Kassai Károly

A kibertér műveleti képesség szerepének, jelentőségének és fókuszának evolúciója a NATO stratégiai dokumentumai alapján

Military and Intelligence CyberSecurity Research Paper
2022/9.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROGRAM


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

A kibertér napi életünkben számtalan formában megjelenő, esetenként pontosan nem megfogalmazott közeg, melynek sajátosságaira az elmúlt években egyre több figyelem irányul.[1] A nemzetközi történések politikai, gazdasági, műszaki, jogi, gazdasági, rendvédelmi, nemzetbiztonsági, katonai és egyéb szempontból egyaránt rávilágítanak, hogy a korábban csak műszaki, vagy informatikai „dolog"-nak (vagy számítástechnikai területű kérdésnek) tekintett kibertér – mint környezet – sokszínű lehetőségeket, illetve ezzel párhuzamosan számtalan fenyegetést hordoz magában.

Hazánkban lassan publikációkban is követhető a katonai műveleti alkalmazásra vonatkozó igények megjelenése, ugyanakkor a kérdés átfogó vizsgálata még várat magára. A helyzetet nehezíti, hogy a katonai kiberműveleti képességeket az általános szintnek megfelelő említéseknél részletesebb, konkrét információkat feltáró publikációk száma erősen korlátos. Vélhető, hogy a nemzeti képességekre vonatkozó adatok, működési paraméterek inkább minősített adatkörbe tartoznak.

Ugyanígy problémás lehet a kiberműveletek kérdésének megközelítése a nemzeti felelősség oldaláról, ahol az esetek nagy részében a békeállapotú, a válsághelyzeti és háborús feladatok elkülönítése nem minden esetben érzékelhető, illetve az ezen helyzetekre vonatkozó nemzeti követelmények is erősen eltérnek.[2]

A katonai erő alkalmazása katonai nemzetbiztonsági (és egyéb nemzetbiztonsági) támogatás nélkül megvalósíthatatlan, így ezzel a kiegészítéssel, komplexen célszerű kezelni és vizsgálni ezt az összetett feladatrendszert.

A magyar képességek kialakítása és fejlesztése napjainkban önállóan nem értelmezhető folyamat, figyelemmel NATO és EU tagságunkra és az ebből következő együttműködési kötelezettségre. Ezt fókuszban tartva jelen publikáció nem a kérdés magyar megoldását célozza, hanem annak megalapozása érdekébe a NATO stratégiai szintű folyamatok áttekintését vállalja a helyzet tisztázás érdekében. Terjedelmi okok miatt a vizsgálat elsődleges források tükrözésére korlátozódik. Másodlagos források felbukkanása már érzékelhető, de e kör feldolgozása következő lépésként képzelhető el az egymásra épülés logikája szerint, lényegesen szélesebb erőforrások bevonásával.

Az említett, elsődleges forrásfeldolgozás magyar szempontból nem tekinthető teljesen kihasználtnak, de két

[1] A mű a Katonai Nemzetbiztonsági Szolgálat TKP2021-NVA-24 azonosító számú „A mesterséges intelligencia alkalmazásának kutatása a katonai nemzetbiztonsági célú adatszerző, adatfeldolgozó és vizualizációs eljárásokban, és kapcsolódó fejlesztések elvégzése" elnevezésű projektje keretében, az Innovációs és Technológiai Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával valósult meg.

[2] A nemzetközi kommunikáció során kiemelt figyelmet kell fordítani e sajátosságokra, különben nagyon könnyen téves kép alakulhat ki egy-egy megjegyzés, lábjegyzet figyelmen kívül hagyása miatt (pl. „csak háborús helyzetben", „csak nemzeti alkalmazásra", „külön kormányzati felhatalmazás alapján").

példa említést érdemel. Szentgáli Gergely 2013-as munkájában áttekintette az 1999-2013-as időszak NATO stratégiai szintű történéseit. Feldolgozása jól követhetően összegzi az időszak történéseit. Javaslatai (naprakészen frissített tudás és rendszer, offenzív képesség és elrettentés, együttműködés, kibervédelmi gyakorlatok, stratégiai szintű gondolkodás) a mai napig helytállónak tekinthetők.[3]

Fekete-Karydis Klára – Lázár Bence 2020-as cikkükben átfogóan bemutatták a NATO kibervédelem szempontjából legfontosabb védelempolitikai szintű eseményeit. A beszámoló értéke a NATO szakmai koncepció és politika lényegi ismertetése, illetve az kiber szakterület szempontjából lényeges szakmai szervezetek és testületek bemutatása.[4]

Adminisztratív megjegyzés, hogy az adatgyűjtés és adatfeldolgozás tudatosan csak nyílt adatokra korlátozódik, így a bizalmasság magasabb szintjét elérő adatok, következtetések e munka eredményeképpen nem lesznek elérhetők.

A KATONAI ALKALMAZÁS SZÜKSÉGESSÉGE A KIBERTÉRBEN – AZ 1999-ES NATO STRATÉGIAI KONCEPCIÓ ÉRVÉNYESSÉGE IDEJÉN

A publikációk gyakran idézik a *2016-os Varsói NATO Csúcsértekezlet döntését*, mely szerint a kibertér a szárazföldi, tengeri vagy légi területekhez hasonlóan műveleti területként kezelendő,[5] így a köztudatban ez az esemény könnyen azonosítható a kibertér katonai alkalmazására vonatkozó stratégiai döntések eredőjeként.

E kiindulási pont mellett megemlítendő egy évtizeddel korábbról származó nemzeti forrás. Az amerikai *2004-es Nemzeti Katonai Stratégia* megfogalmazta, hogy Fegyveres Erőknek rendelkezni kell képességekkel a levegőben, szárazföldön, tengeren, világűrben vagy a kibertérben – a harctér műveleti területein – műveleti képességekkel.[6] Ez konkrét feladatszabás a *2006-os Nemzeti Katonai Kibertér Műveleti Stratégia* számára, ami bevezetésként megállapítja, hogy a Védelmi Minisztérium függ a kibertértől a nemzeti katonai célok megvalósítása során katonai, hírszerző és adminisztratív (business) területeken.

[3] Szentgáli Gergely: The NATO Policy on Cyber Defence: The Road so Far. *AARMS*, 2013/1. szám, 83–91 o.

[4] Fekete-Karydis Klára – Lázár Bence: A kibervédelem katonai dimenziói. *Hadtudományi Szemle*, 2020/3. szám, 44–48. o.

[5] Pontos fogalmazás szerint: „(we) … recognise cyberspace as a domain of operations". 2016 Warsaw Summit Communiqué, 70. E mellett megjegyzendő, hogy a kibertér nem „hadműveleti terület/domain", nem „ötödik domain", illetve nem „ötödik haderőnem".

[6] The Military Strategy of United States of America (A Strategy for Today; A Vision for Tomorrow), 2004; 18. o.

A minisztériumnak teljes körű katonai műveleteket kell végrehajtani a kibertérben vagy azon keresztül az amerikai érdekek elleni fenyegetések legyőzése (defeat), az eltántorítás (dissuade) és elrettentés (deter) érdekében. A minisztérium hálózat felderítést (exploitation) fog végezni a hírszerzési adatok beszerzése érdekében és a szükséges mértékben alakítani fogja a kiberteret integrált offenzív és defenzív műveleteket formájában.

A kibertérben vagy azon keresztül végzett műveletek a kívánt hatások elérése érdekében megkövetelik a szervezetek, képességek, funkciók, technológiák és műveletek integrálását. A követelményeknek összhangban kell lennie a jogi és politikákban megfogalmazott követelményekkel, kommunikálni kell a partnerekkel.

A tervezés korai összehangolása segít megoldani a szervezetek együttműködési gondjait, csökkenti az erőforrások hiányosságaiból adódó problémákat, így növeli a kibertér műveletek sikerét.

A törvényes célmeghatározást (targeting) biztosító eljárások integrálása kulcsfontosságú eleme a kibertér műveletek tervezésének.[7]

Gyakorlati szempontból a NATO kiberfenyegetésekre történő első nagyobb szervezeti reagálása 1999 április elején a dél-szláv válsághoz köthető, amikor NATO honlapokat, illetve nyílt levelező szolgáltatásokat értek szerb támadások.[8]

A *NATO 1999-es Stratégiai Koncepció* az akkori biztonsági helyzetben (hidegháború utáni változások) a kibertér katonai felhasználhatóságával még nem foglalkozik, de a biztonsági kihívásokra történő reagálások között az információs veszélyek már megjelennek.

A dokumentum fenyegetések területén megállapítja, hogy állami és nem állami ellenfelek megpróbálhatják kihasználni a Szövetség növekvő függőségét az információs rendszerektől, az ilyen rendszerek megzavarására tervezett információs műveletekkel. Ezek a szereplők megpróbálhatnak ilyen stratégiákat alkalmazni a NATO hagyományos fegyverek területén lévő fölénye ellen.

A megfelelő katonai képesség fenntartása, a felkészültség, a közös védelem érdekében történő fellépés továbbra is központi szerepet játszik a Szövetség biztonsági céljai között.[9]

Abban az időszakban a délszláv válság nehezítette az amúgy is bonyolult 199-es NATO csatlakozási folyamatot. A szövetségi követelmények szerint[10] jogszabályokkal megalapozottan azonosítani kellett a NATO minősített adatok biztonságáért felelős nemzeti szervezetet (Nemzeti Biztonsági Felügyelet),[11] ki kellett alakítani a NATO rejtjelanyagok és a NATO minősített adatok centralizált cseréjét és felügyeletét

[7] National Military Strategy for Cyberspace Operations; 2006; előszó, 2, 10. o.
[8] Serbs launch cyberattack on NATO, 1999.
[9] The Alliance's Strategic Concept (1999) Approved by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington D.C; 23, 28. o..
[10] C-M (55) 15 (FINAL) Security within the North Atlantic Treaty Organization (hatályon kívül). Az akkor érvényben lévő törvény fordítása szerint „Biztonsági Szabályzat" - a NATO szóhasználat a dokumentumot egyszerűsítve „Security Policy"-nak nevezi.
[11] A Nemzeti Biztonsági Felügyeletről szóló 1998. évi LXXXV. törvény (hatályon kívül).

biztosító szervezeteket a Nemzeti Rejtjelelosztó Központ (National Disrtibution Authority)[12] és a Központi Nyilvántartó (Central Registry)[13] formájában.

Látható, hogy a NATO minősített adatok védelmére vonatkozó követelmények önálló jogszabályokban jelentek meg, párhuzamosan a nemzeti minősített adatok védelmére vonatkozó szabályokkal.[14]

Kiemelt fontosságú technikai és biztonsági feladatként meg kellett teremteni a NATO-val történő minősített elektronikus adatkapcsolathoz szükséges feltételeket.[15]

Az említett központi feladatok mellett az egész országra kiterjedően ki kellett alakítani a NATO minősített adatcserét biztosító szolgáltatásokat is, ami nem csak katonai feladat, így az érintett egyéb minisztériumok számára is feladatok jelentek meg. A későbbi években intenzíven kezdtek megjelenni a NATO beruházási programok, ami jelzi, hogy az azokban résztvevő (illetve pályázó) cégeknek is teljesíteni kellett a NATO minősített adatkezelésre vonatkozó összes követelményt.

Ez mutatja, hogy a kétezres évek első fele a NATO információvédelmi követelményeinek megismerésével és egyre kiterjedtebb alkalmazásával telt. Az időszakra vonatkozóan részletesebb szakmai publikációk nem születtek. A NATO követelmények ismertetése egy kiadványban történt,[16] az időszakra vonatkozó elektronikus információbiztonsági szakmai érdekességek – a NATO-val kapcsolatos specialitásokkal együtt – egy korábbi cikkben olvashatók.[17]

Az említett törekvések egyértelműen csak a minősített adatkezelés védelmét célozták, a nyílt (nem minősített) adatkezelés jogszabályi követelményei még nem álltak rendelkezésre.[18] Így ebben az időszakban hivatalos kibervédelmi (vagy kibertér műveleti) nemzeti

[12] A rejtjelzésre is vonatkozó, az elektronikus információvédelemről szóló 33/2022. (HK. 13.) HM utasítás a nemzeti és a NATO követelmények együttes végrehajtását célozta, de megfogalmazása csak a Központi Rejtjelfelügyeletre terjed ki, a Nemzeti Rejtjelelosztó Központot nem említi annak ellenére, hogy ez a szervezet is a szakmai struktúra része volt.

[13] 4/2000. (II. 29.) HM rendelet a Központi Nyilvántartó, a nyilvántartó és az ellenőrző pont működési rendjéről (hatályon kívül). A részletes feladatokat a Magyar Köztársaság NATO-NYEU Központi Nyilvántartó, Ellenőrző pontok és a biztonsági megbízottak által vezetendő okmányokról szóló 13/2000. (HK. 6.) HM utasítás (hatályon kívül) szabályozta.

[14] A nemzeti feladatokat az állam és szolgálati titokról szóló1995. évi LXV. törvény szabályozta. E törvény módosításával jelent meg a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített, valamint korlátozottan megismerhető adat védelmének eljárási szabályairól szóló 56/1999. (IV. 2.) Korm. rendelet (hatályon kívül), melynek feladata kifejezetten a NATO követelmények megvalósítása.

[15] 82/2002. (HK. 26.) HM utasítás a NATO Irodaautomatizálási rendszer (NIAR) biztonságával kapcsolatos feladatokról

[16] *Biztonság és Titokvédelem a NATO szabályai szerint*, Budapest, Honvéd Kiadó, 1999, 1.o.

[17] Kassai Károly: Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005-2015 közötti időszakban. *Hadmérnök*, 2015/3. szám 279–291. o.

[18] A NATO minősített adatok védelmére vonatkozó szabályok egy része tartalmazott nyílt (nem minősített) adatok védelmére vonatkozó követelményeket is.

megfogalmazások nyilvánosan nem azonosíthatók.

A *2002-es NATO Prágai Csúcsértekezleten* megfogalmazott Prágai Képesség Kötelezettség Vállalás (Prague Capabilities Commitment - PCC) jóváhagyása – mint a Szövetség folyamatos erőfeszítéseinek része –, egyértelmű válasz az érzékelt fenyegetésekre. A Vállalás célja a magas fenyegetettségű környezetben új katonai képességek erősítése és fejlesztése a modern hadviselés érdekében. Itt már megjelenik a kibertér biztonsága, mert a deklaráció szerint *meg kell erősíteni a kibertámadások elleni védelmi képességeket*.[19]

A 2002-es év az új Biztonsági Politika megjelenésével a NATO minősített adatok védelmére vonatkozóan fontos mérföldkő.[20] Az addigi szabályozási struktúra megőrzésével a Politika rögzíti az minősített adatok védelmére vonatkozó stratégiai követelményeket, illetve a fizikai, személyi, adminisztratív, elektronikus információvédelmi és iparbiztonsági követelményeket a NATO szervezetek és tagállamok részére.

A következő szabályozási szinten a szakterületeket szabályozó direktívák (kötelező szabályok és eljárások), ajánlások és támogató dokumentumok találhatók. Ebben a rendben már azonosíthatók olyan elektronikus információvédelmi szakfeladatok (pl. kockázatelemzés, detektálás, eseménykezelés, biztonsági audit, helyreállítás) ami napjainkban a kibervédelmi szakfeladatokkal is kapcsolatba hozhatók.

