A NATO Kibervédelmi Kiválósági Központ bemutatása
Presentation of the NATO Cooperative Cyber Defence Centre of Excellence

Tóth Tamás[1]

Absztrakt:

A NATO[2] az információs társadalom új kihivásainak a tükrében, az információs művelteken belül, kifejezetten a kiberhadviselés okozta fokozott sérülékenység proaktív, valamint reaktív módon történő, egységes tagállami reagálása érdekében 2008. május 14-én létrehozta a NATO Kooperatív Kibervédelmi Kiválósági Központot[3]. A Központ székhelyéül az észtországi Tallinn került kiválasztásra. Feladata a NATO-tagállamok és partnereik kibervédelmi kapacitásainak erősítése a tapasztalatcsere, az oktatás és kutatás-fejlesztés területén.[4] A tanulmány a Központ kialakulásának történetét, szervezeti felépítését, feladatait és jelentősebb projektjeit hivatott ismertetni.

Kulcsszavak: NATO CCD COE, kiberbiztonság, kiválósági központ

Abstrakt:

The NATO challenges in the new information system society consisted of cyber warfare with continuous sensitivity in the matter of proactive as well as reactive related information operation. NATO created the Cooperative Cyber Defence Centre of Excellence on May 14, 2008. The Center is headquartered in Tallinn, Estonia. The mission of this center is to share their knowledge and information experiences of cyber defense with members of NATO and its partners. This study demonstrates and informs people of the history of the center through its structure, mission, and main projects.

Keywords: NATO CCD COE, cyber security, center of excellence

---

[1] ORCID azonosító: 0000-0003-4977-6355

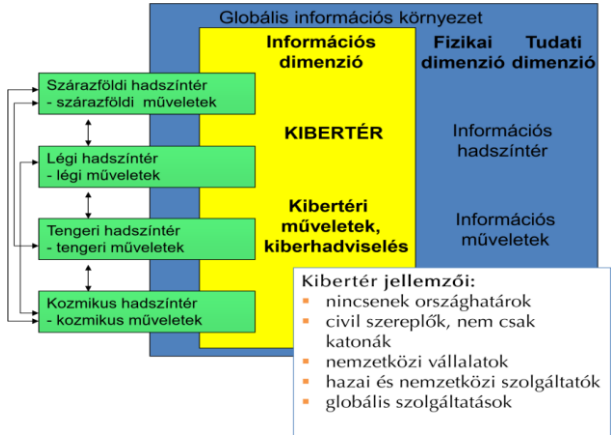
[2] North Atlantic Treaty Organisation – Észak-atlanti Szerződés Szervezete

[3] NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)

[4] BODA József: „Szigorúan Titkos!"? – Nemzetbiztonsági almanach, Zrínyi Kiadó, Budapest, 2016. p. 125.

Bevezetés – A NATO CCD COE kialakulásának története

A hidegháború befejezése után megjelenő új típusú biztonsági kihívások közül, napjainkra a kiberberbiztonságot veszélyeztető tevékenységek jelentik a legnagyobb kockázatot. Az információs műveletek szegmensén belül, megjelent a kiberhadviselés, mely a hadszínterek 5. dimenziójában,[5] a kibertérben[6] fejti ki műveleti hatásait.



1.ábra: A kibertér értelmezése[7]

A NATO először az 1999. évi koszovói bombázásokat követően detektált kibertámadást a rendszerei ellen, mely során kezdetben a Fekete Kéz szerb hacker cso-

[5] Warsaw Summit Communiqué – Varsói NATO Csúcs Közleménye 70. 71. pont, Varsó, 2016. július, https://www.nato.int/cps/en/natohq/official_texts_133169.htm (letöltés ideje: 2018. április 29.)

[6] SIMON László – DR. MAGYAR Sándor: A terrorizmus és indirekt hatása a kibertérben, In: Nemzetbiztonsági Szemle, 2017/III. szám, NKE NBI, p. 96-97. https://www.uni-nke.hu/document/uni-nkehu/nemzetbiztonsagiszemle-2017-3-1.original.pdf (letöltés ideje: 2018. április 29.)

[7] KOVÁCS László: Kiberhadviselés Magyarországon, Ludovika Szabadegyetem, Budapest, 2015. https://www.uni-nke.hu/document/uni-nke-hu/7-kovacs-laszlo.original.pdf (letöltés ideje: 2018. február 19.)

port, majd a belgrádi Kínai Nagykövetség bombázását követően kínai, és orosz hackerek hajtottak végre főleg DDOS,[8] valamint deface[9] támadásokat.[10] Ennek eredményeképpen, a 2002-es prágai NATO csúcstalálkozó után különösen nagy jelentőséget kapott a NATO kibervédelmi politikájának kialakítása.[11]

A következő offenzívát 2007-ben szenvedte el a szervezet, Észtország ellen indított kibetámadás-sorozat formájában.[12] Kétségtelen, hogy ez a támadás gyakorolta a legnagyobb hatást a NATO kibervédelmi struktúrájára, hiszen néhány támadás esetében sikerült azokat visszanyomozni, és orosz szerverekhez kötni. Az offenzíva azt követően érte Észtországot, miután eltávolították a tallinni II. világháborús szovjet hősi emlékművet. A fő célpontok az észt közigazgatás, a pénzügyi szektor, valamint az információs infrastruktúrák voltak.[13] Az akciók jellege és szervezettsége alapján kijelenthető, hogy ez volt az első kiberháborús tevékenység két ország között. Egy évvel később Oroszország szintén kiberhadművelet alkalmazása mellett döntött. A 2008 augusztusában kitört dél-oszétiai háború során az orosz és grúz erők között kialakuló fegyveres konfliktus eszkalációjának jelentős kiber aspektusai is detektálhatóak voltak. Oroszország blokád alá vonta a grúz internethálózatot, valamint nagyszabású deface támadásokat hajtott végre a grúz kormányzati rendszerek ellen. A kormányzati weboldalakat megbénították, majd Mihail Szakasvili elnököt náci diktátorként ábrázoló képeket osztottak meg felületükön. Ezzel párhuzamosan a grúz vezetést lejárató, dezinformációs weblapok is megjelentek a világhálón.[14]

---

[8] Distributed Denial of Service – Szolgáltatásmegtagadással járó támadás

[9] Egy adott weboldal nyitólapjának megváltoztatására irányuló támadás, melynek célja, hogy azt a támadók a saját közlendőjük megosztására használják fel.

[10] Új fenyegetések: a kiberdimenzió, NATO Tükör, 2011, https://www.nato.int/docu /review/2011/11september/Cyber-Threads/HU/index.htm (letöltés ideje: 2018. április 24.)

[11] TÓTH András: A prágai NATO csúcstalálkozót követő határozatok, megállapodások a parancsnoki rendszer-és a vezetési rendszer korszerűsítésére, valamint az együttes tevékenység képesség fejlesztésére, In.: Hadmérnök, 2016/ 3. sz. p. 214. http://hadmernok.hu/163_17_tothandras.pdf (letöltés ideje: 2018. április 29.)

[12] MÜLLER Tamás: Kiberfenyegetések és kibervédelem, Infojegyzet 2016/44. sz. OGY Hivatal Közgyűjteményi és Közművelődési Igazgatóság Képviselői Információs Szolgálat, 2016.http://www.parlament.hu/documents/10181/595001/Infojegyzet_2016_44_kibervedelem .pdf/d1ca0029-dc3f-4cb3-8d5c-9ed0592d2f1d (letöltés ideje: 2018. április 29.)

[13] KELEMEN Roland: A kibertámadás minősülhet-e fegyveres konfliktusnak? In.: Jogász/Világ, 2015. https://jogaszvilag.hu/rovatok/szakma/a-kibertamadas-minosulhet-e-fegyveres-tamadasnak (letöltés ideje: 2018. április 29.)

[14] BERKI Gábor: A kibertéri konfliktusok változásai, In.: Hadmérnök, 2013/1. sz. 2013. p. 175. http://hadmernok.hu/2013_1_berkig.pdf (letöltés ideje: 2018. április 29.)

Az utóbbi két támadás-sorozat rámutatott az információs műveletek, azokon belül is a kiberhadviselés egyre jelentősebb szerepére. A NATO tagországok védelmi minisztereinek 2007 évi brüsszeli találkozóján már megfogalmazódott az igény egy egységes kibervédelmi arculat kialakítására, amely eredményeként 2008 januárjában elfogadták a NATO „*Kibervédelmi Irányelvek*"[15] című dokumentumot. A dokumentum „*szerint a NATO-nak és a nemzeteknek is meg kell védeniük a kulcsfontosságú informatikai rendszereiket, meg kell osztaniuk a legjobb gyakorlatokat és olyan képességekkel kell rendelkezniük, hogy egy szövetséges állam segítségére siethessenek egy kibertámadás elhárítására.*"[16]

Az irányelveket a 2008. április 2–4. között rendezett bukaresti NATO csúcson az államfők egyhangúan meg is erősítettek.

„A NATO továbbra is elkötelezett, hogy megerősítse a Szövetség kulcsfontosságú információs rendszereit a kibertámadásokkal szemben. Nemrég elfogadtunk egy Kibervédelmi Irányelvet, és továbbra is fejlesztjük az ezt megvalósító szervezeteket és hatóságokat. A Kibervédelmi Irányelv hangsúlyozza, hogy a NATO-nak és a nemzeteknek is meg kell védeniük kulcsfontosságú informatikai rendszereiket saját felelősségi körükben; meg kell osztaniuk a legjobb gyakorlatokat; és biztosítaniuk kell azokat a képességet, amelyekkel erre vonatkozó kérést követően egy szövetséges állam segítségére siethetnek egy kibertámadás elhárítására. Bízunk benne, hogy folytatódik a NATO kibervédelmi képességeinek fejlesztése és a kapcsolatok erősítése a NATO és a nemzeti hatóságok között."[17]

Az Észak-atlanti Szerződés Szervezete kibervédelmi-politikájának tükrében, a megfogalmazott kötelezettségek végrehajtására, a NATO Szövetséges Transzformációs Parancsnokság[18] alárendeltségében 2008. május 14-én létrehozta a NATO Kooperatív Kibervédelmi Kiválósági Központot. Az Észak-atlanti Tanács a Központ-

[15] NATO Policy on Cyber Defence, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf (letöltés ideje: 2018. április 29.)

