



FARKAS ÁDÁM

KIBERTÉR MŰVELET: HÍRSZERZŐ,
RENDÉSZETI ÉS KATONAI
MŰVELETEK ELEGYE?
GONDOLATOK AZ ANGOL NATIONAL CYBER
FORCE KAPCSÁN

MILITARY AND INTELLIGENCE CYBERSECURITY RESEARCH PAPER

2021/1.



A tanulmány célja áttekinteni az Egyesült Királyságban 2020 novemberében hivatalosan bejelentett új kiberképesség, a National Cyber Force (NCF) főbb jellemzőit és kérdéseit. A szerző a napvilágot látott érvek és kritikai észrevételek mellett a feltételezhető háttérokokra is rá kíván világítani. Mindezeket túl a dolgot az NCF kapcsán a hírszerzési és katonai együttműködés, illetve a hírszerző és katonai műveletek metszésében elhelyezkedő tevékenységek kérdéskörét is fókuszba kívánja állítani.

Kulcsszavak: kibertér, offenzív képesség, hírszerzés, fegyveres erők, együttműködés

The study aims to review the main features and issues of the new cyber capability, the National Cyber Force (NCF), officially announced in the UK in November 2020. In addition to the arguments and critical remarks that have come to light, the author also wants to shed light on the possible backgrounds. In addition, the paper focuses on the issues of intelligence and military cooperation in the case of NCF, as well as activities located at the intersection of intelligence and military services.

Keywords: cyberspace, offensive capability, intelligence, armed forces, cooperation

BEVEZETÉS

2020. November 19-én Boris Johnson, az Egyesült Királyság miniszterelnöke egy jelentős, négy éves védelmi költségvetésnövelést és képességfejlesztést jelentett be, melynek részeként egy új Űrparancsnokság (Space Command) és a **Nemzeti Kiber Erő (National Cyber Force, a továbbiakban: NCF) létrehozásáról is beszámolt.**

Ezt követően az NCF több szakmai portálon¹ is érdemi – esetenként kritikus –

figyelmet kapott. Ezt a kibertérben történő hírszerző és katonai együttes feladatellátással, az offenzív szemlélettel és portfólióval, valamint a belbiztonságitól a katonain át a hírszerzési feladatokig terjedő portfólióval, illetve e szférák személyi állományának vegyítésével is meg lehet okolni.

Az NCF vonatkozásában mégis azt mondhatjuk, hogy nemzetközi viszonylatban a **fő kérdésekként: (1) a több szervezet együttműködésén és személyi állományának fuzionálásán alapuló feladatellátás; (2) a kifelé irányuló – offenzív**

¹ Marcus WILLET: *Why the UK's National Cyber Force is an important step forward?*. International Institute for Strategic Studies, <https://www.iiss.org/blogs/analysis/2020/11/uk-national-cyber-force>, letöltve: 2021.03.05.; Danny STEED: *The National Cyber Force: directions and implications for the UK*. Elcano Royal Institute, http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL

CONTEXT=/elcano/elcano_in/zonas_in/ari18-2021-steed-the-national-cyber-force-directions-and-implications-for-the-uk, letöltve: 2021.03.05.; Antonia GOUGH: *UK Government Announces New National Cyber Force*. Global Risk Insight, <https://globalriskinsights.com/2021/01/uk-government-announces-new-national-cyber-force/>, letöltve: 2021. 03.05.

– küldetés; valamint (3) a szervezeti és ebből adódó jogi sajátosságok azonosíthatók.

E kérdések ugyanis túlmutathatnak az Egyesült Királyság kibertérműveleti ambícióin és ebből következő stratégiai és geopolitikai irányultságán, ami már önmagában is jelentős viszonylat mind európai, mind globális értelemben.

A fenti kérdések áttekintése ezen felül közelebb vihet minket annak megválaszolásához, hogy ezzel a lépéssel *az Egyesült Királyság egy új modellt és fejlesztési pályáivet alapozott meg, vagy csupán egy átmeneti megoldást dolgozott ki* a védelmi és biztonsági ágazatokon átívelő kibertér műveletek jogi és szervezeti kereteinek tisztázásáig?

Jelen dolgozat célja a fő kérdések mentén áttekinteni az NCF létrejöttét, mivel ez egy lehetséges mintát vagy fejlesztési irányt is kirajzolhat akár hazánk számára is a kibertér műveletek fejlesztése és szabályozása kapcsán.

A NATIONAL CYBER FORCE

ALAPVETŐ JELLEMZŐI

Az NCF kapcsán számos kulcsfontosságú tényezőt közölt a miniszterelnök, illetve az ő nyilatkozata alapján aztán hivatalosan az intézménynek otthont adó Government Communications Headquarters (GCHQ)².

Ezen információk és maga a tény, hogy egy – részint – katonai feladatokat is ellátó kibertér műveleti erő egy nemzetbiztonsági szolgálat bázisán került

felállításra, már önmagában korszakos változást sejtetnek.

Az angol kormányzati kommunikáció alapján *az NCF a GCHQ – mint nemzetbiztonsági szolgálat – és a védelmi minisztérium (a továbbiakban : MoD, ideértve az alárendeltségébe tartozó haderőt is) együttműködésében jön létre.*

Személyi állományát a GCHQ, a védelmi minisztérium (és alárendeltjei), az MI6³, valamint a Védelmi Tudományos és Technológiai Laboratórium⁴ szakemberi biztosítják, de egységes parancsnokság alatt. Ezzel a tevékenységi köréhez személyi oldalról biztosított lesz a katonai műveleti szaktudás (MoD), a tudományos és technikai képesség (DSTL), a globális technikai hírszerző kapacitás (GCHQ), valamint a toborzás és ügynöki tevékenység (MI6). Mindezek tehát már önmagukban egyértelműsítik, hogy az alapvetés egy védelmi és biztonsági funkciókon és szervezeteken átívelő együttműködés, amely igazodni tud a kibertér sokrétűségéhez és az ott jelentkező fenyegetési mátrixhoz.

A feladatrendszer kapcsán rögzítésre került, hogy az a diplomáciai, gazdasági, politikai és katonai képességek alkalmazása mellett, illetve a hírszerzési és rendészeti feladatellátással szoros összhangban került kialakításra. E feladatrendszerben lényegében a kibertérben végezhető bármely művelet számításba jöhet a terrorellenes tevékenységek megelőzését szolgáló lehallgatástól, a gyermekek szexuális zaklatására irányuló kiemelt bűncselekmények felderítésén át a katonai

² GCHQ: *National Cyber Force transforms country's cyber capabilities to protect the UK*. GCHQ, <https://www.gchq.gov.uk/news/national-cyber-force>, letöltve: 2021.03.05.

³ Az Egyesült Királyság hírszerző szolgálata.

⁴ Defence Science and Technology Laboratory, DSTL.

műveletek kibertér műveleti támogatásáig, illetve a klasszikus hírszerző tevékenységekig.

Az NCF *rendeltetése tehát lényegében a nemzet biztonságát veszélyeztető fenyegetések teljes körére kiterjedhet, amennyiben azok kezelése kibertér művelet végrehajtását indokolja akár hazai, akár külföldi viszonylatban.*

Rögzítésre került, hogy az NCF *független* a 2016-ban a GCHQ részeként felállított *National Cyber Security Centre (NCSC) szervezetétől és feladataitól is*, mivel annak feladata egyértelműen az Egyesült Királyság digitális védelmére irányul. Ez az elhatárolás és a feladatrendszer nyilvánvalóvá tette, hogy az NCF rendeltetése nem, vagy nem kizárólag hazai és védelmi műveletek végrehajtása.