A további, felső szintű NATO védelempolitikai dokumentumok egyre összetettebben említik a kibertérben érzékelhető fenyegetéseket és a szükséges képességfejlesztést. A ***2004-es Isztambuli Csúcsértekezlet*** kivételnek tekinthető, mert szorosan kapcsolódó követelményeket, megállapításokat nem fogalmaz meg.[21]

A *2006-os NATO Rigai Csúcsértekezlet* a kapacitások fejlesztése céljaként említi a Szövetség műveleteiben *az adatok, hírszerzési információk megbízható, biztonságos és késedelem nélküli megosztását, közben javítva a kulcsfontosságú információs rendszerek kibertámadások elleni védelmét*.[22]

A *2006-os (NATO Rigai Csúcsértekezleten elfogadott) NATO Átfogó Politikai Irányelv* megállapítja, hogy a NATO elleni jövőbeli támadások az aszimmetrikus eszközök használatának fokozott kockázatával járnak.

A NATO-nak meg kell őriznie képességét a missziók teljes körének lebonyolítására, a magas intenzitásútól az alacsonyig, különös figyelmet fordítva a legvalószínűbb műveletekre, reagálva a jelenlegi és jövőbeli hadműveleti követelményekre.

[19] Prague Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague, Czech Republic, 2002, 4. c, f. p. Ez alapján kezdődött meg a NATO eseménykezelő Központ (NATO Computer Incident Response Capability – NCIRC) kialakítása.

[20] C-M (2002) 49 Security within the North Atlantic Treaty Organization.

[21] Istanbul Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council, 2004.

[22] Riga Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006; 24. o.

Tekintettel a jövőbeli biztonsági környezet jellegére, annak hatásaira, a Szövetségnek mozgékonyságra és rugalmasságra van szüksége az összetett és kiszámíthatatlan kihívások megválaszolásához, amelyek a tagállamok határaitól távol alakulhatnak ki és rövid időn belül mutatkoznak meg.

Az Irányelv a következő 10–15 évre a fejlődő biztonsági környezet, valamint a hagyományos és különösen az aszimmetrikus fenyegetések, kockázatok kezelése érdekében azonosítja a szükséges képesség követelményeket. Ebben szerepel a létfontosságú infrastruktúrák és katonai erők védelme, a Szövetség számára kritikus fontosságú információs rendszerek kibertámadások elleni védelme, illetve a műveletek vezetéséhez szükséges képességek (figyelemmel a tapasztalható fenyegetésekre).[23]

2006-os nemzeti esemény, hogy a Puskás Tivadar Közalapítvány keretein belül működő Kormányzati Hálózatbiztonsági Központ nemzetközi minősítést ért el, amivel teljes körű tagjává vált az európai CERT[24] közösségnek. Ez kezdeti lépés, hogy megkezdődhessen a nemzeti szinten értelmezhető eseménykezelés, illetve a nemzetközi eseménykezelőkkel történő együttműködéssel riasztási, értesítési információkat kaphassanak az érintettek, illetve szakértői szintű konzultációk támogassák egy-egy technikai ügy megoldását.

A *2008-as NATO Bukaresti Csúcsértekezlet* megállapítja, hogy a NATO továbbra is elkötelezett a Szövetség kulcsfontosságú információs rendszereinek megerősítésében a kiber támadások ellen. A Kibervédelmi Politikára[25] hivatkozva hangsúlyozza annak szükségességét, hogy a NATO és a nemzetek saját felelősségük szerint védjék meg a kulcsfontosságú információs rendszereket, osszák meg bevált gyakorlataikat és legyenek képesek felkérésre segítséget nyújtani más szövetséges nemzeteknek kibertámadás esetén.[26]

A 2008-as év eseménye, hogy a 2007-es Észtországot ért elektronikus szolgáltatások elleni súlyos támadások a nemzetközi és a NATO figyelmet a kibervédelemre irányították. A NATO saját rendszerek védelmére irányuló erőfeszítése mellett a kutatási, képzési feladatok, kibervédelmi gyakorlatok és egyéb jövőbeli képességek támogatására irányuló tevékenységek érdekében Tallinnban megalakult a NATO Kibervédelmi Kiválósági Központ.[27]

---

[23] Comprehensive Political Guidance, 2006; 5, 7, 10, 16. c, d, e. p.

[24] Computer Emergency Response Team (CERT), az eseménykezelést, koordinálást végző szakértő szervezet egyik nemzetközi megnevezése. Ebben az esetben „CERT – Hungary" azonosítással az említett szervezet akkreditált taggá vált.

[25] Policy on Cyber Defence.

[26] Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008; 47. o.

[27] NATO Cooperative Cyber Defence Center of Excellence (NATO CCD COE). Centre is the first International Military Organization hosted by Estonia, (https://ccdcoe.org/news/2008/centre-is-the-first-international-military-organization-hosted-by-estonia/).

A 2008-as évben indult a NATO Cyber Coalition kibervédelmi gyakorlat sorozat, ami azóta az egyik legnagyobb ilyen típusú rendezvény a világon. A gyakorlatot a NATO Transzformációs Parancsnokság tervezi és irányítja a NATO Katonai Bizottság felügyeletével.

A gyakorlat sorozat a NATO szervezetek, a szövetségesek és a partnerek kiberkoalícióját képviseli, hogy megerősítse a Szövetség képességét a kibertérben és azon keresztüli fenyegetésekkel kapcsolatos elrettentésre, védelemre és a fenyegetések elleni küzdelemre, támogatva a NATO alapvető feladatait az együttműködési és kibertéri műveletek gyakorlásával.[28]

A 2008-as év egyben a Gripen vadászrepülők rendszerbeállítását is jelenti. A stratégiai szintű feladatok mellett - a részeltek említése nélkül - érdemes röviden említeni, hogy ebben az esetben a NATO elektronikus információvédelmi keretrendszerének alkalmazására volt szükség a levegő-levegő és föld levegő valamint földi kiszolgáló elektronikus információs rendszerek biztonságának szavatolása érdekében.[29]

A *2009-es NATO Strasbourg - Kehl Csúcsértekezlet* deklarálása szerint a Szövetség továbbra is elkötelezett a kommunikációs és információs rendszerek kibertámadások elleni megerősítése mellett, amelyek kritikus fontosságúak a NATO számára.[30] A támadások megelőzése, az azokra adandó válaszreagálások érdekében – összhangban a Kibervédelmi Politikával –, Kibervédelmi Menedzsment Felügyelet[31] alakult a meglévő Számítógépes Incidenskezelő Képesség[32] hatékonyságának növelése érdekében, illetve Észtországban megalakult a NATO Kibervédelmi Kiválósági Központ.[33] A fenyegetések ellensúlyozása érdekében a Szövetség felgyorsítja kibervédelmi képességek fejlesztését a teljes felkészültség elérését célozva. E mellett a kibervédelem a NATO gyakorlatok szerves részévé válik.

A Szövetség tovább erősíti a kapcsolatokat a NATO és a partnerországok között a kiber támadások elleni védelem terén.[34]

A 2009-es évhez tartozó nemzeti esemény a minősített adatok védelme szempontjából sorsfordulatot jelentő törvény,[35] valamint az ezt követően megjelenő végrehajtási rendeletek, melyek egyértelmű megfogalmazással már együttesen kezelték a NATO, EU (és egyéb

---

NATO opens new centre of excellence on cyber defence (https://www.nato.int/cps/en/natohq/news_7266.htm).

[28] Cyber Coalition: NATO's Flagship Cyber Exercise (https://www.act.nato.int/cyber-coalition)).

[29] Mit tud egy magyar Gripen (https://honvedelem.hu/hirek/mit-tud-egy-magyar-gripen.html).

[30] Állami és nem állami szereplők megpróbálhatják kihasználni a Szövetség és szövetségeseinek egyre növekvő függőségét e rendszerektől.

[31] Cyber Defence Management Authority.

[32] Computer Incident Response Capability – CIRC.

[33] NATO Cooperative Cyber Defence Centre of Excellence – NATO CCD COE.

[34] Strasbourg / Kehl Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl, 2009; 49. o.

[3535] Mavtv.

külföldi) valamint nemzeti minősített adatok védelmét.[36]

Az egységesített szabályok mellett megjegyzendő, hogy ekkor következett be a most is tapasztalható állapot, mely szerint a nemzeti, NATO, EU (vagy egyéb külföldi) minősített adat felügyeletét a korábbi megosztott szerepek helyett[37] egy szervezet – a Nemzeti Biztonsági Felügyelet – látja el.

A *2010-es NATO Lisszaboni Csúcsértekezlet* megállapítja, hogy a kiber fenyegetések száma növekszik, bonyolultságuk erősödik. A folyamatos és szabad kibertér hozzáférésének biztosítása- valamint a kritikus fontosságú rendszerek sértetlenségének biztosítása érdekében a Szövetség doktrínális területen is figyelembe veszi a modern konfliktusok kiber dimenzióját[38] és fejleszti képességeit a detektálás, vizsgálat, megelőzés, védelem és helyreállítás érdekében a Szövetség számára kritikus fontosságú rendszerek elleni kibertámadások esetén.

A Szövetség kiemelten törekszik, hogy 2012-re gyorsítsa a NATO Számítógépes Eseménykezelő Képesség teljes készenlétét[39] és az összes NATO szervezetet központosított kibervédelem alá vonja.

A NATO védelmi tervezési folyamatot[40] felhasználva történik a szövetségesek kibervédelmi képességeinek fejlesztésének elősegítése, az egyes szövetségesek kérésre történő segítése, valamint az információmegosztás, az együttműködés és az interoperabilitás optimalizálása.

A kibertérből fakadó biztonsági kockázatok kezelése érdekében a Szövetség szorosan együttműködik más szereplőkkel, például az ENSZ-szel és az EU-val (megállapodásnak megfelelően).[41]

2010-es esemény, hogy a NATO Nemzetközi Törzsön belül megalakult Új Típusú Biztonsági Kihívások Igazgatóság[42] a növekvő, nem hagyományos kockázatok kezelése érdekében. Az új szervezet feladata a terrorizmus, a tömegpusztító fegyverek kereskedelme, a kibervédelem és az energiabiztonság kérdéseinek kezelése. Feladata lesz továbbá stratégiai szintű elemző képesség biztosítása, illetve a nemzetközi folyamatok követése, a fejlesztési folyamatokban való részvétel a

[36] Ez a szabályozási környezet nem vonatkozik a nyílt (nem minősített) adatk védelmére.

[37] Korábban a nemzeti titokvédelemért a Belügyminisztérium, a rejtjelzés felügyeletéért az Országos Rejtjelfelügyelet, illetve a NATO, EU minősített adatok védelmének felügyeletéért a Nemzeti Biztonsági Felügyelet volt felelős.

[38] A megállapítás a NATO Összhaderőnemi Doktrína (AJP 01) első olyan módosítására utal 2010-ben, ahol megtörtént a kibertér szempontjainak figyelembevétele. Ez kritikus fontosságú szabályozási kérdés, mert rámutat arra, hogy összetett szabályozási környezetben a „fentről – lefelé" elvet kell követni. Először meg kell fogalmazni a legmagasabb szintű követelményeket, elvárásokat, melynek eredményeképpen az alacsonyabb szintű szabályozókban ezek a követelmények tovább bonthatók, fejleszthetők a jogi normák és egyéb irányelvek figyelembevételével.

[39] Full Operational Capability – FOC.

[40] NATO Defence Planning Process – NDPP.

[41] Lisbon Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 2010; 40. o.

[42] Emerging Security Challenges Division (ESCD).

NATO biztonságára hatással bíró esetekben.[43]

A 2010-es év eseménye, hogy a NATO Kibervédelmi Kiválósági Központ csatlakozott a NATO Cyber Colalition kibervédelmi gyakorlat tervezési, szervezési és végrehajtási folyamataihoz.[44]

2010-ben zajlott a NATO Kibervédelmi Kiválósági Központ rendezésében az első Locked Shields kibervédelmi gyakorlat. Az azóta is folyamatosan fejlődő, bővülő gyakorlat kezdetben erősen technikai szempontú volt, célként kitűzve egy adott infrastruktúra üzemeltetését egyre erősödő támadó körülmények között. Ez a védelmi - támadó tevékenység[45] virtuálisan kialakított különböző infrastruktúrák túléléséért történik, stratégiai döntéshozatallal, jogi kérdések megoldásával, illetve kommunikációs kérdésekkel kiegészítve.[46]

A 2010-es év magyar vonatkozása az első Magyar – NATO Kibervédelmi Együttműködési Megállapodás[47] megkötése a fentiekben említett szövetségi – nemzeti kapcsolattartás erősítése érdekében. A nemzeti kapcsolattartói feladatokat a Miniszterelnökség irányítása alatt álló kormányzati szervezet látta el.

Az évben megtörtént a magyar csatlakozás a NATO Kibervédelmi Kiválósági Központhoz. A feladat új kihívásokat jelentett a Központ akkori nemzetközi közösségének, mert a megalakulás óta eltelt két évben még nem volt példa új nemzet csatlakozási kérelmének befogadására.[48] A csatlakozással megnyílt a lehetőség a Központ által szervezett tanfolyamok látogatására, a kibervédelmi gyakorlatokon való részvételre, ami azonnali nemzeti hasznosítást is jelent.

Az 1999-es NATO Stratégiai Koncepció érvényességének időszakában megkezdődött a Szövetség összetett folyamataiban és szervezeti rendjében a kibertér fenyegetések súlyosságnak megfelelően történő kezelése. Ennek jól érzékelhető mozzanata a NATO rendszerek védelmi szintjének emelésére irányuló törekvés és a működést biztosító, egész világot hálózatot behálózó rendszerek központosított eseménykezelési rendjének kialakítása.

A 2001-es amerikai 9/11-es, súlyos terrorcselekmény az általános nemzeti és nemzetbiztonsági fenyegetettségre irányította a figyelmet, míg a 2007-es észt kibertámadások miatt a kiberbiztonság került fókuszba. Ekkor szakmai koncepció, majd politika született a szövetség szintű követelmények, irányelvek rögzítése érdekében. Ezzel megjelent az első

[43] New NATO division to deal with Emerging Security Challenges (https://www.nato.int/cps/en/natohq/news_65107.htm)

[44] Centre Supports NATO's Cyber Coalition 2010 (https://ccdcoe.org/news/2010/centre-supports-natos-cyber-coalition-2010/).

[45] Szakmai megfogalmazás szerint „Blue Team - Red Team".

[46] A NATO Kiválósági Központ nem NATO szervezet, így ez a gyakorlat sem szövetségi gyakorlat, de említést érdemel, mint egyértelmű gyakorlási lehetőség a Központ támogató nemzetei, valamint a NATO szervezetek – napjainkban már az EU számára is. Locked Shields (https://ccdcoe.org/exercises/locked-shields/).

[47] Memorandum of Understanding – MoU.

[48] Hungary joins the Centre (https://ccdcoe.org/news/2010/hungary-joins-the-centre/).

felelősséget tisztázó megfogalmazás, mely szerint a NATO elsődleges feladata a saját rendszerek védelme és a szövetségesek évről-évre szélesebb körű támogatása, míg a szövetségesek felelősek a nemzeti szintű kibervédelemért.