[16] SIPOSNÉ KECSKEMÉTHY Klára NATO-csúcstalálkozó az elrettentés és a védelem jegyében, In.: Hadtudomány, 2017/1-2. sz. 2017. p. 117. http://real.mtak.hu/54740/1/HT_2017_114_126_u.pdf (letöltés ideje: 2018. április 29.)

[17] Bucharest Summit Guide – Bukaresti NATO csúcs közleménye 47. pont, Bukarest, 2008. április, http:// www.nato.int/cps/en/natolive/official_texts_8443.htm (letöltés ideje: 2018. április 29.) (fordította: Szentgáli Gergely)

[18] NATO Allied Command Transformation (ACT)

tot 2008. október 28-ai dátummal jogelméleti szempontból is a nemzetközi katonai szervezetek[19] közé sorolja.[20]

A NATO CCD COE működése és felépítése

A központ felállításáról szóló tárgyalások 2007-ben kezdődtek meg, az ACT parancsnokának jóváhagyásával. Az alapításról szóló egyetértési megállapodást 2008 májusában 7 szponzor ország írta alá, Észtország, Lettország, Litvánia, Németország, Olaszország, Spanyolország és Szlovákia vonatkozásában.

Csatlakozás éve	Csatlakozó államok
2008. május 14.	Észtország, Lettország, Litvánia, Németország, Olaszország, Spanyolország, Szlovákia
2010. június 23.	Magyarország
2011. december 16.	Lengyelország, Amerikai Egyesült Államok
2012. április 05.	Hollandia
2014. május 08.	Ausztria (pártoló tag)
2014. június 03.	Csehország, Franciaország, Egyesült Királyság
2015. november 11.	Görögország, Törökország, Finnország (pártoló tag)
2017. május 30.	Belgium, Svédország (pártoló tag)
2018. április 24.	Portugália

2.ábra: A NATO CCD COE tagállamainak csatlakozási ideje[21] (Szerkesztette: Tóth Tamás)

[19] International Military Organisation (IMO)

[20] Centre is the first International Military Organization hosted by Estonia, 2008. https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html (letöltés ideje: 2018. április 29.)

[21] History, https://ccdcoe.org/history.html (letöltés ideje: 2018. április 29.)

A Központ székhelye Tallinnban került felállításra az észt Híradó Zászlóalj épületében, amely modernizálását követően az egyik legjobb technikai eszközökkel felszerelt kibervédelmi objektummá vált globális szinten. Jelenleg 21 ország tagja a Központnak, Japán, Ausztrália és Norvégia jelezte csatlakozási szándékát.[22]

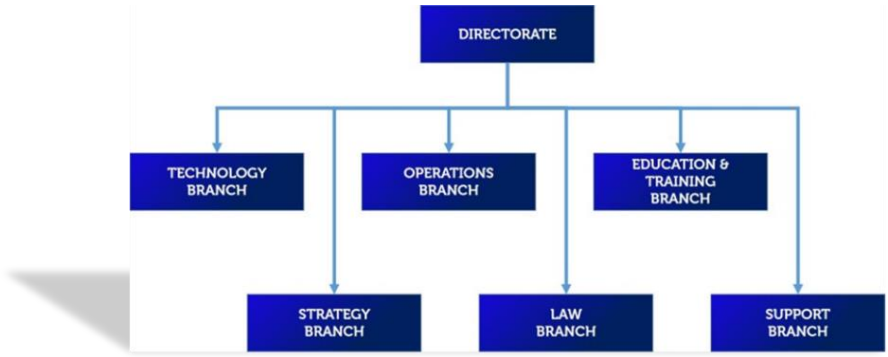
A Központ, finanszírozási oldalról vizsgálva nem tartozik a NATO által gazdasági szempontból fenntartott szervezetek közé. Megállapodás alapján a szponzorállamok biztosítják a működéshez szükséges anyagi forrásokat. A tevékenységhez szükséges infrastrukturális háttér, valamint az adminisztratív költségek biztosítását Észtország vállalta magára. A központ nem része a NATO vezetési rendszerének, azonban a katonai parancsnoki struktúrának részét képezi. Minden NATO tagállam számára biztosított a lehetőség, hogy részt vegyen a Központ munkájában. A szervezet irányítását a támogatónemzetek által delegált tagságból álló több nemzeti vezetői testület[23] hajtja végre. A támogató országok azonos szavazati jogokkal rendelkeznek. *„A központ a kiberbiztonság területén oktatással, konzultációval, kutatással és fejlesztéssel foglalkozik, számos online és nyomtatott formában is elérhető kiadványuk kötődik a kiberkonfliktusok és kiberhadviselés etikai, illetve jogi kérdéseihez, a megfelelő kibervédelem kialakításához. Foglalkoznak technológiai témákkal, valamint a kiberbiztonsági stratégiák elkészítésével és fejlesztésével*."[24] A Központ számos nemzetközi kibervédelmi gyakorlatot, valamint konferenciát szervez a tagállamok között. [25]

[22] NATO CCD COE, 2018. https://ccdcoe.org/tallinn-based-nato-cooperative-cyber-defence-centre-excellence welcomed-portugal-new-member.html (letöltés ideje: 2018. április 30.)

