HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 3. szám 119–137.
DOI: 10.32567/hm.2021.3.7

Kovács László[1]

Offenzív kiberműveletek II.: Kibererők és képességeik

Offensive Cyber Operations Part Two: Cyber Units and Their Capabilities

A kibertér biztonságának megteremtése számos tevékenység összehangolt megvalósítását igényli. A kiberbiztonság komplex rendszerében a szabályozási és eljárási kérdések mellett aktív kibervédelmi műveleteket is találunk. Ugyanakkor a védelmi célú kibertérműveletek önmagukban nem mindig elégségesek a teljes és átfogó kiberbiztonság megteremtéséhez. Így a védelmi kibertérműveletek mellett offenzív kiberműveletek végrehajtására is szükség lehet. Emellett az offenzív kibertérműveletek, és az abban foglalt eszközök és eljárások természetszerűleg nemcsak a saját oldali rendszereink védelméhez járulnak hozzá, hanem az ellenérdekelt fél infokommunikációs rendszereinek lefogásával, azok működésének akadályozásával, vagy azokból információk kinyerésével más műveleti terekben végrehajtott tevékenységek támogatásához járulnak hozzá hatékony módon. Jelen tanulmány első része az offenzív kiberműveletek általános jellemzőit mutatta be, a második rész, azaz jelen írás az offenzív kiberműveleti képességek gyakorlati megvalósítását és alkalmazhatóságát elemzi, valamint kitér a kiberműveleti erőkre, az általuk alkalmazható eszközökre és eljárásokra.

Kulcsszavak: **kiber, offenzív kiberképesség, támadás, hadviselés, kiberstratégia**

Creating cybersecurity requires coordinated implementation of many activities. In the complex system of cybersecurity, in addition to regulatory and procedural issues, we also find active cyber defence operations. However, cyberspace operations for defence purposes alone are not always sufficient to provide full and comprehensive cybersecurity. Thus, in addition to defence cyberspace operations, it may be necessary to perform offensive cyber operations. The offensive cyberspace operations, together with tools and procedures, naturally not only contribute to

[1] Magyar Honvédség Parancsnoksága, kibervédelmi haderőnemi szemlélő, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Elektronikai Hadviselés Tanszék, egyetemi tanár, e-mail: kovacs.laszlo@uni-nke.hu

the protection of our own systems, but also effectively support activities in other dimensions by intercepting, disrupting, or extracting information from counterparty infocommunication systems. The first part of the present study presents the general characteristics of offensive cyber operations, the second part analyses the practical implementation and applicability of offensive cyber operations capabilities and covers the forces of cyber operations and the tools and procedures they can apply.

Keywords: **cyber, offensive cyber capability, attack, warfare, cyber strategy**

1. Bevezetés

A kiberbiztonság és annak megteremtése jelen korunk egyik nagy kihívása. A 21. században általunk használt és alkalmazott ezernyi infokommunikációs eszköz, rendszer, megoldás és szolgáltatás olyannyira a mindennapjaink részévé vált, hogy azok valódi létfontosságú elemekké váltak életünkben.

Így a biztonság megteremtése létkérdés ezen rendszerek esetében. A fentiekben megfogalmazottak azonban magukkal hozták a hadviselés változását is, hiszen egy ország elleni támadás ma már nem igényli fizikai határainak átlépését, a globális hálózatoknak köszönhetően a rosszindulatú beavatkozás egy-egy jól kiválasztott információs rendszerbe – jellemzően számítógép-hálózatba, vagy annak egyes elemeibe – gyakorlatilag a világon bárhonnan kivitelezhető, és abban komoly – akár a teljes működésképtelenséget is előidéző – kár okozható. A hadviselés tehát változik, mint az emberi történelem során eddig mindig.

Ahogy a korábbi nagy technikai felfedezések, úgy a kibertérben használt infokommunikációs eszközök és rendszerek is változást eredményeznek a hadviselés eljárásaiban és a harcok megvívásának elveiben is. A kibertér jellemzői nagyban segítik azokat az eljárásokat, amelyekkel a hadviselést egyébként jellemezni szoktuk. A különböző támadásokhoz, az azok előkészületeihez szükséges információszerzéstől kezdve a rejtőzködésen át a nagy távolságból végrehajtott csapásokig a kibertér ideális terep a hadviselés számára.

Természetszerűleg jelent meg tehát a hadviselés eddig is színes palettáján a kibertéri műveletek egész sora, amelyekkel a fenti támadások megvalósíthatók. A kérdés csak az, hogy szükséges-e egy adott ország számára kibertámadó, illetve a tágabb értelemben vett offenzív kiberképességeket kiépíteni, azokat fenntartani. A válasz már jelen tanulmány első részéből is körvonalazható volt. Ez a válasz pedig egyértelműen igen, szükséges ilyen képességekkel rendelkeznie egy országnak.

Jelen tanulmány első része az offenzív képességek általános hátterét vizsgálta. Ennek során az olyan kérdések elemzését végeztük el, mint az offenzív kiberképességek összetevői és az offenzív kiberképességek stratégiai megfontolásai. Az írás első részében megvizsgált kérdések egy végső következtetés levonását indukálták, amely nem más, mint annak megállapítása, hogy a jövőben a kibertéri dominancia és a kibertér uralása elengedhetetlen lesz a győzelem kivívásához. Ezért a kibertéri fölény, illetve a kibertérben történő sikeres tevékenység offenzív a kibertéri képességeket is magában foglaló kibererők felállítását igényli. Ma már ezek a képességek elengedhetetlen részét képezik az adott ország biztonsági összetevőinek.

Amennyiben a fentieket elfogadjuk, úgy egy másik, nem sokkal egyszerűbb kérdést, illetve kérdések egész sorát kell megválaszolnunk. Ez pedig nem más, mint az, hogy hogyan is nézzen ki az a szervezet, amely mindezeket a képességeket fel tudja mutatni. Egyáltalán milyen elvek mentén szükséges ezeket a képességeket kialakítani? Ki legyen a felelőse a képességek kialakításának? Milyen módszerek és eljárások járulhatnak hozzá a kiberbiztonsági stratégiákban meghatározott kiberképességek kialakításához? Milyen szerepe van az egyes tagországoknak a NATO offenzív kiberképességének kialakításában?

Ezernyi kérdés, amelyekre jelenleg nem, vagy csak nagyon nagy vonalakban tudunk válaszolni. Jelen írás ezekre a kérdésekre igyekszik – tudományos munka esetében eléggé el nem ítélhető módon a teljesség igénye nélkül – választ adni.

A tanulmányban összegzett vizsgálatok irodalomkutatásra építenek, esetenként az összehasonlító elemzés, majd szintézis módszerének alkalmazásával kiegészítve.

Az elvégzett vizsgálatokból levont következtetések a szerző sajátjai, azok nem feltétlenül esnek egybe sem a Nemzeti Közszolgálati Egyetem, sem a Magyar Honvédség hivatalos véleményével vagy álláspontjával.

2. Az offenzív kiberképességek szükségessége

Az offenzív kiberképességek kialakításának egyik legfőbb indoka az, hogy a lehető legtávolabb tartsuk a potenciális támadó (szemben álló fél, ellenség) rosszindulatú kibertevékenységét a saját rendszereinktől. Ez akkor a leghatékonyabb, amennyiben még a rendszereink megtámadása előtt a potenciális támadót elrettentjük a támadás kivitelezésétől – például olyan védelmi rendszer kiépítésével, amely csak aránytalanul nagy energiabefektetéssel törhető át –, vagy olyan mértékben csökkentjük képességeit, amelyekkel már nem tud hatékony támadást indítani rendszereink ellen. Ez utóbbi esetben van szükség az offenzív kiberképességek meglétére.