A NATO rendszerek védelme, az eseménykezelés biztosítása mellett jelentkező szükségletek alapján újabb szervezeti elemek alakultak a nemzetekkel történő folyamatos technikai szint feletti kapcsolattartás biztosítása-, illetve az új típusú fenyegetések kezelése érdekében.

A kibervédelmi kérdések technikai kezelési szükségleteinek felismerésem mellett kielemelt fontosságú e szakterületen is a hírszerzési képesség (lehetőségek) alkalmazásának fontossága.

Az elméleti jellegű kérdések kutatása, az oktatás és képzés támogatása érdekében szakterületű kiválósági központ alakult, illetve a NATO kialakította a kibervédelmi gyakorlatok rendjét.

A NATO – nemzeti gyakorlati együttműködés érdekében kirajzolódott egy együttműködési megállapodásokkal kijelölt keretrendszer.

A vizsgálati cél nem tartalmazza a NATO elektronikus információvédelmi kérdések feldolgozását, de szükség van annak kielemelésére, hogy a védelempolitikai, stratégiai szintű kiberbiztonság (később kibertér művelet) egyszerűen nem tekinthető létező fogalomnak az elektronikus információvédelmi feladatrendszer (követelmények) nélkül.

A fenti események jogosan nevezhetők az első NATO kibervédelmi lépéseknek, melyhez az eseményekhez köthetően egyértelműen azonosíthatók az első magyar katonai erőfeszítések is.

TOVÁBBI LÉPÉSEK AZ ÚJ STRATÉGIAI KONCEPCIÓ NYOMVONALÁN

A *NATO Lisszaboni Csúcsértekezleten elfogadott Stratégiai Koncepció (2010)* szerint a kibertámadások egyre gyakoribbak, szervezettebbek és költségesebbek az általuk okozott kár tekintetében, melyek sértik a kormányzati adminisztrációt, a vállalkozásokat, a gazdaságot és potenciálisan a közlekedést, az ellátási hálózatokat és egyéb kritikus infrastruktúrákat.

A támadások elérhetik azt a küszöböt, ami fenyegeti az euro-atlanti jólétet, biztonságot és stabilitást. A támadások forrásai lehetnek külföldi katonai és hírszerző szolgálatok, szervezett bűnöző csoportok, terroristák és/vagy szélsőséges csoportok.

A Szövetség gondoskodni fog arról, hogy a NATO rendelkezzen a fenyegetések elleni elrettentéshez és az ellenük való védelemhez szükséges képességek teljes skálájával. Tovább fejleszti képességeit a kibertámadások megelőzése, észlelése és védelme érdekében, valamint a támadások után szükséges visszaépítéshez, többek között a NATO védelmi tervezési folyamat felhasználásával a nemzeti kibervédelmi képességek fokozására és koordinálására, az összes NATO szervezet központi kibervédelem alá vonásával, valamint a kibertudatosság, a figyelmeztetések és

válaszlépések jobb integrálásával a tagállamokkal együttműködésben.[49]

A *2011-es NATO Politikai Iránymutatás* a stabilizációs és helyreállítási tevékenységeket tartalmazó műveletekre fókuszálva határoz meg általános követelményeket. E tevékenységek általában civil hatóságok, szervezetek feladatai (de a NATO-nak gyakran szerepet kell vállalnia ezekben a feladatokban is), így ez a dokumentum zömében e speciálisnak tekinthető műveletre, főleg a civil – katonai együttműködésre koncentrál. Lényegi – más esetben is értelmezhető eleme –, hogy egy művelet előtti elkötelezettség előtt a NATO-nak átfogó elemzést és értékelést kell végeznie a lehetséges műveleti területen a politikai, társadalmi-gazdasági és intézményi helyzetről, valamint a fizikai infrastruktúráról.[50]

2011-es esemény, hogy jogszabály jelent meg a válságkezeléshez szükséges Nemzeti Intézkedési Rendszer kialakításáról, összhangban a NATO Válságreagálási Rendszerrel.[51] A feladatrendszer a napi élt során felmerülő, normál üzemű működéstől eltérő, egyedi intézkedések kezelésének lehetőségét biztosítja. A meghatározott Nemzeti Intézkedések Gyűjteménye (NIGY) a NATO hasonló intézkedéseivel szinkronizált, ami biztosítja a két válságkezelési rendszerben az azonos értelmezést, intézkedések bevezetését.[52]

Az év eseménye az első magyar részvétel a NATO Cyber Coalition kibervédelmi gyakorlatsorozat éves rendezvényén. A nemzetek számára 2010-ben megnyitott kibervédelmi gyakorlaton a magyar szereplőket a Nemzeti Biztonsági Felügyelet koordinálta.[53]

További nemzeti esemény a kibertér műveleti képességek kialakítására vonatkozó koncepció kialakításának elrendelése, ami egyben a NATO képességfejlesztéssel történő összehangolási lépés is.

A szövetségesek előtt álló feladat, hogy nemzeti fejlesztéseiket hangolják össze a NATO képességfejlesztéssel.[54] Az erre vonatkozó honvédelmi ágazati szintű koncepció kidolgozásának elrendelése miniszteri utasítás formájában történt meg.[55]

A *2012-es NATO Chicago-i Csúcsértekezlet* deklarációja az idézett, korábbi dokumentumokkal összhangban folytatólagosan megállapítja, hogy a kibertámadások száma továbbra is jelentősen növekszik, kifinomultságuk és

[49] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization 2010, 12, 19. o.

[50] Political Guidance on ways to improve NATO's involvement in Stabilisation and Reconstruction, 2011, 6. o.

[51] NATO Crisis Response System (NCRS).

[52] 278/2011. (XII. 20.) Korm. rendelet a NATO Válságreagálási Rendszerével összhangban álló Nemzeti Intézkedési Rendszer rendeltetéséről, feladatairól, eljárási rendjéről, a közreműködők kötelezettségeiről.

[53] Sikeres volt a kibervédelmi gyakorlat, (https://honvedelem.hu/hirek/honvedelmi-miniszter/sikeres-volt-a-kibervedelmi-gyakorlat.htm).

[54] Ez nem jelent akadályozást semmilyen önálló nemzeti cél kitűzése és megvalósítása területén, mert a nemzeti képességfejlesztések egyértelműen nemzeti hatáskörben kezelendő ügyek.

[55] 81/2011. (VII. 29.) HM utasítás a honvédelmi tárca Kibernetikai Védelmi Koncepció kialakításához szükséges feladatok meghatározásáról, 3. §. 5-6. o.

összetettségük fejlődik. Emiatt a szövetségesek megerősítik a Lisszaboni Csúcstalálkozón tett kibervédelmi vállalásukat.

A NATO meglévő képességeire építve a NATO Számítógépes Incidenskezelő Képesség kritikus elemei elérték a teljes működési képességét, a legtöbb üzemeltetési helyszín és felhasználói szám elérésével.

A Szövetség elkötelezte magát, hogy erőforrásokat biztosítva, a szükséges reformokat végrehajtva valamennyi NATO szervezet központosított kibervédelem alá kerüljön.

A szövetségesek a kibervédelmi intézkedéseket tovább integrálják a Szövetség struktúráiba és eljárásaiba és mint egyes nemzetek, továbbra is elkötelezettek a nemzeti kibervédelmi képességek azonosítása és megvalósítása mellett, amelyek erősítik a Szövetség szintű együttműködést és interoperabilitást, beleértve a NATO védelmi tervezési folyamatait is.

A Szövetség tovább fejleszti a képességeket a kibertámadások megelőzésére, felderítésére, az azok elleni védelemre és az azokból történő helyreállítás érdekében.[56]

A *NATO főtitkár 2012-es évről szóló jelentése* szerint a NATO a 2011. októberében indított Intézkedési Terv (Action Plan) révén folytatta az új Kibervédelmi Politika végrehajtását.

2012 tavaszán a NATO fontos szerződést kötött, hogy jelentősen fejlessze egyedi kibervédelmi képességét (NCIRC). A projekt befejezésével 2013 őszén valamennyi NATO hálózat központosított védelem alatt áll, így a NATO képesség jelentősen bővül a saját hálózatok védelmében a behatolás és támadás minden típusa ellen.

A NATO jobb helyzetbe kerül ahhoz, hogy segítse a szövetségeseket és partnereket a kibertámadások felderítésében, az azok elleni védelemben és a támadás utáni helyreállítási tevékenységben, valamint kérésre gyorsreagálású csoportok[57] telepítésében.

A kibervédelmi képességek továbbfejlesztése érdekében a NATO létrehozott egy kiberfenyegetettség értékelő szervezeti elemet,[58] ami megtartotta első teljes körű, kibervédelmi forgatókönyvön alapuló válságkezelési gyakorlatát. A másik éves gyakorlat a „Cyber Coalition" volt, ahol a szövetségeseket és partnereket bevonva tesztelés bizonyította az eseménykezelési és a válságkezelési eljárások hatékonyságát.[59]

A *NATO főtitkár 2013-ról szóló éves jelentés* megállapítja, hogy az év jelentős előrelépést jelent a NATO kiber támadásokkal szembeni védelme érdekében.

A NATO Számítógépes Incidenskezelő Képesség által biztosított központosított védelem bevezetése megtörtént a NATO szervezeteknél, így az 51 NATO-helyszínen található NATO-hálózatok átfogó (24/7) felügyelet alatt állnak, továbbfejlesztett

[56] Chicago Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012; 49. o.

[57] Rapid Reaction Teams.

[58] Cyber Threat Assessment Cell.

[59] The Secretary General's Annual Report 2012, "Cyber defence" fejezet, 17. o.

érzékelőkkel és behatolásérzékelő technológiákkal védettek.

Kiber területen (mint műveleti területen) a NATO elsődleges szerepe a saját hálózatok védelme. 2013-ban a Szövetség kibővítette erőfeszítéseit a kiberfenyegetések kezelésére. A kibervédelem most először került be a NATO védelmi tervezési folyamatba. Ez támogatást nyújt, hogy a szövetségesek rendelkezzenek az alapvető szervezetekkel, képességekkel és interoperabilitással egymás segítése érdekében.

A NATO az évben folytatta a kibervédelmi forgatókönyvek kialakítását a gyakorlatokon, kiképzéseken és oktatások során.[60]

2013-as speciális szakmai eseménynek tekinthető a NATO Kibervédelmi Kiválósági Központ szervezésében egy nemzetközi jogászcsoport több éves együttműködésén és kiterjedt szakértői konzultációján alapuló kutatás lezárása és a „Tallinn Manual"[61] kiadása. A gyűjtemény kiadása frappáns választ ad a nemzetközi jog alkalmazhatóságára a kibertéri események megoldása érdekében. A sokat hangoztatott év, mely szerint nincs kialakult nemzetközi jogi norma a kibertérre, így az ott elkövetett ügyeket nem lehet megítélni, ezáltal más megvilágítást kap. A gyűjtemény a háborús cselekmények megítélésében ad segítséget. A rengeteg forgatókönyvet bemutató munka nem NATO szabálykönyv, kézikönyv (szabályokkal) vagy jogszabály – hanem a szerzők szakmai véleményét tartalmazó, a szabályok alkalmazhatóságára vonatkozó példagyűjtemény, melynek tanulmányozása, az analógiák felismerése segíthet egy-egy kibertéri történés jogi megítélésében.[62]

2013-ban belga kezdeményezéssel indult nemzetközi útjára a Károskód Információcsere Platform,[63] melynek célja a rosszindulatú kódok jellemzőivel kapcsolatos információk megosztása egy megbízható közösségen belül a támadás részleteinek megosztása nélkül. A platform már működik néhány nemzet és a NATO Számítógépes Incidenskezelő Képesség között. A projekt végső célja egy olyan NATO-képesség kialakítása, ami minden NATO nemzet számára elérhető és amire a nemzetek rábízzák az információk megosztását.[64]

2013-as nemzeti esemény, hogy kormányhatározat döntött a kormányzati hálózatbiztonsági feladatokat ellátó Puskás Tivadar Közalapítvány megszüntetéséről. Ennek megfelelően a kormányzati feladatok a Nemzetbiztonsági Szakszolgálathoz kerültek, figyelemmel a kiadás előtt álló, elektronikus információbiztonsági törvényre.[65]

A határozat egyben emlékeztet, hogy Hazánkban 2005-ben kezdődött hivatalosan a kormányzati eseménykezelés,

[60] The Secretary General's Annual Report 2013, „Cyber defence" fejezet, 18. o.
[61] Tallinn Manual on the International Law Applicable to Cyber Warfare.
[62] Peacetime Regime, (https://ccdcoe.org/news/2013/newsletter-peacetime-regime/).
[63] Malware Information Sharing Platform (MISP).
[64] Sharing malware information to defeat cyber attacks, (https://www.nato.int/cps/en/natohq/news_105485.htm).
[65] 1284/2013. (V. 27.) Korm. határozat a Puskás Tivadar Közalapítvány megszüntetésével kapcsolatos feladatokról.

információcserét, konzultációt biztosítva az igénylő szervezetek részre. Honvédelmi szempontból ez még nem jelentett napi jellegű technikai információcserét, de részletek említése nélkül is kijelenthető, hogy az eseti jellegű együttműködés hatékony segítség volt a felek számára.

Az évben később megjelenő elektronikus információbiztonságról szóló törvény[66] több szempontból is kritikus eleme a magyar elektronikus információbiztonságnak. Ezt megelőzően az elektronikus információs rendszerek biztonságára vonatkozóan nem állt rendelkezésre egyértelmű, jogszabályokban meghatározott követelmény.

Az új jogszabályok (a törvény és végrehajtási rendeletei) meghatározzák az alapvető feladatokat, kijelölik a nemzeti szintű felelős szervezeteket (eseménykezelés és elektronikus biztonsági hatóság) és meghatározzák például az események bejelentésére vonatkozó kötelezettséget, ami egyértelműen segíti a honvédelmi és a nemzeti szintű együttműködést.[67]

2013-ban a vonatkozó jogszabályi követelmények szerinti ágazati szinten meg kellett határozni az elektronikus információs rendszerek biztonságával kapcsolatos felelősségeket, hatásköröket. Ennek megfelelően megtörtént a honvédelmi ágazati kijelölés, miniszteri rendelet formájában.[68]

A *2014-es NATO Wales Csúcsértekezlet* további lényeges tartalmi elemeket határoz meg. A fenyegetések kapcsán a dokumentum megállapítja, hogy a kibertámadások elérhetik azt a küszöböt, ami veszélyezteti a nemzeti és euro-atlanti jólétet, biztonságot és stabilitást. Hatásuk ugyanolyan káros lehet a modern társadalmakra, mint egy hagyományos támadás. Ezért a Szövetség megerősíti, hogy a kibervédelem a NATO alapvető feladatának, a kollektív védelemnek a része.

A szövetségesek elkötelezettek a nemzeti kibervédelmi képességek tovább fejlesztésében és erősíteni fogják azon nemzeti rendszerek kiberbiztonságát, melyektől a NATO alaprendeltetésű feladatai függenek, a Szövetség ellenálló képessége és teljes mértékű védelme érdekében.

