Spiesz Bianka

Maszkirovka

Az orosz hibrid műveletek biztonság- és védelempolitikai, valamint alkalmazott társadalomtudományi aspektusai napjainkban

„*MASKIROVKA* IS NOT ONLY THE SHIELD BUT ALSO THE SWORD OF THE RED ARMY."[1]

1. ábra: A címadó szlogent egy szovjet magazin, a Vörös Csaló címlapján olvashatjuk, amely a Nemzetközi Kémmúzeum Francis Lara-gyűjteményében meg is tekinthető. A borítón a Vörös Hadsereg egy katonája látható, körbevéve forradalmi jelképekkel
Forrás: David M. Glantz: A Deception Primer for the Fledgling Red Army. *War on the Rocks,* 2016. május 20.

[1] Красный маскировщик 1923. február. Címlap.

https://doi.org/10.36250/01095_08

Bevezető gondolatok

Kutatásom alapvető célja, hogy megvizsgáljam: miféle történeti előzményekre támaszkodva, milyen stratégiai célok érdekében, milyen eszközrendszerrel és módszertannal, hogyan alkalmazza az Oroszországi Föderáció napjainkban a hibrid műveleteket, és hogyan juttatja érvényre az orosz stratégiai és hadikultúrában mélyen gyökerező úgynevezett *maszkirovka*, vagyis az álcázás elveit.

Választott kutatási témakörömnek különös aktualitást ad Oroszország felerősödött hibrid műveleti aktivitása az Európai Unió és az Észak-atlanti Szerződés Szervezetének tagországaival szemben, mind az állami-kormányzati szinten, mind pedig az adott társadalmak irányában. Hazánk új nemzeti biztonsági stratégiája is prioritásként kezeli a hibrid műveleteket a külső potenciális kockázatok, fenyegetések és veszélyek beazonosítása kapcsán.[2]

A *maszkirovka* szó eredeti jelentése „álcázás, elrejtés, megtévesztés", amely nem csupán a jelenkori orosz fegyveres, információs műveleti (s azon belül is különösen a lélektani hadviselési) koncepciók kialakulásának és megvalósításának egyik fontos mozgatórugója, de különös jelentőségre tett szert az internet korában, a közösségi média adta technikai-technológiai és társadalombefolyásolási lehetőségeket maximálisan kihasználva.

Kutatásom három előfeltevésen alapszik:

1. Egyre fokozódik a nemzetközi kapcsolatok alakulásában a hibrid hadviselés, az információs és a lélektani műveletek hagyományos és modern módszereinek és eszközeinek bevetése és alkalmazása.
2. Oroszország a közelmúltban jelentős katonai és politikai előnyt szerzett sikeres hibrid hadviselési formák kialakításával és eredményes InfoOps- és PsyOps-műveletek végrehajtásával.
3. Az orosz hibrid műveletek egyértelmű stratégiai célokat követnek – többek között a NATO- és EU-tagországok közötti egység megbontásának célját –, és már mostanra is számos probléma forrásává váltak, minthogy úgy tűnik: a NATO- és EU-országok többsége pillanatnyilag még nem képes kellőképpen hatékonyan reagálni sem egyénileg, sem együttesen az ilyen jellegű kihívásokra.

[2] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 1. melléklet: Magyarország Nemzeti Biztonsági Stratégiája. „Biztonságos Magyarország egy változékony világban".

Munkám során változatos kutatásmódszertani eszköztárat alkalmaztam, amelyben szerepel egyebek között a vonatkozó nemzetközi (elsősorban angol és orosz nyelvű), valamint hazai szakirodalom feldolgozása, dokumentumelemzés, statisztikai adatok saját szempontú másodelemzése és kontextuális elemzés egyaránt. A fentieken túl elvégeztem már lezárult és aktuálisan zajló nemzetközi válságreagáló műveletek tapasztalatainak saját szempontú feldolgozását is.

A kutatási eredmények nyomán szükség szerint javaslatokat fogalmaztam meg arra vonatkozóan, hogy mivel érdemes kiegészíteni, illetve módosítani az új nemzeti biztonsági stratégiát, hogy hazánk megfelelően felkészült legyen, és kellő hatékonysággal tudjon reagálni az esetleges hibrid műveleti próbálkozásokra, beszivárgási és fellazítási stratégiákra, továbbá a *maszkirovka* alkalmazására irányuló esetleges külföldi törekvésekre.

Elméleti és empirikus kutatási eredményeimre támaszkodva javaslatokat kívánok megfogalmazni az adott szakterület elméleti vizsgálatával és gyakorlati művelésével foglalkozó magyar nemzeti, valamint európai uniós és NATO nemzetközi biztonság- és védelempolitikai szakemberek részére.

Értelmezési keretek

Hibrid műveletek

A hibrid hadviselés nem rendelkezik általánosan elfogadott definícióval, hiszen egyfajta állandóan változó, „kaméleonként”[3] alkalmazkodó, komplex jelenségről és kihívásról beszélünk. Inkább stratégiai modellként tanulmányozható.

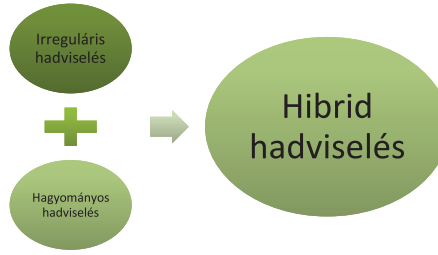
Maga a „hibrid hadviselés”[4] fogalom első ízben 2002-ben W. J. Nemeth amerikai tengerészgyalogos őrnagy diplomamunkájában jelent meg az orosz fegyveres erők ellen küzdő irreguláris és reguláris csecsen erők gerillahadviselésének kombinációjaként, majd 2014-ben kapott nagyobb figyelmet a Krím félsziget annektálása kapcsán.[5] Nemzetközi szinten eltérő megközelítésben

[3] Carl von Clausewitz *A háborúról* című művében alkalmazta a hasonlatot (Budapest, Zrínyi, 2014).

[4] William J. Nemeth: *Future War and Chechnya: a Case for Hybrid Warfare.* Monterey (Cal.), Naval Postgraduate School, 2002.

[5] Másutt is alkalmazzák, lásd Andrii Ivashchenko – Olha Salnikova – Igor Sivokha: Strategic Communication in the Modern Hybrid Warfare. *Journal of Scientific Papers – Social Development and Security,* 9. (2019), 5. 133–142. (A teljes szöveg ukrán nyelven olvasható.)

értelmezik, hiszen bár általános meghatározással nem rendelkezik, definiálni mégis elengedhetetlen ahhoz, hogy meg lehessen érteni, és megfelelően fel lehessen készülni az általa jelentett kihívásokra.[6]



1. ábra: Hibrid hadviselés
Forrás: saját szerkesztés

Az Észak-atlanti Szerződés Szervezete értelmezésében

Az ukrán válság miatt kiemelten jelentős a 2014. szeptemberi walesi NATO-csúcstalálkozó, amelynek zárónyilatkozata átfogó megközelítésben mutatta be az orosz hibrid hadviselést, széles körű nyílt és fedett katonai, paramilitáris és civil eljárások fokozottan integrált műveleti kivitelezéseként jellemezve azt. Az orosz kivitelezés módozatainak tekinthetőek többek között a dezinformációk terjesztése, a kiberműveletek, a pénzügyi és gazdasági nyomásgyakorlás, a propaganda, az irreguláris fegyveres csoportok és a reguláris fegyveres erők bevetése is.

2. ábra: Szürke zónás műveletek
Forrás: saját szerkesztés

[6] Lásd: Jovana Marovic: Wars of Ideas: Hybrid Warfare, Political Interference, and Disinformation. In Tomáš Valášek (szerk.): *New Perspectives on Shared Security: NATO's Next 70 Years.* Brussels, Carnegie Europe, 2019.

A 2014-es csúcsot[7] követően 2015-ben megszületett egy stratégia a NATO szerepéről a hibrid háborúk elleni küzdelemben.[8] E stratégia három fő hívószava a felkészültség, az elrettentés és a védelem.

Az Oroszországi Föderáció értelmezésében

Az Orosz Föderációban egyszerre nevezhető jelenkorinak és több évszázados múltúnak a hibrid hadviselés és annak eszköztára. Maga a „hibrid háború" kifejezés (oroszul: *gibridnaja vojna*)[9] meglehetősen új, csak azután terjedt el a használata, miután a nyugati sajtó és szakirodalom ekképp nevezte az oroszok által kivitelezett kelet-ukrajnai műveleteket. Nyugati értelemben vett hibrid hadviselésről ugyanakkor nem beszélhetünk az orosz hivatalos katonai, védelempolitikai és stratégiai dokumentumokban. Az orosz hivatalos narratíva szerint a modern korban a hibrid műveleteket elsőként az amerikaiak használták, az oroszok csupán reagáltak ezen kihívásokra.

Maszkirovka

Az Orosz Föderáció a *maszkirovká*t mint átfogó gyűjtőfogalmat használja mindazon, a megtévesztés művészetét szolgáló eszközökre és tevékenységekre, amelyeket már a történelem során számtalanszor bevetettek. A tradicionális *maszkirovka* művelet álcázásból, megtévesztésből, megakadályozásból, felforgatásból, szabotázsból, kémtevékenységekből, propagandából és lélektani tevékenységekből tevődött össze.[10]

[7] NATO: *Wales Summit Declaration. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales.* Sajtóközlemény (2014. szeptember 5.).

[8] NATO: *Warsaw Summit Communiqué. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8-9 July 2016.* Sajtóközlemény (2016. július 9.).; továbbá NATO Strategic Communications Centre of Excellence: *Hybrid Warfare and its Challenges for NATO Countries* (2015. április 17.).

[9] Az orosz szakirodalomban gyakrabban találkozhatunk a „hibrid háború" *(гибридная война)* kifejezés helyett a *(нелинеарная война)* szókapcsolattal, amely nemlineáris hadviselésként fordítható.

[10] Lásd erre klasszikus példaként az orosz történelemből: Roger Beaumont: *Maskirovka: Soviet Camouflage, Concealment and Deception.* College Station (Tex.), Center for Strategic Technology, The Texas Engineering, Experiment Station of the Texas ASM University System, 1982.

Új típusa, a több szakértő által[11] „*maszkirovka* 2.0”-nak nevezett tevékenység egyrészt követi a több évszázados megközelítést, másrészt kiegészül új kormányzati és technológiai módszerekkel: kényszerítéssel, médiamanipulációval, kibertámadásokkal, a fosszilis tüzelőanyagokhoz való hozzáférés korlátozásával, politikai agitációval, felforgató szervezetek bevetésével, titkos státusú katonai erők bevetésével, tartalékos csapatok fejlesztésével, valamint fegyverek, felszerelések, kiképzés, hírszerzési és logisztikai támogatás biztosításával.

1. táblázat: Maszkirovka és maszkirovka 2.0 – összehasonlító táblázat

Maszkirovka		*Maszkirovka 2.0*
támogatás nyújtása a harcmezőn, katonai sikerek biztosítása	**Cél**	befolyási övezet kiterjesztése, a Nyugat terjeszkedésének meggátlása
álcázás, megtévesztés, megakadályozás, felforgatás, szabotázs, kémtevékenységek, propaganda és lélektani tevékenységek	**Eszközök és módszerek**	a *maszkirovka* eszközei és módszerei + kényszerítés, médiamanipuláció, kibertámadások, a fosszilis tüzelőanyagokhoz való hozzáférés korlátozása, politikai agitáció, felforgató szervezetek bevetése, titkos státusú katonai erők bevetése, tartalékos csapatok fejlesztése; fegyverek, felszerelések, kiképzés, hírszerzési és logisztikai támogatás biztosítása
háború	**Bevetési időszak**	béke és úgynevezett „szürke zóna”
a meglepetés ereje – és ezáltal a győzelem esélye – nő; az ellenséges erők csapatainál és a vezetésben bizonytalanság, illetve káosz alakul ki	**Eredmények**	a regionális nagyhatalom és a megbízható szövetségesi partner látszat keltése; az Amerikai Egyesült Államok befolyási övezetének korlátozása; földrajzi-gazdasági-politikai célok elérése

Forrás: saját szerkesztés

Célpontjai közé gyakran a nyugati, illetve a Nyugattal szimpatizáló államok kerülnek, amelyek földrajzilag az Oroszországi Föderáció érdekkörének

[11] Lásd például J. B. Vowell cikkét, aki több mint 25 éve teljesít aktív szolgálatot az Amerikai Egyesült Államok haderejében, és megannyi bevetésben részt vett Afganisztánban (Maskirovka: From Russia, With Deception. *Real Clear Defense,* 2016. október 30.). www.realcleardefense.com/articles/2016/10/31/maskirovka_from_russia_with_deception_110282.html (Utolsó letöltés időpontja: 2020. 08. 29.)

közelében helyezkednek el, és integrálódni szeretnének az Európai Unióba, valamint a NATO tagállamai közé. Ezenkívül a közel-keleti országok felé is expanzív politikát folytat Oroszország, amelynek célkitűzése, hogy ellensúlyozza az Egyesült Államok befolyási övezetének térnyerését a térségben.

Oroszország éppen amiatt szignifikáns fenyegetés a régió stabilitására, a NATO-ra és az Amerikai Egyesült Államokra nézve, hogy alkalmazzák a „maszkirovkát", kiegészítve a hadviselés jellegét permanensen változtató technológiai fejlesztésekkel és kormányzási lehetőségekkel egy olyan állam- és kormányformával rendelkező föderációként, amely a Nyugattól merőben eltérő értékeken és erkölcsi-etikai elveken nyugszik.

Orosz maszkirovka műveletek

Országspecifikus fejlődés

Putyin hatalomra kerülésétől napjainkig

Vlagyimir Vlagyimirovics Putyin 2002-es hatalomra kerülése és az energiaeladásokból származó bevételek fokozott gyarapodása megalapozta az Oroszországi Föderáció Fegyveres Erőinek modernizációs lehetőségét. A szakértői és ezáltal elméleti hátteret Szergej Ivanov védelmi miniszter biztosította, aki kiadta Oroszország 2000. évi Katonai Doktrínáját, 2003-ban *Az Oroszországi Föderáció Fegyveres Erőinek fejlesztéséről* című fehér könyvet, végül pedig 2005-ben reformprogramot hirdetett meg.

A nyugati felfogással szemben – ahol a technika a mérvadó – az orosz megközelítésben az információ áll a hadviselés középpontjában. Szergej Pavlovics Rasztorgujev orosz gondolkodó szerint[12] az úgynevezett információs fegyverekkel érhetők el a legkönnyebben a külpolitikai célok, már akár fegyveres erők bevetése nélkül is.

Az elmúlt időszak információs hadviselési cselekményei[13] – az Észtország elleni 2007-es és a Grúzia elleni 2008-as orosz kibertámadás, a 2010-es arab tavasz, a 2011-es líbiai polgárháborúba történő beavatkozás, a 2014-es krími

[12] Timothy L. Thomas: *Comparing US, Russian, and Chinese Information Operations Concepts.* Fort Leavenworth (Kan.), Foreign Military Studies Office, 2004.

[13] Nem mind szerepel részletesen a tanulmányban.

inváz ió, majd a 2016-os amerikai választásokba történő beavatkozás – elsősorban a háborús állapotokat megelőző, valamint a konfliktus folyamán bevetett információs műveletek típusai. Általuk látható, hogy 1. a szovjet tapasztalatok és a gazdasági nehézségek hatására kaptak ekkora szerepet az aszimmetrikus hadviselési módszerek, amiket 2. a konfliktusokban megtapasztaltakhoz igazítottak annak tudatában, hogy 3. „a 21. századi hadviselés legfőbb terepe az emberi elme lesz".[14]

Kivitelező szervezetek

Állami kivitelezők

Az információs műveleteket az Oroszországi Föderáció Fegyveres Erőinél az információvédelemért és a jel-, valamint rádiófelderítésért felelős szakcsapatok hajtják végre. Ezenkívül akárcsak Nyugaton, az Oroszországi Föderációban is van hálózatbiztonsági vészhelyzeteket elhárító csoport és hálózatbiztonsági incidenskezelő csoport, amelyeket a Számítástechnikai Sürgősségi Reagálóegység fog össze.

Mindemellett az információs műveletekhez hozzájárulnak a polgári és a katonai nemzetbiztonsági és hírszerző szervezetek is: a Katonai Felderítő Főcsoportfőnökség, a Külföldi Hírszerző Szolgálat és a Szövetségi Biztonsági Szolgálat.[15]

Egyéb kivitelezők

Az egyéb kivitelezőknél az egyre közismertebbé váló katonai magánvállalatok – köztük is főként a Wagner Csoport[16] – szerepét és működését tekintjük át annak érdekében, hogy láthatóvá váljon az orosz fegyveres erők között elfoglalt helye és kapcsolódása a *maszkirovka* elveihez és módszereihez.

[14] Fekete Csanád: Az információs hadviselés orosz koncepciójának fejlődése a hidegháború végét követően. *Hadtudományi Szemle,* 11. (2018), 3. 28–44.

[15] Giles Keir részletesen ír róluk tanulmányában: *Handbook of Russian Information Warfare*. Rome, NATO Defense College – Research Division, 2016.

[16] Jelenleg 11 PMC-ről tudunk Oroszországban, az alábbi cikkben bővebben olvashatunk róluk: PMC Rush – Russian Private Armies. *Inform Napalm,* 2018.

Nyugati társaikkal ellentétben az orosz katonai magánvállalatokról alig lelhető fel nyilvános információ és adat, nem rendelkeznek saját weboldallal sem. A nemzetközi közösség is csak a közösségi médiából[17] értesült a Wagner Csoport létezéséről és az állammal való kapcsolatáról.

Az orosz törvények szerint csak magánszemélyek, szállítmányok és területek védelmét ellátó biztonsági vállalatok működhetnének, a zsoldos katonai tevékenységeket és formációkat szigorúan tiltják,[18] valamint külföldi szolgálat is csak a Szövetségi Biztonsági Szolgálat engedélyével végezhető. A Wagner Csoport tehát „nem legális keretek között működik, tevékenységi köre nem nyilvános, nem az állami reguláris hadsereg kiegészítéseképpen szolgál,[19] de mindenekelőtt a legfontosabb, hogy nem haszonorientált vállalkozás".[20] Egyfajta proxyhadseregként vetik be olyan fegyveres konfliktusokban, ahol fontos, hogy ne derüljön fény az orosz érintettségre. Feladataik közé tartozik 1. a harci övezetben lévő konfliktusban való műveleti kivitelezés, 2. új fegyveres konfliktusok kiprovokálása (lásd Kelet-Ukrajna), és 3. a külföldi műveletek során a támogatott haderő kiképzése.

Összegzések, következtetések, javaslatok

Tanulmányozva a világban folyó, kiemelten az Oroszországból vezényelt hibrid, információs és lélektani befolyásoló műveleteket, felmerül a kérdés, hogy Magyarország képes-e hatékonyan tenni ezen törekvések ellen, hiszen bár a 2017-ben elindított *Zrínyi 2026* honvédelmi és haderőfejlesztési program[21] keretében a Magyar Honvédség elkezdte fejleszteni hagyományos katonai

[17] A 2016. december 9-én tartott állami ünnep alkalmával, amikor közös kép készült Putyin elnökről és a Wagner Csoport vezetőségéről (Dmitrij Utkin és parancsnokhelyettese: Andrej Trosev).

[18] Az orosz büntető törvénykönyv 208. cikke rendelkezik az illegális fegyveres alakulatokról, a 348. cikk pedig kifejezetten a zsoldosokról szól, továbbá természetesen az illegális fegyverkereskedelmet is tiltják. A hazai törvények kikerülése végett volt például a Slavonic Corps PMC Hongkongba bejegyezve. 2016. novemberében elfogadtak egy olyan törvényt, amely lehetővé teszi az állampolgárok egy évnél rövidebb szerződéses katonai szolgálatteljesítését.

[19] Az Oroszországi Föderáció Fegyveres Erőivel azonban van, hogy osztoznak az eszközökön és fegyvereken, valamint a Wagner Csoport tagjainak kiképzése is egy állami bázison történik, Molkinóban.

[20] Hart Endre: Az orosz katonai magánvállalatok és a Wagner Csoport szerepe, illetve működése. *Nemzet és Biztonság,* 11. (2018), 2. 44–56.

[21] Draveczki-Ury Ádám: Zrínyi 2026. *Honvédelem,* 2017. január 16.

képességeit, valamint megfogalmazta a kiberképességek fejlesztésére irányuló törekvéseket, a folytonosan változásban lévő nemzetközi biztonsági környezet miatt célszerű lenne a hibrid eszközökre és módszerekre nagyobb hangsúlyt helyezve korszerűsítéseket végrehajtani, valamint a kutatás-fejlesztésben aktív szerepet vállalva világszínvonalú technikákat és képességeket létrehozni.

A 2012. évi 19. *Magyar Közlöny*ben megjelent Nemzeti Biztonsági Stratégia[22] még a 2014-es kelet-ukrajnai konfliktus előtt született, ezért nem használta a „hibrid" kifejezést, és az információs, illetve lélektani műveletekről sem tett említést. Viszont egy bekezdése foglalkozott a kiberbiztonsággal, feladatként jelölte meg a potenciális fenyegetések és kockázatok felmérését a kibertérben, a társadalmi tudatosság fejlesztését, a kormányzati koordináció fontosságát és a nemzetközi kooperációs lehetőségek kiaknázását, főként EU-s kereteken belül. Emellett kiemelt jelentőséget tulajdonít a dokumentum a kritikus információs infrastruktúrának.

Magyarország 2012-ben kiadott Nemzeti Katonai Stratégiája,[23] akárcsak a 2012-es nemzeti biztonsági stratégia, nem használta a „hibrid" kifejezést, viszont szintén felhívta a figyelmet, hogy a kibertér jelentősége egyre nagyobb lesz az ott kivitelezett támadások újszerűsége, valamint károkozási potenciálja miatt. A nemzeti katonai stratégia az állami szereplők mellett fokozott figyelmet fordított a politikailag nem ellenőrzött, nem állami szereplőkre, és az ezen személyek és szervezetek által alkalmazott modern infokommunikációs eszközökre, amelyek a kialakulóban lévő információs társadalomra nézve akár biztonsági kockázatot is jelenthetnek. Végül az információszerző és -értékelő eszközökre, módszerekre és szervekre fektette a hangsúlyt, kezdve a hazai szolgálatok nemzetközi együttműködési képességei fejlesztésének szükségességével.

Magyarország 2020-ban kiadott, 179 pontból álló Nemzeti Biztonsági Stratégiája[24] *Biztonságos Magyarország egy változékony világban* alcímmel már alkalmazza a hibrid kifejezést: 17 biztonsági kihívást és kockázatot azonosít, amelyek közül az első ötben szerepel Magyarország hibrid fenyegetése és a kiberfenyegetés is. Lényeges kiemelni, hogy a nemzeti biztonsági stratégia egy összkormányzati dokumentum, amely rendelkezik az ágazati stratégiai dokumentumok elkészítéséről. Ezen stratégiai dokumentumoknak, köztük az új nemzeti katonai

[22] 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

[23] 1656/2012. (XX. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájának elfogadásáról. 1. melléklet: Magyarország Nemzeti Katonai Startégiája.

[24] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

stratégiának is 2020. december 31-ig kell elkészülnie,[25] mindazonáltal már maga a biztonsági stratégia is kiemel számos katonai, illetve hibrid műveletekkel kapcsolatos szegmenst. Az alábbiakban a dolgozatom tárgya szempontjából releváns elemek bemutatása következik.

A *negyedik fejezetben* Magyarország alapvető adottságainak számbavétele kapcsán két pont foglalkozik a hibrid támadások elleni védekezéssel és a kiberhadviseléssel. Hangsúlyozza, hogy az ellenálló képesség alappilléreként a demokrácia szilárdsága, a közös nyelv és a nemzet egysége szolgál, és emellett elengedhetetlen a hatékony és szervezett döntéshozatal megléte, valamint a szoros együttműködés kialakítása a honvédelmi és a rendvédelmi erők, valamint a releváns polgári szervek, szervezetek között. A stratégia kiemeli, hogy az új kihívások miatt az információs és kiberhadviselés elleni védekezési képességekben és rendszerekben állandó fejlesztés, továbbá a felhasználók információbiztonsági oktatása is szükséges, hogy az úgynevezett *social engineering,* azaz a pszichológiai manipuláció elkerülhető lehessen.

Az *ötödik fejezet* Magyarország nemzetközi biztonsági környezetét mutatja be: a globalizáció hatásaként kölcsönös függőség alakult ki, és a fenyegetések a világ minden országára kihatással lehetnek. A fenyegetések okozta válságok egyre gyakrabban aszimmetrikus vagy hibrid hadviselés eredményeként jelennek meg. Ahogyan a dolgozatban már kiemeltem, a kivitelezők célja, hogy a nyílt háborús szint alatt tartsák a konfliktust, ami ellen a védekezés vagy válaszlépés nem megfelelő védelmi képességek hiányában lassú és eredménytelen. A dokumentum felsorolja a lehetséges befolyásolóeszközöket. Ezek lehetnek állami és nem állami szereplők által szponzorált, nemzetközi szinten Magyarországot lejáratú kampányok, gazdasági, politikai és társadalmi nyomásgyakorlás álhírekkel és dezinformálással a közösségi médiában információs műveletekként végrehajtva, vagy akár maga a tömeges, ellenőrizetlen és illegális migráció is a hibrid hadviselés eszközévé válhat.

A *hatodik fejezet* az alapvető érdekekről szól, köztük a hibrid hadviselés – és a kiberműveletek – elleni nemzetközi fellépésről az EU és a NATO kötelékében, fokozott körültekintés mellett. Mindeközben szerepet kívánunk vállalni a forradalmi technológiák (például az autonóm rendszerek, biotechnológia, kibervédelem, mesterséges intelligencia) fejlesztésében is. Pozitívumként értékelhető, hogy a nemzetközi kapcsolatok építéséről értekezve a stratégia csakis olyan mértékű elköteleződést irányoz elő egy másik ország oldalán, amely

[25] A tanulmány lezárásáig ezen ágazati stratégiai dokumentumok nem készültek el.

még nem veszélyezteti a kritikus infrastruktúránkat és az ország infokommunikációs hálózatát.

A *hetedik fejezet,* amely a kiemelt biztonsági kockázatokról rendelkezik, újra felsorolja a hibrid háború eszköztárát és kivitelezésének módozatait, kihangsúlyozva a kiberműveleteket.

A *nyolcadik fejezet* Magyarország biztonsággal összefüggő stratégiai céljait ismerteti. 2030-ra ütemezi a nemzeti ellenálló, elrettentő-, védelmi, válságkezelési és koordinációs képességek kifejlesztését a változékony nemzetközi környezethez igazítva.[26]

A *kilencedik fejezetben* kiemeli a stratégia: az átfogó feladatok és eszközök között meghatározó jelentőségű a hibrid támadások elhárításában való szerepvállalás. Nemcsak az elhárítás a lényeges, hanem hogy potenciális ellentámadásra is képes legyen Magyarország a számára adott műveleti terekben: levegőben, kibertérben és szárazföldön egyaránt. A közbiztonság fenntartása érdekében az álhírek és terjesztőik azonosítása hatékony felderítés, hírszerzés és elhárítás révén a nemzetbiztonsági szolgálatok feladata. Erősíteni kell a saját stratégiai kommunikációs képességeket is a kormányzati kommunikáció részeként, információbiztonsági tudatosságra kell oktatni a magyar lakosságot, továbbá a létfontosságú infrastruktúrák védelme – a nukleáris szektor fokozottan – is kiemelt nemzeti feladat. Végül a *záró rendelkezések* iránymutatást adnak az ágazati dokumentumok elkészítéséhez.

Véleményem szerint Magyarország nemzeti biztonsági stratégiája átfogó módon mutatja be a globalizált világ új kihívásait – köztük a hibrid hadviselést és a kiberműveleteket is – és az ezekre adandó válaszokat, a kialakítandó eszköztárat, infrastruktúrát és stratégiai gondolkodást. Az ágazati stratégiákkal bizonyára még árnyaltabb képet kapunk majd, így érdemes lesz figyelni, hogy a nemzeti katonai stratégia milyen megközelítést alkalmaz majd, és milyen mélységben fog értekezni ezekről az új kihívásokról.

Ugyanakkor a 2030-as határidő a képességek megteremtéséhez túl távoli időpontnak tűnik, hiszen látható, hogy az orosz vezetés – de akár Észak-Koreát vagy Kínát is említhetnénk – már most miként gyakorol hatást információs konfrontációval számos nyugati országban a mindennapi életre. Erre gyors, határozott és hatékony válaszreakció egyelőre sem a NATO, sem az EU tagállamai részéről nem látható.

[26] A dokumentum többször is említi, hogy a technológiai fejlesztésbe a magánszektort is be kell vonni.

Annak érdekében, hogy minél hamarabb képesek legyünk a védekezésre, fokozni kell a hazai kutatások intenzitását,[27] fejleszteni kell az információs környezetet, nemzetközi jogszabályi hátteret kell kialakítani, valamint tudatosságra nevelni a lakosságot, hogy ellenállóak legyenek a külföldről érkező, bomlasztó információs műveletek technikáival szemben. Az információtudatosságra nevelésre Magyarországon jó példaként szolgál a *Digitális Jólét Program* elnevezésű kezdeményezés.[28]

Hosszú távon érdekes lehet még megvizsgálni a világban megjelenő új tendenciákat – kezdve az internet szabályozásával kapcsolatos, differenciáltan, a helyi sajátosságokat figyelembe vevő újonnan megjelent jogszabályokkal. Oroszország az internet szuverenitásával kapcsolatban[29] egészen drasztikus megközelítést alkalmaz. Teljesen másként alakul azonban az internet cenzúrázásának folyamata egy nyugati ország esetében, példaként a német, brit és francia gyakorlat emelhető ki.

Németországban 2017 októberében fogadták el, és 2018 januárjában lépett hatályba a Hálózat Végrehajtási Törvény (NetzDG), amely elsősorban a 2 milliónál több felhasználóval rendelkező közösségi platformokat (például Facebook, Instagram, Snapchat, Twitter, YouTube) szeretné arra ösztönözni, hogy „az eddigieknél sokkal gyorsabban, 24 óra alatt vizsgálják felül és távolítsák el felületeikről a gyűlöletbeszédet. Amelyik vállalat ezt nem teljesíti, akár 50 millió eurós, rekordléptékű bírsággal is számolhat. Az egynapos határidő az egyértelműen jogsértő tartalmakra vonatkozik, a bonyolultabb ügyeknél hét nap áll a közösségi médiás cégek rendelkezésére."[30] Számos szakember és agytröszt[31] vetette fel annak a kérdését, hogy ez vajon egy demokratikus államban milyen mértékben legitim intézkedés, hiszen bár segítséget jelent a káros és befolyá-

[27] A kutatásokhoz iránymutatóként szolgálhat Thomas Kent 2020 szeptemberében publikált könyve, amelyben javaslatokat fogalmaz meg arra vonatkozóan, hogy a Nyugatnak miképpen kellene hatékonyan fellépnie az orosz dezinformációs műveletek ellen, miközben demokratikus értékeit sem hagyja el. (Thomas Kent: *Striking Back: Overt and Covert Options to Combat Russian Disinformation*. Washington, The Jamestown Foundation, 2020.)

[28] Az alábbi weboldalon még több információ érhető el a programról: Rólunk. *Digitális Jólét Program,* (é. n.).

[29] Kevin Limonier: Az orosz internet kivételes helyzete a messzi múltból ered. *Le Monde diplomatique – Magyar Kiadás,* 2017. december.

[30] NMHH: *Németország keményen fellép a közösségi oldalakon terjesztett gyűlöletbeszéd ellen* (2018. február 12.).

[31] A *Reason* magazin hasábjain erről bővebben olvashatunk. Lásd J. D. Tuccille: German-Style Internet Censorship Catches On Around the World. *Reason,* 2020. október 12.

soló tartalmak visszaszorításában, ugyanakkor a szólásszabadságot korlátozza. A francia alkotmánybírósági szerv (Conseil constitutionnel) pont júniusban nyilvánította alkotmányellenesnek azt a májusi nemzetgyűlési törvénytervezetet, amely a német példát követte volna. Mindazonáltal például az Amerikai Egyesült Államok,[32] Ausztria, Brazília és az Egyesült Királyság is fontolóra vette a NetzDG-hez hasonló gyakorlat kialakítását.

Tanulmányom utolsó szakaszában egy olyan képesség fokozott fejlesztését szeretném javasolni, amely elengedhetetlen a permanensen változó világban a hatékony válaszreakciók foganatosításához. Ez nem más, mint a reziliencia,[33] más néven rugalmas ellenállási képesség, azaz „valamely rendszernek – legyen az egy egyén, egy szervezet, egy ökoszisztéma […] – azon reaktív képessége, hogy erőteljes, meg-megújuló, vagy akár sokkszerű külső hatásokhoz sikeresen adaptálódjék".[34] A 2001. szeptember 11-i terrortámadás után az Amerikai Pszichológiai Társaság publikációiban egyre nagyobb szerephez jutott,[35] majd a hibrid háború térnyerésével növekedett az igény és szükség a katonák mentális felkészítésére a jövő hadviselésének tükrében. Magyar sikerként, valamint követendő példaként említeném a Motivive csapat 2019-ben bemutatott szoftvermegoldását, amelyet a *NATO Innovációs Kihívás* döntőjén különdíjjal jutalmaztak. Gáll Tamás, a Motivive ügyvezető partnere ismertette a szoftver működését:

> „a platform egy energiafókuszú rezilienciatréningen vezeti végig a felhasználókat, amelynek tartalma számos szakember (idegtudósok, pszichológusok és katonai szakértők) bevonásával lett összeállítva. A reziliencia négy alappillérére támaszkodó program során a NATO katonáinak fizikai, érzelmi, szellemi és mentális kihívásokat is teljesíteniük kell. Mindezt egy játékos keretrendszerben, ahol lényegében mindenkinek saját maga

[32] Lásd például az interaktív digitális technológiák visszaélésszerű és mértéktelen elhanyagolásának felszámolásáról szóló, 2020. évi törvényjavaslatot, amelyet az Egyesült Államok Képviselőházában szeptemberben terjesztettek elő. Lásd S.3398–EARN IT Act of 2020.

[33] Porkoláb Imre az „adaptáció" kifejezést alkalmazza tanulmányában [Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? *Hadtudomány,* 25. (2015), 3–4. 36–48.]. Véleménye szerint csupán a gyors adaptáció – mind a vezetői gondolkodás, mind a „különböző szervezetek szervezeti kultúrájának harmonizációja terén" – biztosíthat védelmet a hibrid fenyegetésekkel szemben.

[34] Békés Vera: A rezilienciajelenség, avagy az ökologizálódó tudományok tanulságai egy ökologizált episztemológia számára. In Forrai Gábor – Margitay Tihamér (szerk.): *Tudomány és történet.* Budapest, Typotex, 2002.101–107.

[35] Kovács László – Urbán Nóra: A pszichológiai reziliencia mint integrált alkalmazkodó rendszer *Honvédorvos,* 68. (2016), 3–4. 43–50.

legjobbjának kihozatala cél. A felület testreszabható a különböző NATO-tagországokra, azok kulturális sajátosságait figyelembe véve."[36]

A szoftvernek civil felhasználása is lehetséges. A program sikere és hasznossága is tökéletesen mutatja, hogy van létjogosultsága a kis- és középvállalkozások bevonásának a haderőfejlesztési programba.

Felhasznált irodalom

Jogszabályok és doktrínák

1956. évi I. törvény az Egyesült Nemzetek Alapokmányának törvénybe iktatásáról, 51. cikk

1999. évi CXVII. törvény az Észak-atlanti Szerződés tagállamai közötti, fegyveres erőik jogállásáról szóló Megállapodáshoz történő csatlakozásról, a Megállapodás kihirdetéséről, valamint a Megállapodáshoz kapcsolódó egyes jogszabályok módosításáról

1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

1656/2012. (XX. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájának elfogadásáról. 1. melléklet: Magyarország Nemzeti Katonai Startégiája. Online: https://njt.hu/jogszabaly/2012-1656-30-22

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 1. melléklet: Magyarország Nemzeti Biztonsági Stratégiája. „Biztonságos Magyarország egy változó világban". Online: https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001.txt

S.3398–EARN IT Act of 2020. Online: www.congress.gov/bill/116th-congress/senate-bill/3398

USSR Report. Military Affairs – Provisional Field Regulations for the Red Army. Springfield, U.S. Department of Commerce, 1986.

[36] Játékos módszerrel fejlesztik a NATO-katonákat, a megoldás díjat is nyert. *HR Power,* 2019. november 14.

Könyvek és tanulmányok

Beaumont, Roger: *Maskirovka: Soviet Camouflage, Concealment and Deception*. College Station (Tex.), Center for Strategic Technology, 1982. Online: https://apps.dtic.mil/sti/pdfs/ADB971047.pdf

Békés Vera: A rezilienciajelenség, avagy az ökologizálódó tudományok tanulságai egy ökologizált episztemológia számára. In Forrai Gábor – Margitay Tihamér (szerk.): *Tudomány és történet.* Budapest, Typotex, 2002. 101–107.

Brangetto, Pascal – Matthijs A. Veenendaal: *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*. Tallinn, NATO CCD COE Publications, 2016.

Clausewitz, Carl von: *A háborúról*. Budapest, Zrínyi, 2014.

Deák Anita: *Az orosz katonai gondolkodás átalakulása a 21. században az Oroszországi Föderáció hidegháborút követő katonai doktrínáinak tükrében.* Budapest, Nemzeti Közszolgálati Egyetem, 2018.

Glantz, David M.: *Soviet Military Deception in the Second World War*. Oxon, Frank Cass and Company, 1989.

Hart, B. H. Liddell: *Strategy*. New York, Frederick A. Praeger, 1954.

Ivashchenko, Andrii – Olha Salnikova – Igor Sivokha: Strategic Communication in the Modern Hybrid Warfare. *Journal of Scientific Papers – Social Development and Security,* 9. (2019), 5. 133–142. Online: https://paperssds.eu/index.php/JSPSDS/article/view/146/148. (A teljes szöveg ukrán nyelven olvasható.)

Keir, Giles: *Handbook of Russian Information Warfare*. Rome, NATO Defense College – Research Division, 2016.

Kent, Thomas: *Striking Back: Overt and Covert Options to Combat Russian Disinformation*. Washington (D.C.), The Jamestown Foundation, 2020.

Kiss Zoltán László: *Válságreagáló műveletek alkalmazott társadalomtudományi aspektusai*. Budapest, Zrínyi, 2015.

Marovic, Jovana: Wars of Ideas: Hybrid Warfare, Political Interference, and Disinformation. In Tomáš Valášek (szerk.): *New Perspectives on Shared Security: NATO's Next 70 Years.* Brussels, Carnegie Europe, 2019. Online: https://carnegieendowment.org/files/NATO_int_final1.pdf

Mukics Gergely: *A NATO védelmi minisztereinek brüsszeli találkozója*. Budapest, Antall József Politika- és Társadalomtudományi Tudásközpont, 2015.

Nemeth, William J.: *Future War and Chechnya: a Case for Hybrid Warfare.* Monterey (Cal.), Naval Postgraduate School, 2002.

Qiao, Liang – Xiangsui Wang: *Unrestricted Warfare*. Beijing, PLA Literature and Arts Publishing House, 1999.

Resperger István: *A válságkezelés és a hibrid hadviselés*. Budapest, Dialóg Campus, 2018.

Robert, James Q.: *Maskirovka 2.0: Hybrid Threat, Hybrid Response*. Tampa, JSOU Press, 2015.

Szun-ce: *A háború művészete*. Budapest, Helikon, 2018.

Thomas, Timothy L.: *Comparing US, Russian, and Chinese Information Operations Concepts.* Fort Leavenworth (Kan.), Foreign Military Studies Office, 2004. Online: www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf

Weber, Max: *Gazdaság és Társadalom*. Budapest, Közgazdasági és Jogi, 1987.

Folyóiratban megjelent tanulmányok

Andersson, Jan Joel: Hybrid Operations: Lessons from the Past. *Brief Issue – European Union Institute for Security Studies,* 2015. október. 1–4. Online: www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2033%20Hybrid%20operations.pdf

Baylen, Joseph O. – James S. Herndon: Col. Philip R. Faymonville and the Red Army, 1934–43. *Slavic Review,* 34. (1975), 3. 483–505.

Bogdanov, S. A – S. G. Chekinov: The Nature and Content of a New-Generation War. *Military Thought,* 2015. 12–23. Online: www.usni.org/sites/default/files/inline-files/Chekinov-Bogdanov%20Miltary%20Thought%202013.pdf

Fekete Csanád: Az információs hadviselés orosz koncepciójának fejlődése a hidegháború végét követően. *Hadtudományi Szemle,* 11. (2018), 3. 28–44. Online: https://folyoirat.ludovika.hu/index.php/hsz/article/view/3819/3089

Герасимов, Валерий: Ценность науки в предвидении. Военно-промышленный курьер,2013. február 27. Online: https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html

Hart Endre: Az orosz katonai magánvállalatok és a Wagner Csoport szerepe, illetve működése. *Nemzet és Biztonság,* 11. (2018), 2. 44–56. Online: https://folyoirat.ludovika.hu/index.php/neb/article/view/3587

Hoffman, Frank G.: *Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges. Prism,* 7. (2018), 4. 30–47. Online: https://cco.ndu.edu/news/article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/

Jójárt Krisztián: Az orosz haderőreform értékelése III. – Műveleti tapasztalatok. *Nemzet és Biztonság,* (2017), 5. 79–110. Online: www.nemzetesbiztonsag.hu/cikkek/nb_2017_05_07_jojart_k_-_az_orosz_haderoreform_ertekelese_iii_-_muveleti_tapasztalatok.pdf

Kaiser, T. B. – X. H. Kramer – V. A. Lefebvre – S. E. Schmidt: From Prediction to Reflexive Control. *International Interdisciplinary Scientific and Practical Journal,* 2. (2003), 1. 86–102. Online: www.reflexion.ru/Library/EJ2003_1.pdf

Красный маскировщик [Krasznij maszkirovscsik], 1923. február.

Molnár Mihály: A NATO és az Orosz Információs Műveletek aktuális helyzete. *Hadtudományi Szemle,* 10. (2017), 1. 84–97. Online: http://real-j.mtak.hu/16788/1/hadtudomanyi_szemle_2017_01.pdf

Pechatnov, Vladimir: Exercise in Frustration: Soviet Foreign Propaganda in the Early Cold War, 1945-47. *Cold War History,* 1. (2001), 2. 1–27.

Porkoláb Imre: *Hibrid hadviselés: új hadviselési forma, vagy régi ismerős?* Hadtudomány, 25. (2015), 3–4. 36–48. Online: http://real.mtak.hu/29824/1/2015_3_4_5.pdf

Rogers, James – Andriy Tyushka: 'Hacking' into the West: Russia's 'Anti-Hegemonic' Drive and the Strategic Narrative Offensive. *Defence Strategic Communications,* (2017), 2. 35–60. Online: https://stratcomcoe.org/cuploads/pfiles/WEB_Rogers-Tyushka1.pdf

Simicskó István: *A hibrid hadviselés előzményei és aktualitása. Hadtudomány,* (2017), 3–4. 3–16. Online: http://real.mtak.hu/67458/1/Ht_201734_5_18_u.pdf

Internetes források

1929 – Field Regulations 29. *Global Security,* 2011. július 11. Online: www.globalsecurity.org/military/world/russia/army-cccp-fr-29.htm

Bodnár Zsolt: Jön a kibervasfüggöny, Oroszország a legmagasabb fokozatra kapcsolta az internet cenzúráját. *Qubit,* 2019. december 4. Online: https://qubit.hu/2019/12/04/jon-a-kibervasfuggony-oroszorszag-a-legmagasabb-fokozatra-kapcsolta-az-internet-cenzurajat

Draveczki-Ury Ádám: Zrínyi 2026. *Honvédelem,* 2017. január 16. Online: https://honvedelem.hu/hirek/hazai-hirek/zrinyi-2026-2026.html

Glantz, David M.: A Deception Primer for the Fledgling Red Army. *War on the Rocks,* 2016. május 20. Online: https://warontherocks.com/2016/05/a-deception-primer-for-the-fledgling-red-army/

Játékos módszerrel fejlesztik a NATO-katonákat, a megoldás díjat is nyert. *HR Power,* 2019. november 14. Online: http://hrpwr.hu/aktualis/cikk/jatekos_modszerrel_fejlesztik_a_nato_katonakat__a_megoldas_dijat_is_nyert#

Limonier, Kevin: Az orosz internet kivételes helyzete a messzi múltból ered. *Le Monde diplomatique – Magyar Kiadás,* 2022. december. Online: www.magyardiplo.hu/

archivum/2017/230-2017-december/2490-az-orosz-internet-kiveteles-helyzete-a-messzi-multbol-ered

NATO: *Wales Summit Declaration. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales.* Sajtóközlemény (2014. szeptember 5.). Online: www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO: *NATO's Readiness Action Plan* (2015. február). Online: www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_02/20150205_1502-Factsheet-RAP-en.pdf

NATO: *Warsaw Summit Communiqué. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8-9 July 2016.* Sajtóközlemény (2016. július 9.) Online: www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

NATO Strategic Communications Centre of Excellence: *Hybrid Warfare and its Challenges for NATO Countries* (2015. április 17). Online: https://stratcomcoe.org/events/stratcomevent-hybrid-warfare-and-its-challenges-for-nato-countries/6

NMHH: *Németország keményen fellép a közösségi oldalakon terjesztett gyűlöletbeszéd ellen* (2018. február 12.). Online: https://nmhh.hu/cikk/193390/Nemetorszag_kemenyen_fellep_a_kozossegi_oldalakon_terjesztett_gyuloletbeszed_ellen

PMC Rush – Russian Private Armies. *Inform Napalm,* 2018. Online: http://informnapalm.rocks/pmc_rush

Президент России: Военная доктрина Российской Федерации 2014 . *Kremlin,* 2014. december 26. Online: www.kremlin.ru/events/president/news/47334

Путин поддержал идею создания в России частных военных компаний. РИА Новости, 2012. április 11. Online: https://ria.ru/20120411/623227984.html

Rempfer, Kyle: SOCOM Needs to Step Up Its Propaganda Game, Pentagon Deputy Says. *Military Times,* 2019. február 6. Online: www.militarytimes.com/news/your-military/2019/02/06/socom-needs-to-step-up-its-propaganda-game-pentagon-deputy-says/

Tuccille, J. D.: German-Style Internet Censorship Catches on around the World. *Reason,* 2020. október 12. Online: https://reason.com/2020/10/12/german-style-internet-censorship-catches-on-around-the-world/

Указ Президента Российской Федерации от 31.12.2015 № 683 „О Стратегии национальной безопасности Российской Федерации". Российская газета, 2015. december 31. Online: https://rg.ru/documents/2015/12/31/nac-bezopasnost-site-dok.html

Vowell, J. B.: Maskirovka: From Russia, With Deception. *Real Clear Defense,* 2016. október 30. Online: www.realcleardefense.com/articles/2016/10/31/maskirovka_from_russia_with_deception_110282.html