban tudják megakadályozni, illetve az incidenseket minél hatékonyabban legyenek képesek kezelni.

A média és a biztonság mérőszámai – intuitív megközelítés

A jelenlegi probléma véleményem szerint az, hogy ugyan a mutatószámok használatának kialakult gyakorlata van, s a médiatervezés során – ahogy azzal tanulmányomban már foglalkoztam – a mutatószámok meghatározása és értelmezése révén a kommunikációs kampány viszonylag egzakt módon, számszerűsítve értékelhető, s bizonyos információbiztonsági folyamatok ugyancsak egzakt mérésére is számos példa van, a két terület metszéspontjában megjelenő mérés- és kiértékelés a módszertan vonatkozásában meglehetősségen hiányos.

A digitális kommunikáció mérésénél tanulmányom média mutatószámainál leírt gondolatok jó alapot jelenthetnek. Ezek a weboldal leterheltségére, a látogatók számára, az adott oldalon eltöltött időre, az ismerősök számára, az oldalon tanúsított látogatói aktivitásokra utalnak. Miközben a kampányok sikerességeinek egyik ismérve lehet az, ha az adott kampányidőszakban jelentősen megnövekszik az oldalra látogatók száma, a kampányidőszakon kívüli kiugró látogatás információbiztonsági szempontból gyanús lehet. Ugyancsak gyanús lehet, ha ugyan sokan látogatnak az oldalra, de ott csak nagyon rövid időt töltenek el. Pozitívan értékelendő, ha valakinek/valaminek egy tudatos kampány részeként rövid idő alatt sok ismerőse/követője lesz a Facebookon, Linkedinen, de nem a megszokott kommunikációs aktivitásra utal az, ha a kampányidőszakon kívül közel egy időben 10-15 olyan személy jelöl ismerősnek, akinek nincs semmilyen közös pontja velünk.

Az intuitív megközelítés mellett a különböző mutatószámok használatával egy objektívebb képet tudunk alkotni arról, hogy az online kommunikációs felülettel kapcsolatban tanúsított aktivitás egy normális folyamat része, vagy érdemes biztonsági ellenőrzést végezni.

A folyamatok mérőszámai

A szakirodalom (Parmenter, 2010, Hubbard és Seiersen, 2016, Baroudi, 2010, Tipton és Krause, 2008, Frey, Lüthje és Reich, 2013, Zimmerman, 2017, valamint ETSI és Deloitte ajánlásai) számos mutatószám-csoportot nevez meg, úgymint: KPI (teljesítménymutató), KRI (kockázatmutató), KRA (területek eredményei), KPA (teljesítményterület), KCI (ellenőrző indikátor), KPX (teljesítménymutató index), ISI (információbiztonsági indikátor), KPSI (biztonsági indikátor) melyek közül tanulmányomban hangsúlyosan a KPI-val, illetve érintőlegesen a KPX-vel foglalkozom.
A KPI (key performance indicator – legfontosabb teljesítménymutatók) célja, hogy magas szintű áttekintést nyújtson a szervezet és főbb operatív egységeinek múltbéli teljesítményéről, amelyek szinte kizárólag a történelmi adatokra (megtörtént, rögzített események) irányulnak. A KPX (key performance index – legfontosabb teljesítménymutató index) egy vagy több KPI összefoglalója vagy korrelációja, amely jelzi a folyamat egy meghatározott területének általános teljesítményét.
A KPI-ok és a KPX meghatározásának a lépései a következők:

1. A célok meghatározása
2. Kritikus sikertényezők meghatározása
3. KPI-ok meghatározása
4. Adatgyűjtés
5. KPI-ok kiszámítása
6. KPI-okból KPX-ek meghatározása/kiszámítása
7. Szofisztikált elemzés
8. Következtetések megfogalmazása

A (1) ***célok meghatározásánál*** érdemes konkrétan megfogalmazni az elvárásokat. A szervezeti (digitális) kommunikáció biztonságosabbá tétele célkitűzés ugyan filozófiai szinten kiváló gondolat, de a gyakorlatban a célt úgy kell megalkotni, hogy abból a (2) ***kritikus sikertényezők*** meghatározhatóak legyenek. Ilyen sikertényező lehet az, hogy egy éven belül 20%-kal csökken a végpontokra (felhasználók számítógépére) érkező fertőzött e-mail-ek száma. Természetesen a sikertényezők eléréséhez szükség lehet erőforrások hozzárendelésére is, pl.: új hardver- és szoftverkomponensek beszerzése és üzembe helyezése, munkatársak (tovább)képzése, stb. A (3) ***KPI-ok meghatározásánál*** a Deloitte ajánlást ismertetem az alábbiakban (1. táblázat):

1. táblázat *A Deloitte ajánlása a KPI-lap elkészítésére (saját szerkesztés)*

KPI neve	A KPI rövid neve, verziószáma, készítés dátuma, sorszáma
KPI státusza	Kidolgozás alatt, tesztelés alatt, bevezetve, kivezetve
Leírás	A KPI leírása, mit takar/jelent az adott mutató
Feladat	Mi a feladata, mit kér a KPI, miért fontos ez a mutató
Érdekelt felek	Kire vonatkozik a KPI
Típus	Mennyiségi, minőségi, mérföldkő, küszöb, tartomány

Fontosság	Alacsony, közepes, magas
Egység/osztály	Milyen szervezeti egységet érint
Módszer	Annak a módszere, hogy hogyan kell mérni a KPI-t
Mérés tárgya	SOC[5] hatékonyság, vállalati fenyegetettség, IBIR[6], érettség…
Eszközök	Azok az eszközök, amelyek a mérést és jelentést támogatják
Gyakoriság	Nap, hét, hónap, negyedév, év, több, mint egy év
Megjegyzés	Kiegészítő információk. A szabály megalkotásához, vagy a szabályozáshoz szükséges?

A KPI-lap összefoglalja az adott KPI-val kapcsolatos fontosabb tudnivalókat. Ezek közül a típus ötféle KPI-t különböztet meg, úgymint:

1. Kvantitatív: objektíven merhető, mennyiségi adatok: bejelentett biztonsági események száma
2. Kvalitatív: minőségi adatok: különböző tesztek eredményei
3. Mérföldkő: bizonyos időpont, vagy tevékenység elvégzésének dátuma: tanúsítvány felülvizsgálati ideje
4. Küszöbérték: elér valamilyen szintet, vagy beleesik valamilyen tartományba: informatikai incidensek gyakorisága tartósan átlag feletti szinten van
5. Tartomány: minimum és maximum értékek, melyek között a mért érték elfogadható

A fontosság és a gyakoriság között a gyakorlatban kapcsolat van. Azok a teljesítménymutatók, melyekről úgy döntöttek az információbiztonsági szakemberek, hogy fontosak (magas), azok méréséhez erőforrásokat is rendeltek annak érdekében, hogy a mérés gyakorisága biztosítható legyen.

Az (4) ***adatgyűjtés*** előtt meg kell határozni azokat a mérőpontokat és eszközöket, ahonnan az adatokat gyűjteni lehet. Mivel a digitális kommunikáció biztonságának mérésénél nem csak a gazdasági, hanem a biztonság-fókuszú mutatószámok megalkotása is cél, ezért rendszerint a szervezetbe érkező adatforgalmat fogadó/küldő hálózati eszközök, routerek, tűzfalak, stb. valamint az ezeken futó szoftverek és alkalmazások jelentik azokat a mérőpontokat, amelyek adatokat tudnak szolgáltatni. A gyakorlatban az alábbi dolgok mérése szükséges:

- Idő
    - Válaszidő
    - Reakció idő
- Mennyiség
    - Db.
    - Érintettek száma
    - Adatok, információk mennyisége

[5] SOC: Security Operations Center, Biztonsági Központ, a szervezetnek az a része (osztálya, részlege), amelyiknek az a feladata, hogy megelőzze és elhárítsa a szervezet ellen irányuló kibertámadásokat, valamint naprakészen tartsa a szervezet információ- és informatikai biztonsági rendszereit.

[6] IBIR: információbiztonsági irányítási rendszer

- Költség
- Stb.

Az eszközök és a szoftverek/alkalmazások működésével kapcsolatban – jobb esetben – folyamatosan gyűjtenek és rögzítenek adatokat a logfájlokba, s a fejlettebb rendszereknél arra is lehetőség van, hogy amennyiben a meghatározott szint fölé/alá kerül egy érték, vagy elér egy bizonyos szintet, akkor a rendszer riasztást küldjön a szakembereknek.
A (5) ***KPI-ok számítása*** rendszerint egyszerű feladat, mivel vagy eleve a mért adat egyben KPI is lehet (pl.: a szervezetbe meghatározott idő alatt érkező e-mail-ek száma), vagy könnyen kiszámítható (pl.: a szervezetbe érkező fertőzött e-mail-ek aránya az összes e-mailhez képest). Néhány példa a KPI-okra:

- Adott idő alatt a felhasználók által küldött e-mail-ek
- Adott idő alatt a felhasználók által fogadott e-mail-ek
- A küldött e-mail-ekből hány % volt fertőzött
- A fogadott e-mail-ekből hány % volt fertőzött
- A biztonságos/folytonos üzletmenetet veszélyeztető kockázatok előfordulási gyakorisága
- Fenyegetésfajták száma/aránya
- Naponta/hetente/havonta mennyi időt áll az info-kommunikációs rendszer
- A jelzéstől az incidens kezelésének a megkezdéséig eltelt idő
- Átlagos ügykezelési idő
- Hibásan spamnak minősített üzenetek aránya

(6) ***KPI-okból KPX-ek meghatározása***. Az említett szakirodalmak nem egységesek a KPI-ok számát illetően. Azok a szerzők, akik nem foglalkoznak a KPX-ekkel, egy bizonyos terület mérésére maximum 8-10 KPI-t javasolnak, míg azok, akik számára a KPI csak jó alap a KPX-ek meghatározásához, inkább a KPX-ek számát maximalizálják 8-10-re, s a KPI-okkal kapcsolatban általánosságban úgy fogalmaznak, hogy annyi KPI-nak kell rendelkezésre állnia, hogy a KPX-ek az elvárt gyakoriság és pontosság mellett legyenek meghatározhatók. A KPX-ek a KPI-okhoz képest komplexebb jelentéssel bírnak, s lehetővé teszik kevesebb mutatószám mellett is a digitális info-kommunikációs folyamatok viszonylag egzakt nyomon követését, ellenőrzését. KPX írja le többek között a rendszer rendelkezésre állási idejét, a hálózati infrastruktúrát, a jogosultságkezelést, az info-kommunikációs eszközökön futó szoftverek és alkalmazások frissítéseinek a kezelését. A KPX-ek és az ezeket támogató KPI-ok megalkotása összességében megalapozott segítséget nyújt az olyan kérdések eldöntéséhez, hogy a szervezet változtasson-e stratégiai irányt az információbiztonság területén (ami közvetlen hatással van a szervezeti kommunikációra is), hogyan lehet támogatni a szervezet vízióját, misszióját és stratégiáját. Mivel a KPI-ok és a KPX-ek gyakran a vezetőknek szóló, jelentésekben is szerepelnek, ezért nagyon fontos, hogy a nem informatikai végzettséggel rendelkező menedzsment is értelmezni tudja ezek tartalmát. Pl.: a KPI-ok/KPX-ek alapján meghatározták, hogy a közösségi média munkahelyi használata veszélyt jelent a szervezet számára. A vezető ilyenkor olyan döntést hoz(hat), hogy tiltja ezeknek a használatát, holott ezzel a szervezet kommunikációs igazgatóságának/osztályának a munkáját is megnehezíti. A helyes döntés ilyenkor inkább az, hogy felülvizsgálják az adott munkakörhöz tartozó informatikai és kommunikációs jogosultságokat, majd ennek alapján

bizonyos munkaköröknél továbbra is engedik a közösségi média használatát, de ezzel párhuzamosan a használóknak egy biztonságtudatosságot erősítő rövid képzést is tartanak.
Bár már a KPX-ek is komplexebb képet adnak a KPI-okhoz képest, az info-kommunikációs rendszer és környezete (értve ezalatt a belső-külső humán kommunikációs ágenseket is) működésének a vizsgálata amellett, hogy új és izgalmas terület, sokkal hatékonyabbá tudja tenni a szervezeti biztonság védelmét jelen és jövő időben egyaránt. A (7) ***szofisztikált elemzés*** révén megalapozott válaszokat lehet találni a rendszer és környezetének megannyi eseményére többek között az alábbi elemzési módszerek segítségével:

- Okok értelmezése
- A rendelkezésre álló tények elemzése
- Idősoros elemzés: trendvonal, szezonalitás, prognózis
- Gyakoriság, átlag, módusz, medián, terjedelem, szórás
- Becslés
- Valószínűségszámítás
- Korrelációszámítás
- Hálózatkutatás, szociometria -> KPI-metria
- Adatvizualizáció
- A használt KPI-ok/KPX-ek újragondolása

Az elemzés után a folyamat zárásaként a (8) ***következtetések megfogalmazása*** következik. Miközben a kommunikációs kampányok mutatószámainak elemzésekor rá lehet mutatni, vagy következtetni lehet a kampány erős és gyenge oldalaira, a hiányosságokra, az alul- illetve felülteljesítés okaira, addig a KPI-ok és KPX-ek alkalmazásának első időszakában rendszerint nem a következtetések megfogalmazása a legfontosabb, hanem – ahogy a hetedik pontban utaltam rá – a használt KPI-ok/KPX-ek újragondolása annak érdekében, hogy a szervezet ki tudja alakítani azt a mérési rendszert, amelyiknél hosszabb távon már csak kisebb korrekciókra van szükség. Ezért is fontos a KPI-lapokon feltüntetni a teljesítménymutató verziószámát, a készítés és az aktualizálás/frissítés dátumát. A szervezetek infokommunikációs rendszere mérésének ebben az érettségi szakaszában az teljesen elfogadott, hogy a KPI-okat és a KPX-eket cserélgetik, esetleg a mérési pontok helyében, vagy az azok által szolgáltatott adatok mintavételezési gyakoriságában változtatnak.

ZÁRÓ GONDOLATOK

A szervezet céljaiért elkötelezett munkatársainak érdeke, egyfajta belső késztetése, s bizonyos esetekben munkaköri kötelessége is, hogy kommunikáljanak a szervezet külső és belső érintettjeivel, reagáljanak a szervezettel kapcsolatos hírekre, megjegyzésekre, munkálkodjanak a szervezet márkájának és különféle márkadimenzióinak a kommunikációján. Ugyancsak érdeke a szervezet céljaiért elkötelezett munkatársainak, hogy mindent megtegyenek annak érdekében, hogy a szervezet a biztonság komplex értelmezésében – s így az információbiztonság és a gazdasági biztonság területén is – minél alacsonyabb kockázat mellett működjön. Rendszerint belső szabályzatok foglalkoznak azzal, hogy a szervezet mely munkavállalói nyilatkozhatnak a szervezettel kapcsolatban, illetve, hogy milyen helyes és biztonságtudatos magatartást kell tanúsítania a munkavállalóknak. A párhuzamos gondolatmenet mentén az is megállapítható, hogy a szervezetek kommunikációs aktivitásai mellett már

a szervezetek információbiztonsági folyamatai is mérhetők. A feladat az, hogy ezek az egymással gyakorlatilag párhuzamosan futó területek minél hamarabb találkozzanak annak érdekében, hogy az információbiztonság ne menjen a kommunikációs aktivitás rovására és fordítva, a kommunikációs aktivitások ne veszélyeztessék az információbiztonságot. Tanulmányomban azt szerettem volna érzékeltetni, hogy a két területnek számos olyan közös pontja van, amelyik lehetővé tudja tenni az együtt gondolkodást, s a kellő intelligenciával bevezetett és elemzett, az információbiztonsághoz kapcsolódó mutatószámok nem csak az információbiztonság, hanem a (digitális) kommunikáció biztonságosabbá és ezáltal hatékonyabbá tételében is lehetőséget jelentenek. Jelenkorunkban, az adatok korában ugyanis a szervezetek valamennyi folyamata mérhetővé válik, de ezek a területenkénti mérések csak akkor vezetnek eredményre, ha az elemzések során a komplex szemléletmód, a valamennyi terület fejlődését szem előtt tartó vezetői döntések érvényesülnek.

FELHASZNÁLT IRODALOM

Balassa Lilla – Klausz Melinda (2015): *A közösségi média mérése. Hogyan elemezd a mutatókat és hozz ki minél többet az oldalaidból*. szerzői kiadás, Veszprém.
Baroudi, Rachad (2010): *KPI mega library*. author's edition, Scott Valey.
Deloitte (2006): *You Can't Manage It If You Can't Measure It*.
Európai Távközlési Szabványok Intézete (ETSI) ajánlása „Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection" címmel.
http://www.etsi.org/deliver/etsi_gs/ISI/001_099/003/01.01.02_60/gs_isi003v010102p.pdf (letöltés ideje: 2019.01.10.)
Fazekas Ildikó – Harsányi Dávid (2004): *Marketingkommunikáció*. Szókratész Külgazdasági Akadémia, Budapest.
Frey, Stefan – Lüthje, Claudia – Reich, Christoph (2013): *Key Performance Indicators for Cloud Computing SLAs*. EMERGING 2013: The Fifth International Conference on Emerging Network Intelligence.
Haig Zsolt (2015): *Információ, társadalom, Biztonság*. NKE Szolgáltató Kft, Budapest.
Hamburger Béla (1995): *A médiatervezés módszertana*. Magyar Reklámszövetség, Budapest.
Hubbard, W. Douglas – Seiersen, Richard (2016): *How to measure anything in cybersecurity risk*. John Wiley & Sons, New Yersey.
Incze Kinga – Pénzes Anna (2002): *A reklám helye. A hatékony médiatervezés és –vásárlás kézikönyve*. Stardust Publishing Kft, Budapest.
Kollár Csaba (2004): *Reklám- és reklámszöveg kutatás*. PREMA Consulting, Budapest.
Magyarországi Kommunikációs Ügynökségek Szövetsége: Briefing útmutató médiatenderek esetén. http://maksz.com/downloads/mediaugynoksegi-briefing-utmutato.pdf (letöltés ideje: 2019.01.10.)
MSZ ISO/IEC 27001:2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Következmények.
Munk Sándor (2008): *A kritikus infrastruktúrák védelme információs támadások ellen*. In.: Hadtudomány, XVIII. évf., 2008/1, 95-106 p.
Parmenter, David (2010): *Key performance indicators*. John Wiley & Sons, New Yersey.

Shannon, Claude E. – Weaver, Warren (1949): *THE MATHEMATICAL THEORY OF COMMUNICATION*. The University of Illinois Press, Urbana.
Szabó D. Tamás (1999): *Médiatervezés a reklámban*. Budapesti Közgazdaságtudományi Egyetem, Budapest.
Tipton, Harold F. – Krause, Micki (szerk., 2008): *Information Security Management Handbook*. Auerbach Publications, Boca Raton.
Virányi Péter (szerk., s.a.): *Fogalomtár a reklámról*. KOTK, Budapest.
Zimmerman, Timothy A. (2017): *Metrics and Key Performance Indicators for Robotic Cybersecurity Performance Analysis*. National Institute of Standards and Technology, https://doi.org/10.6028/NIST.IR.8177 (letöltés ideje: 2019.01.10.)

AZ ELRETTENTÉS ÉS A RESILIENCE EGYSÉGE

UNITY OF DETERRENCE AND RESILIENCE

RAJNAI ZOLTÁN[1], SZAKALI MIKLÓS[2]

ABSZTRAKT

A cikkben egy régi koncepció újjászületésére szeretném felhívni a figyelmet, amely ugyan a 2016. évi NATO csúcstalálkozójának döntései közé tartozott, azonban nem kapott elég figyelmet és így nem vált közismertté. Fontosnak tartom annak megértését, hogy a resilience hogyan erősíti a NATO elrettentésre es kollektív védelemre épülő stratégiáját. Érdemes áttekinteni a biztonsági körülmények változásait is, amelyek életre hívták, majd megszüntették aztán ismét feleleventettek a koncepciót. A magyar szabályozáson keresztül pedig röviden összehasonlítom a témakörben az EU es a NATO megközelítésbeli különbségeit illetve javaslatot teszek a követelmények összehangolására.

Kulcsszavak: elrettentés, resilience, kollektív védelem**,** NATO csúcstalálkozó

ABSTRACT

In this article I would like to draw your attention to the renascence of an old concept, which was among the decisions of the NATO Summit in Warsaw 2016 but it did not receive enough attention to become generally known. I consider it very important to understand how resilience strengthens NATO`s deterrence and collective defence the basic strategic essence of the Alliance. It also helps better understanding if we look into the continuous changes of the security environment which first brought resilience into being, than abolished and now revitalized it again. Through the Hungarian regulation of this field I compared the EU`s and

[1] rajnai.zoltan@bgk.uni-obuda.hu | ORCID: 0000-0002-9139-736X | egyetemi tanár, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] mszakali@hotmail.com | ORCID: 0000-0002-8983-3855| doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

NATO`s different approaches and focuses in development of resilience and made a suggestion for synchronization of requirements.

Keywords: deterrence, resilience, collective defence, NATO Summit

BEVEZETÉS

A 2016-os NATO Varsói Csúcstalálkozója (NATO Warsaw Summit Communiqué, 2016) egyértelműen a 2014-es walesi csúcstalálkozó döntéseinek (NATO Wales Summit Declaration, 2014) megerősítéséről és továbbviteléről szólt, tekintettel az időközben folyamatosan romló biztonsági környezet kihívásaira. A varsói csúcstalálkozó záródokumentumának 5. pontja felsorolja mindazokat a széles skálán mozgó biztonsági kihívásokat és fenyegetéseket, amelyek megkövetelik a Szövetség reagálását. Így a felsorolás magában foglalja az állami szereplők által jelentett hagyományos katonai fenyegetést, a nem-állami szereplőkre jellemző terrorizmust, a kiber és hibrid hadviselési formákat, valamint a tömeges migrációt, amelyek mind veszélyt jelentenek a NATO szövetségesek biztonságára és egyre kiszámíthatatlanabbá teszik a biztonsági helyzetet.

Mindezek alapján a Szövetség megerősítette elkötelezettségét a kollektív védelem és az elrettentés stratégiája iránt, amelyet az alábbi döntésekkel nyomatékosított.

Készenléti csoportosítást hozott létre „***megerősített előretolt jelenlét***" (enhanced forward presence) megnevezéssel, amely keretében négy zászlóaljharccsoport (összesen 4000-5000 katona) települ Lengyelország és a három balti NATO-tagállam területére, így erősítve meg a szövetség keleti szárnyát. A déli szárnyon pedig egy Romániában felállításra kerülő többnemzeti dandár biztosítja az elrettentéshez és védelemhez szükséges jelenlétet a Fekete-tenger térségében az „***arányos előretolt jelenlét***" (tailored forward presence) keretében.

A varsói csúcstalálkozón döntöttek arról is, hogy a váratlan és meglepetésszerű katonai fenyegetések kezelésére létrehozott Nagyon Magas Készenlétű Összhaderőnemi Kötelék (2-5 nap) (Very High Readiness Joint Task Force – VJTF) létszámát növelik, az egységben résztvevő hét keretnemzet számára pedig rotációs tervet dolgoznak ki 2022- ig. A főtitkár szerint a VJTF nem csupán a szövetség keleti szárnyán, de Dél-Európában is alkalmazható lesz. A NATO Reagáló Erőinek (NATO Response Force – NRF) erejét jelentősen megnövelik, így az NRF hadosztály szintű szárazföldi komponense megfelelő légi, tengeri és különleges műveleti támogatást fog kapni, az alkalmazott erők összlétszáma 40 ezer fő körül várható.

Szintén Varsóban jelentették be, hogy a NATO rakétavédelmi rendszere elérte az kezdeti készenléti állapotot (Initial Operational Capability), valamint a NATO Állandó Haditengerészeti Erőinek (NATO Standing Naval Forces) tovább növelik a képességeit.

A fentiek alapján teljes joggal, a varsói csúcstalálkozó a kollektív védelemre való elkötelezettség megszilárdításával, valamint az elrettentés és védelem stratégiájával válik emlékezetessé és vonul be a történelembe.

Ezek után nem véletlen, hogy a legfontosabb és egyben leglátványosabb döntések kerültek mind a szakértők, mind pedig a közvélemény figyelmének központjába. Ezért a cikk további részében egy olyan képességre szeretném felhívni a figyelmet, amely szorosan az elrettentés és védelem stratégiájához tartozik, azonban – méltánytalanul - lényegesen kevesebb érdeklő-

dést váltott ki még szakmai körökben is és nem került be a köztudatba. Ez a képesség a resilience, amelyet ugyan megemlítenek a zárónyilatkozat 4. pontjában (NATO Warsaw Summit Communiqué, 2016:4. p.), illetve egy egész bekezdést szentelnek a kérdésnek a 73. pontban (NATO Warsaw Summit Communiqué, 2016:73. p.) azonban a fentiek ismeretében ezek a pontok nem vonzottak magukra kiemelt figyelmet.

A RESILIENCE JELENTÉSE ÉS TARTALMA

Fontosnak tartom tisztázni a resilience szó jelentését és tartalmát ahhoz, hogy megértsük a fontosságát. A (Lasconjarias, 2017) több megközelítésből is vizsgálja a resilience szó jelentését és tartalmát, amely szerinti fordítása rugalmasságot, stressz tűrő képességet, illetve visszapattanást jelent. Elsődleges tartalma a fizika anyagvizsgálat tudományából származik, amely az anyag azon képességét írja le, ahogyan az anyag külső fizikai hatást követően visszanyeri méretét és alakját. Később az ökológia is átvette ezt a fogalmat az ökológiai rendszerek azon tulajdonságainak kifejezésére, hogy a rendszer mennyi változást képes elnyelni és feldolgozni úgy, hogy közben megőrzi életképességét. A biztonságtudományok körében is népszerűvé vált a resilience az alapértelmezett visszapattanás (bounce back) jelentéssel, arra a jelenségre utalva mikor egy normálistól eltérő helyzetből (politikai, gazdasági, katonai, stb.) helyreáll a rend és működőképesség. A másik fontos megállapítás, amelyet a biztonságtudomány felismert és elismer, hogy általánosságban nem létezik teljes biztonság. Különösen a jelenlegi teljesen kiszámíthatatlan biztonsági környezetben nem lehet erre alapozni, tekintettel a kihívások széles skálájára, a természeti katasztrófáktól, a terrorista támadásokon keresztül a nukleáris és hagyományos hadviselés eshetőségéig. Ezekben a helyzetekben lehetetlen biztosítani a teljes védelmet és a sértetlenséget, ezért előtérbe kerül az estleges csapások túlélésének, következményei kezelésének fontossága, valamint a csapásokból való talpraállás, felépülés képessége.
Elfogadott definíció hiányában a resilience általános értelmezése (Lasconjarias, 2017:2) szerint ***„a közösség, a szolgáltatások, egy ágazat/terület vagy infrastruktúra képessége a pusztító kihívások felismerésére, megakadályozására, vagy ha szükséges az ellenállásra, illetve a következmények kezelésére és a következmények hatásaiból való felépülésre.”*** Mint látjuk a resilience fogalmát tágabban kell értelmezni, mint az infrastruktúrák, szolgáltatások és egyéb fizikailag megjelenő dolgok és tevékenységek összességét, az a társadalom egészére érvényes. Felmerül a kérdés, hogy milyen összefüggés van az elrettentés és védelem valamint a resilience között, amikor ezek egymástól teljesen eltérő tartalmú tevékenységek.

- Jelen esetben a védelem és a támadás (elrettentés) egységéről és egymást kiegészítő hatásáról beszélhetünk. Sporthasonlattal élve csak támadójátékkal, megfelelő védekezés nélkül még egy csapat sem nyert jelentős mérkőzést.
- A resilience részét képezi annak a „társadalmi szerződésnek” amely az állam és az állampolgárok között létrejön minden demokratikus társadalomban, vagyis az államnak törődnie kell a polgárai védelmével és biztonságával. Ezek a közös értékek jelentették a Szövetség létrehozásának alapját és továbbra is ezen értékek határozzák meg a működését, ezért a Szövetség elvárja a tagállamaitól is a közös értékrend követését.
- Biztosítani kell a hátország biztonságát és működőképességét. Egy összeomló, demoralizált hátország nem képes támogatni az elrettentésre irányuló katonai törekvéseket. Egy vezetetlen, gazdaságilag működésképtelen és a mindennapos túlélésért küzdő tár-

sadalom nem képes biztosítani az elrettentéshez szükséges erőforrásokat sem, és a morális támogatást sem, inkább erodálja a katonai erőfeszítéseket, gyengíti az elkötelezettséget.

- A felkészületlenül ért csapás, válsághelyzet következményeinek kezelése, hatásainak felszámolása vagy minimalizálása, illetve az eredeti helyzet visszaállítása nem tervezett erőforrásokat vonhat el a katonai műveletektől, ezzel is csökkentve a közös erőfeszítés hatékonyságát, illetve előnyt biztosít az agresszor részére.
- A hátország védelme és működőképességének fenntartása mellett a szövetséges műveletek sikerének előfeltétele a polgári eszközökre és szolgáltatásokra való támaszkodás. Kiterjedt műveletek esetében közel 90%-a a katonai szállításoknak polgári eszközök igénybevételével történik, amelyet a magánszektor biztosít.
- A katonai kommunikáció több mint 50 %-a a polgári műholdakon és hálózatokon keresztül kerül végrehajtásra.
- A Befogadó Nemzeti Támogatás/BNT (Host Nation Support/HNS) kb. 75 %-a a helyi kereskedelmi infrastruktúrákból és szolgáltatásokból kerül biztosításra.

Mindezek alapján nem nehéz belátni, hogy a NATO műveletek szempontjából is kiemelkedő szerepe van a hátország, a polgári szektor működőképessége megőrzésének, fenntartásának. A fentiek alapján érthetővé válik az a kijelentés, hogy az elrettentés és a resilience ugyanannak az éremnek a két oldala. Egyik sem létezhet a másik nélkül. Ugyanakkor a resilience következtében biztosítható támogatások a szövetségesek közötti arányos tehervállalásnak (fair burden sharing) is részét képezik, amely jelenleg a Szövetség egyik leginkább figyelembe vett alapelve.

Felmerül a gondolat, vajon a resilience egy teljesen új követelmény, nem volt még ilyen soha? A válasz ismét egyszerű, a koncepció nem új, már volt ilyen a Szövetség történetében. A Szövetség alapító okirata is foglalkozik a kérdéssel a 3. cikkelyében (North Atlantic Treaty, 1949: 3. cikk) : „***Azért, hogy a szerződés célkitűzéseit hatékonyabban elérjük, a résztvevőknek, külön és együtt, az ön -, és kölcsönös segítségnyújtás eszközével fenn kell tartani és fejleszteni kell az egyéni és a kollektív kapacitásaikat, hogy ellenálljanak a fegyveres támadásnak***”. Az idézetből úgy tűnik, hogy az alapító tagok már akkor gondoltak a resiliencre, mint alapelvre és elkötelezték magukat a potenciális sokkhatásokra (abban az időben jellemzően egy hagyományos fegyveres konfliktus formájában) való felkészülésre és az azokból való felépülésre. A Szövetség már akkor megfogalmazta, hogy a hátország (nemzeti) ereje jelenti az egész Szövetség erejének a forrását.

A hidegháború éveiben a 80-as évek végéig a NATO jelentős erőfeszítéseket tett a resilience biztosítása érdekében, tervezőkapacitást működtetett a Polgári Felkészülés és Polgári Veszélyhelyzeti Tervezés keretében és nyolc polgári ügynökséget tartottak fent egy esetleges háború idejére:

- Védelmi Szállítmányozó Ügynökség;
- Ügynökség az Európai Belföldi Szárazföldi Szállítások Koordinálására;
- Dél-európai Szállítási Szervezet;
- Polgári Repülési Ügynökség;
- Szövetségesek Biztosítási Szervezete;
- Központi Ellátó Ügynökség;
- NATO Háborús Olaj Szervezete;

- NATO Menekült Ügynökség.

Az ügynökségek alapvető feladata volt biztosítani a NATO parancsnokainak a polgári eszközökhöz, szolgáltatásokhoz és kereskedelmi piacokhoz való hozzáférését és az onnan történő ellátását. Szintén nélkülözhetetlen volt menekültek tömeges mozgásának koordinálása a katonai műveletek akadályozásának elkerülése érdekében, valamint a polgári műveletek és ellátás fenntartása a hátország szétesésének elkerülésére.

A hidegháború befejezésével és a keleti blokk széthullását követően ezeknek a feladatoknak a fontossága is csökkent, ezért az ügynökségek is lassan megszűntek. Mindez az 1990-es években, a biztonsági környezetben bekövetkezett változások következménye volt.

A Szövetség a bipoláris világrendszer széthullását követően küldetéstudati válságba került, már nem volt közös ellenség, amellyel szemben erősíteni kellett volna a közös védelmi képességeket és a kollektív védelem keretei között megvédeni a tagállamok területi sérthetetlenségét, illetve lakosságát az ellenség lehetséges csapásainak következményeitől. Megszűntnek tekintették a nagy kiterjedésű hagyományos fegyveres konfliktus veszélyét, amelyben háborús körülmények között kellett volna biztosítani a tagországok politikai vezetéseinek szilárdságát, a gazdasági termelést a katonai és a polgári igények kielégítésére, illetve az alapvető szolgáltatásokat az életkörülmények biztosítására, úgy, hogy közben ne zavarják, sőt inkább támogassák a katonai műveleteket.

A biztonsági környezetben további jelentős változást hozott Jugoszlávia szétesése és az ezzel összefüggő balkáni fegyveres konfliktusok, melyekre válaszul a Szövetség átalakította feladatrendszerét. A tagállami szuverenitás védelmének erősítéséről (lévén, hogy azt senki sem veszélyeztette) a hangsúly a békeműveletek végrehajtására került. A Szövetség feladatrendszerében a következő változást a 2001. szeptember 11-ei amerikai terrortámadások eredményezték. Ekkor a terrorizmus elleni fellépés és ennek keretében az afganisztáni műveletek kerültek a Szövetség prioritási listájának az élére.

A biztonsági környezetben bekövetkezett változások erős hatást gyakoroltak a Szövetség katonai képességeinek követelményrendszerére. A keleti blokk tömeges hadereje által okozott fenyegetettség megszűnt, így szükségtelenné vált a Szövetség tömeghadseregeinek fenntartása. Jelentős csökkentések történtek a nemzeti haderőkben a vezetési szintek, a személyi állomány és a technikai eszközök tekintetében. A szövetségi területeken kívüli békeműveletek és a terrorizmus elleni harc a saját területen folytatott védelmi műveletektől eltérő katonai képességeket igényelt. Így megkezdődött az új típusú katonai képességek kialakítása. Ennek következtében olyan fogalmak láttak napvilágot, mint a telepíthetőség, expedíciós jelleg, alkalmazhatóság és fenntarthatóság. A nehéz fegyverzet és technika háttérbe szorult, teret nyertek a tengeri és légi úton gyorsan szállítható könnyű erők és eszközök. Az állandó vezetési pontok és eszközök helyett a telepíthető és modul jellegű vezetési rendszerekre volt szükség. Megnövekedett a hadszíntéren kívüli és azon belüli szállítóképesség és logisztikai biztosítás fontossága. A hagyományos védelmi műveletekben megszokottól eltérő szemléletű és eszközrendszerű felderítő, hírszerző és híradó-informatikai képességet kellett kialakítani. Különösen a terrorizmus elleni műveletekben megnőtt az igény a különleges erők és a precíziós eszközök alkalmazására.

A fentiek alapján érthető, hogy a hagyományos fenyegetettség jelentős csökkenése, az új típusú kihívásoknak való megfelelési kényszer és az ennek érdekében történő fejlesztések nagy forrásigénye (különösen a 2008-as pénzügyi válságot követően) nem ösztönözte a döntéshozókat az ország- és kollektív védelemnek jobban megfelelő nehéz erők és eszközök, stacioner vezetési elemek és rendszerek, valamint a hagyományos területvédelmi képességek fenntartására,

fejlesztésére. Ezért ezek lassan elavultak, háttérbe szorultak. A katonai képességekkel összhangban szintén háttérbe szorultak a resilience-hez köthető képességek fejlesztése és fenntartása is. A gazdasági megfontolások játszották a legfontosabb szerepet a polgári képességek, a korábban állami tulajdonú források és infrastruktúrák privatizálásakor is (nem csak a volt keleti blokk országaiban). A profitorientált megközelítéssel összeegyeztethetetlenné vált a tartalék, kiegészítő rendszerek fenntartása ezért azok kiszervezésre, eladásra kerültek, így az államnak a legtöbb esetben nem maradt beleszólása a védelemre is igénybe vehető erőforrások és infrastruktúrák felhasználásába. Tovább fokozta a tagállamok külső és belső sérülékenységét, hogy az új technológiák fejlesztésében is az üzleti szféra szerepe vált meghatározóvá, az államoknak sok esetben nem maradt jelentős irányítási, döntési jogköre, így az új technológiákat csak drágán a piacról és sokszor utólag tudta beszerezni.
A biztonsági környezet ismételt változása, a Krím-félsziget orosz megszállása, illetve a hibrid hadviselés megjelenése kellett ahhoz, hogy ismét előtérbe kerüljön a kollektív védelem és az ahhoz kapcsolódó stratégiák. Ismét rá kellett ébredni, hogy egy jelentős katonai erővel rendelkező állam potenciális csapásaival szemben hátországaink fokozott sérülékenységgel bírnak, különös tekintettel a hibrid hadviselés minden domaint támadó kihívásaira. Ezek a stratégiák nem elsősorban a szembenálló fél területeinek elfoglalását és katonai erőinek megsemmisítését célozzák, hanem az egész társadalom működése ellen irányulnak, különösen a kritikus infrastruktúrák kapcsolódási pontjainak rongálásával, megsemmisítésével, amelyet a kiber, terrorista, proxy-csoportok, energiaszolgáltatási zsarolás, információs és hagyományos katonai műveletek kombinációival érnek el.
A kihívásra válaszul olyan védelmi stratégia kidolgozására volt szükség, amely a katonai erő mellett magában foglalja a kormányzat polgári szerveit és a magán szektor kulcsszereplőit is, vagyis össztársadalmi megközelítésre épül. A walesi döntést követően a szövetség kidolgozta az alapkövetelményeket a nemzeti resilience-re (Baseline Requirements for National Resilience) (SACT and City of Norfolk, 2017:2) hét területet vizsgál, melyeken a nemzeteknek fenn kell tartani a működőképességet a NATO katonai erőfeszítéseinek támogatása és a nemzeti hátországok alapvető életfeltételei biztosítása érdekében.
Ezek a következők:

- a kormányzati tevékenység folyamatossága,
- az energiaellátás fenntartása,
- a civil kommunikációs szolgáltatások fenntartása,
- az élelmiszer-, és vízellátás biztosítása,
- képesség a tömeges migráció kezelésére,
- képesség a tömeges sérültellátásra,
- a polgári szállítási rendszerek fenntartása.

Az alapkövetelmények teljesítése nemzeti felelősségi körbe tartozik, nem merült fel olyan közös ügynökségek létrehozása, mint amilyenek a hidegháború időszakában működtek. Ezzel bizonyítja minden kormány az elkötelezettségét a közös műveletek és a nemzeti hátországa iránt. Szövetségi szinten ezeket az alapkövetelményeket - főleg a közös műveletek támogatása szempontjából - ítélték fontosnak, ami nem jelenti, hogy a nemzetek saját érdekeik figyelembevételével nem határozhatnak meg más területeket/ágazatokat is kritikus fontosságúnak.

A resilience kérdésének fontosságát mutatja, hogy a (The NATO Defence Planning Process, 2016) által meghatározott Védelmi Tervezési Képesség Felülvizsgálat (Defence Planning Capability Survey/DPCS) már a 2017-ben kérte (első alkalommal) a nemzetek beszámolóját a nemzeti polgárvédelmi és vészhelyzeti rendszereikről, illetve azoknak a NATO által meghatározott alapkövetelményeknek való megfeleléséről. Ez azért jelentős, mert a NATO védelmi tervezési folyamata ugyan nem zárja ki a polgári képességek tervezését, de alapvetően a katonai képességek fejlesztését célozza. Mivel nem volt előzetes képességkövetelmény meghatározva a Szövetség részéről, ezért a nemzetek önkéntes alapon jelentették értékeléseiket. Természetesen a 2019-es DPCS-nek is részét képezik a nemzetek resilience képességeire irányuló kérdések, annak érdekében, hogy feltérképezzék a Szövetség egészének képességeit, megállapítsák a nemzetek által elért fejlődést, illetve azonosítsák a szövetségi szintű képességhiányokat és javaslatot tehessenek azok csökkentésére, megszüntetésére. Mivel a resilience nemzeti felelősség ezért a NATO nem támaszt részletes követelményeket, csak információ-megosztással és szakmai tanácsadással segíti a nemzeteket.

A RESILIENCE HAZAI MEGKÖZELÍTÉSE ÉS SZABÁLYZÁSA

Magyarország jelentős mértékben resilient a különböző biztonsági kihívásokkal szemben. Mindez szorosan kapcsolódik az EU-s szabályozáshoz a kritikus infrastruktúrák azonosításáról és védelmük lehetőségeiről. A 2004. évi madridi és 2005. évi londoni terrortámadásosokat követően az Európai Tanács a kritikus infrastruktúrák védelmét szolgáló átfogó stratégia kialakítására kérte fel a Bizottságot. Ennek keretében a Bizottság előbb közleményt fogadott el „***A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben***” címmel, majd Zöld Könyvben (Európai Közösségek Bizottsága, 2005) fogalmazta meg a Kritikus Infrastruktúra Védelem Európai Programjának (EPCIP) általános célkitűzésit.

Közösségi szintű tanácsi irányelv azt a célkitűzést szolgálta, hogy kiegészítse a nemzetek létfontosságú infrastruktúráinak védelmét célzó már meglévő programjait. Ahhoz, hogy ez megvalósulhasson Magyarországon is, hazánknak el kellett fogadnia a saját nemzeti programját. Azonban akkor még a létfontosságú infrastruktúrákkal kapcsolatos tevékenység szabályozása hiányzott a magyar jogrendszerből, akárcsak az Európai Unió tagállamainak többségében. A kritikus infrastruktúrák azonos értelmezése érdekében és a nemzeti jogalkotás könnyítésére a Zöld könyv mellékleteként ajánlást adtak ki a kritikus infrastruktúrák szektorairól és azok által biztosított termékekről és szolgáltatásokról. A törvényalkotás mind az EU, mind pedig nemzeti tekintetben hosszadalmas folyamat volt. Magyarországon 2012-ben elfogadták a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvényt. (CLXVI, 2012) törvény az európai kritikus infrastruktúrák azonosításáról és kijelöléséről és védelmük növelésének szükségességéről szóló 2008-as (EU, 2008), valamint a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016. évi tanácsi irányelvnek (EU, 2016) való megfelelést szolgálja. A törvény kiegészítésein nyomon lehet követni a kritikus infrastruktúrák védelmének területén időközben bekövetkezett változásokat, illetve a törvényalkotás reakcióidejét a változások követésére.

Jól megfigyelhető a NATO és az EU koncepciók közötti különbség, míg a NATO a széleskörű és komplex biztonsági kihívásokkal szembeni katonai műveletek támogatására törekszik a resilience kiépítésével, addig az EU nem műveleti szempontból közelíti meg a kérdést hanem a

nemzetközileg közösen használt kritikus infrastruktúrákra és a társadalmi és közösségi szintű működőképesség megóvására koncentrál. Ugyanakkor az EU megközelítése bár szélesebb kört foglal magában, de más az elsődleges célja és ebből adódóan a feladatrendszere is. Alapvetően az EU irányelvei és ebből adódóan a hazai törvényalkotás is a védelemre, azon belül is a terrorizmus elleni védelemre és következményeinek kezelésre összpontosít, nem pedig a kritikus infrastruktúra által nyújtott termék, vagy szolgáltatás esetleges támadás alatti folyamatos biztosítására. Ezért sem az EU, sem pedig a nemzeti szabályozás nem határoz meg követelményt a működőképesség folyamatos fenntartása érdekében a tartalékképzésre, a pótlásra, illetve az infrastruktúra kiesése, megsemmisülése esetén a kritikus termék vagy szolgáltatás más forrásból, ágazattól történő időszakos vagy huzamosabb időn keresztül való biztosítására. Mindezen eltérések ellenére az EU követelményei szerinti felkészülés jó alapot biztosított a NATO alapkövetelményeihez való közelítéshez illetve megfeleléshez. Azonban nem csak az EU követelményeknek való megfelelés segítette az ország felkészítését, hanem az időközben bekövetkezett biztonsági kihívások és katasztrófák kezeléséből nyert tapasztalatok is. Ilyen volt a 2015-ös migrációs válság, melynek komplex tapasztalatai (szállítás, elhelyezés, ellátás, egészségügyi ellátás, biztonsági ellenőrzések és rendszabályok rendszere) beépítésre kerültek a nemzeti tervekben a megfelelő anyagi-technikai és pénzügyi források hozzárendelésével.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi törvény mellékleteiben megjelent táblázatokon láthatjuk, hogy az ágazatok és alágazatok kijelölése az EU Zöld könyvében (Európai Közösségek Bizottsága, 2005:26) kiadott ajánlásoknak megfelelően készült. Tekintettel a nemzeti jogszabályi és ágazati strukturális sajátosságokra, a szabályozás néhány területen túllépi az ajánlásokat. Az agrárgazdaság és a társadalombiztosítás beemelésével új elemeket minősít létfontosságú rendszereknek, illetve az ágazatok és alágazatok bontását is eltérően használja. Az EU a polgári közigazgatás részeiként értelmezi a kormányzati, a fegyveres erők, a közigazgatási és a postai szolgáltatási alágazatokat, míg a magyar törvényben a közbiztonság-védelem és a honvédelem külön ágazatként szerepelnek. A törvényi felsorolás nem tér ki kormányzati és adminisztratív, valamint a vegyi és nukleáris ágazatokra, de az űrtechnológia és kutatás sem esik a szabályozás hatálya alá.

Az alábbi (1. számú) táblázat komplexen foglalja össze a magyar szabályozás megfeleltetését a tárgyban született EU tanácsi irányelveknek és ajánlásoknak.

	ÁGAZAT	ALÁGAZAT	A 2016/1148 EURÓPAI PARLAMENTI ÉS TANÁCSI IRÁNYELV SZERINTI ÁGAZAT VAGY ALÁGAZAT	MEGFELELTETÉS
1	Energia	villamosenergia-rendszer létesítményei (kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek)	Villamosenergia	igen
2		kőolajipar	Kőolaj	igen
3		földgázipar	Földgáz	igen

4	Közlekedés	közúti közlekedés	Közúti közlekedés	igen
5		vasúti közlekedés	Vasúti közlekedés	igen
6		légi közlekedés	Légi közlekedés	igen
7		vízi közlekedés	Vízi közlekedés	igen
8		logisztikai központok		
9	Agrárgazdaság	mezőgazdaság		
10		élelmiszeripar		
11		elosztó hálózatok		
12	Egészségügy	aktív fekvőbeteg-ellátás	Egészségügyi ellátó	igen
13		mentésirányítás	létesítmények (beleértve a	igen
14		egészségügyi tartalékok és vérkészletek	kórházakat és a magánklinikákat is)	igen
15		magas biztonsági szintű biológiai laboratóriumok		
16				
16a		gyógyszer-nagykereskedelem		
16b	Társadalombiztosítás	társadalombiztosítási ellátások igénybevételéhez kapcsolódó informatikai rendszerek és		
17	Pénzügy	pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei	Pénzügyi piaci infrastruktúrák	igen
18		bank- és hitelintézeti biztonság	Banki szolgáltatások	igen
19		készpénzellátás		
26	Infokommunikációs technológiák	internet-infrastruktúra és internet hozzáférés szolgáltatás	Digitális infrastruktúra	igen
27		vezetékes és vezeték nélküli elektronikus hírközlési szolgáltatások, vezetékes és vezeték nélküli hírközlő hálózatok		
28		rádiós távközlés		
29		űrtávközlés		
30		műsorszórás		
31		postai szolgáltatások		
32		kormányzati informatikai, elektronikus hálózatok		
33	Víz	ivóvíz-szolgáltatás	Ivóvízellátás és -elosztás	igen
34		felszíni és felszín alatti vizek minőségének ellenőrzése		
35		szennyvízelvezetés és -tisztítás		
36		vízbázisok védelme		

37		árvízi védművek, gátak		
38-40*	Hatályon kívül helyezve 2019.01.01-től			
41	Közbiztonság - Védelem	rendvédelmi szervek infrastruktúrái		
42	Honvédelem	honvédelmi rendszerek és létesítmények		

1.táblázat *A törvényben meghatározott létfontosságú rendszerek és létesítmények hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i (EU) 2016/1148 európai parlamenti és tanácsi irányelv szerinti ágazatok, illetve alágazatok megfeleltetése (CLXVI. tv. 4. mell.,2012)*

A törvény alapvetően a fenti ágazatok, illetve alágazatok kijelölésének és védelmének szabályozását látja el. Különös figyelmet fordít az üzemeltetői biztonsági terv elkészítésére, amelyben meg kell jelölni a létfontosságú rendszerelemeket és azt a szervezeti és eszközrendszert, amely biztosítja azok védelmét. Az üzemeltetői biztonsági tervben kell megjelölni azokat a biztonsági intézkedéseket is, amelyek kialakítása és működtetése biztosítja az európai létfontosságú rendszerelem vagy a nemzeti létfontosságú rendszerelem védelmét, továbbá meg kell határozni azokat az ideiglenes intézkedéseket, amelyeket a különböző kockázati és veszélyszinteknek megfelelően foganatosítani kell.

Véleményem szerint itt merülnek fel az alapvető kérdések: lehetséges vajon akár csak ágazati szinten is megfelelően koherens biztonsági tervrendszert elkészíteni? Nagyon jól tudjuk, hogy az állami szektorban működő egy-egy ágazat esetében is nagyon bonyolult és időigényes feladat egy tervet (biztonsági, fejlesztési, pénzügyi, stb) elkészíteni, ott is felmerül az alágazatok közötti rivalizálás a szakmai érdekek érvényesítéséért és az erőforrásokért. A táblázatban felsorolt ágazatok jelentős részében a szolgáltatók a magánszektorhoz tartoznak, különböző érdekekkel, szakmai és technológiai eltérésekkel, illetve hasonló tevékenységi kör esetén figyelembe kell venni a piaci versenyhelyzetet is, amely még külön megnehezítheti a koordinált tervezést.

Teljesíthetőek-e az üzemeltetők által kidolgozott biztonsági tervek, illetve minősített helyzetben a fokozott biztonsági intézkedések bevezetése, mikor ugyanez a törvény határozza meg az üzemeltetőnek a biztonsággal összefüggésben felmerülő költségek viselését is. Különösen igaz a felvetés a profitorientált magántulajdonban lévő cégekre, amelyek elsődleges érdeke a termelés/szolgáltatás fejlesztése és a bevétel fokozása, nem pedig a kiadások növelése. Tovább árnyalja a helyzetet a békében is speciális biztonsági igényeknek megfelelni köteles ágazatok helyzete. A teljesség igénye nélkül ezek közé tartoznak a kormányzat folyamatosságának biztosítása, a pénzügyi szektor bank-, és hitelintézeti objektumai, valamint az egészségügyi ágazat kórházai és magánklinikái.

Kormányzati szinten mind törvényi, mind személyi és tárgyi feltételek szempontjából rendezettnek tekinthető a helyzet. Magyarország Alaptörvényének 48-54. cikkeiben vannak meghatározva, hogy milyen időszakok esetén léptethető életbe az ún., különleges jogrend. Ebben a jogalkotó konkrétan megfogalmazza az egyes eseteket, hogy milyen helyzet fennállása esetén, mely intézkedések szükségesek az állam működésének fenntartása érdekében, majd azokat további sarkalatos törvénybe foglalva részletezi. Magyarországon a védett személyek és a kijelölt

létesítmények védelméről, jogszabály alapján a Rendőrség és a Terrorelhárítási Központ köteles gondoskodni. A Rendőrségről szóló 1994. évi törvény felhatalmazása alapján a 160/1996. kormányrendelet tételesen felsorolja a személy és létesítményvédelmi feladatokat mindkét szervezet számára. Ugyan a fenti jogszabályok nem a legfrissebbek, de a biztonsági kihívásokra való reagálásként folyamatosan frissítésre kerültek. Így például a belügyminiszter a terrorveszéllyel kapcsolatban felhatalmazást kapott - az 1824/2015. (XI. 19.) Kormányhatározat alapján - a fenyegetettségnek megfelelő fokozatot Magyarország egész területére, vagy csak annak egy részére elrendelni.

Nem tekinthető ennyire rendezettnek a pénzügyi és az egészségügyi ágazat biztonsági szabályozottság tekintetében. Nincs egységes szabályozás az ágazatok általános biztonsági követelményeire, illetve azon belül a speciális biztonsági igényű alágazatokra, szolgáltatásokra vagy objektumokra vonatkozóan. A tulajdonos vagy az üzemeltetők saját jogkörükben, működési sajátosságaiknak megfelelően, a vonatkozó jogszabályok esetleges figyelembe vételével határozzák meg biztonsági követelményeiket és eljárásrendjüket.

A bankbiztonság és a kórházbiztonság (Dr. Berek Lajos - Dr. Berek Tamás - Berek László, 2016:100-102) munkájában olyan speciális objektumvédelmi feladatokat jelentenek, amelyek nélkülözhetetlenek az ország működése szempontjából és alapvető feladatuk van a társadalmilag minimálisan elvárt biztonság, egészségügyi, gazdasági működőképesség fenntartásában. Ezeken a területeken a speciális biztonsági követelmények békében is komplex védelmi rendszer meglétét és folyamatos fejlesztését kívánják az üzemeltetőtől, ami jelentős erőforrásokat igényel. Könnyen belátható, hogy a védelmi komplexum bármely részelemének hiánya vagy gyengesége kihat a teljes biztonsági rendszer hatékonyságára. A komplex rendszer részelemei is bonyolult biztonsági alrendszerek (beléptető rendszer, biztonsági monitoring rendszer stb.). Az elektronikai és mechanikai védelmi alrendszerek magas fokú integráltsága mellett továbbra is fontos szerepe van az azokat üzemeltető emberi tevékenységnek és felkészültségnek. Ezeket a költségigényes és komplex biztonsági rendszereket kellene megerősíteni minősített helyzetben úgy, hogy megfeleljenek a fokozott kihívásoknak és megfelelő védelmet nyújtsanak az intézmény dolgozóinak és klienseinek, ugyanakkor ne akadályozzák az intézmény alaptevékenységét. Ismerve például a magyar közegészségügy helyzetét, úgy gondolom, hogy egy rövid idő alatt bekövetkező tömeges katasztrófa vagy több területet is érintő szervezett támadás esetén (pl. hibrid hadviselés) kétségesnek tartom a fenti ágazatok jelenleg rendelkezésre álló biztonsági rendszereinek működőképességét illetve hatékony megerősítésüket.

ZÁRÓ GONDOLATOK

Úgy gondolom, hogy a megváltozott biztonsági körülményekre való tekintettel szemléletváltásra van szükség a hátország működőképességének fenntartásához, a műveletek polgári eszközökkel és szolgáltatásokkal való biztosításához. Az eddig prioritásként meghatározott létfontosságú rendszerek és létesítmények védelméről, illetve a védelem folyamatos korszerűsítéséről természetesen nem mondhatunk le, de előtérbe kell helyezni a legfontosabb rendszerek folyamatos üzemeltetésének követelményét. Biztosítani kell a tartalék-, pót-, és váltórendszereket a szünet nélküli tevékenység biztosítása érdekében.

Szükségesnek tartom nemzetközi szinten (NATO, EU) a szabályozás és a követelményrendszer harmonizálását. Jelenleg 22 nemzet tagja mindkét szervezetnek ezért a különböző követelményrendszereknek való megfelelés zavaró és fölösleges forrásfelhasználást eredményezhet.

Sokkal eredményesebb és költséghatékonyabb végrehajtást eredményezne egy közös lista a létfontosságú rendszerekről, létesítményekről és szolgáltatásokról, azok védelmi, tartalékképzési, fenntartási és pótlási követelményeiről.
A NATO követelményeinek figyelembevételével javaslom az aktuális nemzeti szabályzók áttekintését és szükség szerinti módosítását.
Nemzeti vonatkozásban szükségesnek látom a prioritások felállítását. A jelenlegi listán szereplő ágazatok és alágazatok nagy száma nem teszi lehetővé a koherens tervezést, begyakoroltatást és hatékony ellenőrzést. Véleményem szerint egy szűkített listával és pontos követelményrendszerrel jelentősen nőne a hatékonyság és erőforrásokat lehetne megtakarítani.
Mindehhez nemzeti szinten egységes és erős központi irányításra van szükség, amely biztosítja a védelemhez és a folyamatos működtetéshez a biztonsági és szakmai irányelveket, a jogszabályi hátteret, valamint a tevékenység szakmai és pénzügyi támogatását és ellenőrzését.
Úgy gondolom, hogy a resilience a társadalom egészére nézve jogokat és kötelezettségeket tartalmaz, ezért szükség van az állampolgárok széleskörű tájékoztatására, oktatására, gyakorlatoztatására és lehetőség szerint a feladatokba való bevonására.

FELHASZNÁLT IRODALOM

ACT and City of Norfolk (2017): *Building Resilience*, Norfolk.
Dr. Berek Lajos - Dr. Berek Tamás - Berek László (2016): *Személy- és vagyonbiztonság*, ÓE-BGK 3071, Budapest.
CLXVI. törvény (2012): *a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*, Budapest.
EU (2008): *2008/114/EK tanácsi irányelvek az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről*, Brüsszel.
EU (2016): *2016/1148 európai parlamenti és tanácsi irányelvek a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről*, Brüsszel.
Európai Közösségek Bizottsága (2005): *Zöld Könyv a kritikus infrastruktúra védelmének európai programjáról*, COM(2005) 576 final, Brüsszel.
Lasconjarias, Guillaume (2017): *Deterrence through Resilience*, NATO Defence College, Eisenhower Paper Nr.7. May, Roma,
NATO Warsaw Summit Communiqué (2016), Warsaw.
https://www.nato.int/cps/en/natohq/official_texts_133169.htm (letöltés ideje: 2018.09. 06.)
NATO Wales Summit Declaration (2014), Wales.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/351406/Wales_Summit_Declaration.pdf (letöltés ideje: 2018. 09. 10.)
North Atlantic Treaty (1949): Washington.
https://www.nato.int/cps/ic/natohq/official_texts_17120.htm (letöltés ideje: 2018. 11. 10.)
The NATO Defence Planning Process(NDPP)(2016), Brussels.

HAIG ZSOLT: INFORMÁCIÓS MŰVELETEK A KIBERTÉRBEN

Dialog Campus Kiadó, Budapest, 2018, 343 oldal

BEREK LÁSZLÓ[1], KOLLÁR CSABA[2]

ABSZTRAKT

Az információbiztonság témájában és a kapcsolódó területeken viszonylag gazdagnak mondható a hazai, magyar nyelvű szakkönyvkínálat. E könyvek közül szakmai igényességével és a terület fejlődését elősegítő értékes gondolataival emelkednek ki a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar oktatójának, Haig Zsolt professzornak a könyvei. Most a legújabb, 2018-ban megjelent „Információs műveletek a kibertérben" című monográfiáját mutatjuk be.

Kulcsszavak: információbiztonság, információs műveletek, kibertér, infokommunikáció

ABSTRACT

In the field of information security and related areas, the Hungarian, Hungarian-language literature supply is relatively rich. The books of Professor Zsolt Haig, Professor of the National University of Public Service, Faculty of Military Sciences and Officer Training, are emerging from these books with their professional skills and valuable ideas to promote the development of the area. Now we are presenting his latest monograph, title: Information Operations in Cyberspace, published in 2018.

Keywords: information security, information operations, cyberspace, infocommunications

A SZERZŐ SZAKMAI ÉLETÚTJA

Prof. Dr. Haig Zsolt ezredes 1961-ben született Salgótarjánban. Felsőfokú tanulmányait a Zalka Máté Katonai Műszaki Főiskola Rádióelektronikai szakán és a Zrínyi Miklós Katonai

[1] berek.laszlo@lib.uni-obuda.hu | ORCID: 0000-0002-4126-1528 | könyvtárigazgató, Óbudai Egyetem
[2] kollar.csaba@phd.uni-obuda.hu | ORCID: 0000-0002-0981-2385 | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

Akadémián végezte. Végzettségei szerint rádióelektronikai tiszt, híradástechnikai üzemmérnök (1983), illetve harcászati-hadműveleti képesítésű rádióelektronikai tiszt (1989). 1996-ban egyetemi doktori fokozatot (dr.univ.), 1998-ban pedig tudományos doktori (PhD) fokozatot szerzett hadtudomány területen. 2009-ben habilitált katonai műszaki tudományokból.

Pályafutása 1983-tól a Magyar Honvédséghez és elődszervezetéhez, valamint a katonai – elsősorban – műszaki tudományok egyetemi szintű oktatásához kötődik. Tudását többek között a Rádióelektronikai Tanszék, az Elektronikai Harc Tanszék, az Elektronikai Hadviselés Tanszék, az Információs Rendszerszervező Tanszék, az Informatikai Tanszék, az Információs Műveletek és Elektronikai Hadviselés Tanszék, illetve az Informatikai és Elektronikai Hadviselés Tanszék főállású oktatójaként, 2010-től egyetemi tanáraként osztotta meg a hallgatókkal.

1998-tól lát el vezetői feladatokat, melynek fontosabb állomásai az Elektronikus Hadviselés Tanszék (tanszékvezető helyettes, majd mb. tanszékvezető), az Információs Rendszerszervező Tanszék (mb. tanszékvezető helyettes), a Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar (tudományos és nemzetközi kapcsolatok dékánhelyettes), a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola (iskolavezető). 2013-tól a Nemzeti Közszolgálati Egyetem Védelmi vezetéstechnikai rendszertervező mesterszak felelőse.

Ösztöndíjai közül említést érdemel a Széchenyi István Ösztöndíj, valamint az MTA Bolyai János Kutatói Ösztöndíj. Több mint tizenöt kitüntetést, illetve szakmai díjat kapott, többek között az Árvízvédelemért Szolgálati Jelet, a Bolyai Gyűrűt, Dísztőrt a korszerű műszaki tisztképzésért és a honvéd hagyományápolásért, Babérkoszorúval Ékesített Szolgálati Érdemjelet, a Szolgálati Érdemjel Arany fokozatát, a ZMNE Kiváló Oktatója díjat, a Tiszti Szolgálati Jel I., II., illetve III. fokozatát.

Számos szakmai-tudományos szervezet tagja, egyebek mellett Felderítők Társasága, NKE Egyetemi Képzésfejlesztési Tanács, Egyetemi Tudományos Tanács, Doktori Tanács, Katonai Műszaki Doktori Iskola Tanács, Magyar Hadtudományi Társaság, Hírközlési és Informatikai Tudományos Egyesület. Több folyóirat szerkesztőbizottságában tevékenykedik, úgymint a Hadtudomány folyóirat szerkesztőségi tagja, a Hadmérnök online folyóirat alapító és szerkesztőbizottsági tagja, valamint rovatvezetője, a Bolyai Szemle szerkesztőbizottságának az elnökhelyettese. A Magyar Hadtudományi Társaság regisztrált és bejegyzett szakértője az információs műveletek, vezetési hadviselés, elektronikai hadviselés területeken.

A SZERZŐ PUBLIKÁCIÓS TEVÉKENYSÉGE

A Magyar Tudományos Művek Tára aktuális állapota szerint Prof. Dr. Haig Zsoltnak összesen 116 közleménye van, melyekre 622 független, illetve 690 függő hivatkozás történt, Hirsch indexe 15. Szakmai-tudományos publikációi 47-szer jelentek meg lektorált folyóiratban, melyből 5 nemzetközi, 42 hazai kiadású. A szerző szerzőtársaival közösen 7, önállóan 1 könyvet jegyez, ez utóbbiról később még részletesebben szólunk. Nevéhez köthető 19 könyvrészlet, 8 konferenciaközlemény, 9 felsőoktatási tankönyv, illetve 4 további oktatási mű, valamint 20 további tudományos mű.

A KÖTET BEMUTATÁSA

Haig Zsolt ***Információs műveletek a kibertérben*** című monográfiája a Dialog Campus Kiadó gondozásában 2018-ban jelent meg, s a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült. A könyv lektora Ványa László nyugalmazott egyetemi tanár, ezredes, a Nemzeti Közszolgálati Egyetem Katonai Üzemeltető Intézetének korábbi intézetigazgatója.

A monográfia négy nagy fejezetben, összesen 343 oldalon ad átfogó ismereteket az információs és kommunikációs technikák és technológiák fejlődéséről, a jelenleg használatos hálózatos infokommunikációs technológiákról, az információs műveletekről, a kibertérben megvalósuló információs műveleti képességekről.

A szerző a könyv 15. és 16. oldalán adja meg a szakmaterület legújabb megközelítései alapján a fontosabb szakkifejezéseket. A 17. oldalon kezdődő első fejezet címe: A távírótól az internetig: rövid történeti áttekintés. A távközlés hőskorának, s azon belül elsőként a vezetékes távközlés kialakulásának bemutatása kellően részletes, s örvendetes, hogy a technikatörténeti áttekintés szöveges részei mellett a szerző igényes képanyaggal is illusztrálja mondanivalóját. Hasonló mondható el a vezeték nélküli távközlés kezdetének a bemutatásáról is, melyet szerző a következő gondolattal zár: *„Mindezek a technológiai vívmányok voltak az alapjai annak a mai korban használatos infokommunikációs technológiának, amely az információ kezelésének teljesen újszerű, minden korábbinál hatékonyabb lehetőségeit teremti meg".* A téma polgári megközelítése mellett a szerző törekedett a téma katonai technikatörténeti vonatkozásait is bemutatni „A rádió megjelenése a katonai vezetésben" című alfejezetben, majd ezt követően az „Elektronikai technológiák fejlődése a második világháborúban" című alfejezetben. Külön alfejezet taglalja a földi mobiltávközlés fejlődését, valamint a műholdas rendszerek kialakulását és fejlődését. Az első fejezetet a számítógépek, illetve a számítógép-hálózatok fejlődésével foglalkozó alfejezetek zárják. Ez az első, közel hatvan oldalas fejezet önmagában is alkalmas arra, hogy akár a polgári, akár a katonai oktatásban megalapozza a technikatörténeti fejlődést, illetve rámutasson a technikai és technológiai fejlesztések és találmányok kontinuitásának fontosságára.

Jelenkorunk hálózati infokommunikációs technológiáival a második fejezet foglalkozik. A szerző külön alfejezetben mutat rá a big data problémájára. Hivatkozott szekunder kutatási eredményei frissek, relevánsak. Ugyancsak külön alfejezetben értekezik az infokommunikációs technológiák konvergenciájáról, rámutatva, hogy a különböző információk formájuktól függetlenül továbbíthatók ugyan azon a kommunikációs csatornán.

A „Feltörekvő infokommunikációs technológiák" címet viselő 2.1.3. alfejezet már a jövőbe vezeti el az olvasót, s többek között az 5G hálózat, a mesterséges intelligencia, az IoT tömeges elterjedését vetíti előre.

A civil és katonai hálózat-alapú infokommunikációs technológiákról a szerző a 2.2. fejezetben ír, s ennek részeként a felhő alapú számítástechnikáról, ezek fajtáiról, katonai alkalmazási lehetőségeiről, az IoT-ról, annak kommunikációs megoldásairól és katonai felhasználási lehetőségeiről, a szenzorhálózatokról, a katonai szenzorokról és szenzorhálózatokról, ezek biztonsági kérdéseiről, a katonai műveleti hálózatkoncepciókról, a hálózatközpontú hadviselésről értekezik.

A harmadik fejezetben az információs műveletek kerülnek a középpontba. Részletesen olvashatunk a műveletek információs környezetéről, az információs hadszíntér három egymással összefüggő dimenziójáról (fizikai, információs, kognitív), az információs műveletek kialakulásáról, a ma már haditechnika-történetnek számító információs művelet-példákról. A szerző részletesen ismerteti az információs műveletek elméleti alapjait, s ennek részeként az információelméleti megközelítést, az információs fölényt és a befolyásolás elméletét. Az információs műveletek fejlődésével foglalkozó 3.4. alfejezet ismerteti a fejlődés korai szakaszait, a hadviselés és a műveleti környezet változásával kapcsolatos tudnivalókat. Ezt követően az információs műveletek kiterjedésével foglalkozik a szerző, s ezen belül nevesíti, illetve ismerteti az Egyesült Államok információs műveletek koncepciójának a változását, az információs műveletek NATO-értelmezését, Oroszország információs hadviselésének fejlődését, Kína információs hadviselési felfogását, s az alfejezet zárásaként a hazai megközelítést is. A 3.6. alfejezet „Az információs műveleti koncepciók szintézise és átfogó értelmezése" címet kapta. A téma megértését segíti szerző saját átfogó rendszerábrája, valamint az információs műveletek műveleti tartományának bemutatása is. Jelen könyvben – a nemzetközileg elfogadott értelmezéshez hasonlóan – az információs műveletek három célcsoportját nevesíti a szerző: szemben álló fél, saját erők, civil szereplők. Az információs műveletek céljainak bemutatásakor szerző úgy véli, hogy „a negyedik generációs katonai műveletekben az információs fölény klasszikus kialakításának modellje nem alkalmazható teljeskörűen, mivel a műveletekben a civil szereplők is jelentős súllyal vannak jelen". Ezen véleményével nem csak mi, hanem a nemzetközi szakírók is egyet értenek. Az információs műveletek képességei a technikai és a kognitív felosztás alapján kerülnek ismertetésre, a megértést ugyancsak a szerző saját, „Az információs műveletek információs képességei és hatásuk" című rendszerábrája segíti.

A negyedik fejezet a kibertérben zajló információs műveleti képességekkel foglalkozik. A kibertér fogalmának hazai és nemzetközi heterogenitása miatt a szerző több oldalt szentel a fogalmi értelmezésnek, melyet a következő summázattal zár: *„A kibertér az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot"*. A kibertér struktúráját a 4.1.2. alfejezet mutatja be. Ezt követően a szerző a kibertéri műveletekkel, s azon belül részletesebben a kiberfölénnyel és a kibertéri befolyásoló hatásokkal, a kibertéri műveletek értelmezésével, a kibertéri műveletek információs képességeivel, az elektronikai felderítéssel, a számítógép-hálózati műveletekkel, az elektronikai hadviseléssel, a műveleti biztonsággal, a megtévesztéssel, a pszichológiai műveletekkel, a civil-katonai együttműködéssel, a tömegtájékoztatással foglalkozik. A kibertéri információs műveletek vonatkozásában is lehet értelmezni a kölcsönhatásokat, ahogy azt a szerző a 4.3. alfejezetben teszi. A megértést ugyancsak segíti a saját rendszerábra, valamint a kibertéri technikai információs képességekkel, Kína és az USA kibertéri elektronikus hadviselésével, a kiberparancsnokság kialakításának fontosságával, a kognitív befolyásolással, az álhírek terjesztésével, a kiberterrorizmussal foglalkozó részek.

Az írásművet az összegzések, következtetések fejezet zárja.

Szerző egy feszes, jól követhető logikai kerettel, mondanivalójában a teljességre törekvő részletesen taglalt témákkal, gazdag hazai és nemzetközi szakirodalmi hivatkozásokkal maximálisan teljesítette könyve bevezető részében megfogalmazott négy célt. Ezek a következők:

1. Igazolta a hálózatosítás általánossá válását, valamint azt, hogy a hálózatok nem csak a polgári életben, hanem a katonai műveletekben is meghatározó jelentőséget kapnak.
2. Feltárta az információs műveletek kialakulásának és fejlődésének főbb sarokpontjait, valamint bebizonyította, hogy a változó műveleti környezetben az információs műveletek funkciói és képességei is megváltoznak.
3. Bebizonyította a kibertér értelmezésének és tartományainak kibővülését, s igazolta a sokrétű információs tevékenységek létjogosultságát a kibertéri műveletek sorában.
4. Igazolta, hogy az információs műveleti képeségek egymásra hatása egyre jelentősebbé válik a katonai és a polgári környezetben.

Összegzésképpen és a könyv bemutatásának zárásaként úgy gondoljuk, hogy a szerző olyan monográfiát írt, amelyik nagymértékben hozzájárul a kibertérben zajló információs műveletek jobb megértéséhez, megtervezéséhez, megvalósításához, illetve kivédéséhez. Haig Zsolt „Információs műveletek a kibertérben” című könyvét jó szívvel ajánljuk a téma iránt érdeklődő civil és katonai szakembereknek, döntéshozóknak, valamint a témával még csak most ismerkedő egyetemi és főiskolai hallgatóknak is.

A KÖTET KÖNYVÉSZETI ADATAI

Haig Zsolt(1961-) Információs műveletek a kibertérben. - Budapest : Dialóg Campus Kiadó, 2018. - 344 p. : ill. Bibliogr.: p. 311-330. ISBN 978-615-5945-04-5 (nyomtatott) ; ISBN 978-615-5945-05-2 (elektronikus)

A KÖTET ELÉRHETŐSÉGE

A könyv szabadon elérhető az alábbi linken:
https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_Informacios_muveletek_a_kiberterben.pdf

A KÖTET BORÍTÓJA