A szoros kétoldalú és multinacionális együttműködés kulcsfontosságú szerepet játszik a Szövetség kibervédelmi képességeinek fejlesztésében.

A szövetségesek folytatják a kibervédelem NATO műveletekbe, hadműveletekbe és a folytonossági (contingency) tervekbe történő integrálását és erősítik az információcserét és a

[66] 2013. évi L. törvény az állami és önkormányzati szervezetek elektronikus információbiztonságáról.

[67] A törvény a bevezetőben megfogalmazza, hogy a kiberbiztonság a bizalmasság, sértetlenség és a rendelkezésre állás megvalósulával biztosítható. Ezzel együtt a törvény az elektronikus információbiztonságról szól, így túlzásnak tekinthető azt „kibertörvény”-ként említeni.

[68] Szakmai érdekesség, hogy a NATO csatlakozás idejében szükséges jogi szabályozáson kívül miniszteri rendelet ezen a szakterületen nem jelent meg. 16/2013. (VIII. 30.) HM rendelet a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről (hatályon kívül).

helyzetismeret képet (situation awareness) a szövetségesek között. [69]

2014-es esemény, hogy a nemzeti felkészülés érdekében megjelent a NATO elektronikus információbiztonsági és kiberbiztonsági[70] minimum követelmény rendszer azon nemzeti információs infrastruktúrák számára, melyek kritikusan fontosak a Szövetség alaprendeltetésének biztosításához.

A *NATO főtitkár 2014-es évre vonatkozó jelentése* szerint előre tekintve látható, hogy a számítógépes fenyegetések és támadások egyre gyakoribbak, kifinomultabbak és potenciálisan károsak.

A kiber domain változó kihívásaira reagálva a NATO vezetői a szeptemberi Walesi Csúcstalálkozón jóváhagyták a NATO Megerősített Kibervédelmi Politikát és az Intézkedési Tervet. A Politika megállapítja, hogy a kibervédelem a Szövetség kollektív védelem alapfeladatának része, megerősíti, hogy a nemzetközi jog érvényes a kibertérben, illetve fokozni kell a NATO és az ipar közötti együttműködést.

A NATO kibervédelem legfontosabb prioritása a NATO tulajdonában lévő és üzemeltetett kommunikációs rendszerek védelme.

2014 májusában a NATO Számítógépes Incidenskezelő Képesség elérte a teljes működési képességet, és a NATO hálózatok védelmét 52 helyszínre bővítette.

A NATO 2014-ben is folytatta a kibervédelmi komponensek beépítését gyakorlatokba, képzésekbe és az oktatásba.

2014 novemberében a Szövetség megtartotta eddigi legnagyobb kibergyakorlatot a NATO Cyber Range (teszt labor) segítségével, ami egy szoftveralapú megoldások tesztelésére és értékelésére szolgáló platform a biztonsági problémák megoldása érdekében.[71]

A *NATO főtitkár 2015-ös évre vonatkozó jelentése szerint a* NATO folyamatosan figyelemmel kíséri a kiber domain-ben tapasztalható fenyegetések gyors evolúcióját – nem csak mennyiség, hanem a bonyolultság tekintetében is.

Növekvő jelleggel tapasztalható a kártékony szereplők előnyszerzése a digitális alvilágban, mint a gyors és költséghatékony megoldás a céljaik elérése (szolgáltatás megszakítás vagy sérülések okozása).

A Szövetség az első Kibervédelmi Politikát 2008-ban adta ki, röviddel az Észtországot érő súlyos kibertámadások után. A NATO 2014-ben elfogadta az új Megerősített Kibervédelmi Politikát és az Intézkedési Tervet.

A Politika megfogalmazza, hogy a kollektív védelem részeként a kibervédelem a NATO alaprendeltetésű feladata (core task), megerősíti, hogy a nemzetközi jogot alkalmazni kell a kibertérben, és fokozni kell a NATO együttműködését az ipari szektorral.

Az elsődleges feladat (top priority) Szövetség tulajdonában, vagy üzemeltetésében lévő CIS védelem.

A NATO a kibervédelmet integrálta a védelmi tervezési folyamatba, a műveleti

[69] Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 2014, 72–73. o.

[70] Pontos kifejezés szerint: CIS Security (including cyber defence).

[71] The Secretary General's Annual Report 2014, „Cyber security" fejezet, 15. o.

tervezésbe, a válságkezelési rendszabályokba, valamint a katonai és politikai jellegű gyakorlatokba.

Új Kibervédelmi Katonai Koncepció[72] kiadása történt 2015. szeptemberben, a NATO struktúráján belüli a kibervédelem keretrendszer meghatározása érdekében.

A NATO Számítógépes Eseménykezelő Képesség a NATO rendszereket védi központosított, folyamatos (round-the-clock) kibervédelmi támogatást nyújtva a NATO helyszínek felé.

A NATO Kommunikációs és Információs Ügynökség[73] a monsi NATO Számítógépes Incidenskezelő Képesség, Technikai Központon (Technical Centre) keresztül felelős a NATO szintű technikai jellegű kibervédelmi és információvédelmi[74] támogatásért. Kezeli és jelenti az incidenseket, terjeszti a fontos incidensekkel kapcsolatos információkat a rendszer- a biztonsági menedzsmentek és a felhasználók felé.

Az évben megtörtént a kibervédelmi képesség célkitűzések integrálása a NATO védelmi tervezési folyamatba. Az EU-val és az EBESZ[75]-el szoros az együttműködés különösen a kiberfenyegetésekkel kapcsolatos információmegosztás és a bizalomerősítő rendszabályok[76] kialakítása a kibertérben területeken. [77]

2015-ben egy NATO híradás számol be a NATO Kiber Gyorsreagáló Csoport (2013-as) felállításáról. Cél a kibertámadást elszenvedő NATO nemzetek, létesítmények felé történő segítségnyújtás.

A kibertámadások pusztító következményekkel járhatnak, amelyek olyan súlyosak is lehetnek, mint a hagyományos támadások bombákkal és harckocsikkal. A csoport minden szükséges felszereléssel rendelkezik: számítógépes és telekommunikációs eszközök, behatolásérzékelők, műszaki elemzés (távolról vagy az érintett rendszeren), sérülékenységvizsgálat, hálózatbiztonság. A csoport nem egy hétköznapi kibervédelmi probléma vagy napi szintű kibertámadások megoldására alakult, a bevetés soha nem tervezett – ez a végső megoldás.[78]

Egy korábbi híradás szerint a gyorsreagáló csoport aktivizálása szabályozott. Bármely NATO-tagország, amely jelentős kibertámadást szenved el, igényelheti a NATO segítségét. A kérelmet a Kibervédelmi Menedzsment Felügyelet bírálja el.

A NATO-n kívüli országokból érkező kérelmeket az Észak-atlanti Tanácsnak kell jóváhagynia.[79]

A *2016-os NATO Varsói Csúcsértekezlet* a publikációelején már idézett követelmény mellett megállapítja,

[72] Military Concept for Cyber Defence.
[73] NATO Communications and Information Agency – NCIA.
[74] Information Assurance.
[75] Európai Biztonsági és Együttműködési Szervezet (EBESZ). Organisation for Security and Co-operation in Europa (OSCE).
[76] Confidence-building measures.
[77] The Secretary General's Annual Report 2015, „Cyber Security" fejezet, 23. o.

[78] Men in black – NATO's cybermen (https://www.nato.int/cps/en/natohq/news_118855.htm).

[79] NATO Rapid Reaction Team to fight cyber attack (https://www.nato.int/cps/en/natohq/news_85161.htm).

hogy a kibertámadások egyértelmű kihívást jelentenek a Szövetség biztonsága szempontjából és ugyanolyan károsak lehetnek a modern társadalmakra, mint a hagyományos támadások.

Walesben megállapodás történt, hogy a kibervédelem a NATO alapvető feladatának, a kollektív védelemnek része.

Varsóban a Szövetség megerősítette a védelmi mandátumot és a kiberteret olyan műveletek területnek ismerte el, amelyben a NATO-nak ugyanolyan hatékonyan kell védenie önmagát, mint a levegőben, a szárazföldön és a tengereken.

A dokumentum szerint a Szövetség megerősíti az elkötelezettséget, hogy a nemzetközi joggal – beleértve az ENSZ Alapokmányt, a nemzetközi humanitárius jogot és az emberi jogokat – összhangban jár el. A Szövetség továbbra is a visszafogottság elvét fogja követni és támogatni fogja a nemzetközi béke, biztonság és stabilitás fenntartását a kibertérben.

A Szövetség üdvözöli a felelős állami magatartás önkéntes nemzetközi normáival és a kibertérrel kapcsolatos bizalomépítő intézkedésekkel kapcsolatos munkát.

A szövetségesek a Kibervédelmi Kötelezettségvállalással egyértelműen jelezték, hogy prioritásként kezelik a nemzeti hálózataik és infrastruktúráik kibervédelmének megerősítését. Minden szövetséges tiszteletben tartja felelősségét az ellenálló képesség és a kibertámadásokra adott gyors és hatékony válaszadás növelése érdekében, beleértve a hibrid összefüggéseket is.

A NATO készen áll arra, hogy segítsen egy szövetségest a hibrid kampány bármely szakaszában. A kollektív védelem részeként a Szövetség és a szövetségesek készen fognak állni a hibrid hadviselés elleni küzdelemre.[80]

A 2016-os NATO Kibervédelmi Kötelezettségvállalás alapján a szövetséges állam- és kormányfők ígéretet tesznek, hogy a Szövetség lépést tart a kiberfenyegetettség gyorsan fejlődő környezetével és a nemzetek képesek lesznek megvédeni magukat a kibertérben, mint a levegőben, szárazföldön és a tengeren.

A szövetségesek megerősítik nemzeti felelősségüket a nemzeti infrastruktúrák és hálózatok kibervédelmének fokozásában, valamint elkötelezettségüket a szövetséges biztonság és kollektív védelem oszthatatlansága mellett, összhangban a Walesben elfogadott a NATO Megerősített Kibervédelmi Politikával.

A szövetségesek megerősítik a nemzetközi jog alkalmazhatóságát a kibertérben, és elismerik az érintett nemzetközi szervezetekben végzett munkát, többek között a felelős állami magatartás önkéntes normái és a kibertérben a bizalomépítő intézkedések terén.

A szövetséges állam- és kormányfők ígéretet tesznek arra, hogy prioritásként megerősítik, fokozzák a nemzeti hálózatok és infrastruktúrák kibervédelmét. A NATO kibervédelmi képességeinek folyamatos adaptálásával együtt - a NATO hosszú távú alkalmazkodásának részeként -, ez megerősíti a Szövetség kibervédelmét és

[80] Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016; 70–72. o.

általános ellenálló képességét. Kötelezettségvállalási célok:

1) A képességek legszélesebb skálájának fejlesztése a nemzeti infrastruktúrák és hálózatok védelme érdekében; különösen a kibervédelem legmagasabb stratégiai szintű kezelése a védelemmel kapcsolatos szervezeteken belül, a kibervédelem további integrálása a műveletekbe és a képességek kiterjesztése a telepíthető hálózatokra.
2) Nemzeti szintű, megfelelő források elkülönítése a kibervédelmi képességek megerősítése érdekében.
3) A nemzeti kibervédelemért felelős szervezetek közötti kooperáció erősítése, az együttműködés mélyítése és a bevált gyakorlatok cseréje érdekében.
4) A kiberfenyegetések megértésének fejlesztése, beleértve az információ megosztás és a vizsgálatok fejlesztését.
5) Az alapvető kiber higiéniához szükséges szakértelem és tudatosság növelése egészen a fejlett és robosztus kibervédelmi szint biztosításáig nemzeti szinten a szükséges felelős szervezeteknél.
6) A kibervédelmi erők oktatásának, képzésének és gyakorlásának elősegítése, az oktatási intézmények fejlesztése a Szövetségen belüli bizalom és tudásbázis kiépítése érdekében.
7) Az elfogadott kibervédelmi kötelezettségvállalások végrehajtásának felgyorsítása, beleértve azokat a nemzeti rendszereket is, amelyek a NATO felé nyújtanak szolgáltatást (és ezáltal függőséget jelentenek).

A szövetségesek a Kötelezettségvállalást évente áttekintik.[81] Az évek során kialakult a vállalással kapcsolatos eljárásrend, ami az éves változások közlése mellett szervezett konzultációt biztosít, illetve a további részben látható éves konferencia ezen túlmenően is információcsere lehetőséget teremt a szövetségesek között és a szövetséges – NATO viszonylatban is.

A 2016-os év eseménye annak megerősítése, hogy a kibertámadások növekvő fenyegetésével szemben a NATO és EU hasonló kihívásokkal néz szembe a hálózatok védelme területén. Annak érdekében, hogy mindkét szervezet jobban megfeleljen a kihívásnak, technikai megállapodás született a NATO Számítógépes Eseménykezelő Központ (NCIRC) és az EU Számítógépes Eseménykezelő Központ[82] között. A technikai megállapodás keretet biztosít az eseménykezelő szervezetek közötti információcseréhez és a bevált gyakorlatok megosztásához. *Kiterjed a konkrét kiberfenyegetésekkel kapcsolatos információcserére, valamint a műszaki eljárásokra, a hálózatok konfigurálására és az iparággal való partnerségre vonatkozó bevált gyakorlatok megosztására*.[83]

A *NATO állam és kormányfők 2016-os Varsói Nyilatkozata* szerint a szövetségesek

[81] Cyber Defence Pledge, 1, 3, 5. o. (https://www.nato.int/cps/en/natohq/official_texts_133177.htm).

[82] Computer Emergency Response Team (CERT-EU).

[83] NATO and the European Union enhance cyber defence cooperation

elkötelezték magukat, hogy továbbra is fokozzák ellenálló képességünket a teljes spektrumú fenyegetésekkel szemben - beleértve a hibrid fenyegetéseket -, bármilyen irányból is érkezzenek azok.

Növelik az ellenálló képességet a robusztus, rugalmas és interoperábilis katonai képességekbe történő befektetéssel, összhangban a NATO ambíciói szintjével és a Walesi Csúcstalálkozón tett védelmi beruházásokra tett ígéretekkel.

Védeni fogják a katonai ellátási láncokat és azon dolgoznak, hogy adott esetben nemzeti erőfeszítések és multinacionális együttműködés révén kezeljék az orosz forrásokból származó örökölt katonai felszerelések meglévő függőségeit.

Kiemelten megerősítik és fokozzák nemzeti infrastruktúrák és hálózatok védelmét a növekvő fenyegetés és a nagy bonyolultságú kibertámadások ellen.[84]

A *NATO főtitkár 2016-os évre vonatkozó jelentése szerint* ***a*** kiberfenyegetések és támadások egyre gyakoribbak, kifinomultabbak és károsabbak. Ezek a támadások leállíthatják az infrastruktúrákat, aláásható a demokratikus rendszereket és hatással lehetnek a katonai műveletekre.

A változó biztonsági környezet fényében a kibervédelem kulcsfontosságú prioritássá vált. A technikai lehetőségből egy olyan műveleti területté fejlődött, ahol a NATO-nak ugyanolyan hatékonyan kell fellépnie, mint a szárazföldön, a levegőben vagy a tengeren.

Más szervezetekhez hasonlóan a NATO-nak is gyorsan változó kibervilággal kell szembenéznie, ahol egyre gyakoribbak a konkrét és célzott támadások. Az ilyen támadások észlelése a hatalmas mennyiségű hagyományos online tevékenység közepette kifinomult képességeket és szakértelmet igényel.

A NATO Varsói Csúcstalálkozón a szövetségesek két fontos döntést hoztak a változó kiberfenyegetési kép[85] ellensúlyozása érdekében.

A szövetségesek a kiberteret műveleti területként ismerték el, ahol a NATO-nak meg kell védenie magát hasonlóan a légi, földi, vagy tengeri műveletekhez. Így a NATO struktúra képes lesz kiemelt figyelmet fordítani a missziók és műveletek védelmére a kiber fenyegetések ellen, koncentrálva a kiberrel kapcsolatos képzésekre, illetve kétséges vagy sérült biztonságú kiberkörnyezetben történő művelettervezésre. Ez nem jelent változást a NATO missziók mandátumaiban, melyek továbbra is védelmi jellegűek maradnak, követve a nemzetközi normák által meghatározottakat.

A szövetségesek kötelezettséget vállaltak a kibervédelmi képességek prioritással történő megerősítésére és kiterjesztésére – beleértve a nemzeti infrastruktúrák és hálózatok védelmét is.

Technikai eredmény, hogy 19 nemzet frissítette a NATO-val történő együttműködési megállapodást, illetve e

(https://www.nato.int/cps/en/natohq/news_127836.htm).

[84] Commitment to enhance resilience Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016, 1, 6, 7. o.

[85] Cyber threat landscape.

mellett a NATO Számítógépes Incidenskezelő Képesség és az EU Számítógépes Eseménykezelő Központ[86] együttműködési megállapodást kötött.[87]

2016-os nemzeti esemény, hogy a honvédelmi ágazati elektronikus információbiztonsági hatósági felügyeleti feladatok elkülönültek az állami és önkormányzati szervezetekre vonatkozó szabályozásban és a KNBSZ főigazgató hatáskörébe kerültek.[88]

Az évben megújult a korábban említett, 2010-ben megkötött NATO - magyar kibervédelmi együttműködési megállapodás. A kapcsolattartási feladatok ezzel a lépéssel a honvédelmi ágazathoz kerültek.

A „második generációs" együttműködési megállapodás fókuszában a védelempolitikai szintű kapcsolattartás mellett a szövetségesi együttműködést támogató, azonnali információcsere szükséglet áll. A szövetségi vagy magyar rendszereket ért incidensekről, sérülékenységekről szóló azonnali intézkedést kiváltó kölcsönös riasztások, tájékoztatások a technikai szintű, napi működés támogatását szolgálják. A NATO felől érkező adatok feldolgozás után a Nemzeti Kibervédelmi Intézet felé történő továbbítása biztosítja az érintett magyar kormányzati vagy egyéb szervezetek információkkal történő támogatását.[89]

A *2017-re vonatkozó NATO főtitkári éves jelentés* megállapítja, hogy a mai világban a kiberfenyegetések egyre kiterjedtebbek, kifinomultabbak és károsabbak, mint valaha. Egy kibertámadás legrosszabb esetben veszélyeztetheti egy ország kritikus infrastruktúráját, megbéníthatja kormányát, alááshatja demokratikus rendet, vagy befolyásolják a fegyveres erők műveleti hatékonyságát.

A NATO fokozta a Szövetség kommunikációs hálózatainak és információs rendszereinek védelmét, az egyes szövetségesek támogatását a nemzeti kibervédelemben, illetve a testre szabott tanácsadást a partnerek számára.

2017-ben növekedett a választék a szolgáltatások megzavarására alkalmazott technikákban, a kémkedésben vagy a Szövetség reputációjának megsértésében, beleértve a NATO webhelyek szolgáltatásainak megszakítására tett kísérleteket is.

A NATO folyamatos védelmet nyújt hálózatok számára a NATO Kommunikációs és Információs Ügynökség által biztosítva, illetve gyors reagálású kibervédelmi csoportokat tart készenlétben, rövid reagálási idejű telepíthetőséggel (a NATO infrastruktúra védelme és a szövetségesek támogatása érdekében).

Az évben a NATO illetékes szervezetei folytatták a tervek, képzések pontosítását a missziók és műveleteket kiber fenyegetések

[86] EU Computer Emergency Response Team – CERT.
[87] The Secretary General's Annual Report 2016, „Cyber Defence" fejezet, 24. o.
[88] 22/2016. (II. 17.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet módosításáról, 1. §.
[89] Hungary signs new MoU on cyber defence cooperation; (https://nicp.nato.int/hungarysigns-new-mou-on-cyber-defence-cooperation/index.html).

elleni védelme érdekében a Varsói Csúcstalálkozón a kibertér műveleti területté történő kinyilvánítás követéseként, mely szerint a NATO-nak képesnek kell lenni megvédeni önmagát, akárcsak a levegőben, a szárazföldön, és tengeren.

A kibervédelem szerepet játszik a NATO parancsnoki struktúra adaptálásáról szóló egyeztetésekben, a szövetségesek nemzeti kiber képességeinek a NATO műveletekbe történő legjobb integrálása érdekében. Ez egy új kiber műveleti központ kialakítására vonatkozó lehetőség vizsgálatát jelenti. Mint minden más műveleti területen, a NATO működése a kibertérben is védelmi jellegű, arányos műveleteket alkalmazó (proportionate) és teljes körűen összhangban áll a nemzetközi joggal.

A robusztus kibervédelem megköveteli a Szövetségtől, hogy lépést tartson a technológiai változások gyors ütemével. A NATO konzultál, együttműködik és valós idejű információkat oszt meg a kiberfenyegetésekről szövetségeseivel, partnereivel és más nemzetközi szervezetekkel, például az EU-val, valamint az iparral.

Például a 2017-es nagy horderejű WannaCry és NotPetya kibertámadások során a NATO kibervédelmi szakértői gyorsan egyeztettek a szövetségesekkel, az EU partnerekkel, az ipari partnerekkel, hogy a legfrissebb képet kaphassanak a bonyolult és gyorsan fejlődő eseményekről.[90]

A 2017-es év nemzeti eseménye a korábban jelzett honvédelmi felelősségi kör kijelölésének folytatásaként, hogy a jogszabályokban meghatározott szakfeladatok végrehajtása érdekében megjelent az eseménykezelésre, sérülékenységvizsgálatra és hatósági feladatokra vonatkozó HM utasítás.[91]

A *2018-as NATO Brüsszeli Csúcsértekezlet* megállapítása szerint a Szövetség veszélyes, előre jelezhetetlen és képlékeny (fluid) biztonsági környezetben, tartós fenyegetésekkel és kihívásokkal találkozik minden stratégiai irányból, állami és nem állami szereplőkkel-, katonai erővel-, terroristákkal-, kiber és hibrid támadásokkal szembe – beleértve a megtévesztő kampányokat[92] és a kártékony célú kibertevékenységeket.[93]

A Szövetség folytatja a hírszerzés optimalizálását, elősegítve a NATO időbeli és relaváns döntés előkészítését és műveleteit, beleértve az előrejelzést és a hírszerzési adatok megosztását, kiemelten a terrorizmus, hibrid és kiber területeken.

A kibervédelem része a NATO kollektív védelmének. Ugyanolyan hatékonyan kell működni a kibertérben, mint a levegőben, a szárazföldön és a tengereken, megerősítve és támogatva a Szövetség általános elrettentési és védelmi jellegét. Ezért folytatni kell a kibertér műveleti területként történő alkalmazásának megvalósítását.

---

[90] The Secretary General's Annual Report 2017, „Investing in Cyber Defence" fejezet, 19–20. o.

[91] 15/2017. (IV. 28.) HM utasítás a honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság és a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ feladatainak végrehajtásáról, valamint a sérülékenységvizsgálat lefolytatásának szabályairól.

[92] Disinformation campaigns.

[93] Malicious cyber activities.

A szövetségesek megállapodtak az önkéntesen biztosított kiberhatások[94] erős politikai felügyelet keretében történő integrálásában a Szövetség műveleteibe és misszióiba.

Megerősítve a NATO védelmi jellegét, a szövetségesek elhatározták, hogy a képességek teljes skáláját alkalmazzák az elrettentés és a védelem érdekében a kiberfenyegetések teljes spektruma ellen, beleértve a hibrid kampány részeként végrehajtottakat is.

További lépésként meg kell erősíteni a hírszerzés által vezérelt helyzetismeretet[95] a NATO döntéshozatalának és műveleteinek támogatása érdekében. Olyan intézkedéseket kell kidolgozni, amelyek alapján növekedjenek a költségei azoknak, akik ártani akarnak a Szövetségnek.

A szövetségesek adott esetben fontolóra vehetik a rosszindulatú kiberaktivitás betudását (attribution) és az arra történő koordinált válaszadást, ezzel egyidejűleg megerősítve, hogy a betudás szuverén nemzeti hatáskör.

A Szövetség megerősíti kötelezettségvállalását abban, hogy cselekvései összhangban lesznek a nemzetközi joggal – beleértve az ENSZ Alapokmányát, a nemzetközi humanitárius jogot és az emberi jogokat –, ahol azok alkalmazása szükséges.

A Szövetség támogatja továbbá a munkát a kibertérben a nemzetközi béke és biztonság fenntartása-, valamint a stabilitás elősegítése és a konfliktusok kockázatának csökkentése érdekében, felismerve, hogy a normákon alapuló (norms-based), kiszámítható és biztonságos kibertér mindenki számára hasznos lehet.

A Szövetség Kibertér Műveleti Központot[96] alakít Belgiumban, helyzetismeret képet és koordinációt biztosítva a NATO műveletekhez a kibertérben.[97]

A *NATO főtitkár 2018-as évre vonatkozó jelentése* szerint az ellenálló képesség a sokkszerű hatásokkal szemben történő ellenállást, illetve visszaállítás képességét jelenti természeti katasztrófa, hagyományos fegyveres támadás vagy hibrid művelet esetén. A szövetségesek ellenálló képessége és civil felkészülése létfontosságú a NATO kollektív védelme és biztonsága érdekében. Az ellenállóképesség a védelem első vonala.

A fegyveres erők erősen függenek a civil infrastruktúráktól és képességektől beleértve az élelmiszert és vizet, kommunikációt és szállítást. Az országok civil infrastruktúrájának ellenállóképessége ugyanolyan fontos, mint a katonai infrastruktúrák, így a civil felkészülés alapvető fontosságú a NATO elrettentési és védelmi képessége szempontjából.

A NATO Brüsszeli Csúcstalálkozón (2018) a szövetségesek kinyilvánították, hogy a kibervédelem a NATO kollektív védelmének, alapfunkciójának része, így a Szövetségnek hatékonyan kell működnie a kibertérben, mint azt teszi a levegőben,

[94] Sovereign cyber effects.
[95] intelligence-led situational awareness.
[96] Cyberspace Operations Centre.

[97] Brussels Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018; 1, 13, 20, 29. o.

szárazföldön és tengereken. A NATO elsődleges prioritása marad a saját hálózatok védelme, világszerte.

2018-ban a szövetségesek a Kibervédelmi Kötelezettségvállalás mentén folyamatosan dolgoztak a saját nemzeti hálózatok ellenálló képességének növelésén.

A NATO-nak nincs saját offenzív kiber képessége és nincs terv ilyen képesség kifejlesztésére. Más műveleti területekhez hasonlóan a NATO a szövetségesek által felajánlott képességekkel fog rendelkezni. A 2017-es politikai irányelvek szerint néhány szövetséges nyilvánosan felajánlotta nemzeti kiber kapacitásának integrálását szövetségi műveletekbe és missziókba (szükség esetén).

A kibervédelem fontos együttműködési terület az EU-val. A NATO és EU törzsek növekvő számban vesznek részt közösen gyakorlatokon[98] melyek kiber elemeket is tartalmaznak.

A 2016-os közös deklaráció óta a két szervezet kiterjedt, részletekre kitérő információcserét folytat a kiber krízisek kezelésének megközelítéséről.[99]

A 2018-as párizsi Kibervédelmi Kötelezettségvállalás Konferencián a NATO főtitkár összefoglalta a közelmúlt legfontosabb történéseit. Rámutatott, hogy 2014-ben a NATO vezetői egyetértettek abban, hogy egy kibertámadás elindíthatja az Alapszerződés 5. cikkét. Ennek értelmében egy szövetséges elleni támadást minden szövetséges elleni támadásként kell kezelni. Hagyományosan az 5. cikk szerinti támadás harckocsikkal, repülőgépekkel és katonákkal történik. Most kibertámadás formájában is megvalósulhat. A kiber a tevékenységek középpontjába került.

2016-ban a NATO vezetői a kiberteret „műveleti területnek (domain)" azonosították a szárazföld, a tenger és a levegő mellett. Ez azt jelenti, hogy felül kell vizsgálni mindent, a legmagasabb szinttől a legalacsonyabbig.

Ugyancsak 2016-ban a nemzetek vezetői egyetértettek a Kibervédelmi Kötelezettségvállalással. Ennek eredményeként kevesebb, mint két év alatt szinte minden szövetséges korszerűsítette a kibervédelmet.

Az új parancsnoki struktúra részeként megalakult a NATO Kibertér Műveleti Központ. Megkezdődött a kiber integrálása a tervezésbe és a műveletekbe. Üdvözletes, hogy néhány szövetséges nemzeti kiber képességeivel hozzájárul a NATO műveletekhez.

A NATO gyorsreagálású csoportjai[100] készenlétben állnak a szövetségesek segítésére a nap 24 órájában.

A súlyos kibertámadásokra a Szövetség választ tud adni akkor is, ha azok nem lépik át az 5. cikk szerinti küszöböt. De bármi legyen is a válasz, a NATO továbbra is a visszafogottság elvét (restrain principle) fogja követni és a nemzetközi jognak megfelelően jár el.

Gyakran nehéz tudni, hogy ki áll a támadás mögött – legalábbis kezdetben. A betudás (attribution) fontos szerepet

[98] NATO's Cyber Coalition and the EU's Parallel and Coordinated Exercise.

[99] The Secretary General's Annual Report 2018, „A More Resilient NATO" és „Securing Cyberspace" fejezetek, 22, 24. o.

[100] Cyber Rapid Reaction Teams.

játszhat a jövőbeli támadások elrettentésében is.[101]

A 2018-as év nemzeti eseménye a magyar csatlakozás a Károskód Információmegosztó Platformhoz, ami folyamatos technikai információcsere lehetőséget biztosít az eseménykezelés támogatása érdekében.

A megalakult NATO Kibertér Műveleti Központ kezdő csapatában egy magyar tábornok – Vass Sándor – látott el vezetői beosztást, ami egyértelmű büszkesége lehet a nemzeti színeknek.

A 2019-es Londoni Csúcsértekezlet deklarációja szerint a Szövetség folytatja a társadalom, a kritikus infrastruktúra és az energia biztonság területén az ellenállóképesség növelését.

A NATO és a szövetségesek elkötelezettek a saját hatáskörön belül a kommunikáció biztonságában (beleértve az 5G technológiát), felismerve a rendszerek biztonságának és ellenálló képességének fontosságát.

A Szövetség fejleszti eszközeit a kibertámadások elleni válaszokra és erősíti képességeit felkészülés, elrettentés és a hibrid taktikák elleni védelem területein, melyek a társadalom és a biztonság aláaknázását célozzák.[102]

A *2019-re vonatkozó NATO főtitkári éves jelentés* szerint a kibervédelem a NATO kollektív védelemre vonatkozó alaprendeltetés része. A súlyos hatásokkal járó kibertámadások kiválthatják az 5. cikkely alkalmazását.

A NATO tagállamok elsődleges felelőssége a nemzeti kibervédelem – és mivel a NATO kibervédelme az összekapcsolásokon alapul –, így az olyan erős, mint a leggyengébb láncszem. Emiatt a szövetségesek kötelezettséget vállaltak, hogy a kibervédelem megerősítését prioritással kezelik. A NATO támogatni fogja szövetségeseit ebben az erőfeszítésben.

A NATO szervezeti struktúra modernizálás keretében a Kibertér Műveleti Központ elérte a műveleti képességét. A szövetségesek egyetértettek abban, hogy saját kibertér műveleti képességeikkel támogatják a NATO műveleteit, így számos nemzet felajánlotta már képességeit. A szövetségesek teljes mértékben megtartják felügyeleti jogaikat saját nemzeti kiberműveleti képességeik felett a NATO missziók és műveletek támogatása során.

A NATO folytatólagosan támogatta a szövetségeseket a Kibervédelmi Kötelezettségvállalás teljesítésében a három évvel korábban, Varsóban tett vállalás szellemében a nemzeti kiber ellenállóképesség erősítése érdekében.

A szövetségesek fejlesztették jogi és szervezeti keretrendszerüket, folyamatosan erősítették pénzügyi és humán erőforrásaikat a kiberfenyegetések ellensúlyozása érdekében.[103]

A *2019-es londoni Kibervédelmi Kötelezettségvállalás Konferencián NATO főtitkár szerint* a kiber támadások egyre gyakoribbak, összetettebbek és

[101] Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole militaire, Paris) (2018).

[102] London Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London 3-4 December 2019, 6. o.

[103] The Secretary General's Annual Report 2019, „Cyberspace as Part of NATO's Core Task of Collective Defence" fejezet, 27. o.

pusztítóbbak. A NATO nem immunis. Minden nap érzékelhetők gyanús események a NATO kiber rendszerei ellen.

A kiber fenyegetések az új technológiák fejlődésével veszélyesebbé válnak, mint például a mesterséges intelligencia, a gépi tanulás és a deep fakes.[104] Ezek a technológiák alapvetően megváltoztatják a hadviselés jellegét, legalább annyira, mint az ipari forradalom. A NATO alkalmazkodik ehhez az új valósághoz.

A NATO vezetői megállapodtak abban, hogy egy kibertámadás aktivizálhatja az Alapszerződés 5. cikkét. E szerint egy szövetséges elleni támadást mindenki elleni támadásként kell kezelni. A NATO a kiberteret katonai műveleti területnek jelölte ki, a szárazföld, a tenger és a levegő mellett.

A 2018-as Brüsszeli Csúcstalálkozón megállapodás született a Kibertér Műveleti Központ létrehozásában. Megállapodás történt a nemzeti kiber (vagy offenzív) képességek Szövetség műveleteibe és misszióiba történő integrálásába.

A Kibervédelmi Kötelezettségvállalás segíti a szövetségeseket a védelem fokozásában. A szövetségesek megerősítették kiber képességeiket, javították jogi és intézményi kereteiket, növelték a kiber fenyegetések kezelésére fordított erőforrásokat - munkaerőt és pénzeket.

Ahhoz, hogy az elrettentés teljes hatást érjen el, a potenciális támadóknak tudniuk kell, hogy a NATO nem korlátozódik a kibertérben történő válaszadásra, amikor a kibertérben éri támadás. A rendelkezésre álló képességek teljes skáláját tudjuk és fogjuk alkalmazni.

A NATO 70 éve tartja biztonságban az embereket a fizikai világban. Most a NATO-nak ugyanezt kell tennie a kiber világban is. Ehhez meg kell tartani a technológiai előnyt, biztosítani kell az új technológiák lehetséges előnyeinek kiaknázását, a lehetséges kockázatok minimalizálása mellett.

A kiber túlmutat a technológián. A technológia mögött álló emberek ugyanolyan fontosak. A jövőbeli kiber specialistákból („future cyber defenders”) erős és sokféle munkaerőt kell építeni.

Gondoskodni kell arról, hogy a készségek rendszeres gyakorlatok révén bevethetők (élesek) legyenek, ahogyan az a NATO Cyber Coalition – a világ egyik legnagyobb kibervédelmi gyakorlata – révén történik.[105]

2019-ben nemzeti szempontból jelentős esemény a Magyar Honvédség Parancsnokságának megalakulása. A Parancsnokságon belül kibervédelmi szakfeladatok ellátására a haderőnemi szemlélőségek rendjében kijelölt szervezeti elem jelenik meg, a haderőnemi szemlélő (kibervédelmi). A funkció részletezése nélkül megállapítható, hogy a korábbi, kibervédelmi szervezetépítési események mellett ez az első olyan lépés, ami a Honvédségnél a kibertérben rejlő lehetőségek katonai megvalósítását célozza.

A *NATO 2020-ra vonatkozó főtitkári éves jelentés* szerint a biztonságos kibertér elengedhetetlen a Szövetség minden

[104] Deep fakes: *pontos fordítás még nem alakult ki, jelentése: mesterséges intelligencia segítségével módosított (hamisított) média tartalom.*

[105] Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London.

tevékenységéhez. Ezért a kibervédelem része a NATO kollektív védelem alapvető feladatának. A NATO világossá tette, hogy egy súlyos kibertámadás a Washingtoni Szerződés 5. cikkének alkalmazásához vezethet.

A Szövetség folytatja a doktrínák kidolgozását, valamint kiképzéseket és gyakorlatokat annak biztosítására, hogy a kibertérben ugyanolyan hatékony legyen, mint a szárazföldön, a levegőben és a tengeren. 2020-ban megjelent az első kiber doktrína. Ez fontos lépés a kibertérbeli műveletekre vonatkozó útmutatáshoz.

Az éves NATO Cyber Coalition gyakorlat az aktuális fenyegetésekből merítve tesztelte a résztvevők valós idejű reakcióit a kiber incidensekre, például a titkosított hálózatok feltörésére, a kritikus infrastruktúra kommunikációs rendszereinek megzavarására és az okostelefonos alkalmazásokon keresztül történő kémkedésre.

A szövetségesek a 2016-os Varsói Csúcstalálkozón vállalt kötelezettségüknek megfelelően folytatták nemzeti kiber ellenálló képességük fokozását. Stratégiai iránymutatások kiadásával és felülvizsgálatával erősítették kiber ellenálló képességüket, beleértve az ellátási láncokat érintő kiberkockázatok kezelését, a szervezeti reformok végrehajtását és a képzésbe való befektetést.

Az információmegosztás soha nem volt ennyire kritikus. A NATO Kommunikációs és Információs Ügynökség a Kiber Együttműködési Hálózaton[106] keresztül továbbra is elősegítette a NATO-szövetségesek közötti kiberfenyegetésekkel és incidensekkel kapcsolatos információcserét.[107]

A NATO főtitkár-helyettes egy 2020-as szakmai konferencián történt előadása szerint sok évszázadon át a biztonság a szárazföldön és a tengeren jelentkező fenyegetések kezelését jelentette, az elmúlt évszázadtól már a levegőben lévő fenyegetések is megjelentek.

A technika számos közelmúltbeli fejlődése átalakítja a fenyegetéseket, amelyek ma több formát is ölthetnek és egyszerre több irányból is érkezhetnek. Közelről kézi módszerekkel vagy nagyon messziről, külső közvetítéssel. Emberektől vagy személyzet nélküli rendszerekből. Az űrből vagy a kibertérből. Ezeket a trendeket fokozzák az olyan gyorsan fejlődő technológiák, mint a mesterséges intelligencia és a robotika.

Alkalmazkodni kell annak érdekében, hogy Szövetség felkészült legyen a fenyegetések kezelésére mind a fizikai, mind a virtuális világban. A kiber fenyegetések ezek közé tartoznak, melyek egyre gyakoribbak, összetettebbek és pusztítóbbak.

Az elmúlt években fontos döntések születtek a NATO jobb „kiber készenléte" („cyber-ready") és „kiber biztonságossá" („cyber-secure") tétele érdekében.

Megállapodás született, hogy egy kibertámadás is elindíthatja az Alapszerződés 5. cikkét. Ahol egy szövetséges elleni támadást mindenki elleni támadásként kezelnek.

[106] Cyber Collaboration Network.

[107] The Secretary General's Annual Report 2020, „Deterrence and Defence in Cyberspace" fejezet, 23-24. o.

Megtörtént a kibertér katonai műveleti területként történő azonosítása a szárazföld, a tenger és a levegő mellett. Az űr is műveleti területévé vált a vezetők tavaly londoni döntése szerint.

Szintén megállapodást történt arról, hogy katonai vezetési struktúra központjában egy Kibertér Műveleti Központ alakuljon.

További megállapodás volt, hogy a nemzeti kiberhatásokat - vagy offenzív kiber műveleteket - („offensive cyber") integrálni kell a Szövetség műveleteibe és misszióiba.

Megszületett a Kibervédelmi Kötelezettségvállalás, ami elengedhetetlen a kiberfenyegetésekkel szembeni ellenálló képességek fokozásához.

Júniusban a NATO Szövetségesek közös nyilatkozatot adtak ki, amelyben elítélik a pandémiával összefüggésben zajló destabilizálást és rosszindulatú kiberaktivitásokat. A nyilatkozat felszólított továbbá a nemzetközi jog normák tiszteletben tartására és a felelős állami viselkedésre a kibertérben.[108]

2020-as nemzeti vonatkozású esemény, hogy Hazánk korlátozás nélküli bevezetéssel ratifikálta a NATO Kiberműveleti Doktrínát. Ez a lépés biztosítja az interoperabilitást a NATO missziók támogatása során szükséges nemzeti – NATO, vagy szövetséges – szövetséges típusú együttműködés során a legfontosabb kérdésekben a Doktrína fogalmi rendszerén belüli közös tevékenységet.[109]

A *NATO 2021-es Brüsszeli Csúcsértekezlet* megállapítása szerint a Szövetség biztonságát fenyegető kiber fenyegetések egyre összetettek, pusztítóbbak, kényszerítőbbek és gyakoribbak. Ezt szemléltetik a nemrég történt kritikus infrastruktúrákat és demokratikus intézményeket célzó zsarolóvírus (ransomware) incidensek és egyéb rosszindulatú kiberaktivitások, melyek rendszerszintű, jelentős károkat okozhatnak.

A változó kihívásnak való megfelelés érdekében megtörtént a NATO Átfogó Kibervédelmi Politika[110] elfogadása, ami támogatja a NATO három alapvető feladatát, az általános elrettentést, a védelmi jelleget és az ellenálló képesség fokozását.

A NATO védelmi mandátumát megerősítve a Szövetség eltökélt szándéka, hogy a minden időben a képességek teljes skáláját aktívan alkalmazza az elrettentés, a teljes spektrumú kiberfenyegetések elleni védelem ellen érdekében – beleértve a hibrid kampányok részeként lebonyolított műveleteket –, összhangban a nemzetközi jog követelményeivel.

A szövetségesek megerősítik, hogy az Észak-atlanti Tanács eseti alapon dönt arról, hogy a kibertámadás mikor vezet az 5. cikk alkalmazásához. A szövetségesek elismerik, hogy a jelentős, rosszindulatú

[108] Speech by NATO Deputy Secretary General Mircea Geoană at the CYBERSEC GLOBAL 2020 virtual conference (https://www.nato.int/cps/en/natohq/opinions_178335.htm).

[109] NATO Cyber Operations Doctrine (AJP 3.20). 42/2020. HM utasítás egyes NATO egységesítési jelzések elfogadásáról, 5. §.

[110] Comprehensive Cyber Defence Policy.

kibertevékenységek halmozódó hatása[111] bizonyos körülmények között fegyveres támadásnak tekinthető.

A Szövetség továbbra is elkötelezett a nemzetközi joggal összhangban történő cselekvésre, beleértve az ENSZ Alapokmányt, a nemzetközi humanitárius jogot és a nemzetközi emberi jogi jogszabályokat, ahol azok alkalmazhatók.

A Szövetség elősegíti a szabad, nyitott, békés és biztonságos kibertér kialakítását, és további erőfeszítéseket fog tenni a stabilitás fokozása és a konfliktusok kockázatának csökkentése érdekében a nemzetközi jog támogatásával és a felelős állami viselkedés önkéntes normáival[112] a kibertérben.

A NATO, ha szükséges, költségeket okoz azoknak, akik sérelmet okoznak a Szövetségnek. A válasznak nem szükséges a kiber területre korlátozódnia.

Növelni kell a helyzetismeretet a NATO döntéshozatal támogatása érdekében.

A Kibervédelmi Kötelezettségvállalás adoptálása után öt évvel a Szövetség továbbra is elkötelezett az erős nemzeti kibervédelem támogatásában, prioritásként. Folytatódik a „kibertér, mint műveleti terület" elv megvalósítása.

Erős politikai felügyelet keretében növelni kell a szövetségesek által önkéntesen biztosított szuverén kiberhatások hatékony integrálását a kollektív védelembe, a szövetségi műveletekbe és missziókba.

A Szövetség tovább törekszik a kölcsönösen előnyös és hatékony együttműködések kialakítására, beleértve a partnerországokat, a nemzetközi szervezeteket, az ipart és az oktatást, illetve folytatja az erőfeszítéseket a nemzetközi stabilitás fokozása érdekében a kibertérben.

A Szövetség üdvözöli a közelmúltban Portugáliában megnyílt NATO Kommunikációs és Információs Akadémiát.[113] [114]

A *NATO 2021-es Brüsszeli Ellenálló Képesség Megerősítéséről Szóló Kötelezettségvállalás* nem kifejezetten a kibertér műveleteket célozza, ennél szélesebb és magasabb szintű követelményeket fogalmaz meg, melyeknél pontosan azonosítható a kibertér műveleti szakmai érintettség is. A vállalás szerint az ellenálló képesség nemzeti felelősség és kollektív kötelezettségvállalás.

A szövetségesek javaslatot dolgoznak ki az ellenálló képesség – mint célkitűzés – megállapítására, értékelésére, felülvizsgálatára és nyomon követésére, hogy irányítsák a nemzeti szinten kidolgozott ellenálló képességi célokat és végrehajtási terveket. Minden egyes szövetségesnek el kell döntenie, hogyan kell meghatározni a nemzeti ellenálló képességi célokat és teljesíteni a végrehajtási terveket, lehetővé kell tenni, hogy ezt olyan módon tegyék, ami kompatibilis a nemzeti hatáskörökkel, struktúrákkal, folyamatokkal

[111] The impact of significant malicious cumulative cyber activities.
[112] Voluntary norms of responsible state behaviour.
[113] NATO Communications and Information Academy.
[114] Brussels Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021, 32. o.

és kötelezettségekkel – ahol szükséges – az EU kötelezettségekkel.

Az ellenálló képességet fenyegető veszélyek és kihívások állami és nem állami szereplőktől erednek, különböző formákat öltenek és különféle taktikákat és eszközöket használnak. Ide tartoznak a hagyományos, nem hagyományos és hibrid fenyegetések és tevékenységek, a terrortámadások, a növekvő és egyre kifinomultabb rosszindulatú kiber tevékenységek, az egyre szélesebb körben terjedő ellenséges információs tevékenységek, beleértve a dezinformációt, amelyek célja a társadalmak destabilizálása és közös értékek aláásása és beavatkozási kísérlet a demokratikus folyamatokba, a hatékony kormányzásba.

Fokozni kell az erőfeszítéseket az ellátási láncok biztosítása és diverzifikálása-, a kritikus infrastruktúrák (szárazföldön, tengeren, űrben és a kibertérben) és kulcsfontosságú iparágak ellenálló képességének biztosítása érdekében, beleértve a káros gazdasági tevékenységek ellen.

Kezelni kell a fejlődő technológiák hatását, biztosítva a következő generációs kommunikációs rendszerek – és a szellemi tulajdon védelmét.[115]

A *2021-re vonatkozó NATO főtitkári éves jelentés* szerint az évben a kiberfenyegetések tovább fejlődtek. Megszaporodtak a megszakító jellegű (distruptive) és rosszindulatú kiberkampányok, beleértve az állami és nem állami szereplők által elkövetett zsarolóvírus támadásokat is. Ezek a rosszindulatú támadások a kritikus infrastruktúrát és ellátási láncokat célozták a szövetséges és a partnerországokban.

A kihívás megoldása érdekében a szövetségesek támogatták a NATO Átfogó Kibervédelmi Politika[116] kiadását. Ez mérföldkövet jelentett a NATO kibervédelemmel kapcsolatos megközelítésének meghatározásában a következő évtizedre.

A szövetségesek hangsúlyozzák, hogy a Szövetséget érő kiberfenyegetések összetettek, pusztítóak, kényszerítőek és egyre gyakoribbá válnak, miközben a kibertér egyes kérdései vitatottak.

A Szövetség eltökélt szándéka, hogy – a NATO védelmi mandátumával és a nemzetközi joggal összhangban – képességeinek teljes skáláját alkalmazza a kiberfenyegetések ellen és azok elrettentése érdekében, beleértve azokat is, melyek hibrid kampányok részeként történnek.

A hatékony kibervédelem átfogó megközelítést igényel, ami egyesíti a politikai, katonai és technikai szintű erőfeszítéseket.

A NATO-nak képesnek kell lennie arra, hogy megvédje hálózatait, zökkenőmentesen működjön a kibertérben és elő kell mozdítania a normákon alapuló megközelítést a kibertérben. Ez megkívánja a szövetségesek közös helyzetismeretét, valamint a behatolások valós idejű észlelésének, megelőzésének és reagálásának képességét.

A kibertérben a Szövetség csak annyira erős, amennyire a leggyengébb láncszem. A 2021-es Csúcstalálkozón a szövetségesek egyetértettek abban, hogy

[115] Strengthened Resilience Commitment (2021), 4, 5, 7, 8. o.

[116] NATO Comprehensive Cyber Defence Policy.

az ellenálló képesség, valamint az új sebezhetőségek észlelésének, megértésének és az azokra való reagálás képessége egyre fontosabbá válik.

A 2016-ban a Varsói Csúcstalálkozón elfogadott Kibervédelmi Kötelezettségvállalás továbbra is a nemzeti ellenálló képesség kiépítésének kulcsfontosságú eszköze. A Kötelezettségvállalás révén a szövetségesek azon dolgoznak, hogy fejlesszék a kiber munkaerőt, szakértőket toborozzanak olyan innovatív megközelítések révén, mint például a kibertartalékos programok és befektetnek a kibervédelmi képességekbe és szakértelembe.

A NATO a védelmi erőfeszítéseket a kormány egészére kiterjedő megközelítéssel folytatja,[117] ami elismeri a katonaság, a kormány, az ipar és a tudományos élet szerepét az ellenálló képes kibervédelem megvalósításában.[118]

A *NATO főtitkár helyettes 2021-es londoni Kibervédelmi Kötelezettségvállalás Konferencián* tett felszólalása szerint az elmúlt évben az új biztonsági fenyegetések, trendek megjelenése felgyorsult. Világszerte soha nem látott számú ember dolgozik, kommunikál, vásárol és szocializálódik otthonról. Képernyőkön keresztül a szemtől szemben kapcsolat helyett és interneten keresztül történik az információk megszerzése.

A kibertámadások száma növekszik, céljuk az emberek, a vállalkozok és végső soron a társadalmak; megpróbálják aláásni a demokratikus folyamatok és intézmények iránti bizalmat.

Fel kell készülni az ellenálló képesség biztosítására és a gyors helyreállításra bármilyen kibertámadásról is legyen szó.

A NATO-nak és minden szövetségesnek folytatnia kell az alkalmazkodást annak érdekében, hogy a digitális világban ugyanolyan legyen a biztonság és az ellenálló képesség, mint a fizikai világban.

A Kibervédelmi Kötelezettségvállalás 2016-os elfogadása óta a Szövetség hosszú utat tett meg.

A szövetségesek megállapodtak abban, hogy egy kibertámadás kiválthatja a kollektív védelmi záradék az 5. cikk aktivizálását.

A kiberteret katonai műveleti területként azonosította a Szövetség a szárazföld, a tenger, a levegő és most az űr mellett.

A szövetségesek megállapodtak a nemzeti kiberhatások – más néven „offenzív kiber" –integrálásába a Szövetség műveleteibe és misszióiba - növelve a válaszadási lehetőségeket.

A Szövetség egy új Kibertér Műveleti Központot alapított a helyzetismereti kép javítása és a jobb műveleti koordináció érdekében.

Együtt jobban kialakíthatók a kibertér globális szabályai és normái, illetve biztosítható, hogy azok megfeleljenek a szabadság, a demokrácia értékeinek és a jogállamiság követelményeinek.

A NATO ideális szerepet játszik a kibertér biztonságához szükséges szabályok, szabványok és normák kialakításához szükséges egyeztetésekhez,

[117] Whole - of - government approach.

[118] The Secretary General's Annual Report 2021, „Comprehensive Approach to Cyber Defence" fejezet p. 30–31. o.

támogató folyamatokhoz, valamint az erőforrások összehangolásához annak érdekében, hogy e szabályok betartsák.

A NATO Európában és Észak-Amerikában platform szerepet játszik a szövetségesek számára, hogy összehangolhassák a rosszindulatú kibertámadásokra adott válaszokat.

A szövetségesek nyilvánosan elítélik a destabilizáló és rosszindulatú kibertevékenységeket és szorgalmazzák a nemzetközi jog és normák tiszteletben tartását, a felelős magatartást a kibertérben.[119]

2021-es esemény a NATO átfogó műveletttervezési irányelvének legújabb változatának megjelenése, integrálva a kibertér műveleti kérdéseket is. A dokumentum a NATO stratégiai szintű tervezési feladatokat szabályozza, amivel egyértelmű iránymutatást ad az alacsonyabb szintű feladatok tervezésére, beleértve a NATO – nemzeti feladattervezést is.[120]

A *NATO állam és kormányfők 2022-es Brüsszeli Nyilatkozata* szerint a szövetségesek növelik a társadalom és az infrastruktúrák ellenálló képességét Oroszország rosszindulatú befolyása ellen. Bővítik a kiberképességeket és védelmet, támogatást nyújtanak egymásnak kibertámadás esetén.

A szövetségesek készek költségeket róni azokra, akik a kibertérben károkozásra törekednek, fokozzák az információcserét és a helyzetfelismerést, a civil felkészültséget és erősítik a dezinformációra való reagálási képességet.[121]

A *2022-es Madridi Csúcsértekezlet* deklarációja szerint a Szövetség kiber-, űr-, hibrid és egyéb aszimmetrikus fenyegetésekkel, valamint az új típusú és minőségugrást biztosító technológiák[122] rosszindulatú felhasználásával áll szemben. A Szövetség rendszer szintű versennyel áll szembe azokkal – köztük a Kínai Népköztársasággal –, akik kihívást jelentenek az érdekek, a biztonság és az értékek ellen, és a szabályokon alapuló nemzetközi rend aláásására törekszenek.

A Szövetség új alapkövetelményeket[123] határoz meg az elrettentés és védelem érdekében.[124]

A NATO továbbra is megvédi lakosságot és mindenkor megvédi a

[119] Speech by NATO Deputy Secretary General at NATO Cyber Defence Pledge Conference 2021, London.

[120] Allied Command Operations: Comprehensive Operations Planning Directive (COPD, version 3.0).

[121] Statement by NATO Heads of State and Government, Brussels 24 March 2022.

[122] Emerging and disruptive technologies – EDT. A kifejezés magyar honosítása még nem történt meg. Tartalmilag az olyan megoldások felbukkanását jelenti, amelyek jelentősen felülírják a megjelenésük előtti eljárásokat, alapelveket (pl. a kvantum technológia fenyegetése a rejtjelző megoldások feltörésére, vagy önmagában a mesterséges intelligencia megjelenésének hatásai).

[123] Set a new baseline.

[124] A kibertér műveleteknél lényegesen magasabb szintű az a fogalmi megközelítés, hogy a korábbi stratégia megfogalmazásokban olvasható „védelem és elrettentés" kifejezés 2022-ben „elrettenés és védelem"-é alakult. A jövőben látható lesz, hogy el a súlyponteltolódás milyen konkrét folyamatokat erősít vagy indít el a Szövetségben. Most felelősségteljesen csak annyi jelenthető ki, hogy az eddigi trendeknek megfelelően ez a változás le fog csapódni a kibertér műveleti területre is, a stratégiai, hadműveleti és harcászati szintek szerint értelmezett folyamatokkal és képességekkel.

szövetséges területek minden centiméterét. Építeni fog az újonnan kiterjesztett struktúrára és jelentősen megerősíti az elrettentést és a védelmet, hogy hosszú távra szavatolja valamennyi szövetséges biztonságát és védelmét. Ez a 360 fokos megközelítéssel összhangban a szárazföldi, légi, tengeri, kiber- és űr területeken, minden fenyegetés és kihívás elleni védelmet jelenti.

Az ellenálló képesség nemzeti felelősség és kollektív elkötelezettség. A szövetségesek növelik ellenálló képességüket, többek között nemzeti szinten kidolgozott célok és végrehajtási tervek révén, a közösen kidolgozott célkitűzések által vezérelve. Minden területen felgyorsítják az alkalmazkodást, növelve a kiber- és hibrid fenyegetésekkel szembeni ellenálló képességet, erősítve interoperabilitást.

A szövetségesek integrált módon alkalmazzák politikai és katonai eszközöket. A fokozott polgári-katonai együttműködés révén jelentősen megerősítik a kibervédelmet.

A szövetségesek önkéntes alapon és nemzeti eszközök felhasználásával úgy döntöttek, hogy virtuális gyorsreagálású kiber képességet[125] építenek ki és készítenek fel a jelentős hatású rosszindulatú kibertevékenységekre[126] történő reagálás érdekében.[127]

A *2022-es NATO Stratégiai Koncepció* megfogalmazása szerint a kibertérben folyamatosan küzdelem van. Rosszindulatú szereplők arra törekszenek, hogy akadályozzák a kritikus infrastruktúrák működését, beavatkozzanak kormányzati szolgáltatásokba, hírszerzési információkat szerezzenek meg, szellemi tulajdont lopjanak el és akadályozzák a katonai tevékenységeket.

A stratégiai verseny környezetben fokozni kell a globális tudatosságot; minden műveleti területen – irányban a 360 fokos megközelítéssel összhangban lévő elrettentést és védelmet kell kialakítani.

A NATO szintű elrettentés és védelem kialakítása a nukleáris, a hagyományos és a rakétavédelmi képességek megfelelő összetételén alapul, amelyet űr- és kiberképességek egészítenek ki. Ez defenzív, arányos és teljes mértékben összhangban van nemzetközi kötelezettségvállalásokkal.

A katonai és nem katonai eszközök arányos, koherens és integrált módon kerülnek alkalmazásra minden biztonsági fenyegetésre történő reagálásként, saját választás szerinti módszerrel, időzítéssel és alkalmazási területen.

A szövetségesek tovább erősítik haderejük kollektív készenlétét, reagálóképességét, bevethetőségét, integrációját és interoperabilitását. Egyedileg és közösen biztosítják az elrettentéshez és a védelemhez szükséges erők, képességek, tervek, erőforrások, eszközök és infrastruktúra teljes skáláját, beleértve a nagy intenzitást is.

Erősítik a képzést és a gyakorlatokat, átalakítják és racionalizálják döntéshozatali

[125] Virtual rapid response cyber capability.
[126] Significant malicious cyber activities.
[127] Madrid Summit Declaration Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022, 6, 9, 10. o.

folyamataikat, javítják tervezésüket és válságreagáló rendszerünk hatékonyságát.

A Szövetség felgyorsítja a digitális átalakulást, hozzáigazítja a NATO parancsnoki struktúrát az információs korhoz és fejleszti kibervédelmet, a hálózatokat és infrastruktúrákat.

A hatékony elrettentés és védelem a kulcsa a világűr és a kibertér biztonságos használatának és a korlátlan hozzáférés biztosítása érdekében. A Szövetség javítani fogja a képességeket, hogy hatékonyan működjön az űrben és a kibertérben a fenyegetések teljes spektrumának megelőzése, észlelése, leküzdése és az azokra való reagálás érdekében, minden rendelkezésre álló eszköz felhasználásával.

Egyetlen művelet, vagy halmozódó rosszindulatú kibertevékenységek, esetleg ellenséges műveletek az űrbe, az űrből vagy az űrben elérheti a fegyveres támadás szintjét, amikor az Észak-atlanti Tanács az Észak-atlanti Szerződés 5. cikkét lépteti érvénybe.

A Szövetség elismeri nemzetközi jog alkalmazhatóságát és előmozdítja a felelős magatartást a kibertérben és az űrben.[128]

A 2022-es római NATO Kibervédelmi Kötelezettségvállalás Konferencián a NATO főtitkár megállapította, hogy Oroszország agressziójának része egy láthatatlan háború a kibertérben, amire példát jelentenek az orosz erők határátlépése előtti órákban és a későbbiekben is érzékelt kibertámadások.

A kiber állandóan vitatott tér. A béke, válság és konfliktus közötti határvonal elmosódott. Emiatt a NATO régóta komolyan veszi az állami és nem állami szereplők kibertérben érzékelhető fenyegetéseit.

A kibertevékenységek kiválthatják a kollektív védelmi záradék, az 5. cikkely aktivizálását. Ez a kollektív védelem alapja. Ahol egy szövetséges elleni támadás mindenki elleni támadásnak minősül.

A kiber(tér) ma már műveleti terület, egyenlően a szárazföldi, tengeri, légi és űrbeli műveletekkel. Több szövetséges felajánlotta nemzeti kiber hatásainak (cyber effects) használatát.

A NATO Kibervédelmi Kötelezettségvállalás következtében a szövetségesek növelték a kiber beruházásaikat, javították nemzeti stratégiáik végrehajtásához szükséges készségeiket és képességeiket.

A NATO rendszeres gyakorlatokat tart. Beleértve a NATO Cyber Coalition „zászlóshajó" - gyakorlatot, ami a világ legnagyobb gyakorlata.

A NATO egyedülálló platform, ahol a szövetségesek információkat osztanak meg, feltárják aggályaikat, megosztják egymással a bevált gyakorlatokat és mérlegelik kollektív válaszokat.

Szeptemberben az Észak-atlanti Tanács határozottan elítélte az Albánia nemzeti információs infrastruktúrája elleni közelmúltbeli kibertámadást, miközben a NATO személyzete Tiranába ment és támogatást nyújtott. Albánia és más szövetségesek ezt a támadást Iránnak tulajdonították. Ez egy példa arra, hogy a NATO-szövetségesek összefognak és egységesen válaszolnak.

A NATO szorosan együttműködik az EU-val kiber ügyekben is. A szakértők (cyber

[128] NATO 2022 Strategic Concept; 15, 20, 22, 24 és 25. o.

defender) információkat osztanak meg a kiberfenyegetésekről és részt vesznek egymás gyakorlatain, beleértve a NATO Cyber Coalition kibergyakorlatot is.

A NATO szorosan együttműködik partner országokkal és magáncégekkel is, amelyek kulcsszerepet játszottak az ukrán kibertér védelmében. A Starlink műholdak biztonságos kommunikációt és internet-hozzáférést tesznek lehetővé. A Microsoft és az Amazon éppen akkor tudta feltölteni Ukrajna minisztériumait a felhőbe, amikor a szervereit az orosz lövedékek támadták. A YouTube és a közösségi média cégek blokkolták vagy korlátozták az orosz állami média- és troll fiókokat.

A kormányok és a technológiai vállalatok közötti együttműködés jelentősen megnőtt. Például a NATO és a Microsoft információkat cserél a szövetségesekre és Ukrajnára gyakorolt rosszindulatú támadások hatásainak mérséklésére

A júniusi Madridi Csúcson megállapodás történt, hogy tovább fejlesztjük az iparral való együttműködést, kiterjesztve azt az online szabványok és viselkedési normák kialakítására.

A kibertér nem lehet mindenki számára ingyenes „Vadnyugat". Minden szövetséges egyetért abban, hogy az alapvető jogok és a nemzetközi jog éppúgy érvényesül online, mint offline.[129]

Szükség van a felelős használat elveinek kialakítására, amelyek tükrözik demokratikus értékeinket és emberi jogainkat.

1949-ben Truman elnök úgy jellemezte a NATO-t, mint „pajzsot az agresszió és az agressziótól való félelem ellen". Ma ez a pajzs a kibertérre is kiterjed.

„A kibertérből származó fenyegetés valós és növekszik, ezért fontos a Kibervédelmi Kötelezettségvállalás. Ezért felkérem a szövetségeseket, hogy kötelezzék el magukat a kibervédelem mellett, több befektetéssel, több szakértelemmel, megerősített együttműködéssel.
Ez a kollektív védelmünk létfontosságú része."[130]

2022-es nemzeti esemény, hogy a NATO Kiberműveleti Doktrína kötelező jellegű érvényesülése mellett a Magyar Honvédség Parancsnoksága parancsnokának szakutasításaként[131] megjelent az MH Kibertér Műveleti Doktrína.[132]

Szervezetfejlesztési esemény, hogy az évben megalakult az MH Kiber és Információs Központ a korábban már

[129] (…) apply just as much online as they do offline.
[130] Keynote address by NATO Secretary General Jens Stoltenberg at the NATO Cyber Defence Pledge Conference in Italy (https://www.nato.int/cps/en/natohq/opinions_208925.htm).
[131] A szakutasítás jellegénél fogva – szervezet szabályozó közjogi eszközként – kötelező érvényű az MHP és alárendelt szervezetek esetében. Tartalmi kérdéseket tekintve az is nyilvánvaló, hogy a doktrína csak alapelvekkel, irányok meghatározásával ad segítséget az alkalmazó katonai szervezeti vezetőknek, konkrét feladatszabás helyett. Ez a kettősség aláhúzza a katonai vezetők képzésének szükségességét a viszonyrendszer helyes értelmezése és alkalmazása érdekében.
[132] 175/2022. (HK 4.) MH PK intézkedés a Magyar Honvédség Kibertér műveleti doktrína (1. kiadás) című szolgálati könyv kiadásáról. Megjelent a Magyar Honvédség Kibertér műveleti doktrínája (https://jogalappal.hu/megjelent-a-magyar-honvedseg-kiberter-muveleti-doktrinaja/).

szereplő Kiber Akadémia és egyéb meglévő szervezetek összevonásával.[133]

***

1999-től kezdve a kezdeti kibertér műveletek általános megfogalmazásai, a fenyegetések említése mellett a NATO felső szintű megfogalmazásai egyre szélesebb körben, egyre több elemet tartalmaznak a kiberbiztonsággal, kibertér műveleti képeségekkel kapcsolatban.

A fenyegetések súlyossága a Szövetség értékelése szerint eléri azt a szintet, ahol már *nemzeti és szövetségi szintű stratégiai kockázatok kezelése szükséges*.

A fenyegetések súlyosságának említése és az ezek ellensúlyozására szolgáló védelem mellett *egyértelműen azonosítható az integrált megközelítés gondolata*, ahol a kibertér nem önállóan jelenik meg – kiemelt elemként –, hanem a többi műveleti terület között foglalja el helyét, integráns részét képezi az összhaderőnemi[134] műveleteknek. Ez egyben „átjárhatóságot" is jelent, azaz kibertér műveletek ellen válasz lehet kibertér műveleti vagy fizikai jellegű, illetve fizikai jellegű műveleteket is támogathat kibertér művelet. A fantasztikus filmek szintjét elérő „kibertér művelet – kibertér művelet ellen" speciális eset az előbbiek mellett szintén elképzelhető, de ez napjainkban még nem képez elsődleges megoldást – de nem jósolható meg, hogy mikor kerül sor az első ilyen konfliktusra.

Az áttekintett források *többszörösen megfogalmazzák a kibervédelem, kibertér műveletek vonalán a hírszerzési információk integrálásának szükségességét a szövetségi folyamatokba*. A NATO-nak és szövetségeseknek egyaránt létfontosságú a hírszerzési funkciók kibertérben történő megvalósítása.

A NATO védelmi jellégnek hangsúlyozása mellett egyértelmű, hogy a Szövetség nem mond le a katonai műveleteket támogató kibertér műveletek alkalmazási lehetőségről, beleértve az offenzív hatásokat (offensive effects) is, ami jelenleg nemzeti végrehajtásban elképzelt.

Kezdetben a NATO hálózatok biztonságának növelését célzó hálózatfejlesztési kérdések és ehhez tartozóan az eseménykezelés centralizált kezeléséhez szükséges szervezetépítés és képességfejlesztés volt fókuszban. Ezt a vonalat erősítve megjelentek a védelempolitikai, stratégiai együttműködési feladatokat szolgáló szervezeti elemek, illetve a szövetségesekkel történő közös platformot biztosító keretek (Policy, Strategy). Ennek a sornak legutolsó eleme a NATO Kibertér Műveleti Központ megalakítása Mons-ban, ami a NATO hálózatok eseménykezelési feladatai mellett a katonai műveletekbe történő integrálást célzó lépés.

Nem felejthető, hogy *az elektronikus szolgáltatások, hálózatok biztonságának alapvető pillére az üzemeltetési és az*

[133] 32/2021. (VII. 23.) HM utasítás a Magyar Honvédség Kiber- és Információs Műveleti Központ kialakításával összefüggő egyes feladatokról.

[134] Az aktuális megközelítés szerint az „összhaderőnemi" megfogalmazás helyett pl. hatás alapú, átfogó megközelítésű, multi domain műveletek.

infomációvédelmi (benne elektronikus információvédelmi)[135] *követelmények sikeres teljesítése.*

Több mint tíz évvel ezelőtt *megkezdődött a szövetségesek és a NATO eseménykezelését, bevált gyakorlatok cseréjét és egyéb kapcsolattartási célokat szolgáló együttműködési megállapodások rendjének kialakulása*, ami 2016-ban már második fejlettségi fázisba lépett. Az EU eseménykezelő szervezet is csatlakozott ehhez az együttműködési rendhez, illetve 2016-ban legmagasabb szintű együttműködési megállapodás született a NATO és az EU között.

A Szövetség hosszú évek óta következetes, egyértelmű megfogalmazást ad *a nemzetközi normák alkalmazásával kapcsolatos elkötelezettségéről,* illetve fontos kérdésként kezeli a helyes állami viselkedési normák önkéntes alapú kialakítását.

Több mint tízéves múltja van a szövetségi kibervédelmi gyakorlatoknak, a NATO gyakorlatokba történő kiber forgatókönyvek bedolgozásának, illetve kialakult ez a gyakoroltatási lehetőség a NATO Kibervédelmi Kiválósági Központ szervezésében is. Az észt tulajdonú és üzemeltetésű Cyber Range mindkét rendezvénytípus kiszolgálását végzi.

Képzés területén a NATO kiképző központok által biztosított lehetőség mellett a NATO Kibervédelmi Kiválósági Központ biztosít technikai, jogi, hadműveleti alkalmazási és egyéb szaktanfolyamakat, ami jelzi a szakterüket

A NATO műveletтervezési eljárásrendben részletesen megjelentek a kibertér műveleti kérdések, illetve a magasabb szintű doktrínák általános irányelvei mellett megjelent a NATO kibertér Műveleti Doktrína is a műveletek végrehajtása során szükséges szakmai támogatás érdekében.

A katonai kibertér műveleti alkalmazásra vonatkozó NATO stratégiai szintű vizsgálat tudatosan szűkített célt jelent, de a 2010-es évek közepétől *jól felismerhető az ellenálló képesség és a hibrid műveletek témakörök egyre erősödő, tartalmilag szélesedő megjelenése*. Emiatt – és *az elrettentés fogalmának helyes megközelítése érdekében* – szükséges annak rögzítése, hogy a kibertér műveletek védelempolitikai, stratégiai szintű értelmezése kizárólag e *három fogalmi kör figyelembe vételével történhet*.

FŐBB FELHASZNÁLT FORRÁSOK

[1] Szentgáli Gergely: The NATO Policy on Cyber Defence: The Road so Far. *AARMS*, 2013/1. szám, 83–91 o.
[2] Fekete-Karydis Klára – Lázár Bence: A kibervédelem katonai dimenziói. *Hadtudományi Szemle*, 2020/3. szám, 44–48. o.
[3] The Military Strategy of United States of America (A Strategy for Today; A Vision for Tomorrow), 2004.
[4] National Military Strategy for Cyberspace Operations; 2006.
[5] The Alliance's Strategic Concept (1999) Approved by the Heads of State and Government participating in the meeting

[135] A magyar jogszabályok minősített adatkezelés esetén az „elektronikus információvédelem”, nem minősített adatok kezelése esetén az „elektronikus információbiztonság” kifejezést alkalmazzák. Ezt az elkülönítést a NATO nem alkalmazza.

of the North Atlantic Council in Washington D.C.
[6] C-M (55) 15 (FINAL) Security within the North Atlantic Treaty Organization.
[7] A Nemzeti Biztonsági Felügyeletről szóló 1998. évi LXXXV. törvény.
[8] Az elektronikus információvédelemről szóló 33/2022. (HK. 13.) HM utasítás.
[9] A Központi Nyilvántartó, a nyilvántartó és az ellenőrző pont működési rendjéről szóló 4/2000. (II. 29.) HM rendelet.
[10] A Magyar Köztársaság NATO-NYEU Központi Nyilvántartó, Ellenőrző pontok és a biztonsági megbízottak által vezetendő okmányokról szóló 13/2000. (HK. 6.) HM utasítás.
[11] Az állam és szolgálati titokról szóló1995. évi LXV. törvény szabályozta.
[12] A nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített, valamint korlátozottan megismerhető adat védelmének eljárási szabályairól szóló 56/1999. (IV. 2.) Korm. rendelet.
[13] A NATO Irodaautomatizálási rendszer (NIAR) biztonságával kapcsolatos feladatokról szóló 82/2002. (HK. 26.) HM utasítás.
[14] *Biztonság és Titokvédelem a NATO szabályai szerint*, Budapest, Honvéd Kiadó, 1999.
[15] Kassai Károly: Az elektronikus információvédelem felső szintű szervezeti és szakmai történései a 2005-2015 közötti időszakban. *Hadmérnök*, 2015/3. szám 279–291. o.
[16] Prague Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague, Czech Republic, 2002.
[17] C-M (2002) 49 Security within the North Atlantic Treaty Organization.
[18] Istanbul Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council, 2004.
[19] Riga Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Riga on 29 November 2006.
[20] Comprehensive Political Guidance, 2006.
[21] Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008.
[22] Strasbourg / Kehl Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl, 2009.
[23] Lisbon Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 2010.
[24] A Puskás Tivadar Közalapítvány megszüntetésével kapcsolatos feladatokról szóló 1284/2013. (V. 27.) Korm. határozat.
[25] Az állami és önkormányzati szervezetek elektronikus információbiztonságáról szóló 2013. évi L. törvény.
[26] A Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről szóló 16/2013. (VIII. 30.) HM rendelet.
[27] Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 2014.
[28] Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016.

[29] Cyber Defence Pledge (https://www.nato.int/cps/en/natohq/official_texts_133177.htm).
[30] Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet módosításáról22/2016. (II. 17.) Korm. rendelet.
[31] A honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság és a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ feladatainak végrehajtásáról, valamint a sérülékenységvizsgálat lefolytatásának szabályairól15/2017. (IV. 28.) HM utasítás.
[32] Brussels Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018.
[33] NATO Cyber Operations Doctrine (AJP 3.20).
[34] Egyes NATO egységesítési jelzések elfogadásáról szóló 42/2020. HM utasítás.
[35] Brussels Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021.
[36] Strengthened Resilience Commitment (2021)
[37] Allied Command Operations: Comprehensive Operations Planning Directive (COPD, version 3.0).
[38] Madrid Summit Declaration Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022.
[39] NATO 2022 Strategic Concept.
[40] A Magyar Honvédség Kibertér műveleti doktrína (1. kiadás) című szolgálati könyv kiadásáról szóló 175/2022. (HK 4.) MH PK intézkedés.
[41] A Magyar Honvédség Kiber- és Információs Műveleti Központ kialakításával összefüggő egyes feladatokról szóló 32/2021. (VII. 23.) HM utasítás.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Military and Intelligence CyberSecurity Research Paper 2022/9.

Szerző(k) / Author(s):
Dr. Kassai Károly PhD

Kézirat lezárásának ideje / Manuscript closing time:
2022.11.15.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD
Dr. Magyar Sánor PhD

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Prof. Dr. Resperger István PhD

Elérhetőségek /Contacts:
https://hhk.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/research-paper

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:
2786-3778

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROGRAM