HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 4. szám 109–120.
DOI: 10.32567/hm.2024.4.7

Pozderka Gábor[1]

A NATO kiberműveleti szervezeti elemeinek evolúciós vizsgálata

Evolutionary Analysis of the Elements of NATO's Cyber Operations Organisations

Absztrakt

A NATO 2016-os varsói csúcstalálkozóján az országok vezetői egyetértettek abban, hogy a kibertér önálló hadszíntér (domain), és a védelme részét képezi a NATO kollektív védelmi feladatainak. Ennek megfelelően megkezdődött a korábban széttagoltan létező képességek, és az ezek irányításáért felelős szervezeti elemek feladatrendszerének újragondolása, a feladatok végrehajtásához szükséges akciótervek kialakítása. Jelen publikáció célja a NATO kibervédelmi és kiberműveleti szervezeti elemeinek evolúciós vizsgálata, illetve annak elemzése, hogy ennek következtében milyen feladatok azonosíthatók a nemzeti végrehajtás során. Értelemszerűen ez az evolúciós folyamat nem fejeződött be, a terület sajátosságából adódóan folyamatosan új feladatok jelennek meg akár napi szinten, ezen változások hatással vannak a szervezeti struktúra kialakítására is.

Kulcsszavak: NATO, kibertér, szervezetek, evolúció

Abstract

At the NATO's Warsaw Summit in 2016, leaders agreed that cyberspace is a separated domain and that its defence is part of NATO's collective defence mission. Accordingly, the rethinking of the previously fragmented capabilities and the system of tasks of the organisational elements responsible for managing them began, and the development of action plans necessary for the implementation of tasks. The aim of this publication is to

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: pozderka.gabor@hm.gov.hu

examine the evolutionary elements of NATO's cyber defence and cyber operations and to analyse what tasks can be identified during national implementation as a result. Obviously, this evolutionary process has not yet been completed, due to the peculiarity of this field, new tasks are constantly appearing even on a daily basis, and these changes also affect the formation of the organisational structure.

Keywords: NATO, cyberspace, organisation, evolution

Bevezetés

Az információs technológia és az internet globális elterjedésével párhuzamosan a kiberfenyegetések is egyre nagyobb jelentőséget nyertek a mindennapi életben és a védelmi szektorban egyidejűleg.[2] A North Atlantic Treaty Organization (NATO), mint vezető katonai szövetség, felismerte, hogy a hagyományos katonai fenyegetések mellett a kiberbiztonság, kibervédelem és az ezekre épülő kiberműveletek is fokozatosan kulcsfontosságúvá váltak. Ennek eredményeként a NATO 2016-os varsói csúcstalálkozóján az országok vezetői egyetértettek abban, hogy a kibertér önálló hadszíntér *(domain),* ezért a védelme részét képezi a NATO kollektív védelmi feladatainak, ebben a tekintetben a Szövetségnek ugyanúgy képesnek kell lennie megvédeni a tagállamokat, mint a hagyományos hadszíntereken vívott harcok során.[3]

Természetesen a fenti kinyilatkoztatást számos korábbi lépés előzte meg, aminek egyik fontos előkészítő eleme volt a NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE – NATO Kibervédelmi Kiválósági Központ) megalakítása Észtországban. A lokáció kiválasztásának szimbolikus jelentősége is volt, így üzenve a világnak, hogy a kibertérben elkövetett cselekedeteknek súlyuk van, azokat a NATO figyelemmel kíséri, és megkezdi a szükséges eljárásrendek kidolgozását. A kibervédelmi feladatok megjelenésével értelemszerűen a korábban kialakított infokommunikációs és információvédelmi szervezeti elemek feladatrendszerének újragondolása vált szükségessé, ami a szervezeti elemek strukturális átalakítását is magával hozta.

Jelen publikáció fókuszterülete a műveleti szintű képességelemek és feladatrendszer vizsgálata, azonban érintőlegesen megjelenik a komplexitás megértéséhez szükséges stratégiai keretrendszer is. Ismertetem azokat a szervezeti elemeket, amelyek az evolúciós folyamat részét képezték, valamint elemzem azokat a folyamatokat, amelyek a kibertér jelenleg kialakult keretrendszerét meghatározták. Hipotézisként megfogalmazható, hogy a NATO-ban zajló, kiberteret érintő evolúciós folyamatok hatással voltak a nemzeti szabályzói struktúra kialakítására, illetve a szövetségi szinten jelenleg is zajló átrendeződés befolyásolni fogja a jövőbeni képességek kialakulását, ebben a formában is irányt mutatva a szakterületnek.

[2] Haleliuk 2024.
[3] NATO 2016.

Kezdeti lépések

Fontos megjegyeznünk, hogy mint minden más szakterület esetében, így a kiberterületen is a North Atlantic Council (Észak-atlanti Tanács, NAC), a NATO legfőbb politikai döntéshozó testülete hozza meg azokat a stratégiai döntéseket, amelyek meghatározzák a stratégiai irányokat, figyelembe véve a NATO Military Committee (Katonai Bizottság, MC) által megfogalmazott javaslatokat, amely a tagállamok legfelsőbb katonai vezetőit, a vezérkari főnököket tömörítő testülete a szervezetnek. A vezérkari főnökök általában az úgynevezett állandó katonai képviselők személyével képviseltetik az országukat, de csakúgy, mint a Tanács, időről időre a legmagasabb szinten, a vezérkari főnökök személyes jelenlétével folynak az ülések. A NAC alatt több bizottság végzi feladatait, szakterületet érintően a NATO Cyber Defence Committee (Kibervédelmi Bizottság, CDC), amelynek az evolúció eredményeként jelenleg feladata a NATO kibervédelmi politikáinak és kezdeményezéseinek felügyelete és irányítása, továbbá fő célja, hogy politikai irányítást és stratégiai iránymutatást adjon a kibervédelem területén. A szakterületi képességfejlesztésre szintén hatással vannak a Security Committee (Biztonsági Bizottság, SC) és a Defense Policy and Planning Committee (Védelmi Politikai és Tervezési Bizottság, DPCC) javaslatai.

A NATO számára a kibervédelem jelentősége az évek során egyre nőtt, különösen a 2000-es évek közepétől kezdődően. Kezdetben a tevékenységek a probléma elméleti megértésére korlátozódtak, kerekasztal-beszélgetések során kezdték meg azonosítani a lehetséges sérülékenységi vektorokat. Észtország 2003-ban, már a hivatalos NATO-csatlakozása előtt javaslatot tett egy kiválósági központ létrehozására. A 2006. évi rigai csúcstalálkozó felsorolta a lehetséges számítógépes támadásokat a közös biztonságot érintő aszimmetrikus fenyegetések között, és az információs rendszerek hosszú távú védelmét szolgáló programok szükségességét szorgalmazta. A 2007-es Észtország elleni kibertámadások[4] először világítottak rá a NATO-országok, intézményeik és társadalmaik, sőt maga a NATO esetleges sebezhetőségére az információs és kommunikációs rendszerük megzavarásával. A 2008. áprilisi NATO-csúcstalálkozón Bukarestben a részt vevő államfők közleményben nyilvánították ki elkötelezettségüket amellett, hogy erősítsék a kiberbiztonsági folyamatokat, és felkészülnek a kibertámadások kivédésére.[5]

A kibertérben érzékelhető fokozódó nyomás hatására a valós, kézzelfogható produktumok előállítása nem volt tovább halogatható, ennek eredményeként az első valóban jelentős lépés 2008-ban történt meg, amikor létrehozták Tallinnban a NATO CCD COE-t a NATO teljes jogú szervezeti elemeként. Célja a tapasztalatok és a konzultáció alapján javítani a kibervédelem hatékonyságát, az együttműködést és az információ megosztását a tagországok és a kibervédelemben részt vevő partnerei között. Ez a központ kutatási, elemzési, képzési, valamint gyakorlati támogatást nyújt a tagállamoknak a kibervédelem terén. A tallinni Kibervédelmi Központ egyike annak a 21 akkreditált NATO Kiválósági Központnak, amely a szövetség precíziós technikai műveleteivel kapcsolatos képzést nyújt. Nemzeti és multinacionális alapon

[4] Bányász–Orbók 2013.
[5] Ottis 2007.

finanszírozzák, mivel a központok szorosan kapcsolódnak a Szövetséges Transzformációs Parancsnoksághoz, és elősegítik a szövetség által jóváhagyott fejlesztési célok megvalósulását. Magyarország 2010-ben csatlakozott a központhoz,[6] ezzel is erősítve a nemzeti és nemzetközi információáramlás hatékonyságát, valamint növelve a központ kibertérben való lefedettségét. A Központhoz 2024. év végéig 32 ország csatlakozott szponzorként (további 7 ország jelezte jövőbeni csatlakozási szándékát), feladatrendszeréből adódóan együttműködési kapcsolatokat létesíthet a nem NATO-államokkal, egyetemekkel, kutatóintézetekkel és vállalkozásokkal is, mint közreműködő résztvevőkkel.

Feladatrendszere az évek során folyamatosan bővült és átalakult, jelenlegi portfóliója tartalmazza az alábbi tevékenységeket:

Kezdeti funkciók:

- a kibervédelmi együttműködés javítása a NATO Network Enabled Capability (NATO Hálózat Alapú Képesség – NNEC) környezetében;[7]
- megtervezni a doktrína- és koncepciófejlesztést, valamint előkészíteni azok jóváhagyását;
- az információbiztonsági és a kibervédelmi oktatás, a tudatosság erősítése és a képzés fejlesztése;
- kibervédelmi támogatás biztosítása kísérletekhez (beleértve a helyszínen is);
- a kibervédelem jogi szempontjainak elemzése.

Tapasztalatok alapján bővített funkciók:

- a hozzájárulás a Kibervédelmi Központ gyakorlataihoz és sztenderdjeinek fejlesztéséhez a NATO-val, a PfP[8]-vel, a NATO-jelöltekkel és a nem NATO-államokkal;
- hozzájárulás a kibervédelemmel kapcsolatos NATO biztonsági gyakorlatok kidolgozásához, a katonai felelősségi kör meghatározása a kibervédelemben;
- kibervédelem-központú képzés, figyelemfelkeltő kampányok, workshopok és tanfolyamok szervezése;
- kibervédelem-központú gyakorlatok fejlesztése és lebonyolítása, valamint kibervédelmi gyakorlatok támogatásának képessége;
- kibervédelem biztosítása a NATO-val kapcsolatban álló kkv-k részére, és e kibervédelem hatékonyságának vizsgálata, megerősítése.

Szervezeti változások

Az oktatás és felkészítés mellett fokozatosan egyre nagyobb hangsúly helyeződött a technikai feladat-végrehajtásra, a kiberbiztonsági incidensek egyre nagyobb számban jelentek meg a hagyományos üzemeltetési incidensek mellett. Erre válaszul a NATO Kommunikációs és Információs Rendszerszolgáltatási Ügynöksége (NCSA) szervezetén

[6] CCD COE [é. n.].

[7] NNEC – a Szövetség azon kezdeményezése, amelynek célja, hogy erősítse a képességek integrálását minden szinten, a stratégiai szinttől a taktikaiig, valamint a katonai és polgári területeken egyaránt, egy robusztus információs infrastruktúra segítségével.

[8] Az egyes euroatlanti partnerországok és a NATO közötti kétoldalú együttműködési program.

belül már 2007-től kezdődően egyre jelentősebb mértékben jelen volt a kezdetben INFOSEC[9] terület részeként megjelenő kibervédelem, amely fokozatosan átalakította a rendszerek üzemeltetéshez kapcsolódó feladatrendszerét is. A NATO NCIRC (NATO Computer Incident Response Capability), a NATO Számítógépes Incidens Reagálási Képesség kezdeti kialakítása erre az időszakra tehető. Feladataként határozták meg, hogy észlelje, megelőzze és elhárítsa a NATO informatikai rendszereit fenyegető kiberbiztonsági incidenseket.

A NATO Kommunikációs és Információs Ügynöksége (NCIA) 2012. július 1-jén jött létre a NATO Konzultációs, Vezetési és Irányítási Ügynöksége (NC3A), a NATO ACCS Menedzsment Ügynöksége (NACMA) és az NCSA elemeinek összevonásával. Az Ügynökség létrehozása egy szélesebb körű NATO-reform részeként valósult meg, amely nemcsak a kibervédelemmel kapcsolatos feladatok hangsúlyosabb megjelenését jelentette, hanem a biztonság és üzemeltetés kérdéskörének újragondolását is előrevetítette. Az NCIA feladatrendszerét tekintve mai napig kiszolgálja a NATO szervezeteit és a nemzeteket, mint a NATO informatikai, kibervédelmi és C4ISR szolgáltatója. Az NCIA feladatrendszere fokozatosan egészült ki a NATO-műveletek támogatásához szükséges mobil kommunikációs elemekkel, valamint a szükséges kibervédelmi eljárásokkal.

A NATO annak érdekében, hogy súlyos kibertámadások esetén azonnali segítséget legyen képes nyújtani a NATO-tagállamok részére, 2012-ben létrehozta az első Cyber Rapid Reaction Team (RRT) képességet. Ez egy speciális csapat, amely túlnyomóan civil kiberbiztonsági szakértőkből áll, szükség esetén bevethetők a NATO bázisain vagy a tagállamok támogatására akár helyszínen is. Ezzel a lépéssel kívánták nyomatékosítani, hogy a NATO kollektív védelmi kötelezettségének a kibertér is szerves részét képezi, amely kimondja az Észak-atlanti Szerződés 5. cikkében, hogy egy tag elleni támadást minden tag elleni támadásnak tekintenek. A csapat rendszeres gyakorlatokon vesz részt, annak érdekében, hogy fenntartsa és javítsa felkészültségét és reagálási képességeit. Fontos megjegyezni, hogy ez egy igen korlátozott képesség, a tagállamok csak limitáltan lesznek képesek igénybe venni, ezért saját hasonló képességeik fejlesztése prioritásként kell hogy megjelenjen.

A NATO Cyber Security Centre (NCSC) 2016 októberében kezdte meg működését, székhelye a belgiumi Monsban, a Szövetséges Erők Európai Főparancsnokságán (SHAPE) található. Az NCSC az NCIA része, és elsődlegesen a szövetség kiberbiztonsági képességeinek fejlesztésére és fenntartására irányul, központosított és éjjel-nappal működő kibervédelmi támogatással védi a NATO saját hálózatait. Ez a képesség folyamatosan fejlődik, és lépést tart a gyorsan változó fenyegetési és technológiai környezettel.

A NATO funkciójából adódóan saját, offenzív képességek kialakítására nem fókuszál, ezért 2017-ben a NATO Védelmi Tanácsa döntést hozott arról, hogy SCEPVA (Sovereign Cyber Effects Provided Voluntarily by Allies) megnevezés alatt a tagállamok önkéntes vállalás alapján felajánlhatják nemzeti kiberképességeik integrálását a szövetséges hadműveletek és küldetések támogatására. Ebben a formában offenzív kiberhatásokkal is hozzájárulhatnak a szövetséges hadműveletek és küldetések

[9] INFOSEC – Information Security.

sikerességéhez, a NATO-tagállamok közötti együttműködés keretében a nemzetközi jog szabályainak alkalmazásával.[10]

A kiberszervezeti evolúció egyik jelentős mérföldköve volt, hogy 2018 októberében a NATO bejelentette a NATO Cyber Operation Centre (NATO Kibertér Műveleti Központ, CyOC) kezdeti felállítását és kísérleti fázisban való alkalmazását. A CyOC a NATO kibertérbeli hadszíntéri komponenseként látja el feladatait, felelős az aktuális kiberhelyzetkép kialakításáért, a központosított kibertérműveletei tervezésért, valamint a kibertérműveleti kihívások koordinálásáért. A CyOC parancsnoka szorosan együttműködik az Infokommunikációs szakterület (CIS-J6) vezetőjével, feladatuk összehangolásáért a DCOS (Cyber) felelős, aki közvetlenül a Szövetséges Fegyveres Erők Európai Főparancsnoka (Supreme Allied Commander Europe, SACEUR) részére teszi meg jelentését. Talán kevesen tudják, de fontos megjegyeznem, hogy e nemzetközi szervezeti elem legelső parancsnokának Vass Sándor dandártábornokot választották ki számos nemzetközi jelölt közül. Szakmai munkájával megteremtette a szervezet mindennapi működéséhez szükséges keretrendszert, valamint meghatározta a jövőbeni feladat-végrehajtás irányát.

A VCISC-t (Virtual Cyber Incident Support Capability), magyarul Virtuális Kiberesemény-támogató Képességet 2023-ban, a vilniusi NATO-csúcstalálkozón ratifikálták és vezették be. Ez egy olyan központi NATO-szolgáltatás, amely támogatja a tagállamok nemzeti szintű kiberbiztonsági intézkedéseit jelentős kiberfenyegetések esetén. A VCISC portfóliójának kialakítása jelen pillanatban is zajlik, a csatlakozás hozzá önkéntes alapon állandó vagy megfigyelő nemzetként lehetséges.

A korábban felsorolt erőfeszítések koordinációja érdekében jött létre a NATO Cyber Commanders Forum (CCF), magyarul NATO Kiberparancsnokok Fóruma. Ezen a platformon a NATO-tagállamok és partnerországok kiberparancsnokai évente 2 alkalommal megvitatják a kibervédelemmel kapcsolatos erőfeszítések és feladatok aktuális helyzetét, irányokat határoznak meg az elkövetkező időszakra. A fórum célja, hogy erősítse a szövetséges kibervédelmi képességeket, megoszthassák a legjobb gyakorlatokat és fejlesszék a közös válaszokat a globális kiberkihívásokra. Mivel a NATO- és EU-nemzetek számos esetben átfedést mutatnak, így nem meglepő módon az EU Cyber Commanders Conference (CyberCo)[11] feladatai nagyobbrészt e feladatokkal összhangban vannak, így megvalósítva és biztosítva a szoros szakmai együttműködést.

A szabályzói környezet változása

Az átalakítás fontos része volt az egyes tagállamok nemzeti kiberbiztonsági stratégiáinak kidolgozása és elfogadása. Magyarország már 2013-ban elfogadta a Nemzeti Kiberbiztonsági Stratégiáját, amely hangsúlyozta a kritikus infrastruktúrák védelmét és az információs biztonságot. Ezeket a stratégiákat a NATO szintjén is integrálták, biztosítva ezzel a koherens és hatékony együttműködést.[12] A NATO több straté-

[10] CCD COE 2017.
[11] EU Kiberparancsnokok Konferenciája: https://hungarian-presidency.consilium.europa.eu/hu/esemenyek/eu-kiberparancsnokok-konferenciaja
[12] Kovács 2019.

giai dokumentumot és politikát fogadott el, amelyek a kibervédelem fejlesztésére és koordinálására irányultak. Az egyik ilyen jelentős dokumentum a NATO 2014-es Kibervédelmi Politikai Irányelvei, amely meghatározta a kibervédelemmel kapcsolatos elvárásokat és irányelveket. Emellett létrehozták a korábban említett NCSC-t, amely hatékonyabb technikai szakértelmet, incidenskezelést és kiberbiztonsági szolgáltatásokat biztosít a NATO rendszerei számára.

2016-ban megkezdődött a Cyber Defence Pledge vállalások kialakítása, amelyben a NATO-tagállamok elkötelezték magukat a nemzeti kibervédelmi képességeik megerősítésére és összehangolására, ez szoros kapcsolatban áll a NATO Defence Planning Process (NATO Védelmi Tervezési Folyamat, NDPP)[13] vállalásaival. Ennek további erősítése céljából 2020-ban véglegesítették a 2016-os vállalások végrehajtási tervét, amely konkrét intézkedéseket tartalmaz a tagállamok közötti együttműködés erősítésére. Ez a kidolgozói munka folyamatos megújulást tesz szükségessé a részt vevő nemzetek részéről is, Magyarország ebben aktív szerepet vállal, a meghatározott célok megvalósulására kiemelt figyelmet fordít. 2020-ban a NATO elfogadta a kibervédelmi stratégiáját, amely az országok közötti együttműködést és az információs védelmet hangsúlyozza.[14]

2022-ben az Atlanti Tanács kiadta a *Kibervédelmi Kézikönyv*et, amely részletes útmutatást ad a tagállamok számára a kiberbiztonság megvalósítására, információt nyújt a NATO kibervédelmi megközelítéséről. A kézikönyv különböző kibervédelmi kihívásokat fogalmaz meg, beleértve a kibervédelmi elveket, stratégiákat és a legjobb gyakorlatokat, amelyeket a NATO és tagállamai követnek a hálózataik és információs rendszereik védelme érdekében.

A kézikönyv tartalmazza az alábbi fontos irányelveket:

- *kibervédelmi elvek:* a kibervédelem alapvető fogalmainak és irányelveinek bemutatása;
- *stratégiai és taktikai megközelítések:* a fenyegetések észlelésére, megelőzésére és reagálására vonatkozó részletes stratégiákat és taktikákat;
- *legjobb gyakorlatok:* a múlt kiberincidenseikből származó példák és tanulságok;
- *képzések és gyakorlatok:* információ a képzési programokról és gyakorlatokról, mint például a Cyber Coalition, amely az egyik legnagyobb kibervédelmi gyakorlat a világon;
- *együttműködés és koordináció:* irányelvek a NATO-tagállamok közötti együttműködés és koordináció érdekében a kibervédelmi képességek erősítésére.

A NATO a fenti folyamatok erősítése és tesztelése érdekében kibervédelmi gyakorlatok rendszerét alakította ki, amelyek több szinten valósulnak meg. Némelyek a döntéshozatali szintet célozzák meg és a mandatálási folyamatokra fókuszálnak, másokban a technikai feladatok jelennek meg túlnyomó részben. Tendenciaként megfigyelhető, hogy a komplex gyakorlatok irányába tolódik el a fókuszpont, így is szimulálva a valós, mindennapi élethez hasonlító feladat-végrehajtást. Mivel a nemzetek véges erőforrásokkal rendelkeznek, így megkezdődött e kibervédelmi és kiberműveleti gyakorlatok

[13] NATO 2022.
[14] Păunescu 2021.

újragondolása is, annak érdekében, hogy a valóban releváns folyamatok gyakoroltatása szerepeljen elsődleges prioritásként a jövőben. Egyre hangsúlyosabban jelenik meg eme gyakorlatok során a katonai műveletek sikeres végrehajtása érdekében biztosított civil infrastruktúra védelme, amely előrevetíti a civil szolgáltatókkal való szorosabb együttműködést.

A NATO a nemzetközi együttműködést kiemelt fontosságú területként kezeli, ennek érdekében komplex szervezeti rendszert üzemeltet.[15] Az együttműködés más nemzetközi szervezetekkel, mint például az EU, az ENSZ és az EBESZ, lehetőséget biztosít az információk és legjobb gyakorlatok megosztására, valamint a közös kiberhadgyakorlatok megszervezésére. A NATO és az Európai Unió (EU) közötti technikai szintű kiberbiztonsági kapcsolatokért felelős szervezet a NATO NCIRC és a CERT-EU.[16] Ezek a szervezetek együttműködnek a kiberfenyegetések megelőzése, észlelése és reagálása, valamint az információcsere és a technikai együttműködés érdekében.

Folyamatban lévő változások

A NATO-tagországok 2024. július 10-én megállapodtak egy új központ létrehozásáról az egyre kifinomultabb kiberfenyegetésekkel szembeni hatékonyabb védelem érdekében. A NATO Integrált Kibervédelmi Központja (NICC)[17] a tervek szerint fokozni fogja a NATO és a szövetséges hálózatok védelmét és a kibertér műveleti területként való használatát. Feladata lesz a NATO katonai parancsnokainak tájékoztatása a kibertér lehetséges fenyegetéseiről és sebezhetőségeiről, ez magában foglalja a katonai tevékenységek támogatásához szükséges, magántulajdonban lévő polgári kritikus infrastruktúrák fokozott védelmét is, így erősítve a katonai-civil kapcsolatokat. Nem elképzelhetetlen, hogy a korábban CIMIC[18] funkcióként azonosított feladatrendszer új alapokat fog kapni, és részlegesen kapcsolati link alakul ki a kiberszakterülettel. Ez az új központ különbözik a NATO Kiválósági Központjaitól, amelyeket a tagállamok függetlenül működtetnek, és amelyek a képzésre és a kutatásra összpontosítanak. Az NICC közvetlenül a NATO parancsnoki struktúrája alá tartozik, ötvözve a polgári és katonai vezetést a műveleti támogatás nyújtása és a jövőbeli kiberképességek fejlesztése érdekében.

A pontos tervek jelen pillanatban még nem nyilvánosak, az NICC felépítésére és funkcióira vonatkozó részleteket az elkövetkező hónapokban dolgozzák ki, azonban az már most is látszik, hogy az évek alatt kialakult szervezetek feladatrendszerét ismételten át fogják tekinteni, az integráció elkerülhetetlen a hatékonyság növelésének érdekében. Elhelyezése Belgiumban a Supreme Headquarters Allied Powers Europe (SHAPE)[19] bázisán tervezett, feltételezhetően a publikációban korábban felsorolt szervezeti elemek jelentős része érintett lesz az átalakulásban.

[15] Bányász–Krasznay–Tóth 2021.
[16] Az Európai Unió Kibereseményekre Reagáló Csoportja.
[17] NATO 2024.
[18] Civil-Military Cooperation.
[19] Lásd: https://shape.nato.int/

A tervek szerint 2028-ra teljesen működőképes központi fejlett technológiákat fog alkalmazni a kibertér helyzetismeretének és ellenálló képességének fokozása érdekében, igénybe fogja venni a mesterséges intelligencia által biztosított technikai megoldásokat is. Finanszírozása a NATO közös költségvetéséből és a tagállamok önkéntes hozzájárulásaiból származik majd. Ennek a központnak a létrehozása tükrözi a szövetség válaszát a növekvő kiberfenyegetésekre, amelyeket felerősítenek az olyan geopolitikai feszültségek, mint az ukrajnai háború.

Jövőbeni igények és lehetőségek

A NATO kibervédelmi szervezeti elemeinek folyamatos fejlesztése kulcsfontosságú, hogy lépést tartsanak a gyorsan változó és egyre összetettebb kibertámadásokkal. Az alábbi pontokban megfogalmazott javaslatok figyelembevétele elősegítheti az ezekre a feladatokra való felkészülést nemzeti szempontból is:

- *Innováció és kutatás:* Nagyobb hangsúlyt kell fektetni az új technológiák és kiberbiztonsági megoldások kutatására és fejlesztésére. Ez magában foglalja a mesterséges intelligencia, a gépi tanulás és a kvantum-számítástechnika alkalmazását a kiberfenyegetések észlelésében és elhárításában.
- *Képzés és oktatás:* Folyamatosan frissített és bővített képzési programok biztosítása a kibervédelmi szakemberek számára. Ezzel javítható a szakemberek felkészültsége és reakcióképessége az új típusú támadásokkal szemben.
- *Nemzetközi együttműködés:* Erősíteni kell az együttműködést a NATO részéről más nemzetközi szervezetekkel. Ez lehetővé teszi az információk és legjobb gyakorlatok megosztását, valamint a közös kibergyakorlatok megszervezését. Nemzeti téren ennek szintén kiemelt prioritásként kell megjelennie.
- *Incident Response Capability:* Fejleszteni kell a kibertámadásokra való gyors reagálás képességét, beleértve a jelentős incidensek koordinálását és elhárítását. Ez magában foglalja a gyorsreagálási csapatok (a NATO esetében az RRT) bővítését és az új eszközök és technikák bevezetését.
- *Kiberfegyverzetek szabályozása:* Fontos, hogy a NATO támogassa a nemzetközi szinten elfogadott szabályokat és irányelveket a kiberfegyverzetek használatára vonatkozóan. Ez hozzájárulhat a kiberhadviselés szabályozottabbá és kiszámíthatóbbá tételéhez. A kibertérben való feladat-végrehajtás jogi aspektusainak vizsgálatát tovább kell folytatni, biztosítani kell a kibertérerők számára szükséges felkészülést a kibertérben történő fegyveres konfliktusokra.
- *Integrált kiberbiztonsági stratégiák:* Az egyes tagállamok nemzeti kiberbiztonsági stratégiáinak integrálása és harmonizálása a NATO általános stratégiájával. Ez koherensebb és hatékonyabb védekezést eredményezhet.

Ezek a fejlesztések hozzájárulhatnak ahhoz, hogy a NATO kibervédelmi képességei még hatékonyabbak és ellenállóbbak legyenek a jövőbeni kihívásokkal szemben.

Összegzés

A publikációban felsorolt szervezeti elemek együtt dolgoznak a NATO kibervédelmi képességeinek folyamatos fejlesztésén és fenntartásán, együtt alkotják a szövetség kibervédelmi és kiberműveleti képességeit az ismertetett szabályzói környezetnek megfelelően. A NATO kibervédelmi rendszerének átalakítása egy átfogó és komplex folyamat volt, amely magában foglalta a stratégiai és szervezeti változásokat, a kiberbiztonsági stratégiák és keretrendszer kidolgozását, új szervezetek létrehozását, folyamatos képzéseket és a nemzetközi együttműködést. A NATO ezen evolúciós folyamat következő állomásaként döntött az NICC megalakításáról, a szervezeti elemek ismételt felülvizsgálatáról. Ezek az intézkedések biztosítják a NATO számára a rugalmas és hatékony kibervédelmi képességeket a jövőbeni kihívásokkal szemben.[20]

A NATO rendszereinek alrendszerként részét képezik a nemzeti rendszerek is, ezzel számos jövőbeni veszélyforrás jelentkezik a kibertérből. Ezek közül a jellemzőbb veszélyforrások:

- *Agresszív kiberhadviselés:* Az Oroszország és más államok által végrehajtott agresszív kiberhadviselési támadások jelentős fenyegetést jelentenek. Ezek a támadások gyakran célba veszik a NATO-tagállamok kritikus infrastruktúráit, mint például az energia- és vízszolgáltatási rendszerek, a közlekedési hálózatok és a pénzügyi szektor.
- *Hibrid támadások:* A hibrid támadások kombinálják a kiberfenyegetéseket a fizikai támadásokkal, amelyek célja az infrastruktúra megrongálása és a társadalmi káosz kiváltása. Ezek a támadások komplexek és nehezen megelőzhetők.
- *Szabotázs és káosz:* Az ismert hacker- és APT (Advanced Persistent Threat) csoportok által végrehajtott szabotázsakciók célja a rendszerek leállítása és a hálózatok megrongálása ideológiai vagy financiális célból. Ezek a támadások komoly kárt okozhatnak, különösen akkor, ha célba veszik a kritikus infrastruktúrákat.[21]
- *Erősödő kiberfegyverzetek:* Az országok folyamatosan fejlesztik kiberfegyvereiket, amelyek egyre hatékonyabbak és veszélyesebbek lesznek. Ezek a fegyverek képesek lehetnek komplex támadások végrehajtására, amelyeket nehezen lehet azonnal azonosítani és elhárítani. A korai előrejelző rendszerek alkalmazása fel fog értékelődni, és megjelennek a mesterséges intelligencia használatával kapcsolatos félelmek.
- *Közösségi média és dezinformáció:* A kiberfenyegetések nem korlátozódnak a technikai támadásokra. A dezinformáció és a manipulált információk terjesztése is jelentős veszélyforrás, ami negatív irányba befolyásolja az emberek gondolkodását és a társadalmi bizalmat. A PSYOPS[22] egyre inkább összekapcsolódik a kiberszakterület műveleti feladat-végrehajtásával, valamint a műveleti tervezéssel. Ezeknél a folyamatoknál az előzetes tervezés mellett fontos szerepet játszik az időtényező, a bekövetkezett eseményekre adott válaszidő.

[20] Brent 2019.
[21] Johnson 2015.
[22] PSYOPS – Psychological Operations.

Ezek a veszélyforrások folyamatosan változnak és fejlődnek,[23] így a NATO rendszereinek, folyamatainak, szabályzóinak és szervezeti elemeinek rendszeres felülvizsgálata, modernizálása elengedhetetlen a biztonság megőrzése érdekében. Megállapítható, hogy a nemzeti rendszerek és képességek során elsődlegesen a fenti veszélyforrások kezelésére kell felkészülni, oly módon, hogy a kihívásokra adott válaszok kielégítsék a NATO-szerepvállalásból adódó követelményrendszert is.[24]

A kezdetben megfogalmazott hipotézis igazolása a folyamatok vizsgálata során beigazolódott, egyértelművé vált, hogy a NATO-ban végbement, kiberteret érintő evolúciós folyamatok hatással voltak a nemzeti szabályzói struktúra és szervezeti elemek kialakítására. Ezen logikát követve bizonyítható, hogy a szövetségesi rendszerben jelenleg zajló változások meg fogják mutatni az irányt a nemzeti képességfejlesztés számára, a „jövőbeni igények és lehetőségek" pontban megfogalmazott követelmények minden szervezeti elem számára feladatokat fognak meghatározni, amelyek már most körvonalazódnak. A vállalások összehangolását nagymértékben elősegíti a Cyber Defence Pledge során megfogalmazott irányelvek szisztematikus követése, azonban a nemzeti sajátosságok beépítése prioritást kell hogy élvezzen. A nemzetek hasonló problémákkal fognak szembesülni a feladat-végrehajtás folyamán, a hagyományos határok csekély mértékben értelmezhetők a kibertérben végrehajtandó műveletek során, a civil szolgáltatok szerepe fel fog értékelődni.[25]

Felhasznált irodalom

Bányász Péter – Krasznay Csaba – Tóth András (2021): A NATO kibervédelmi szakpolitikája. In Szenes Zoltán (szerk.): *A mai NATO: a szövetség helyzete és feladatai.* Budapest: HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft., 130–149.

Bányász Péter – Krasznay Csaba – Tóth András (2022): A kibervédelem szakpolitikai szintjének helyzete és kihívásai Magyarországon, az EU-banés a NATO-ban. *Military and Intelligence Cybersecurity Research Paper,* (8), 1–30. Online: https://bit.ly/3TUU2lf

Bányász Péter – Orbók Ákos (2013): A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. *Hadtudomány,* 23(E-szám), 188–209.

Brent, Laura (2019): NATO's Role in Cyberspace. *NATO Review,* 2019. február 12. Online: www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

CCD COE [é. n.]: Hungary Joins the Centre. Online: https://web.archive.org/web/20130430095220/http:/www.ccdcoe.org/188.html

CCD COE (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched.* Online: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

[23] Kovács 2023.
[24] 2024. évi LXIX. törvény.
[25] U.S. Cyber Command 2023.

Dinnis, Heather Harrison (2012): *Cyber Warfare and the Laws of War.* Cambridge: Cambridge University Press.
Haleliuk, Ross (2024): *Cyber for Builders: The Essential Guide to Building a Cybersecurity Startup.* Venture in Security.
Johnson, Thomas A. (2015): *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare.* New York: Routledge.
Kovács László (2019): *Kiberbiztonság és -stratégia.* Budapest: Ludovika.
Kovács László (2023): *Hadviselés a 21. században: kiberműveletek.* Budapest: Ludovika.
NATO (2016): *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.* Online: www.nato.int/cps/en/natohq/official_texts_133169.htm
NATO (2022): *NATO Defence Planning Process.* 2022. március 31. Online: www.nato.int/cps/en/natohq/topics_49202.htm
NATO (2024): *Allies Agree New NATO Integrated Cyber Defence Centre.* 2024. július 10. Online: www.nato.int/cps/en/natohq/news_227647.htm
Ottis, Rain (2007): *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective.* CCD COE. Online: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
Păunescu, Dragoș-Mihai (2021): NATO's Encounters in the Cyber Domain. In Ghiba, Daniel – Popescu, Lucian – Olariu, Cosmin – Mustață, Adi (szerk.): *Proceedings of the 17th International Scientific Conference "Strategies XXI" – Strategic Changes in Security and International Relations*, XVII. 153–158.
Samtani, Sagar – Chai, Yidong – Chen, Hsinchun (2022): Linking Exploits from the Dark Web to Known Vulnerabilities for Proactive Cyber Threat Intelligence: An Attention-Based Deep Structured Semantic Model. *MIS Q, Computer Science,* 46(2), 911–946. Online: https://doi.org/10.25300/MISQ/2022/15392
U.S. Cyber Command (2023): *2023 Posture Statement of General Paul M. Nakasone.* 2023. március 7. Online: www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone

Jogi források

2024. évi LXIX. törvény Magyarország kiberbiztonságáról. Online: https://net.jogtar.hu/jogszabaly?docid=a2400069.tv