[23] Multinational Steering Committee (MSC)

[24] BELÁZ Annamária – BERZSENYI Dániel: Kiberbiztonsági Stratégia 2.0 A kiberbiztonság stratégiai irányításának kérdései, Elemzések 3/2017. sz. NKE Stratégiai Védelmi Kutatóközpont, Budapest, 2017. p. 6. http://real.mtak.hu/67199/1/SVKK_Elemzesek_2017_3_Kiberbiztonsagi_Strategia_2.0_Belaz_A._Berzsenyi_D._u.pdf (letöltés ideje: 2018. április 29.)

[25] CSÁNYI Benedek: A NATO Kibervédelmi Kiválósági Központja, Biztonságpolitika.hu, 2011, http://old.biztonsagpolitika.hu/?id=16&aid=1148&title=a-nato-kibervedelmi-kivalosagi-kozpontja (letöltés ideje: 2018. április 29.)



3.ábra: A NATO CCD COE szervezeti ábrája[26]

Directorate – Igazgatóság (több nemzeti vezetői testület)
Az Igazgatóságot a tagállamokból delegált képviselők alkotják, ez a többnemzeti testület felelős a Központ irányításáért. A vezetői testület élén az Igazgató (*Director*) áll, aki koordinációs és vezetői tevékenységet lát el. 2017. szeptember 1-jei hatállyal a NATO Kooperatív Kibervédelmi Kiválóság Központ Igazgatói beosztását, Merle Maigre tölti be, aki Sven Sakkovot váltotta a pozícióban. Maigre korábban az Észt Elnök Biztonságpolitikai Tanácsadója volt.[27] Az Igazgató közvetlen alárendeltségében működik a Törzsfőnök (*Chief of Staff*), aki egyben Igazgató-helyettesként (*Deputy Director*) is funkcionál. A pozíciót 2016. szeptember 01-től Franz Lantenhammer alezredes tölti be. Lantenhammer 2010 és 2016 között a Német Szövetségi Fegyveres Erők CERTBw-t vezette.[28]

Technology Branch – Technológiai Ág
Az egység az új technológiák alkalmazásának lehetőségeit, valamint a támadások elhárításának vizsgálatát végzi kutatási és fejlesztési területen, tudományos szemszögből. Kiemelkedő szerepet tölt be a tagállamok kiberképességeinek fejlesztése területén.[29]

---

[26] Structure, https://ccdcoe.org/structure-0.html (letöltés ideje: 2018. április 29.)
[27] Merle Maigre to Become Director of the NATO CCD COE, https://ccdcoe.org/merle-maigre-become-directornato-cooperative-cyber-defence-centre-excellence.html (letöltés ideje: 2018. április 29.)
[28] Franz Lantenhammer, https://ee.linkedin.com/in/fla59 (letöltés ideje: 2018. április 30.)
[29] SZENTGÁLI Gergely: A NATO kibervédelmi politikájának áttekintése, Biztonságpolitika.hu, 2011. http://old.biztonsagpolitika.hu/?id=16&aid=1125&title=a-nato-kibervedelmi-politikajanak-attekintese (letöltésideje: 2018. április 30.)

Strategy Branch – Stratégiai Ág
A NATO tagállamok és a partnerországok számára nyújt segítséget kibervédelmi koncepcióik, doktrínáik kidolgozásához, a védelmi stratégia kialakításához, valamint elemző-értékelő tevékenységet hajt végre kiberműveletek vonatkozásában. A kibervédelmi stratégiatervezéshez nyújtott támogatás elengedhetetlen a tagországok védelmi minimumképességeinek biztosítása érdekében.[30]

Operation Branch – Műveleti Ág
Az egység feladata az új technológiai kihívások okozta kockázatok detektálása, valamint kiberharcászati tevékenység észlelése esetén a reagálás, illetve a bekövetkezett támadás negatív hatásainak csökkentése. A tagállamok között koordinálja a kiberműveletek elhárításával, végrajtásával kapcsolatos feladatokat.

Law Branch – Jogi Ág
Feladata a kibertevékenység nemzetközi jogi kereteinek előkészítése, valamint megalkotása a tagállami szinten történő adoptálás elősegítése érdekében. Az egység tevékenységéhez kapcsolódik a kiberhadviselés jogi szempontból történő elemzése-értékelése. Jogi háttértanulmányokat folytat a NATO kibervédelmi tevékenységének fejlesztése céljából.[31] A Központ ezen szakterülete által alkotott legjelentősebb jogi dokumentumok a 2013-ban összeállított Tallin Manual 1.0, ami a „*Kiberhadviselés Nemzetközi Jogának Kézikönyve*"[32] , illetve a 2017-ben kiadott Tallin Manual 2.0, mely „*A Kiberérműveletek Nemzetközi Jogának Kézikönyve"*[33].

Education & Training Branch – Oktatási és Képzési Ág
A képzéssel és oktatási tevékenységgel foglalkozó szakág jelentős szerepet tölt be a szponzorállamok és a NATO tagállamok információbiztonsági oktatása, valamint

[30] Cyber Security Srategy Documents, https://ccdcoe.org/cyber-security-strategy-documents.html (letöltés ideje: 2018. április 30.)
[31] CSÁNYI Benedek: A NATO Kibervédelmi Kiválósági Központja, Biztonságpolitika.hu, 2011. http://old.biztonsagpolitika.hu/?id=16&aid=1148&title=a-nato-kibervedelmi-kivalosagi-kozpontja (letöltés ideje: 2018. április 29.)
[32] lásd: Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare, Cambridge University Press, Cambridge, 2013. http://csef.ru/media/articles/3990/3990.pdf (letöltés ideje: 2018. május 4.)
[33] lásd: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Tallin, 2017. https:// ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html (letöltés ideje: 2018.április 30.)

a folyamatos képzések, szakmai konferenciák és gyakorlatok lebonyolítása területén.[34] Az egység megalkotta a NATO online elérhető Kibervédelmi Könyvtárát,[35] továbbá a nemzetközi konferenciák tekintetében, Tallinnban minden évbe megrendezésre kerül a CyCon[36], valamint végrehajtásra kerül a Locked Shield[37] nemzetközi kibervédelmi gyakorlatok.

Support Branch – Támogató Ág
Az egység feladata a Központ gazdasági, adminisztratív, valamint technikai támogatása a működés biztosítása érdekében. A háttértámogató tevékenység elengedhetetlen az optimális üzemelés és fenntartás elősegítése során.

Főbb projektek

Tallin Manual 1.0/ 2.0
A Tallinn Manual 1.0 azaz a *„Kiberhadműveletek Nemzetközözi Jogának Kézikönyve”* 2013-ban került összeállításra a CCD COE által, a Nemzetközi Vöröskereszttel, valamint a US Cyber Command[38]-del együttműködve.[39] A kézikönyv a kibertérben vívott fegyveres konfliktusoknak, katonai műveleteknek kíván jogi szabályozást biztosítani, különös tekintettel *„A Polgári Lakosság Háború Idején Való Védelmére Vonatkozóan Genfbe, 1949. Augusztus 12-én Kelt Egyezmény (IV. Genfi Egyezmény)”*[40] előírásainak tekintetében, mivel a kézikönyv „B” rész IV. fejezet 1.

[34] SZENTGÁLI Gergely: A NATO kibervédelmi politikájának fejlődése, In.: Bolyai Szemle, 2012/2. sz. Budapest, 2012. p. 82. http://archiv.uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf (letöltés ideje: 2018. április 30.)
[35] lásd: Cyber Defence Library, https://ccdcoe.org/cyber-definitions.html (letöltés ideje: 2018. április 30.)
[36] lásd: Int. Conference of Cyber Conflicts https://ccdcoe.org/cycon-2018.html (letöltés ideje: 2018. április 30.)
[37] lásd: Cyber Defence Workshop, Locked Shields Forensics Challenge Workshop 2018, https://ccdcoe.org/lockedshields-forensics-challenge-workshop-2018.html (letöltés ideje: 2018. április 30.)
[38] lásd: Egyesült Államok Kibervédelmi Parancsnoksága http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/
[39] BODNÁR Ádám: Elkészült a NATO kibervédelmi kézikönyve, 2013, https://www.hwsw.hu/hirek/49922/tallinn-manual-informatikai-hadvieles-nato-biztonsag-krasznay-csaba.html (letöltés ideje: 2018. május 4.)
[40] A Polgári Lakosság Háború Idején Való Védelmére Vonatkozóan Genfbe, 1949. Augusztus 12-én Kelt Egyezmény (IV. Genfi Egyezmény), Genf, 1949. http://www.mfa.gov.hu/NR/rdonlyres/6CF7F4E7-B841-44F08DCE-67D23DCFB6E2/0/GENF4_hu.pdf (letöltés ideje: 2018. május 4.)

szakasz 29. bekezdése kimondja a civil áldozatok elkerülésének kötelmét is.[41] A dokumentum két fő részre tagolható, az első rész szabályozza a nemzetközi kiberbiztonság jogi aspektusait, a második rész pedig a kibertér fegyveres konfliktusainak jogi alapjait határozza meg. A kézikönyv összesen 95 bekezdésre tagolható.[42]

A 2017-es Tallin 2.0, azaz a *„Kiberműveletek Nemzetközi Jogának Kézikönyve"* a kibertérben végrehajtott fegyveres konfliktusokon kívül szabályozza a kiberműveleteket is. *„Ez egy kiemelten fontos téma manapság, hiszen rendszeresen szembesülünk állami és nem állami szereplők nemzetközi jogokat sértő kibercselekményeivel."*[43] A nagyobb hangsúlyt ez a terület kapja a dokumentumban, hiszen a hadijog helyett, a polgári értelemben vett nemzetközi jogsértő cselekmények, azaz a kiberbűncselkemények szabályozására összpontosít.[44]

Nemzetközi konferencia

CyCon International Conference of Cyber Conflict:

A CyCon mai nevén 2012. óta minden év júniusában, a NATO Kooperatív Kibervédelmi Kiválósági Központ szervezésében kerül megrendezésre. A világon az egyik legjelentősebb kiberbiztonsággal foglalkozó szakmai konferencia, melyen összesen ötszáz jogász, kiberbiztonsággal, katonai-, rendvédelmi-, politikai döntéshozatallal kapcsolatos szakember vesz részt. [45] Az ünnepélyes megnyitó után a konferenciák vitaindító beszédekkel kezdődnek, amelyeket több, egyszerre párhuzamosan zajló szekcióban megrendezett kerekasztal beszélgetés, valamint előadássorozat követ. Az elmúlt években megrendezett konferenciák témái között szerepeltek a kibernetikus fegyveres konfliktusok, az emberek és gépek közötti interakciók fejlődése, valamint a kiberhadviselés jelentősége. [46]

---

[41] SCHMITT, Martin N.: Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare, Cambridge University Press, Cambridge, 2013, pp. 90-91 http://csef.ru/media/articles/3990/3990.pdf (letöltés ideje: 2018. május 4.)

[42] SCHMITT, Martin N.: Tallinn Manual 1.0, Cambridge University Press, Cambridge, 2013. http://csef.ru/media/articles/3990/3990.pdf (letöltés ideje: 2018. május 4.)

[43] MEIJ, Kris van der: NATO Kiválósági Program, Isaca Konferencia 2017, Budapest, 2017. https://isaca.hu/conference/index.php/hu/eloadok (letöltés ideje: 2018. május 4.)

[44]Tallinn Manual 2.0, on the International Law Applicable to Cyber Operations 2017. http://www.atlanticcouncil.org/images/publications/CCDCOE_Tallinn_Manual_Onepager.pdf (letöltés ideje: 2018. május 4.)

[45] CyCon 2017, 2017. https://ccdcoe.org/cycon-2017.html (letöltés ideje: 2018. május 4.)

[46] BERZSENYI Dániel: CyCON 2016 – NATO kibervédelem Varsó előtt, Biztonságpolitika.hu, 2016. http:// biztonsagpolitika.hu/cikkek/cycon-2016-nato-kibervedelem-varso-elott (letöltés ideje: 2018. május 4.)

Nemzetközi kibervédelmi gyakorlatok

Locked Shields:
A Locked Shields egy valós idejű, számítógépes hálózat-védelmi gyakorlat, melyet 2010. óta minden évben megszervez a NATO CCD COE. A feladatok végrehajtása során, a résztvevők kibertámadásokat elhárító csapatokat alkotnak. A gyakorlathoz szükséges virtuális teret a Központ biztosítja. A védekező csapatok feladata egy szituációs környezetben, gyorsreagálású egységként fellépni a támadó erőkkel szemben annak érdekében, hogy biztosítsák egy fiktív NATO tagország rendkívül komplex infrastruktúrával rendelkező stratégiailag fontos rendszerének, objektumának, vagy intézményének védelmét, perzisztens működőképességének fenntartását és szolgáltatásainak állandó biztosítását a fokozódó kibertámadások közepette. A védekezés mellett a csapatok számára párhuzamosan szakértői, jogi és stratégiai döntéshozatalt támogató feladatokat is meghatároznak a szervezők.[47]

Crossed Sword:
A technikai gyakorlat célja, hogy a résztvevők megismerhessék a legújabb támadási taktikákat, technikákat, valamint eljárásokat (TTP), melyeket hatékonyan tudjanak alkalmazni más kibervédelmi gyakorlatokon. *Blue team – red team* jellegű az esemény, mely során a vörös csapat az informatikai ellenerő szerepét játssza el, ők biztosítják a TTP-ket. Folyamatosan fejlesztik a technikai tudásukat, valamint az egységek szervezettségét is. A szervezők fokozott mértékben vonnak be oktatási intézményeket, kutatóműhelyeket a gyakorlatok kivitelezésébe. A 2017. évi *Crossed Sword*-on 350 szakértő vett részt.[48]

Oktatás

A Központ kiemelt figyelmet fordít a támogató országok kibervédelmi szakembereinek oktatására, képzésére. Folyamatos kurzusokat indítanak kritikus információs infrastruktúra védelem, nemzetközi kiberjog, valamint technológiai ismeretek térülten.[49] Az oktatási, képzési tevékenység a tapasztalatcsere, az ismeretbővítés, valamint a képességfejlesztés elősegítését célzó szervezett tevékenység, mely a Központ egyik fő profilja, valamint kiemelt szerepet tölt be működése során.

---

[47] NAGY Tamás: Locked Shields 2015 - kibervédelmi gyakorlat, Honvédelem.hu, 2015. https://honvedelem.hu/cikk/50667_locked_ shields_2015-kibervedelmi_gyakorlat (letöltés ideje: 2018. május 4.)

[48] SZABÓ András: Technikai kiberbiztonsági gyakorlatok – Nemzetközi kitekintés, In: Hadmérnök, 2018/I. sz. 2018. p. 297. http://hadmernok.hu/181_23_szabo.pdf (letöltés ideje: 2018. május 06.)

[49] https://ccdcoe.org/event/law-course.html (letöltés ideje: 2018. május 06.)

Összefoglalás

A 2000-es évek elején detektálható egyre intenzívebb és jelentősebb méretű kibertámadások elhárítása, megelőzése, valamint a válaszcsapások eredményességének növelése érdekében, szükségessé vált a NATO tagországok és a szövetségeseik kibertérben megjelenő kollektív reagáló képességének kialakítása. Így indokolttá vált a katonai struktúrába illeszteni, egy az egységes kibervédelmi arculat létrehozásával megbízott szervezeti egységet. Az Észak-atlanti Tanács 2008-ban, az újfajta kihívásokra való válaszul létrehozta a NATO ACT alárendeltségében, a NATO Kooperatív Kibervédelmi Kiválósági Központot, melyet a nemzetközi katonai szervezetek közé sorol.

A Központ fő feladata, hogy a tagállamok és a partnerországok kibervédelmi kapacitását fokozza a tapasztalatcsere, az oktatás és a kutatás-fejlesztés eszközeivel. A NATO CCD COE olyan közös fórummá kíván válni, amely összegyűjti és partnereivel megosztja mindazon nemzetközi tapasztalatot és tudást, mely a katonai szövetség tagjai és partnerei kiberbiztonságának fenntartásához elengedhetetlen. Rendszeresen megrendezésre kerülnek kibervédelmi konferenciák, valamint gyakorlatok, folyamatos az oktatási, képzési tevékenység a nemzetközi kiberjog, a technológiai innováció, valamint a kritikus információs infrastruktúra védelem területén. Jelentős segítséget nyújt a tagállamok kibervédelmi stratégiáinak létrehozásában, illetve a kiberjog nemzetközileg is elfogadott kialakításában.

A kibertér egyre nagyobb jelentősége, a kiberhadműveltekkel, támadásokkal okozható dinamikusan globális szintre eszkalálódó károk minimalizálása, illetve az információs társadalom biztonságának fenntartása érdekében a Központ, a jövőben még hangsúlyosabb szerepet fog betölteni a Szövetség kollektív, minden dimenzióra kiterjedő hatékony védelmi, reagáló képességének biztosítása érdekében. A NATO CCD COE alapját fogja képezni, egy NATO szintű, a tagállamokból delegált, nemzetközi kiberhadtest kialakítása, képzése és fejlesztése területén, mely a lehető leghatékonyabb kollektív fellépést fogja biztosítani az egyes nemzetek ellen intézett külső támadások megelőzése, elhárítása, valamint a válaszcsapások biztosítása érdekében.

Felhasznált irodalom

- A Polgári Lakosság Háború Idején Való Védelmére Vonatkozóan Genfbe, 1949. Augusztus 12-én Kelt Egyezmény (IV. Genfi Egyezmény), Genf, 1949. http://www.mfa.gov.hu/NR/rdonlyres/6CF7F4E7-B841-44F08DCE-67D23DCFB6E2/0/GENF4_hu.pdf
- BELÁZ Annamária1 – BERZSENYI Dániel: Kiberbiztonsági Stratégia 2.0 A kiberbiztonság stratégiai irányításának kérdései, Elemzések 3/2017. sz.

NKE Stratégiai Védelmi Kutatóközpont, Budapest, 2017. p. 6. http://real.mtak.hu/67199/1/SVKK_Elemzesek_2017_3_Kiberbiztonsagi_Strategia_2.0_Belaz_A._Berzsenyi_D._u.pdf
- BERKI Gábor: A kibertéri konfliktusok változásai, In.: Hadmérnök, 2013/1. sz. 2013. p. 175.
- BERZSENYI Dániel: CyCON 2016 – NATO kibervédelem Varsó előtt, Biztonságpolitika.hu, 2016. http://biztonsagpolitika.hu/cikkek/cycon-2016-nato-kibervedelem-varso-elott
- BODA József: „Szigorúan Titkos!"? – Nemzetbiztonsági almanach, Zrínyi Kiadó, Budapest, 2016. p. 125.
- BODNÁR Ádám: Elkészült a NATO kibervédelmi kézikönyve, 2013, https://www.hwsw.hu/hirek/49922/tallinn-manual-informatikai-hadviseles-nato-biztonsag-krasznay-csaba.html
- Bucharest Summit Guide – Bukaresti NATO csúcs közleménye 47. pont, Bukarest, 2008. április, http://www.nato.int/cps/en/natolive/official_texts _8443.htm
- Centre is the first International Military Organization hosted by Estonia, 2008. https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html
- Cyber Defence Workshop, Locked Shields Forensics Challenge Workshop 2018, https://ccdcoe.org/lockedshields-forensics-challenge-workshop-2018.html
- Cyber Security Srategy Documents, https://ccdcoe.org/cyber-security-strategy-documents.html
- CyCon 2017, 2017. https://ccdcoe.org/cycon-2017.html
- CSÁNYI Benedek: A NATO Kibervédelmi Kiválósági Központja, Biztonságpolitika.hu, 2011, http://old.biztonsagpolitika.hu/?id=16&aid=1148&title=a-nato-kibervedelmi-kivalosagi-kozpontja
- U.S. Stategic Command http://www.stratcom.mil/Media/Factsheets /Factsheet-View/Article/960492/us-cyber-command-uscybercom/
- Franz Lantenhammer, https://ee.linkedin.com/in/fla59
- History, https://ccdcoe.org/history.html
- https://ccdcoe.org/event/law-course.html
- International Conference of Cyber Conflicts https://ccdcoe.org/cycon-2018.html
- KELEMEN Roland: A kibertámadás minősülhet-e fegyveres konfliktusnak? In.: Jogász/Világ, 2015. https://jogaszvilag.hu/rovatok/szakma/a-kibertamadas-minosulhet-e-fegyveres-tamadasnak

- KOVÁCS László: Kiberhadviselés Magyarországon, Ludovika Szabadegyetem, Budapest, 2015. https://www.uni-nke.hu/document/uni-nke-hu/7-kovacs-laszlo.original.pdf
- MEIJ, Kris van der: NATO Kiválósági Program, Isaca Konferencia 2017, Budapest, https://isaca.hu/conference/index.php/hu/eloadok
- Merle Maigre to Become Director of the NATO CCD COE, https://ccdcoe.org/merle-maigre-become-director-nato-cooperative-cyber-defence-centre-excellence.html
- MÜLLER Tamás: Kiberfenyegetések és kibervédelem, Infojegyzet 2016/44. sz. OGY Hivatal Közgyűjteményi és Közművelődési Igazgatóság Képviselői Információs Szolgálat, 2016. http://www.parlament.hu/documents/10181 /595001/Infojegyzet_2016_44_kibervedelem.pdf/d1ca0029-dc3f-4cb3-8d5c-9ed0592d2f1d
- NAEL, Merili: Fotod: Merle Maigre astus NATO küberkaitsekoostöö keskuse juhi ameisse, EESTI, Észtország 2017. https://www.err.ee/615869/fotod-merle-maigre-astus-nato-kuberkaitsekoostoo-keskuse-juhi-ametisse
- NAGY Tamás: Locked Shields 2015 - kibervédelmi gyakorlat, Honvédelem.hu, 2015. https://honvedelem.hu/cikk/50667_locked_shields_2015-kiberved elmi_gyakorlat (letöltés ideje: 2018. május 4.)
- NATO CCD COE, 2018. https://ccdcoe.org/tallinn-based-nato-cooperative-cyber-defence-centre-excellence-welcomed-portugal-new-member.html
- NATO Policy on Cyber Defence, https://www.nato.int/nato_ static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf
- SCHMITT, Martin N.: Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare, Cambridge University Press, Cambridge, 2013, pp. 90-91. http://csef.ru/media/articles/3990/3990.pdf
- SHULTZ, Deven: U. S. European Command International Cyber Summit 2018, DVIDS, Németország, 2018. https://www.dvidshub.net/image/4238982/us-european-command-international-cyber-summit-2018
- SIMON László – DR. MAGYAR Sándor: A terrorizmus és indirekt hatása a kibertérben, In: Nemzetbiztonsági Szemle, 2017/III. szám, NKE NBI, p. 96-97. https://www.uni-nke.hu/document/uni-nkehu/nemzetbiztonsagiszemle-2017-3-1.original.pdf
- SIPOSNÉ KECSKEMÉTHY Klára NATO-csúcstalálkozó az elrettentés és a védelem jegyében, In.: Hadtudomány, 2017/1-2. sz. 2017. p. 117. http://real.mtak.hu/54740/1/HT_2017_114_126_u.pdf
- Structure, https://ccdcoe.org/structure-0.html

- SZABÓ András: Technikai kiberbiztonsági gyakorlatok – Nemzetközi kitekintés, In: Hadmérnök, 2018/I. sz. 2018. p. 297.
- SZENTGÁLI Gergely: A NATO kibervédelmi politikájának áttekintése, Biztonságpolitika.hu, 2011. http://old.biztonsagpolitika.hu/?id=16&aid=1125&title=a-nato-kibervedelmi-politikajanak-attekintese
- SZENTGÁLI Gergely: A NATO kibervédelmi politikájának fejlődése, In.: Bolyai Szemle, 2012/2. sz. Budapest, 2012. p. 82. http://archiv.uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf
- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Tallin, 2017. https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html
- Tallinn Manual 2.0, on the International Law Applicable to Cyber Operations 2017.http://www.atlanticcouncil.org/images/publications/CCDCOE_Tallinn_Manual_Onepager.pdf
- TÓTH András: A prágai NATO csúcstalálkozót követő határozatok, megállapodások a parancsnoki rendszer- és a vezetési rendszer korszerűsítésére, valamint az együttes tevékenység képesség fejlesztésére, In.: Hadmérnök, 2016/ 3. sz. p. 214.
- Új fenyegetések: a kiberdimenzió, NATO Tükör, 2011, https://www.nato.int/docu/review/2011/11/september/Cyber-Threads/HU/index.htm
- Warsaw Summit Communiqué – Varsói NATO Csúcs Közleménye 70. 71. pont, Varsó, 2016. július https://www.nato.int/cps/en /natohq/official_texts_133169.htm