Az offenzív, és benne a kibertámadó képességek kialakítása előtt azonban szükséges feltárni azokat a kihívásokat és veszélyeket, amelyek a kibertérben jelentkeznek. Ezek alapján lehet meghatározni az offenzív kiberképességek kialakításához szükséges feltételeket, eszközöket és módszereket. A kihívások és veszélyek feltárása mellett azonban szükség van a köztük lévő összefüggések, illetve azok hatásainak vizsgálatára is.

Az okok között természetesen ott vannak azok a leggyakoribb kibertéri veszélyek, amelyek a technológia sérülékenységeit kihasználva jelentkeznek. Ezek vagy rosszindulatú programokban, vagy az azokra épülő olyan eljárásokban vannak jelen, amelyeket a támadók különböző célokkal alkalmaznak.

Számos olyan infokommunikációs eszközt és rendszert használunk, amelyek vagy vegyes használatúak, azaz polgári és katonai célra egyaránt alkalmazzák őket vagy olyan rendszerek és eszközök, amelyek bár polgári rendszerek (például Commercial off the Shelves, COTS, azaz kereskedelmi forgalomban kaphatók), de mégis katonai célra is használjuk. Ebből következően az ezeket a rendszereket és eszközöket fenyegető veszélyeket is fel kell mérni. A csak katonai célú eszközök és rendszerek esetében a helyzet sok esetben furcsa mód sokkal nehezebb, mint a polgári célú eszközök esetében. Ennek oka elsősorban abban keresendő, hogy a csak katonai

célra alkalmazott eszközök és rendszerek életciklusa – többek között azok bekerülési költsége miatt – sokkal hosszabb, mint ami a polgári rendszerek esetében megszokott. Ennek megfelelően azokat sokkal hosszabb ideig tartjuk rendszerben, így azok időközben napvilágra kerülő sérülékenységei is sokkal hosszabb ideig fennállhatnak. Ráadásul ez a hosszabb időtartam azt is jelenti, hogy a korszerűbb, a kibervédelmet szolgáló megoldások beépítése és alkalmazása egy-egy működő katonai rendszerbe csak lényegesen később és nagyobb energiabefektetéssel valósítható meg.

Egy másik probléma az olyan, a polgári életben már nagy népszerűségnek örvendő és igen elterjedt szolgáltatásoknak a hadseregek életében történő megjelenése, mint amilyenek például a közösségimédia-platformok. Ezek nem önmagukban jelentenek kockázatot vagy veszélyt, hanem a nem tudatos használat révén. A katonák vagy a hadseregben dolgozó civil alkalmazottak meggondolatlan és sok esetben felelőtlen közösségimédia-jelenléte nagyon sokszor komoly információforrást jelent a szemben álló fél vagy a potenciális támadó számára.

A kibertámadó képességek, illetve azok alkalmazásának okait vizsgálva számos közvetett okot is fel tudunk tárni. Ezek közül az első ok azonban rögtön egy komplex problémát takar. Egyrészt ma már számos olyan összetett infokommunikációs rendszert és -eszközt használunk, amelyek mind a civil, mind a katonai (védelmi) szféra működésében megtalálhatók. Sok esetben még ezek felhasználásának primer céljai is azonosak, hiszen alapvetően kommunikációra, adatfeldolgozásra és adattovábbításra használjuk ezeket az eszközöket és rendszereket. A legtöbb esetben még funkcionális értelemben is azonosak a célok, hiszen alapvetően a vezetés támogatása, illetve maga a vezetés megvalósítása az egyik legfontosabb célja ezeknek a rendszereknek. Ennek a problémának a komplexitását azonban az adja, hogy jelen korunk társadalma – és ez alól nem képez kivételt a kor modern hadserege sem – komoly függőséggel rendelkezik ezekkel az eszközökkel és rendszerekkel szemben. A függőség egyben sérülékenységet is jelent. Ráadásul az említett rendszerek komplexitása, a részrendszerek és elemek összekapcsoltsága és egymásra gyakorolt, a működést alapvetően befolyásoló hatása még inkább növeli ezt a sérülékenységet. Ez nyilvánvalóan azt a veszélyt is magában hordozza, hogy egy-egy részelem vagy részrendszer kiesése alapjaiban lehet negatív befolyással az egész rendszerre. Ez adott esetben a társadalom egy-egy funkciójának a teljes leállásához, vagy ezzel analóg módon egy-egy hadsereg valamely fontosabb funkciójának a leállásához vezethet.

Mindezen okok miatt szükséges a lehető legtávolabb tartani a támadó felet a saját rendszereinktől, illetve a védelmi célú kiberműveletek alkalmazása mellett offenzív műveletekkel megfosztani a támadás lehetőségétől.

3. Katonai offenzív kiberműveleti képességek

A 21. századi korszerű hadseregek egyik jellemzője, hogy a katonai céllal készült infokommunikációs eszközök és rendszerek mellett számos civil megoldást is használnak. Ilyen megoldás például a kommunikáció és adatátviteli célokra használt civil mobil kommunikáció, a 4G vagy az 5G mobil technológia. Ennek több oka van, amelyek között az egyik legfontosabb az, hogy a civil eszközök és rendszerek a hadsereg részéről

jelentkező bekerülési és fenntartási költségei jóval kisebbek vagy elenyészők a kimondottan saját katonai célú technológia-fejlesztés költségeihez viszonyítva. Ugyanakkor ezek a technológiák egyfajta limitációt is jelentenek, hiszen értelemszerűen ezeket az eszközöket és rendszereket háborús körülmények között nem, vagy csak időszakosan tudja használni a hadsereg, mert ezek lesznek az ellenérdekelt fél részéről az elsődlegesen pusztítandó olyan célok, amelyek működésének gátlása a hadsereg vezetésének rombolását és így annak részleges működésképtelenségét is jelenti.

Természetesen ez a polgári technológia esetén önmagában is igaz, hiszen minél több fejlett technológiát használ a civil társadalom, annál inkább nő annak a lehetősége, hogy ezeket támadva lehet – akár katonai – eredményeket is elérni. Itt vonatkoztassunk el attól, hogy ez a nemzetközi jogi szabályozásba ütközik-e vagy sem. Jelen tanulmány első része igyekezett a jogi, illetve nemzetközi jogi kérdéseket nagyon röviden felvillantani és részben megvizsgálni.[2]

Ugyanakkor a hivatkozott első részben azt kellett megállapítani, hogy ez ma a gyakorlatban még egyáltalán nem, vagy csak részben szabályozott terület. Ennek ellenére, vagy éppen emiatt jelenthetjük azt ki, hogy a civil infokommunikációs eszközök és rendszerek, ezeken keresztül pedig az adott ország fontos, ráadásul nagyértékű célpontok lesznek egy esetleges fegyveres konfliktusban, illetve az azzal párhuzamosan megjelenő kiberműveletekben. Természetesen az a tény, hogy a hadsereg civil infokommunikációs eszközöket és rendszereket alkalmaz, magával hozza azt is, hogy az ezekben meglévő vagy az ezekben a későbbiekben felfedezett sérülékenységekkel a hadseregnek is számolnia kell.

A katonai kiberképességek egyik legfontosabb célja természetszerűleg a saját infokommunikációs rendszerek kibervédelmének a biztosítása. Emellett értelemszerűen azonban a hadsereg tevékenysége nem korlátozódik csak a saját rendszereinek védelmére. Ezeknek a képességeknek hozzá kell járulniuk az ország szuverenitásának védelme érdekében tett katonai tevékenységek komplexitásához. A magyar honvédelmi törvény által megfogalmazottak szerint műveleti területnek minősül „a műveleti tervben meghatározott és kijelölt földrajzi terület és a felette levő légtér, továbbá a kibertér".[3] A hazai Nemzeti Biztonsági Stratégia (NBS) szintén rögzíti ezt a célt: „[H]aderőt úgy kell fejleszteni, hogy képes legyen hatásokat kiváltani a hazánk szempontjából releváns összes műveleti térben: a szárazföldön, a levegőben és a kibertérben egyaránt."[4]

Mindezekből azt a következtetést kell levonnunk, hogy a katonai kibertérműveleti képességek, köztük az offenzív kiberképességekkel az ország kibervédelmi képességeinek szerves részét képezik. Ezek a képességek – az ország más kibervédelmi és kiberműveleti képességeivel együtt – hozzájárulnak az ország adaptív ellenállóképességéhez.