Ezt az irányt egyértelműsítette annak kiemelése is, hogy az Egyesült Királyság korábban világvezető volt a GCHQ bázisán az offenzív kibertér műveletekben – amely fogalom alá azonban a szövegkörnyezet alapján a hírszerzési műveleteket is besorolják⁵ – és elsőként ajánlott fel ilyen képességet a NATO-nak.

A hírszerzési, katonai, belbiztonsági feladatok együttműködésben történő, de több tekintetben offenzív jellegű végrehajtása és az érintett szervek kooperációra kijelölt erőinek egységes parancsnokság alá vonása tehát az az előrelépés, amit az NCF képvisel az Egyesült Királyság eddigi kibertér műveleti erőihez képest. Fontos volt azonban rögzíteni, hogy ahogy a korábbi, úgy a jövőbeni kibertér

műveletek is jogi keretek között zajlanak az Egyesült Királyságban, amelynek a hírszerző szolgálatokról⁶, illetve a nyomozó hatóságokról⁷ szóló törvény ad majd kereteket.

NYITOTT KÉRDÉSEK ÉS LEHETSÉGES HÁTTÉROKOK

A bejelentéssel nyilvánossá tett újfajta képesség és fellépés védelmi és biztonsági szempontból *egyértelműen előrelépést jelent, sőt szemléletváltást* és egy komoly geopolitikai döntést a digitális tér vonatkozásában⁸.

A szervezet feladatrendszeréből ugyanis az olvasható ki, hogy az Egyesült Királyság a biztonságát és nemzetbiztonsági érdekeit érintő kiber fenyegetések ellen *az eddigi defenzív módozaton túl offenzív jelleggel is fellép, de immár messze szélesebb körben, mint a katonai műveletek támogatása.*

A terrorizmust, a gyermekek elleni internetes szexuális zaklatást, a hírszerzést, a katonai műveletek kibertér műveleti támogatását egyaránt felölelő portfólió értelemszerűen megköveteli a védelmi rendszer szinte minden szegmensének szakértelmét, amely azonban az egységes parancsnoklás révén már *túllép a szervezetek közti együttműködésen, de úgy, hogy eközben az érintett szervezetek klasszikus feladatainak fontosságát nem kérdőjelezi meg.*

⁵ Vö.: GCHQ i.m.

⁶ Intelligence Services Act.

⁷ Investigatory Powers Act.

⁸ A digitális tér geopolitikai jelentősége kapcsán lásd: Amaël CATTARUZZA: *A digitális adatok geopolitikája. Hatalom és konfliktusok a big data korában.*

Budapest, Pallas Athéné Books, 2020.; FARKAS Ádám: *Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája” című kötetének főbb üzenetei.* SmartLaw Research Group Working Paper 2021/1.

Az, hogy ezek a feladatok miként viszonyulnak majd egymáshoz, vagyis arányaiban mely részfeladatok fognak nagyobb figyelmet kapni a feladatrendszeren belül, még nyitott kérdés. Kézenfekvőnek tűnik azonban, hogy ez a belső arány rugalmasan változó és kormányzatilag meghatározott lesz az aktuális biztonsági fenyegetettség és helyzet tükrében.

Nyitott kérdés a feladatvégrehajtás pontos jellege is, különösen a kifelé irányuló fellépés során. E tekintetben *a katonai erő külföldi – más államot érintő – alkalmazására vonatkozó szigorú nemzetközi jogi szabályrendszer*, illetve a katonai fellépéssel szembeni válaszok súlyossága, továbbá a kibertér műveletek fegyveres támadáshoz mérhetőségének nyitott kérdései *miatt kézenfekvőbbnek mutatkozik a hírszerzési műveleti jelleg erősítése. Ez a megoldás nemzetközi jogi szempontból kevésbé kritikus – pontosabban kevésbé szabályozott – másik oldalról pedig jobban is illeszkedik a megjelölt feladatok jelentős többségéhez is.* Ez alól persze kivétel lehet a konkrét katonai műveletek támogatása, ahol a kibertér művelet oszthatja a katonai művelet jogi sorsát.

A jogi keretek megjelölése is az előzőekben leírt logikát látszik alátámasztani, hiszen a hírszerző szolgálatokra, illetve a nyomozó hatóságokra vonatkozó törvényeket veszi alapul. Ezek jellegüknél fogva arra engednek következtetni, hogy előbbi a külföldi műveletekre, illetve a hazai területű titkosszolgálati jellegű műveletekre nézve adnak majd kereteket, míg utóbbi a hazai és inkább rendészeti jellegű feladatok ellátására. E kettősségből jól látszik, hogy a nyilatkozatok szintjén a haderő alkalmazására vonatkozó normarendszer

nem került megjelölésre, mint irányadó keret.

Ezen jogi vonatkozások kapcsán Danny Steed gondolatmenetéből az olvasható ki, hogy *egy ilyen széleskörű feladatrendszer rendkívül jelentős felhatalmazásként értelmezhető, amelyhez a régi jogi keretek alkalmazása bizonytalan garanciaértéket kölcsönöz.* A két törvény alkalmazása ugyanis lényegében a miniszteriális felügyeletnek ad csak alapot, de részletes szabályozási kereteket a feladatrendszer újszerűsége miatt nem adhat. Ebből következően az alkotmányosság és *a jogállami kontroll döntő részben a miniszterek politikai felelősségére épülne, aminek érvényesülését azonban kérdésessé teheti a szóban forgó műveletek titkos jellege.*

Az látható tehát, hogy az NCF kapcsán *a kibertér jelentőségének erősödése és e tekintetben a védelmi és biztonsági képességek és fellépés fokozásának szükségessége nem vitatott, vannak azonban olyan kérdések – különösen a jogi, etikai és működési dimenziókban –, amelyek még megválaszolásra várnak.*

Ez a fajta kétely persze valamelyest a hivatalos kommunikációból is kiolvasható, hiszen az egyrészről az új erő kereteit első lépésként, induló jelleggel ismertette, vagyis kilátásba helyezte a további fejlesztést – és akár az önállósítást is –, másik oldalról pedig hangsúlyozta a jogi keretek fontosságát és ezek szintézisét a nemzetbiztonsági érdekek hatékony érvényesítésével. Az Egyesült Királyság kormányzatai is érzékelték tehát a szabályozási környezet bizonytalanságát vagy vitathatóságát, azonban e tekintetben láthatóan a várható műveletek fedett/titkos jellegére és az érdekérvényesítés hagyományos kereteire figyelemmel

egyértelműen a hírszerzési modell felé mozdították el az új kooperációs sémát.

Amennyiben tehát az NCF kapcsán a háttérokokat is vizsgálni kívánjuk, fontos, hogy *kiemelt helyen jelenjen meg a hírszerzési jelleg súlyozása. Ez feltehetően annak tudható be, hogy a hírszerzés – és elhárítás – lényegét tekintve a béke-háború elhatárolástól függetlenül, állandó jelleggel végzi önálló feladatai révén és azokon túl a diplomácia, a kormányzati döntéshozatal, a gazdasági és geopolitikai érdekérvényesítés, valamint a katonai fellépések műveleti és információs támogatását. Ez a fajta feladatrendszer tehát jobban illeszkedik a kibertérben tapasztalható szakadatlan bizonytalansághoz és fenyegetettséghez, mint a béke-háború/konfliktus duálók mentén alakuló katonai fellépés és annak jogi keretei.*

Másrészről azt is látni kell, hogy bár egyre több stratégia rögzíti, hogy a kibertérből érkező támadások egy bizonyos szinten egy konvencionális válaszcsoportot is megalapozhatnak, a valóságban *a műveletek jó részét a felek tudatosan ezen szint alatt tartják, így azok nem értelmezhetők megfelelően a fegyveres szembenállásra irányadó jogi és döntéshozatali keretrendszerben.*

Harmadrészt azt is fontos számításba venni, hogy *a kibertérben megjelenő fenyegetések jelentős része jobban illeszkedik az új típusú, nem konvencionális és nem állami szereplőkhöz köthető fenyegetésekhez, mint a konvencionális szembenálláshoz.* Ennek megfelelően tehát az is mondhatjuk, hogy a kibertérben jelentkező fenyegetések – a direkt és nyilvánvaló katonai műveletként végrehajtottaktól eltekintve – sokkal inkább hozhatók analógiába a terrorizmus és a nemzetközi szervezett bűnözés jelentette kihívással, mint az államközi konfliktusok logikájával. Ez a sajátosság pedig hasonló kérdéseket nyit meg feltehetően a kibertérben megvalósuló fenyegetések elleni fellépés tekintetében, mint a terrorizmus elleni fellépés vonatkozásában.⁹

Kiemelendő az is, hogy *az új típusú biztonsági kihívások a klasszikus katonai szakaszba lépve is komoly kérdéseket vetnek fel* mind jogi, mind tervezési, mind pedig az összkormányzati felkészülés és reagálás viszonylatában¹⁰. *Erre az Ukrajnában megvalósult hibrid hadviselés egyértelmű példát adott, de mégsem tolta előtérbe a direkt, államközi katonai szembeállást diplomáciai, nemzetközi jog és politikai*

⁹ A téma kapcsán lásd: KAJTÁR Gábor: *A nem állami szereplők elleni önvédelem a nemzetközi jogban.* Budapest, ELTE Eötvös Kiadó, 2015.; SPITZER Jenő: *Önvédelem versus terrorizmus: Az erőszak tilalma és az önvédelem joga a nemzetközi jogban, különös tekintettel az Iszlám Állam elleni nemzetközi fellépés lehetőségeire.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2019.; BARTKÓ Róbert – FARKAS Ádám: *A terrorizmus elleni harc nemzetközi trendjei.* In FARKAS Ádám – VÉGH Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020, 115-131. o.

¹⁰ A téma kapcsán példaként lásd: HÓDOS László: *A hibrid konfliktusok felívelési szakasza, avagy a*

fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai. In Honvédségi Szemle 2020/4., 49-64. o.; KELEMEN Roland: *A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése.* In Honvédségi Szemle 2020/4., 65-81. o.; KESZELY László: *A hibrid konfliktusokkal szembeni átfogó fellépés lehetséges kormányzati modelljei.* In Honvédségi Szemle 2020/4., 24-48. o.; FARKAS Ádám: *Komplex biztonság, hibrid konfliktusok, összetett válaszok.* In Honvédségi Szemle 2020/4., 11-23. o.; VIKMAN László: *A művelettervezés jogi feladatai.* In Honvédségi Szemle 2021/2, 44-56. o.

értelemben sem, hiszen az egyértelmű katonai fellépés az ellenérdekelt fél viszonylatában is megnyitja a teljes katonai eszköztár alkalmazását, ami az eskaláció súlyos lehetőségeivel fenyegethet.¹¹ Így tehát az új fajta „hadviselés” is lényegében érvként értelmezendő a kibertérben végzendő műveleti tevékenységek hírszerzési / nemzetbiztonsági / nyomozóhatósági karakterisztikájának erősítése mellett.

Ha tehát innen nézzük, akkor az NCF tekintetében a hírszerzési/titkosszolgálati jelleg súlyozása nem is tűnik olyan jelentős újdonságnak, hiszen a kibertérrel összefüggő állami fellépés terén a transzatlanti térség számos államában a nemzetbiztonsági szolgálatok kulcsszerepe, majd ezt követően a katonai képességek katonai szegmensre fókuszáló fejlesztése azonosítható.

A lényegi újdonságot a védelmi rendszer érintett szervezeteinek egészét átfogó szaktudás-fúzió és ennek az egységes parancsnokság alá vonása jelenti. Ez a fajta előrelépés ugyanis egyszerre ismeri el az érintett szervek alapfeladatainak fontosságát, de emeli ki azt is, hogy a hagyományos külön parancsnoki láncokra épülő kooperáció a kibertérben zajló ellenérdekelt törekvések kezelése terén időigényessége, eltérő jogi keretei és eltérő minisztériális alárendeltsége miatt sem tartható. Az NCF jelentős újdonsága tehát – a hírszerzési karakter elsőbbségének megerősítése mellett – a fúziós jelleg és kibertér műveletekkel összefüggő

parancsnoki döntéshozatal gyorsítása terén azonosítható talán leginkább.

ÖSSZEGZÉS

Mindezek alapján az NCF felállítása kapcsán az látható, hogy az érdemi előrelépést mutat a kibertérrel összefüggő geopolitikai, illetve ebből adódóan a komplex védelmi és biztonsági fellépést érintő gondolkodásmód viszonylatában is.

Szinte természetszerű, hogy egy ilyen újítást – különösen a digitalizáció mértéke és elterjedtsége miatt – komoly kérdések is öveznek, melyek még megválaszolásra várnak és addig is bizonytalanságot keltenek. Fontos azonban látni, hogy másik oldalról a nyitottságnak stratégiai üzenetértéke van, amely egyik oldalról az Egyesült Királyság polgárainak a megvédésük kapcsán szól, másik oldalról pedig minden az Egyesült Királysággal ellenérdekelt félnek a kibertérben várható angol válaszok és fellépések tekintetében.

Az eddig rendelkezésre álló információk és az azok lehetséges háttérköreit irányuló gondolatok áttekintése alapján az NCF kapcsán az újdonság a védelmi rendszer szinte egészét lefedő szakértelem és feladat fúzió, de egységes parancsnoklás alatt. Ez ugyanis komoly kérdéseket nyit meg a kibertér műveletek jövőjét illetően. Ki kell azonban emelni, hogy ez az újdonság egyértelműen a hírszerzési / nemzetbiztonsági karakter túlsúlyával került kialakításra, amit mind a

¹¹ A téma kapcsán lásd: PORKOLÁB Imre: *Hibrid hadviselés: új hadviselési forma, vagy régi ismerős?* In *Hadtudomány* 2015/3-4., 36-48. o.; RESPERGER István: *A válságkezelés és a hibrid hadviselés*. Budapest, Dialóg Campus Kiadó, 2018.; FARKAS Ádám – RESPERGER István: *Az úgynevezett „hibrid*

hadviselés” kihívásainak kezelése és a nemzetközi jog mai korlátai. In FARKAS Ádám – VÉGH Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl*. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020, 132-149. o.

vonatkozó nemzetközi jogi keretek, mind a hírszerzés tág értelemben vett nemzeti érdekérvényesítéshez való állandó kapcsolódásai, mind pedig a feladatellátás titkos/fedett jellege indokol és megalapoz.

Az NCF kapcsán várható fejlemények szemlélése és értékelése mellett indokoltnak tűnhet tehát ennek a fejlesztési iránynak a további elemzése, elméleti szintű vizsgálata és átgondolása a jövőre nézve, hiszen az Egyesült Királyság ezen lépése várhatóan ösztönzően fog hatni a többi szereplőre is mind a NATO égisze alatt, mind pedig azon kívül.

FELHASZNÁLT FORRÁSOK

- [1] Amaël CATTARUZZA: *A digitális adatok geopolitikája. Hatalom és konfliktusok a big data korában.* Budapest, Pallas Athéné Books, 2020.
- [2] Antonia GOUGH: *UK Government Announces New National Cyber Force.* Global Risk Insight, <https://globalriskinsights.com/2021/01/uk-government-announces-new-national-cyber-force/>, letöltve: 2021. 03.05.
- [3] BARTKÓ Róbert – Farkas Ádám: *A terrorizmus elleni harc nemzetközi trendjei.* In FARKAS Ádám – VÉGH Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020, 115-131. o.
- [4] Danny STEED: *The National Cyber Force: directions and implications for the UK.* Elcano Royal Institute, [http://www.realinstitutoelcano.org](http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari18-2021-steed-the-national-cyber-force-directions-and-implications-for-the-uk), letöltve: 2021.03.05.
- [5] FARKAS Ádám – RESPERGER István: *Az úgynevezett „hibrid hadviselés” kihívásainak kezelése és a nemzetközi jog mai korlátai.* In FARKAS Ádám – VÉGH Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020, 132-149. o.
- [6] FARKAS Ádám: *Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája” című kötetének főbb üzenetei.* SmartLaw Research Group Working Paper 2021/1.
- [7] FARKAS Ádám: *Komplex biztonság, hibrid konfliktusok, összetett válaszok.* In Honvédségi Szemle 2020/4., 11-23. o.
- [8] GCHQ: *NATIONAL CYBER FORCE TRANSFORMS COUNTRY'S CYBER CAPABILITIES TO PROTECT THE UK.* GCHQ, <https://www.gchq.gov.uk/news/national-cyber-force>, LETÖLTVE: 2021.03.05.
- [9] HÓDOS László: *A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai.* In Honvédségi Szemle 2020/4., 49-64. o.
- [10] KAJTÁR Gábor: *A nem állami szereplők elleni önvédelem a*

- nemzetközi jogban. Budapest, ELTE Eötvös Kiadó, 2015.
- [11] KELEMEN Roland: *A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése*. In Honvédségi Szemle 2020/4., 65-81. o.
- [12] KESZELY László: *A hibrid konfliktusokkal szembeni átfogó fellépés lehetséges kormányzati modelljei*. In Honvédségi Szemle 2020/4., 24-48. o.
- [13] Marcus WILLET: *Why the UK's National Cyber Force is an important step forward?*. International Institute for Strategic Studies, <https://www.iiss.org/blogs/analysis/2020/11/uk-national-cyber-force>, letöltve: 2021.03.05.
- [14] Porkoláb Imre: *Hibrid hadviselés: új hadviselési forma, vagy régi ismerős?* In Hadtudomány 2015/3-4., 36-48. o.
- [15] RESPERGER István: *A válságkezelés és a hibrid hadviselés*. Budapest, Dialóg Campus Kiadó, 2018.
- [16] SPITZER Jenő: *Önvédelem versus terrorizmus: Az erőszak tilalma és az önvédelem joga a nemzetközi jogban, különös tekintettel az Iszlám Állam elleni nemzetközi fellépés lehetőségeire*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2019.
- [17] VIKMAN László: *A művelettervezés jogi feladatai*. In Honvédségi Szemle 2021/2, 44-56. o.



Military and Intelligence CyberSecurity Research Paper 2021/1.

Szerző(k) / Author(s):

Dr. Farkas Ádám PhD

Kézirat lezárásának ideje / Manuscript closing time:

2021.03.10.

Szerkesztők / Editors:

Dr. Farkas Ádám PhD

Dr. Magyar Sándor PhD

Kiadó / Publisher:

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

Kiadó képviselője / Representative of the publisher:

Prof. Dr. Resperger István PhD / Prof. István Resperger PhD

Elérhetőségek /Contacts:

<https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/researchpaper>

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

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

ISSN:

2786-3778

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

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

A sorozat egyes számaiban foglalt vélemények, állásfoglalások a szerzők saját véleményét tükrözik. Azok nem tekinthetők sem a kiadó, sem a szerzőt foglalkoztató intézmények hivatalos álláspontjának.

The opinions and resolutions included in each issue of the series reflect the authors' own opinions. They should not be construed as an official point of view of either the publisher or the institutions employing the author.