Ugyanakkor számos egyéb kiberképesség szükséges egy adott ország kiberbiztonságának megteremtéséhez, fenntartásához, illetve a kibertéri szuverenitás biztosításához. Ezek a sok esetben civil képességösszetevők mintegy komplementer-, azaz kiegészítő

[2] Kovács László: Offenzív kiberműveletek I.: Az offenzív kiberműveletek természete. *Hadmérnök,* 16. (2021), 2. 187–204.

[3] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről 80. §. 22.

[4] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 135. pont.

képességként teremtik meg a katonai kiberképességekkel együtt az ország megfelelő kibervédelmi képességét. Az ország megbízhatóan működni képes kibervédelmi rendszere a kibertéri tevékenységekért felelős szervezetek számára világos feladatrendszert, egyértelműen megfogalmazott hatás- és jogköröket kell, hogy jelentsen. Ugyanakkor ennek megteremtése során azt is figyelembe kell venni, hogy ez nem egy állandó, több évre vagy évtizedre meghatározott szisztéma, hanem a társadalmi, valamint a technikai és technológiai változásokat követni, azokhoz megfelelő módon alkalmazkodni képes rendszert szükséges kialakítani és fenntartani. Ennek egyik alapfeltétele az, hogy a kibervédelmi szereplők közel azonos módon lássák és értékeljék a kibertéri helyzetet. Ez már a nemzeti kiberbiztonsági stratégiában rögzített módon meg kell (vagy kellene), hogy jelenjen, hiszen annak felépítésével, azaz a változó kihívásokhoz alkalmazkodni képes stratégiai céloktól kezdődően a stratégia által meghatározott tevékenységeken át, a szintén a stratégia által meghatározott szervezeti struktúráig számos elemnek kell mindezt, vagyis az alkalmazkodásra és szükség esetén változásra való képesség elvét tükröznie.

A katonai offenzív kiberműveletek szükségessége stratégiai szinten abból indul ki, hogy az országnak joga van megvédenie a szuverenitását a kibertérben is, és joga van rosszindulatú kibertevékenységekkel szemben fellépni. A kibertéri védelem pedig sok esetben nem, vagy csak részlegesen működik kizárólag védelmi kiberműveletek alkalmazásával.

Természetszerűleg az offenzív kiberműveletek alkalmazása során nagy jelentősége van a kiberműveletek életciklusának. Ebben – a már korábban bemutatott életcikluselemek mellett – az egyik legfontosabb tényező az, hogy minél kisebb teret engedjünk az ellenérdekelt fél tevékenységének, ugyanakkor a saját tevékenységeink mozgás- és cselekvési szabadságát biztosítsuk a kiber-, fizikai és információs térben egyaránt.

A katonai offenzív kiberműveletek alkalmazása során számolni és tervezni kell a műveletek közvetlen és közvetett következményeivel is. Az offenzív kiberműveletek végrehajtásához számos feltételnek kell teljesülnie. Sok olyan előfeltétel megléte szükséges, amelyek mind jogilag, mind technikailag megalapozzák és lehetővé teszik e műveletek végrehajtását. Ugyanakkor az offenzív kiberképességek alkalmazása során számolni kell azok hatásaival. A hatások előrejelzése, különösen a járulékos, azaz a közvetett hatások felmérése sok esetben nem, vagy nem megfelelő mértékben lehetséges. Ennek oka a korábban már vizsgált infokommunikációs rendszerek intra- és interdependenciája, valamint azok egyéb – például kiberfizikai – rendszerekhez való összetett kapcsolódása.

Ugyanakkor a katonai offenzív kiberműveleti képességek nem nélkülözhetik az ipari, a kis- és a közepes vállalatokkal, valamint az akadémiai szférával és a kutatóintézetekkel történő együttműködést, csakúgy, mint a nemzetközi kooperációt és kapcsolatokat sem.

4. Kibererők: példák és az azokból levonható következtetések

A katonai kibertéri feladatokat ellátó erők országonként eltérő módon épülnek fel. Ezt a felépítést az adott ország kibervédelméért, valamint a kiberműveletekért felelős

szervezetek időbeni kialakítása, a civil és a katonai feladatok felosztása, valamint az adott ország politikai, kiberszakmai döntései és a kialakított jogszabályi háttér határozza meg. Nagyon röviden, nem tudományos alapossággal és csak a legfontosabb tényezőket felvillantva négy ország – az Amerikai Egyesült Államok, Németország, Lengyelország és Magyarország – kiberműveleti erőit tekintjük át, a katonai kibererőkre fókuszálva. A cél az azokban esetlegesen fellelhető azonos pontok feltárása, ezek mentén igyekszünk olyan általános érvényű következtetéseket levonni, amelyekből jól kivehetők a kiberműveleti erők legfontosabb jellemzői.

4.1. Amerikai Egyesült Államok

Az Egyesült Államokban a katonai kibererőket integráló szervezet az Egyesült Államok Kiberparancsnoksága, azaz a US Cyber Command. A szervezet 2009-ben jött létre az Egyesült Államok Stratégiai Parancsnokságának *(US Strategic Command)* alárendeltségében. Mint alárendelt parancsnokság a US Cyber Command 2010-ben érte el a műveleti készenlétet, és 2018-ban vált önálló komponensparancsnoksággá.

Ugyanakkor a szervezet életében az egyik meghatározó mérföldkő ezt megelőzően az úgynevezett Cyber Mission Force, magyarul a Kiberműveleti Erő létrehozása volt 2013-ban, hiszen gyakorlatilag ez a US Cyber Command végrehajtó ereje. A US Cyber Command – jelen tanulmány írásakor – parancsnoka, Paul Nakasone tábornok, aki 2018 óta látja el ezt a tisztséget, és aki nem mellesleg egyben az Egyesült Államok Nemzeti Hírszerző Ügynökségének (*National Security Agency,* NSA) a vezetője is, a szervezet stratégiai jövőképét felvázoló kiadványában így foglalja össze a szervezet legfontosabb feladatát: „A USCYBERCOM hozzájárul a nemzeti stratégiai elrettentésünkhöz. Felkészítjük, működtetjük és együttműködünk a harcoló parancsnokságokkal, fegyvernemekkel, szövetségesekkel és az iparral annak érdekében, hogy folyamatosan akadályozzuk és megmérettessük az ellenséges kibertér szereplőit, bárhol is találjuk őket."[5]

Meg kell jegyezni, hogy az említett kiadványnak már a címe is rendkívül beszédes: „A kibertéri fölény elérése és fenntartása. Parancsnoki jövőkép az Egyesült Államok Kiberparancsnoksága számára" (angolul: *Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command*).[6]

A US Cyber Command 133 Cyber Mission Force (CMF), azaz 133 önálló kiberműveleti csoport kiképzését felügyeli. Ezek az egységek a különböző haderőnemek kiberparancsnokságai alárendeltségében működnek, ugyanakkor maguk a haderőnemi kiberparancsnokságok is a US Cyber Command szakmai felügyelete alá tartoznak. A CMF-ek egységes felkészítése és kiképzése óriási előnnyel jár abból a szempontból, amely az egységes terminológiai értelmezéstől kezdődően a kihívásokra adott egységes és koherens technikai válaszokig bezárólag jelentkezik.[7]

[5] US Cyber Command: Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command. (2018. április).
[6] US Cyber Command (2018): i. m.
[7] US Cyber Command: *Cyber Mission Force achieves Full Operational Capability.* (2018. május)

Meg kell jegyezni azonban, hogy a CMF-ek felkészítése és azok képességeinek magasabb szintre emelése nem megy mindig zökkenőmentesen. Ennek adott hangot az Egyesült Államok Számvevőszéke (*Government Accountability Office,* GAO), amikor kritikát fogalmazott meg ezzel kapcsolatban: „A Védelmi Minisztérium a CMF építéséről annak fejlesztésére helyezte át a hangsúlyt. A minisztérium kidolgozta a CMF transzformációs tervét, amely az alapozó (második fázis[8]) képzési szakasz felelősségét átruházza a haderőnemekre. A szárazföldi haderőnek és a légierőnek azonban nincs elég időkerete az alapozó tanfolyamok CYBERCOM szabványoknak megfelelő érvényesítéséhez. Továbbá a haderőnemek tervei nem tartalmazzák a CMF összes képzési követelményét, például a kiképzésre szoruló létszámot. A CYBERCOM nem tervezi a szükséges független értékelők felállítását a kollektív (harmadik fázis) CMF-képzés következetességének biztosítása érdekében."[9]

A US Cyber Command részt vett az amerikai elnökválasztásba beavatkozni kívánó külföldi kibererők elleni tevékenységben, valamint egy 2018-ban, a Belbiztonsági Minisztérium (*Department of Homeland Security,* DHS) és a Védelmi Minisztérium (*Department of Defense,* DoD) között született megállapodás alapján a kritikusinfrastruktúra-védelemben is komoly szerepet kap. Azonban a US Cyber Command talán egyik leghíresebb művelete az úgynevezett Glowing Symphony művelet volt, amely során a Joint Task Force-Ares – a US Cyber Command által offenzív kiberműveletek végrehajtására dedikált egyik – csapat az ISIS nemzetközi terrorszervezet ellen mért célzott kibercsapásokkal az „ISIS média és online műveleteit célozta meg, megfosztva infrastruktúrájától, és megakadályozva az ISIS tagjait a propaganda kommunikációjában és közzétételében".[10]

A fenti, 2016-ban végrehajtott offenzív kiberművelet, illetve műveletek együttese nagy vonalakban ma már tanulmányozható, hiszen számos olyan dokumentum titkosítását feloldotta az NSA, amilyenek például a támadásokról szóló jelentések voltak. Ugyanakkor ezek a ma már nem titkos minősítésű jelentések legtöbb részletükben kitakartak, így csak a legfontosabb történésekbe kapunk betekintést.[11]

4.2. Németország

Németország meglehetősen egyedi utat választott a kibertérműveleti erők kialakítása során. 2016 áprilisában Ursula von der Leyen, az akkori német szövetségi védelmi miniszter bejelentette, hogy Németország egy Kiber- és Információs Domain Parancsnokságot állít fel, amely közel 13 500 fő katona és civil szakembert foglal majd magában.[12]

[8] A CMF kiképzési modell négy fázisból áll, alap egyéni kiképzés, egyéni alapozó kiképzés, kollektív kiképzés, szinten tartó kiképzés.

[9] United States Government Accountability Office: DOD TRAINING. U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force. (2019. március).

[10] Mark Pomerleau: What Cyber Command's ISIS operations means for the future of information warfare. *C4ISRNet,* 2020. június 18.

[11] National Security Archive: USCYBERCOM 30-Day Assessment of Operation Glowing Symphony. (2016. december 13.).

[12] Zeit Online: Bundeswehr rüstet gegen Attacken aus dem Internet. (2016. április 26.).

A szervezet a Bundeswehr alakulataként 2017 áprilisában létre is jött. Az új Kiber- és Információs Domain Parancsnokság számos korábbi alakulatot integrált, így kiterjedt feladatrendszerrel alakult meg. Ezek közül a feladatok közül – természetszerűleg a Bundeswehr saját információs rendszereinek a védelme és azok üzemeltetése mellett – a legfontosabbak a felderítés (hírszerzés, megfigyelés) a kibertérben és az elektromágneses spektrumban végzett aktív műveletek, valamint a geoinformációs szolgáltatások ellátása.[13]

Ezek a feladatok magukban foglalják tehát a hadsereg infokommunikációs rendszereinek üzemeltetését, azok 24 órás felügyeletét, a szoftverfejlesztést, a szimulációs rendszerek IT- és geoinformációs támogatását.[14] Az offenzív kiberműveleti feladatok mellett megjelenő elektronikai hadviselési tevékenységek jól jellemzik azt a tényt, hogy a német kibertér-értelmezés eltér a hagyományos kibertér-értelmezéstől, például attól, amit a NATO hivatalosan is követ, hiszen a NATO Kibertér Műveleti Doktrínája a kiberteret a következőképpen határozza meg: [Kibertér] „Globális tartomány, amely magába foglalja mindazon infokommunikációs és egyéb elektronikai rendszereket, hálózatokat és azok adatait, beleértve az elkülönült vagy független rendszereket, hálózatokat, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak."[15]

Ezzel szemben, vagy talán ezt megerősítve a német kibertér-értelmezés szerint a kibertér tartalmazza az elektromágneses spektrumot és a kognitív dimenziót is. Ez magyarázhatja az elektronikai hadviselés és a kognitív dimenzióra ható információs domain integrálását is.

A szervezet számos nemzeti és nemzetközi kapcsolatot tart fenn különböző kiberbiztonsági és kiberműveleti szervezetekkel, aminek során az egyik legfontosabb feladat az információcsere megvalósítása.[16]

Az alakulat felállítása és annak széles körű feladatai nagyon jól beleillenek abba a feladatrendszerbe, amelyet a német nemzetbiztonsági stratégia 2016-ban meghatározott.[17] (Németország fehér könyvként adja ki a nemzetbiztonsági stratégiáját, amely nemcsak a biztonságpolitikai célokat, hanem a hadsereg, azaz a Bundeswehr szerepét és stratégiai feladatait is meghatározza.)

4.3. Lengyelország

Lengyelországban a Védelmi Minisztérium égisze alatt alakították meg a Nemzeti Kiberbiztonsági Központot 2019-ben. A központ feladata a védelmi minisztérium és a lengyel hadsereg IT-üzemeltetési és -fejlesztési feladatain túl a nemzeti szintű kiberbiztonság koordinálása, valamint számos kriptográfiai tevékenység ellátása, továbbá a szervezet alárendeltségébe tartozik a katonai eseménykezelő központ

[13] Bundeswehr: Kommando Cyber- und Informationsraum. (é. n.).
[14] Ludwig Leinhos: The German Cyber and Information Domain Service as a Key Part of National Security Policy. *Ethics and Armed Forces,* (2019), 1.
[15] AJP-3.20 Allied Joint Doctrine for Cyber Space Operations Edition A Version 1, 2020. 4.
[16] Bundeswehr: The Cyber and Information Domain Service. (é. n.).
[17] Ludwig Leinhos: Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr. *Connections: The Quarterly Journal,* 19. (2019), 1. 9–19.

(*Computer Security Incident Response Team – Ministerstwa Obrony Narodowej,* CSIRT-MON) is[18]. A Központ egyik fontos szervezeti eleme a Kiberműveleti Központ, amely a „katonai műveletek teljes spektrumában hajt végre kibertéri műveleteket, olyan körülmények között is, amikor a hagyományos erők alkalmazása nem lehetséges vagy nem célszerű".[19]

A központ felállítása előtt a lengyel kiberbiztonsági rendszer sok elemből állt. Az eltérő közigazgatási szervezethez (például különböző minisztériumokhoz) tartozó kiberbiztonsági csoportok és feladataik megosztott helyzetet teremtettek, az abban megvalósuló koordináció, illetve annak nem kielégítő volta azonban sok kritikát kapott. Természetesen volt jól működő eleme is a rendszernek, például az eseménykezelés, amely folyamatosan jól teljesített.[20]

2019-ben a védelmi minisztérium életre hívta az úgynevezett Cyber.Mil.Pl programot, amelynek két legfontosabb eleme a kibertérvédelmi erők létrehozásának támogatása, valamint a védelmi minisztérium kiberbiztonsági feladatainak az integrálása.[21]

A program stratégiai célja természetesen az ország kiberbiztonságának növelése. Ennek érdekében a programban olyan szervezetek is részt vesznek, mint a varsói Katonai Műszaki Egyetem, a lengyel Haditengerészeti Akadémia, a Katonai Kommunikációs Intézet, amely az 1950-es évek óta működő kutatóintézet, valamint szerepet kapnak a programban a lengyel területvédelmi erők is.[22]

2020-ban adták át a Nemzeti Kiberbiztonsági Központ szakmai irányítása alá tartozó Kiberbiztonsági Képzési Kiválósági Központot *(Cyber Training Centre of Excellence),* amely újabb lépés lehet a szakmailag felkészült utánpótlás biztosítására a lengyel kibervédelmi és kiberműveleti erők számára.[23]

4.4. Magyarország

Hazánk szintén sajátos utat jár be a kibererők építése során. A hazai kiberbiztonság megteremtése során az egyik legfontosabb állomás a 2013-ban megjelent információbiztonsági törvény, hivatalos megnevezéssel 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.), illetve annak 2015-ös jelentős módosítása. Ez azonban csak a kiberbiztonság civil szervezeti keretét határozta meg, és csak érintőlegesen tárgyalta a honvédelmi ágazatot, illetve a hadsereg szerepét a kiberbiztonság megteremtésében.[24]

Ennek megfelelően, Magyarországon a kiberbiztonság civil szervezetei közül az egyik legfontosabb elem a Belügyminisztérium irányítása alatt működő Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NKI). Az NKI magában foglalja a nemzeti információbiztonsági hatóságot, a kormányzati hálózat- és eseménykezelő központot,

[18] CSIRT-MON: *Ministerstwa Obrony Narodowej*. (2021)
[19] Cyber.Mil.PL: Cyber Operations Center. (2021)
[20] Joanna Świątkowska – Izabela Albrycht – Dominik Skokowski: National Cyber Security Organisation: POLAND. Tallinn, NATO CCDCOE, 2017. 13.
[21] Cyber.Mil.Pl: O Nas. (2021)
[22] Cyber.Mil.Pl: i. m.
[23] Cyber Security Training Centre of Excellence: What we do. (é. n.).
[24] Kovács László: Kiberbiztonság és -stratégia. Budapest, Dialóg Campus, 2018. 242.

illetve a sérülékenységvizsgálatot végző szervezeti elemet. Ebből következően az NKI elsősorban az eseménykezelésre, az elektronikus információbiztonság hatósági feladataira és a sérülékenységvizsgálatra, valamint nem utolsósorban a biztonságtudatosság növelésére fókuszál. Ugyanakkor sem a civil kiberbiztonsági szervezetek, sem az NKI nem rendelkezik a jelen tanulmányban megfogalmazott kritériumoknak megfelelő kiberműveleti erővel és offenzív kiberképességekkel.

A honvédelmi ágazaton belül két kiberműveleti szervezet alakult meg az elmúlt években. A Katonai Nemzetbiztonsági Szolgálatnál (KNBSZ) 2017-ben létrejött a Kibervédelmi Központ, amely 2021-től új néven, mint KNBSZ Kibertér Műveleti Központ látja el az ágazati elektronikus információbiztonsági eseménykezelés feladatait, valamint e szervezet egyik eleme a honvédelmi ágazati elektronikus információbiztonsági hatóság is. A honvédelmi ágazat másik kiberszervezete a Magyar Honvédség (MH) Parancsnoksága (MHP) alárendeltségében 2019-ben megalakult Kibervédelmi Haderőnemi Szemlélőség, illetve annak szakmai vezetésével várhatóan létrejövő Magyar Honvédség Katonai Kibertér Műveleti Központ (MH KKMK). A Szemlélőség fő feladata, hogy stratégiai szinten felügyelje és irányítsa az MH katonai kibertér műveleti erőinek kialakítását, fejlesztését, majd azok működtetését. A Szemlélőség szakirányítási feladatköre kiterjed a kiberszakterületet érintő valamennyi haderőfejlesztési és -fenntartási programra. A kiberszakterületen „szakmai felelős" jog- és hatáskörrel rendelkezik. A Szemlélőség határozza meg az MH kibervédelmi és kiberműveleti szakterülete vezetéséhez szükséges szervezeti kialakítás alappilléreit, valamint a kialakítandó kibervédelmi szervezetek struktúráját. Természetszerűleg a Szemlélőség szorosan együttműködik az MHP Infokommunikációs és Információvédelmi Csoportfőnökséggel, amely szervezet a honvédség IT-rendszereinek üzemeltetéséért és elektronikus információbiztonságáért felelős. A Szemlélőség szakmai irányításával megkezdődött az MH Katonai Kibertér Műveleti Központ kialakítása, amely a következő években várható folyamatos fejlődése során a katonai kibervédelem és a kiberműveletek szervezeti hátterét is nyújtja majd. Ez azt is jelenti, hogy a szervezet a kiberműveletek tervezéséhez és végrehajtásához szükséges adat- és információfeldolgozó képességgel, valamint offenzív kiberműveleti képességekkel és azok hatásait elemezni képes szervezeti elemekkel is fog rendelkezni. Az MH KKMK magában foglalja a már korábban, 2019-ben megalakult kiberképzési központot (Kiberakadémia) is.

A katonai kiberműveleti képességek kialakításáról a már említett új Nemzeti Biztonsági Stratégia rendelkezik. A stratégia az offenzív kiberműveleti képességeket is magába foglaló katonai fejlesztést és képességépítést a következő módon határozza meg: „A katonai kibervédelmet növekvő mértékben alkalmassá kell tenni a haderő kinetikus műveleteinek kibertérbeli támogatására, ki kell alakítani a kiberműveletekben alkalmazható offenzív képességeket. Ennek érdekében fejleszteni kell a Magyar Honvédség kibervédelmi és kiberműveleti erőit."[25] Az NBS által meghatározott katonai kiberműveleti képességek alkalmazására a honvédelmi törvény ad felhatalmazást, illetve szab feladatot a 2020. január 1-jével a törvénybe bekerült katonai kibertérműveleti erőkre vonatkozó szabályokkal. Ezek többek között tartalmazzák, hogy az MH katonai kibertérműveleti erői folyamatosan ellátják „a honvédelmi szervezetek, gyakorlatok,

[25] 1163/2020. (IV. 21.) Korm. határozat 135. pont, 159. pont.

műveletek kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelmét, az arra történő felkészülést és a kapcsolódó biztonsági feladatokat",[26] „a folyamatban lévő, kibertérből érkező támadás megszakításához szükséges intézkedések végrehajtását, vagy annak kezdeményezését",[27] valamint „külön döntés szerint a Magyarország biztonságát, honvédelmi érdekeit, vagy szövetségesi kötelezettségeit sértő vagy fenyegető rendszerekkel szembeni katonai kibertérműveleti fellépést".[28]

Mindezek a katonai kibertérműveleti erők alkalmazásához szükséges, de nem elégséges feltételek, ugyanis számos egyéb olyan tényező is szükséges ezen erők alkalmazásához, mint amilyenek például a fenti – honvédelmi törvényből idézett – „külön döntés alapján" kitételek. Ez többek között a Kormány döntését jelenti, amely a törvény meghatározása alapján más elemek fennállása – például különleges jogrendi helyzet – esetén szükséges egy-egy támadó jellegű kibertérművelet végrehajtásához.

4.5. A felvázolt kibererők elemzéséből levonható következtetések

Már a fentiekben bemutatott néhány kiberműveletekért felelős szervezet vizsgálata alapján is azonosítani tudunk olyan általános jellemzőket, amelyek a legtöbb ország kibertérműveleti szervezetei esetében igazak. Ezek a szervezetek – természetszerűleg a fentiekben megfogalmazottaknak megfelelően országonként eltérő módon, de mégis jól azonosíthatóan – három nagy területre koncentrálnak. Ezek a területek, amelyeket jelen tanulmány első részében részletesen is bemutattam, az információszerző, célkiválasztó, célazonosító és célkövetési, valamint szimulációs képesség, a kibertámadás képessége és a hatások értékelésének képessége területek. Bár a fent bemutatott kibervédelmi és kiberműveleti szervezetek országonként eltérő feladatrendszerrel rendelkeznek, de többnyire ezek mégis a kibertérre és esetenként az információs dimenzióra vonatkozó feladatokat is jelentenek.

Az azonban a többé-kevésbé eltérő feladatrendszer ellenére is világosan látszik, hogy minden ország a katonai kibererőitől az adott ország teljes kibervédelmi képességeinek a növelését várja, illetve ezekben az erőkben látja ennek garanciáját. A katonai feladatok mellett esetenként megjelenik az adott ország kritikus infrastruktúrája védelmének feladata is. Természetszerűleg az Egyesült Államok katonai kiberműveleti erői sok esetben olyan feladatokat is ellátnak, amelyek egy-egy európai ország katonai kiberműveleti erői esetében békeidőben nem feladatok (például a politikai választások informatikai rendszereinek a védelme, vagy aktív hírszerző/felderítő tevékenység).

A bemutatott katonai kiberműveleti erők elemzése azt is világossá teszi, hogy ezeknek a szervezeteknek a kialakítása, majd felkészítése és aktív, offenzív műveletek végrehajtására is kész képesség birtokába hozása hosszú időt vesz igénybe, ami 3-4 évet, de a teljes készenlét elérése akár 10 évet is jelenthet. Ugyanakkor fontos hangsúlyozni, hogy egy katonai kibertérműveletek ellátására alkalmas szervezetről sosem jelenthető ki, hogy az kész van, hiszen időről-időre újabb és újabb kibertéri

[26] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről, 62/A. §. (1) a) pont.
[27] 2011. évi CXIII. törvény 62/A. §. (1) b) pont.
[28] 2011. évi CXIII. törvény 62/A. §. (1) c) pont.

kihívásokkal kell szembenézni, ami megköveteli a szervezet és/vagy annak képességbeli változását. Ugyanez igaz a személyi állományára is, hiszen az ő felkészítésük nem ér véget egy-egy tanfolyam vagy képzés elvégzésével. A különböző műveletek végrehajtása során felhalmozott tapasztalat és annak átadása szintén hozzájárul az állomány folyamatos fejlesztéséhez. Itt azonban egy problémát szükséges jelezni. Ez pedig a szakértő kiberműveleti állomány megtartása. Megfelelő bérezés, megfelelő munkakörülmények és nem utolsósorban megfelelő és inspiráló szakmai kihívások azok a tényezők, amelyek megtartó erőként szolgálhatnak. Egy ideig. Ugyanis a jól képzett, gyakorlott, megfelelő szakmai és nem utolsósorban műveleti tapasztalattal rendelkező kiberműveleti szakember értéke a munkaerőpiacon évről évre exponenciálisan nő. A civil – főleg a multinacionális – cégek által nyújtott fizetési és egyéb juttatásokkal a közszféra, így a katonai terület sem tud versenyezni. Ez még az Egyesült Államokra is igaz.

Egy másik, bár meglehetősen triviális megállapítás a fentiek alapján, hogy minden ország rendkívül fontosnak tartja a szakemberek utánpótlásának folyamatos biztosítását. Ez már a középiskolák és az ott tanuló diákok képzésében és toborzásában is megjelenik. Ezt teszi a US Cyber Command. A parancsnokság létrehozta a Cyber Patriot STEM (*Science, Technology, Engineering, and Mathematics,* STEM, magyarul mérnöki és matematikatudományi) programot, amely keretében helyi középiskolákkal folytat együttműködést, illetve több mint 50 egyetemmel végez közös munkát, amely egyrészt közös kutatás-fejlesztést, másrészt tehetséges jövőbeni munkavállalók felkutatását és kiválasztását is jelenti.[29]

Hasonló programot indított a lengyel Nemzeti Kibervédelmi Központ is, amely az úgynevezett Cyber.Mil.Pl program keretében a varsói Katonai Műszaki Egyetem támogatásával kiberbiztonsági tematikájú középiskolai osztályt, illetve e mellett kiberbiztonsági egyetemi mesterképzést is indított 2019 őszén.[30]

Németország is hasonló lépéseket tett, hiszen a müncheni Bundeswehr Egyetemen kiberbiztonsági mesterképzést indított.[31]

Hazánk is komoly lépéseket tett az oktatás és az utánpótlás területén. Számos egyetemen indult el az informatikai szakokon kiberbiztonsági témájú tárgy oktatása, illetve a Nemzeti Közszolgálati Egyetem elindította a Kiberbiztonság nevű kétéves mesterképzési szakját is.[32]

A vizsgált országok mindegyikében kiemelt szerepet kap a kutatás-fejlesztés a kiberbiztonság és a kiberműveletek területén. A kibertéri erők ehhez sok esetben igénytámasztóként jelennek meg, de természetszerűleg maguk is kell, hogy rendelkezzenek K + F képességekkel, amelyek a kevésbé energia- és időigényes fejlesztési feladatokat látják el. Ugyanakkor az akadémiai szférával – például egyetemekkel, kutatóintézetekkel –, valamint a civil IT-szektorban és/vagy a kiberbiztonsági iparban dolgozó és kutató vállalatokkal történő kapcsolattartás és szoros együttműködés szintén elengedhetetlen. A jól működő K + F hosszú távú folyamat, amely azokra az igényekre ad gyakorlatban is használható választ (eredményt), amelyek a potenciális

[29] US Cyber Command: Cybercom Media Roundtable. (2019. május 7.)
[30] Cyber.Mil.Pl program i. m.
[31] Universität der Bundeswehr München: Studiengang Master Cyber-Sicherheit. (é. n.).
[32] Nemzeti Közszolgálati Egyetem: Kiberbiztonsági mesterképzési szak. (é. n.).

szemben álló fél polgári és/vagy katonai rendszereinek védelméhez, illetve támadásához szükségesek.

A kutatás-fejlesztés egyik nagyon jó példája, és ha tetszik, reklámja is az amerikai Dreamport kezdeményezés, amelyben azok a legújabb kutatás-fejlesztési és innovációs projektek és azok eredményei kapnak helyet, amelyeket a kormányzati szervezetek – mint például a US Cyber Command –, az akadémiai szféra és az ipari szereplők közösen végeznek és érnek el.[33]

Németország a haderő támogatásával egy kiberbiztonsági kutatóintézetet alapított Berlinben, amely szintén ellát K + F feladatokat.[34] Hazánkban a Nemzeti Közszolgálati Egyetemen alakítottak meg egy Kiberbiztonsági Kutatóintézetet, amely alkalmas lehet a jövőben a kiberterület tudományos alapjainak megteremtése és kutatása mellett K + F feladatok elvégzésére, illetve azok akadémiai szférán belüli koordinálására.

5. Az offenzív kiberképességek és a NATO

A NATO nagy utat tett meg azóta, hogy 2016-ban a Varsói Csúcsértekezleten a negyedik műveleti térré minősítette a kiberteret.

A kibertér műveleti térré nyilvánításával egy időben a tagországok egyöntetűen állást foglaltak abban, hogy kibervédelmi képességeiket fejlesztik. Ez az úgynevezett Cyber Pledge, azaz Kibervállalás, amelyet azóta is évente nagyon következetes módon a NATO ellenőriz. Ennek során nemcsak az ellenőrzésen van a hangsúly, hanem a szervezet tanácsokat és segítséget is nyújt a kibertéri képességek kialakításában, illetve fejlesztésében.

A Cyber Pledge esetében is igaz az a tény, amelyet a nemzeti kibervédelmi képességek során már megállapítottunk. Nevezetesen, hogy ez nem csak katonai, hanem össztársadalmi feladat. Ezt támasztja alá a NATO hivatalos közleménye is, amely a Cyber Pledge-dzsel kapcsolatosan a következőket jelenti ki: „A Pledge-et a washingtoni szerződés 3. cikkével összefüggésben fogadták el, amely kimondja, hogy »a szövetségesek fenntartják és fejlesztik egyéni és kollektív képességüket a fegyveres támadások ellen.« Mivel ebben a térben lehetetlen teljesen szétválasztani a katonai, polgári és ipari kérdéseket, a NATO-nak komoly érdeke fűződik a Szövetségen kívüli szervezetek kibervédelmi képességeinek javításához."[35]

A NATO-nak önmagának nincsenek offenzív kiberképességei. Ilyen képességekkel a tagországok rendelkeznek, de mivel nem minden tagország mutatja be vagy vállalja fel nyilvánosan e képességeit, ezért pontos számot vagy képességet csak becsülni lehet. Néhány ország ezeket a képességeit felajánlotta a NATO számára, így róluk biztosan tudhatjuk, hogy rendelkeznek offenzív kiberképességekkel. A tagállamok által önkéntesen felajánlott offenzív kiberképességekre a NATO egy sajátos terminológiát is alkotott, amelyet az angol kifejezésből származtatott mozaikszóval SCEPVA-nak (*Sovereign Cyber Effects Provided Voluntarily by Allies,* azaz a Szövetségesek Önkéntes

[33] Maryland Innovation & Security Institute: https://dreamport.tech/
[34] Bundeswehr: Zentrum für Cyber-Sicherheit der Bundeswehr. (é. n.).
[35] Laura Brent: NATO's role in cyberspace. NATO, 2019. február 12.

Hozzájárulásán Alapuló Kiberhatások) neveznek.[36] Ennek fontosságát hangsúlyozza Libicki egy tanulmányában: „Bár a NATO-nak nincs saját támadó kiberképessége, de a kiberműveletek növekvő jelentősége a NATO hatékony kollektív védelme és elrettentése szempontjából megköveteli annak alapos megértését, hogy a kiberképességek kihasználása hogyan befolyásolhatja a konfliktusok dinamikáját."[37]

Németország az egyik olyan ország, amely felajánlotta kiberképességeit a Szövetségnek. Az akkori német védelmi miniszter, a már említett Ursula von der Leyen nem részletezte a felajánlott kiberképességek mibenlétét, de úgy fogalmazott: „Ahogy a szárazföldi haderőkkel, a légierővel és a haditengerészeti erőkkel támogatjuk a NATO-t, most abban a helyzetben vagyunk, hogy a rendelkezésünkre álló nemzeti és jogi keretek között biztosítsuk a NATO képességeit kiberügyekben."[38]

Mindezeket a tagországi felajánlásokat is koordinálja a NATO Kibertér Műveleti Központja (*Cyberspace Operation Center,* CyOc), amit a NATO parancsnoki struktúrájának részeként állítottak fel. A CyOc a SHAPE, a NATO Európai Erők Főparancsnokságán (*Supreme Headquarters Allied Powers Europe,* SHAPE) J6 besorolású, azaz az infokommunikációs főnökség része. Dedikáltan ez a – 2017-es felállítását követő három évben magyar tábornok, Vass Sándor által vezetett – szervezet lehet az egyik legfontosabb szereplője a kibertámadások összehangolásának a Szövetségen belül.

Ugyanakkor a kiberműveletek területén a NATO egyik legnagyobb kérdése, ha tetszik legfontosabb problémája a tagországok eltérő kibervédelmi fejlettsége. Ez részben igaz az offenzív kiberképességek területére is. Azért csak részben, mert ezen a területen egyéb kérdések is felmerülnek. Az első ilyen kérdés az, hogy abban az esetben, ha egy tagország felajánlja kibertámadó képességeit a NATO-nak, és azt alkalmazzák, akkor a nemzet vagy a Szövetség lesz-e a felelős a művelet végrehajtásáért, illetve azok esetleges következményeiért?

A fentiek mellett a NATO még egy hatalmas problémával küzd, amely nem más, mint a háborús küszöbszint alatt tartott kiberkonfliktusok problémája. Korábban már említettük, hogy ez a helyzet talán a „még nincs háború, de már nem beszélhetünk békéről" kifejezéssel jellemezhető. Ez az időszak óriási kihívás elé állítja a kiberbiztonság területén dolgozó szakembereket. Az ilyen módon alkalmazott offenzív kiberműveletek nem elsősorban technikai értelemben vett kihívást, sokkal inkább politikai, jogi és diplomáciai problémát jelentenek.

Ezeknek a kérdéseknek a kutatása kiemelten fontos. Itt ki kell emelni a NATO Kibervédelmi Kiválósági Központjának (*Cooperative Cyber Defence Centre of Excellence,* CCDCOE) munkáját. A 2008-ban alakult kutatóközpont a NATO-hoz hasonlóan önmaga is hatalmas utat járt be a kiberbiztonság kutatásának területén, és mára az egyik meghatározó szereplőjévé vált a témának. A stratégiai kérdésektől és az azokban a tagországoknak nyújtott segítségtől kezdődően, a kiberbiztonság területén végzett különböző kutatásokig elmenően hatalmas oktatási, képzési munkát is végez a központ. A szervezet által készített és rendszeresen publikált tanulmányokban nem csak a NATO-tagországokból származó kutatók a fenti kérdésekre keresik a választ.

[36] AJP 3.20 (2020): i. m. 1.16. pont.
[37] Martin C. Libicki – Olesya Tkacheva: Cyberspace Escalation: Ladders or Lattices? In A. Ertan et al. (szerk..): Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO CCDOE, 2020. 61.
[38] AFP: Germany to Let NATO Use its Cyber Skills. *Security Week,* 2019. február 14.

Ezeknek a kérdéseknek a korántsem egyértelmű megítéléséről így ír Libicki és társa a CCDCOE-nek, a NATO-val szembeni kiberfenyegetéseket 2030-as idősíkon elemző kötetében:[39] „A kibertérben véget nem érő konfrontációk ellenére a stratégiai kiberháború azon lehetősége, hogy komoly károkat okozzon a modern gazdaságban, továbbra is vita tárgya […] Minél nehezebb előre kitalálni a [kiberháború] hatását, annál nagyobb a nézeteltérés annak megítélésében, hogy az ilyen műveletek elkezdődnek-e."[40]

6. Összefoglalás, következtetések

Az ma már nem kérdés, hogy a kibertér és annak biztonsága az egyik legfontosabb biztonság- és védelempolitikai és ezzel együtt katonai kérdés is egyben. Az új műveleti tér a hadviselés változásával, és nem utolsósorban az ehhez a térhez (is) történő adaptációjával új típusú katonai szervezetek létrehozását is indukálta világszerte.

A jelen írásban bemutatott néhány ország, köztük hazánk kiberműveleti képességeiből számos következtetés vonható le, amelyek közül az egyik az, hogy e képességek egyre növekvő mértékben tartalmazzák az offenzív kiberműveleti képességeket.

Az offenzív kiberképességek megjelenését leginkább az indokolja, hogy ezzel a képességgel, annak akár aktív alkalmazásával, akár csak egyszerű deklarálásával (amely mögött azonban a korábban említett valódi képességeknek meg kell lenniük) a saját rendszereinktől, legyenek azok katonai vagy civil rendszerek, a lehető legtávolabb tartsuk a potenciális rosszindulatú kibertevékenységeket. Ez jelenthet egyfajta elrettentést is, de jelentheti azt is, hogy olyan mértékben csökkentjük az ellenérdekelt fél (kiber)képességeit, amelyekkel már nem tud hatékony támadást indítani az információs rendszereink ellen.

A katonai kibertérműveleti képességek azonban nem csak, és nem elsősorban katonai célokat szolgálnak. Ezek a képességek az ország kibervédelmi képességeihez alapvető módon járulnak hozzá, annak szerves részét képezik. A katonai kiberképességek, az ország civil kibervédelmi és kiberműveleti képességeivel együtt jelentik az ország adaptív ellenállóképességének egyik igen fontos elemét.

A tanulmányban bemutatott négy ország kiberműveleti erőinek elemzéséből levonható következtetések is mutatják, hogy a katonai kibertéri feladatokat ellátó erőket országonként eltérő módon alakították ki és részben eltérő feladatokat is látnak el. Ugyanakkor – szervezeti kialakítástól függetlenül – megállapíthatók az azonos feladatok és felelősségi területek. Az információszerző, célkiválasztó, célazonosító és célkövetési, valamint szimulációs képesség, a kibertámadás képessége és a hatások értékelésének képessége területek a bemutatott országok katonai kiberműveleti erői esetében is fellelhetők.

A helyenként eltérő feladatrendszer ellenére is világosan látszik, hogy minden országban a katonai kiberműveleti erők az adott ország teljes kibervédelmi képességeinek a növeléséhez szignifikáns módon járulnak hozzá.

[39] A. Ertan et al. (szerk.): Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO CCDOE, 2020.
[40] Libicki–Tkacheva (2020): i. m. 67.

A bemutatott katonai kiberműveleti erők elemzése során látható, hogy ezeknek a szervezeteknek a kialakítása, felkészítése és aktív, offenzív műveletek végrehajtására is kész, egységes szemlélettel rendelkező, ütőképes erővé való fejlesztése minimum 3-4 évet, de azok teljes műveleti készenlétének elérése akár 10 évet is igénybe vehet.

Az elemzésekből levonható további markáns következtetés, hogy a technikai fejlesztéseken kívül a szakemberek utánpótlásának biztosítása, illetve a szakemberek megtartása kiemelten fontos kérdés. Az ezeket a kérdéseket kezelni képes oktatási és továbbképzési rendszer, a szakembereknek a szintén elengedhetetlen kutatás-fejlesztés feladataiba való – minél korábban történő – bevonására is komplex módon ki kell terjedjen.

A NATO-t kiberműveleti szempontból röviden megvizsgálva kijelenthető, hogy a Szövetségnek önmagának nincsenek offenzív kiberképességei. Ilyen képességekkel csak a tagországok rendelkeznek, amelyeket önkéntes alapon ajánlanak fel a szervezetnek. Ezek a felajánlott képességek, illetve azok alkalmazásai, bár hozzájárulnak a NATO elrettentési politikájához, mégis számos – elsősorban jogi és felelősségi – kérdést vetnek fel, amelyekre jelenleg számos tudományos kutatás keresi a választ.

A fentiekben idézett Libicki-gondolat is rávilágít arra, hogy sem a NATO, sem a nagyhatalmak, sem a kisebb országok nem lehetnek teljesen biztosak a kibertér, illetve az abban folytatott műveletek jövőbeni szerepében. Ennek megfelelően szükséges akár a Szövetség, akár az egyes országok kiberképességeit a védelmi képességek mellett az offenzív képességeket is magában foglaló módon építeni.

Felhasznált irodalom

AFP: Germany to Let NATO Use its Cyber Skills. *Security Week,* 2019. február 14. Online: www.securityweek.com/germany-let-nato-use-its-cyber-skills

AJP-3.20 Allied Joint Doctrine for Cyber Space Operations Edition A Version 1, 2020.

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

Bundeswehr: *Kommando Cyber- und Informationsraum.* (é. n.). Online: www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum

Bundeswehr: *The Cyber and Information Domain Service.* (é. n.). Online: www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service

Bundeswehr: *Zentrum für Cyber-Sicherheit der Bundeswehr.* (é. n.). Online: www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-informationstechnik-der-bundeswehr/zentrum-fuer-cyber-sicherheit-der-bundeswehr

CSIRT-MON: *Ministerstwa Obrony Narodowej*. (2021). Online: https://csirt-mon.wp.mil.pl/pl/

Cyber.Mil.PL: *Cyber Operations Center.* (2021). Online: www.cyber.mil.pl/articles/o-nas-f/2018-10-23c-centrum-operacji-cybernetycznych/

Cyber.Mil.Pl: *O Nas.* (2021). Online: www.cyber.mil.pl/o-nas/

Cyber Security Training Centre of Excellence: What we do. (é. n.). Online: https://cstcoe.mil.pl/en/pages/what-we-do/

Ertan, A. – K. Floyd – P. Pernik – T. Stevens (szerk.): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* NATO CCDOE, 2020. Online: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

Kovács László: Offenzív kiberműveletek I.: Az offenzív kiberműveletek természete. *Hadmérnök,* 16. (2021), 2. 187–204. Online: https://doi.org/10.32567/hm.2021.2.13

Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018. Online: http://kovacsx.hu/download/books/KovacsLaszlo_A_kiberbiztonsag_es_strategia.pdf

Leinhos, Ludwig: Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr. *Connections: The Quarterly Journal,* 19. (2019), 1. 9–19. Online: https://doi.org/10.11610/Connections.19.1.02

Leinhos, Ludwig: The German Cyber and Information Domain Service as a Key Part of National Security Policy. *Ethics and Armed Forces,* (2019), 1. Online: www.ethikundmilitaer.de/en/full-issues/20191-conflict-zone-cyberspace/leinhos-the-german-cyber-and-information-domain-service-as-a-key-part-of-national-security-policy/

Libicki, Martin C. – Olesya Tkacheva: Cyberspace Escalation: Ladders or Lattices? In A. Ertan – K. Floyd – P. Pernik – T. Stevens (szerk..): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* NATO CCDOE, 2020. 60–73. Online: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

National Security Archive: *USCYBERCOM 30-Day Assessment of Operation Glowing Symphony.* (2016. december 13.). Online: https://nsarchive.gwu.edu/dc.html?doc=6655596-National-Security-Archive-5-USCYBERCOM

Nemzeti Közszolgálati Egyetem: *Kiberbiztonsági mesterképzési szak.* (é. n.). Online: https://antk.uni-nke.hu/oktatas/mesterkepzes/kiberbiztonsagi-mesterkepzesi-szak

Pomerleau, Mark: What Cyber Command's ISIS operations means for the future of information warfare. *C4ISRNet,* 2020. június 18. Online: www.c4isrnet.com/information-warfare/2020/06/18/what-cyber-commands-isis-operations-means-for-the-future-of-information-warfare/

Świątkowska, Joanna – Izabela Albrycht – Dominik Skokowski: National Cyber Security Organisation: POLAND. Tallinn, NATO CCDCOE, 2017. Online: https://ccdcoe.org/uploads/2018/10/NCSO_Poland_2017.pdf

United States Government Accountability Office: *DOD TRAINING. U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force.* (2019. március). Online: www.gao.gov/assets/gao-19-362.pdf

Universität der Bundeswehr München: *Studiengang Master Cyber-Sicherheit.* (é. n.). Online: www.unibw.de/inf/studium/studiengang-cyber-sicherheit

US Cyber Command: *Achieve and Maintain Cyberspace Superiority, Command Vision for US Cyber Command.* (2018. április). Online: www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

US Cyber Command: *Cyber Mission Force achieves Full Operational Capability*. (2018. május). Online: www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/
US Cyber Command: *Cybercom Media Roundtable*. (2019. május 7.). Online: www.cybercom.mil/Portals/56/Documents/FOIA%20Reading%20Room%20Docs/2019-05-07_CYBERCOM_Media_Roundtable_Transcript.pdf?ver=2020-01-24-095943-620
Zeit Online: *Bundeswehr rüstet gegen Attacken aus dem Internet*. (2016. április 26.). Online: www.zeit.de/politik/deutschland/2016-04/ursula-von-der-leyen-bundeswehr-aufruestung-cyberkrieg-angriffe-internet

Jogi források

2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről
1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról