HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 4. szám 101–112.
DOI: 10.32567/hm.2021.4.8

Bihaly Barbara[1]

Az elektronikai hadviselés eszközei az információs és kibertérműveletek támogatásában az ukrán konfliktus példáján keresztül

Electronic military instruments in support of information and cyberspace operations through the example of the ukrainian conflict

A világ minden eddiginél jobban függ az elektronikai (információs) rendszerektől, ennélfogva az egyre kifinomultabb elektronikai hadviselés, valamint a kibertér- és információs műveletek egyre nagyobb hangsúlyt kapnak az érdekérvényesítés során. Oroszország jelentős jártasságot mutatott e területeken, különösen az ukrajnai válság idején. Oroszország tartós információs műveleti kampányt folytat a geopolitikai érdekszférájában. Aggodalomra ad okot ugyanakkor az EW és a kibertérműveleti képességek potenciális hatása az erők operatív hatékonyságára és túlélőképességére, ha valaha is konfrontáció lép fel.

Kulcsszavak: elektronikai hadviselés, információs műveletek, Ukrajna

The world is more than ever dependent on electronic (information) systems, hence the increasing sophistication of electronic warfare, cyber and information operations with increasing emphasis on advocacy. Russia has shown considerable expertise in these areas, especially during the crisis in Ukraine. Russia is conducting a sustained information operations campaign in its geopolitical sphere of interest. At the same time, the potential impact of EW and cyber capabilities on the operational efficiency and survival of forces, should confrontation ever arise, is a cause for concern.

Keywords: electronic warfare, information operation, Ukraine

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

1. Bevezetés

Oroszország már a bolsevik hatalomátvétel óta használja a dezinformációs műveleteket, és az 1970-es évek óta tanulmányozza, hogyan lehet szoftveresen támadó műveletet végrehajtani. A hadsereg információs térben betöltött szerepének orosz megértése sokkal szélesebb, mint a nyugati modellben. A nyugati gondolkodásmódban a „kibertér" a kulcsfogalom, amely jobban megfelel a katonai környezetnek. Az orosz hadművészet azonban az „információs tér" fogalmát használja, amelyet társadalmi, politikai és civilizációs fenyegetések összefüggésében hoznak fel. Az orosz hadsereg tevékenységének, „információs" jellegének hangsúlyozásával és nem „kiber" jellegével a stratégák az információkra, valamint az általa kiváltott politikai agitációra és mozgósításra összpontosítanak, ami összhangban áll az információk saját személyzetükre és polgári lakosságára gyakorolt hatásával. A szovjet idők óta egy másik tényező, amely súlyosan rányomta bélyegét az orosz stratégiákra, az a tény, hogy Oroszország mindig élesen érzékelte és igyekezett ellensúlyozni technikai és gazdasági alacsonyabb rendűségét azáltal, hogy az aszimmetrikus stratégiákat szisztematikusan feltárta és integrálta a műveleteibe. A legtöbb stratéga hangsúlyozza, hogy az orosz rádióelektronikai harc (oroszul: радиоэлектронная борьба, РЭБ; NATO-meghatározás szerint: electronic warfare, EW) és információs műveleti koncepciók mind a technikai, mind a pszichológiai képességek mesteri kombinációi, a stratégiai céloknak vannak alárendelve azért, hogy túlerőt képezzenek és visszatartsák az ellenérdekelt felet a támadástól.[2]

Oroszország fő fókusza a kutatás-fejlesztés a hadseregen belül, és mindenekelőtt az új mélyreható fegyverek és a fejlett C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance, magyarul: vezetés, irányítás, kommunikáció, számítógépek, hírszerzés, megfigyelés és felderítés) eszközeinek fejlesztése. Ennek ellenére a jelenlegi szelektív befektetési stratégia és a sebezhetőségek körültekintő elemzése megfelelő erőforrások hiányában is lehetővé teheti Oroszország számára, hogy ismét beszálljon a fegyverkezési versenybe, sőt felülmúlja a nyugati erőket bizonyos műveleti résekben – például az információs/(rádió)elektronikai hadviselésben.[3] Az orosz РЭБ-képesség, szemben a nyugati hasonszőrű képességekkel, a hadviselés informatikai-technikai eszközeinek egyik legfontosabb támogatójává vált.

A tanulmány célja bemutatni, hogy az elektronikai hadviselés eszközei milyen módon képesek támogatni az információs és kibertérműveleteket; mindezt az ukrán konfliktus példáján keresztül kívánom elemezni.

2. Az elektronikai hadviselés és funkciói

Az elektronikai hadviselés a modern konfliktusok egyik legtitkosabb és ennélfogva talán legkevésbé megértett aspektusa, gyakran pontatlanul összegzik, mint az ellenfél elektronikai rendszerei korlátozásának képességét. Ennél azonban sokkal többről van

[2] Dévai Dóra: An Overview of the Development of the Russian Information Warfare Concept Part 2. *Hadtudományi Szemle,* 13. (2020), 2. 5–12.

[3] Jolanta Darczewska: Russia's Armed Forces on the Information War Front, Strategic Documents. *OSW Studies (Center for Eastern Studies),* (2016), 57. 1–50.

szó. A hírszerzés az adatbázis építésétől, a műveleti területen való megtévesztésen át az ellenfelek elektronikai rendszerei működésének akadályozásáig, zavarásáig és a működés teljes ellehetetlenítéséig az EW széles körű lehetőséget kínál a döntő fölény megszerzésére. Lényeges, hogy ez az előny a földfelszíntől az űrbe telepített rendszerekig elérhető az elektromágneses spektrum (electromagnetic spectrum, EMS) kihasználásával. Az РЭБ konvergál a kibertér- és információs műveletekkel, hatékony és rugalmas eszközöket kínál a katonai hatás elérésére és az információs tér uralására, több egyidejű támadási vektor révén.

Definíciószerű megfogalmazás szerint az „elektronikai hadviselés: a műveleti (hadműveleti, harc-) támogatás fajtája. Azon tevékenységek összessége, amelyek az elektromágneses spektrum ellenség által történő felhasználásának meghatározására, felderítésére, csökkentésére vagy megakadályozására, illetve az elektromágneses energia és az irányított energia felhasználására, az elektromágneses spektrum saját célú felhasználására, valamint az ellenség vezetési és irányítási rendszerei támadásának támogatására, a saját csapatok védelmére irányulnak".[4]

Hazánkban az elektronikai hadviselés külön dedikált doktrínával rendelkezik, amely szerint e tevékenység fogalma: „[O]lyan hatás-alapú katonai tevékenységek/műveletek összessége, amelyek elektromágneses környezetben, az elektromágneses energia tudatos használatával biztosítják az elektromágneses műveletek részeként végrehajtott támadó és védelmi jellegű hatások/célok elérését."[5]

Ezekből a fogalmi meghatározásokból következtethetően az elektronikai hadviselésnek három funkcionális területe van: elektronikai támogatás, elektronikai ellentevékenység és elektronikai védelem. Az ehhez a három területhez tartozó feladatok is levezethetők. Az elektronikai támogatáshoz tartozó feladatok alatt értjük az elektromágneses spektrumban történő veszélyjelzés, a felderítés és célazonosítás képességekhez való hozzájárulást, valamint a rádióelektronikai felderítés tevékenység támogatását. Az elektronikai ellentevékenység feladatai alatt értjük a légierő műveleteiben a repülőgépek önvédelmi elektronikai hadviselési feladatait, kötelékoltalmazást (zavarást), az ellenséges légvédelem lefogását; szárazföldi tevékenység esetén ezek a feladatok lehetnek a szemben álló fél kommunikációs eszközeinek, radarjainak vagy akár navigációs eszközeinek zavarása vagy megtévesztése. Elektronikai védelem esetében a saját eszközrendszerek védelme, a csapatok közvetlen vagy közvetett oltalmazása, illetve a vezeték nélküli távirányítással működő improvizált robbanóeszközök zavarása a feladat.[6]

Az orosz meghatározást két, az orosz РЭБ-csapatokon belül és a Voronyezsi Légierő Akadémián működő РЭБ Osztálynál szolgáló ezredes foglalta össze egy 2017-ben megjelent cikkben: „A rádióelektronikai harc összehangolt tevékenységek és cselekvések összessége, amely magában foglalja a kontradiktórius rádióelektronikai és információ-technológiai objektumok elleni rádióelektronikai támadásokat, a rádióelektronikai és információs-technológiai objektumok rádióelektronikai védelmét,

[4] Magyar Honvédség Összhaderőnemi Doktrína 3. kiadás. MH Vezetési és Doktrinális Központ, 2012.
[5] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 2. kiadás, 2015.
[6] Kovács László: Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12. (2017), 1. 213–232.

a műszaki felderítéssel szembeni ellenintézkedéseket és a rádióelektronikai információs támogató intézkedéseket."[7]

A korábbi szovjet *Katonai Enciklopédia* meghatározása szerint az РЭБ: „[O]lyan intézkedések összessége, amelyeket a kontradiktív rádióelektronikai berendezések és rendszerek rádiófrekvenciájának azonosítása és későbbi zavarása, valamint a saját erők rádióelektronikai berendezéseinek és rendszereinek védelme érdekében hoznak."[8]

Bár első olvasásra ez az első, 1984-es szovjet meghatározás meghökkentően hasonló a jelenleg érvényben lévő magyar doktrinális megfogalmazáshoz, de a magyar meghatározásban az elektromágneses környezet mint fogalom használata sokkal szélesebb felhasználásra enged következtetni, mint csupán a szovjetek által használt „rádióelektronikai" kifejezés. Ugyanakkor az új, 2017-es orosz meghatározás már utal a teljes „információs térre", amely a magyar definíciónál is tágasabb mozgásteret engedélyez a műveletek számára. Tehát alapvetően, annak ellenére, hogy a mai napig a rádióelektronikai harc kifejezést használják, minden vezeték nélküli eszköz használatát/zavarását értik ezalatt.

A szovjet РЭБ az 1980-as években támadó és védekező РЭБ-intézkedésekre volt felosztva, tehát feladatrendszerük szerint létezett „rádióelektronikai elnyomás" (Радио Электронные по-давление) és „rádióelektronikai védelem" (радиоэлектронная защита). A cél észlelésének és a célmegjelölésnek a folyamatát nem hagyták ki a definícióból, hanem inkább elválaszthatatlanul kezelték a támadó és védekező РЭБ-intézkedésektől.

1990-re a szovjet haditengerészeti szótárban az РЭБ meghatározása néhány, főleg „kozmetikai" változáson ment keresztül. Az 1990-es definíció szerint: „A rádióelektronikai harc olyan intézkedések és tevékenységek összessége, amelyek időben, célokban és feladatokban kapcsolódnak egymáshoz, és amelyeket a csapatok (erők) hajtanak végre az ellenséges rádióelektronikai berendezések és rendszerek felderítése és későbbi (bármilyen típusú fegyverrel történő) megsemmisítése, megszüntetése vagy rádióelektronikai elnyomása érekében, valamint az erők saját rádióelektronikai berendezéseinek és rendszereinek elektronikai védelme céljából. Az РЭБ harci támogató funkció."[9]

A 2017-es meghatározás számos tekintetben eltér a korábbi szovjet és orosz definícióktól. Az első és a leginkább szembetűnő különbség az, hogy további külön területekre osztják az РЭБ-t, hisz külön veszik a műszaki felderítést és az információ elleni tevékenységet, valamint a rádióelektronikai információtámogató intézkedést. Másrészről, a hagyományos РЭБ támadó oldalát, a „rádióelektronikai elnyomást" rádióelektronikai támadás váltja fel. Ily módon a támadó РЭБ-fegyverek sokféleségét kibővítették olyan eszközökkel, amelyek képesek elpusztítani az elektronikai berendezéseket. Ennek megfelelően a radióelektronikai védelemben szereplő intézkedések köre is kibővült. Harmadszor, a korábbi „rádióelektronikai berendezések és rendszerek" információtechnológiai eszközökkel való helyettesítésével a védelemre szoruló saját eszközök és célpontok típusainak köre, amelyekre РЭБ-intézkedések vonatkozhatnak,

[7] V. F. Guzenk – A. L. Morarescu: *Radioelektronnaia borba. Sovremennoe soderzhanie. Tematicheskiy Sbornik. Radioelektronnaia borba v vooruzhennykh silakh Rossiiskoi Federatsii.* Moszkva, Informatsionnyi Most, 2017.

[8] *Military Encyclopaedia: Voennyi Entsiklopedicheskii Slovar.* Moscow, Voennoe Izadatelstvo, 1984.

[9] *Naval Dictionary: Voenno-morskoi Slovar.* Moscow, Voennoe Izadatelstvo, 1990.

kibővültek. Az РЭБ célpontjai tehát nem korlátozódnak az EMS-ben közvetlenül aktív berendezésekre és rendszerekre, például rádiókommunikációs berendezésekre, radarra, elektrooptikai érzékelőkre és így tovább. Az olyan mögöttes rendszerek, mint a számítógépek, az adattároló és az energiaellátó rendszerek, szintén célpontok az РЭБ definíciójának értelmében.

Azt is fontos itt megemlíteni, hogy az eredeti orosz kifejezés, mint „rádióelektronikai harc" a mai napig tartja magát a hivatalos orosz szövegekben, bár a teljes EMS működési tartományt értik alatta, holott az nyilvánvalóan túlmutat a rádiófrekvencián és az ahhoz a hullámhosszhoz tartozó eszközök használatán.

3. Orosz elektronikai hadviselés az ukrán válság során

Az ukrán hadsereg komoly segítséget kapott az Egyesült Államoktól az orosz–ukrán konfliktus során, cserébe az ukrán tapasztalatokat az USA feldolgozta és kielemezte. Az amerikai fél arra a következtetésre jutott elemzései során, hogy „az orosz fél komoly fejlesztéseket hajtott végre a fegyveres erejének modernizációja terén, amely során az elektronikai hadviselési képességek is hatalmas fejlődést mutatnak. Az orosz hadsereg megtartotta, sőt fejlesztette a hagyományos elektronikai hadviselési erőit, ezen belül kiemelt figyelmet fordítottak a rádiózavaró, navigációs eszközöket zavaró, illetve egyéb szárazföldi elektronikai eszközök, valamint rádiólokációt zavaró képességeik fejlesztésére".[10]

Oroszország jelentős beruházásokat hajtott végre az РЭБ-képességek fejlesztésében a 2008-as katonai reformok óta.[11] A РЭБ mára olyan mélyen integrálódott az orosz szárazföldi erőkbe, hogy már nem hajtanak végre úgy műveletet, hogy meg ne jelenne benne az РЭБ mint képesség. Oroszország ukrajnai műveleteit az РЭБ, a kibertér- és az információs műveletek szinergikus alkalmazása támasztja alá, amely az alábbiak szerint jellemezhető.

Az offenzív РЭБ-taktikák között szerepel több elektronikai támadó rendszer alkalmazása az EMS több tartományának egyidejű zavarása, ezáltal lerontva és ellehetetlenítve a globális navigációs műholdas rendszerek (*Global Navigation Satellite System,* GNSS), valamint a harcászati rádió-, mobil és műholdas kommunikáció hozzáférését. Az offenzív РЭБ-taktika különösen jól alkalmazható a hibrid hadviselésben, mivel az РЭБ-rendszerek úgy hangolhatók, hogy finom és kevésbé eszkalatív, nem kinetikus hatásokat hozzanak létre viszonylag rejtett módon, például úgy, hogy átmenetileg ellehetetlenítik a kommunikációt.[12]

Az ukrán védelmi minisztérium megerősítette, hogy Oroszország ezeket a taktikákat alkalmazza a harctéren. Például Oroszország által a Donbas régióban telepített Protek R-330Zh Zhytel rendszer képes a VHF, UHF és L sávokban működő ukrán kommunikációs rendszerek észlelésére, iránymérésére és megzavarására. Egy másik példa az orosz Leer-3 RB-341 rendszer, amely legfeljebb három Orlan-10 pilóta nélküli

[10] Kovács (2017): i. m. 221.
[11] Roger N. McDermott: *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*. Tallinn, International Centre for Defence and Security, 2017. 5–11.
[12] US Army Asymmetric Warfare Group: *Russian New Generation Warfare Handbook*. Version 1, 2016. 17.

repülőgépet (*unmanned aerial vehicle*, UAV) alkalmaz, és az orosz erők a mobil kommunikációs hálózatok megzavarására használták Ukrajnában.[13]

Az ukrán biztonsági erők által a válság korai szakaszában használt harcászati rádiók különösen veszélyeztetettek voltak az orosz elektronikai támadási rendszerekkel szemben. Ukrajna azonban azóta átállt a zavarásnak ellenállóbb, frekvenciaugratásos Harris rádiókra. Ezek a tulajdonságok arra kényszeríthetik a szemben álló felet, hogy új technikákat alkalmazzon, sokkal közelebb vonva őket a harcérintkezés vonalához, ezáltal kiszolgáltatottabbá téve rendszereit az ellentámadással szemben.

Oroszország az ukrán pilóta nélküli légi hírszerző, megfigyelő és felderítő (*intelligence, surveillance and reconnaissance,* ISR) platformokat is megcélozta. Csak 2015 és 2017 között az ukrán biztonsági erők közel 100 UAV-ot veszítettek az orosz GNSS zavaró technikák miatt, ami rontotta az időbeli kritikus hírszerzés képességét az orosz erőkkel kapcsolatban.[14]

Oroszország passzív elektronikai támogatással (*electronic support measures,* ESM) folytatott műveleteket, és rádiófelderítő rendszereket használt az információ összegyűjtésére és a szituációs helyzetkép megszerzésére az ukrán harcászati rádiók, személyi mobil eszközök és radarrendszerek jeleinek felderítésével. Az orosz SIGINT (*signal intelligence,* vagy сигнальная разведка) tevékenységek különösen hatékonyak voltak az ukrán erők által használt, régi titkosítás nélküli kommunikációs eszközök felderítésére.[15] Továbbá Oroszország aktív elektronikai érzékelő képességeket is felhasznált a régió ukrán erőinek megfigyelésére.[16]

A helyzetismeret megszerzése mellett Oroszország az РЭБ-rendszereket is felhasználta az ukrán erők precíziós célmegjelölésére. A kommunikációs zavarások időszakában az, hogy nem képesek a régi harcászati rádiókat használni, arra kényszerítette az ukrán katonákat, hogy személyes mobileszközeiket használják. Ezt az orosz hadsereg kihasználta, mivel könnyedén hozzáfért a mobilok geolokációs adataihoz, ezzel segítve a tűzvezetés precizitását.[17]

Összegezve, a Leer-3 rendszer részeként működő orosz Orlan-10 UAV-okhoz tervezett SIGINT-művelet során az orosz csapatok képesek voltak a bázisállomásokról származó adatok elfogására, hozzáférést biztosítva a mobileszközök geolokációjához, és ezt a helyinformációt megoszthatták más erőkkel. Következésképpen a rejtett célpontú földrajzi helymeghatározási képességek és a tüzérség integrációja meghatározó előnyt biztosított az orosz erőknek az ukrán szárazföldi erőkkel szemben.

[13] Duncan McCrory,: Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States. *The RUSI Journal,* 165. (2020), 7. 34–44.

[14] Joseph Trevithick: Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio "Virus". *The Drive,* 2019. október 30.

[15] Yuir Lapaiev: Ukraine as Clandestine Testing Ground for Russian Electronic Warfare. *Eurasia Daily Monitor,* 15. (2018), 157.

[16] Patrick Tucker: Exclusive: US Intelligence Officials and Satellite Photos Detail Russian Military Buildup on Crimea. *Defense One,* 2019. június 12.

[17] McCrory (2020): i. m.

4. Hogyan támogatták a rádióelektronikai harc eszközei az információs és kiberműveleteket az ukrán válság során?

Az orosz kormányzati és tudományos körökben az információ a nagyhatalom formájának és forrásának tekinthető. Ez igaz volt jóval az internet és a kibertér megjelenése előtt – ami nem változtatta meg az orosz információs háború stratégiáját, hanem csak annak taktikáját.[18]

Ennek az orosz perspektívának a logikus következménye az orosz „információs tér" (информационное пространство) határainak meghatározása és védelme, és ez a filozófia könnyen megtalálható az orosz doktrínákban, stratégiákban és tevékenységekben – például az ukrán konfliktus során végzett műveletekben is. Viszont az orosz perspektívának nincs meghatározása az információs, illetve kiberműveletekre, sokkal inkább csinálják, mint beszélnek róla.

Az orosz szóhasználatok (információs tér és információbiztonság kibertér és kiberbiztonság helyett) tökéletesen rámutatnak arra az összefüggésre, hogy az információs tér egy mindent lefedő műveleti tartomány, amelyben eszközként használhatók a rádióelektronikai harc eszközei, és magában foglalja a kiberteret, valamint a kibertérben zajló műveleteket.

Ennek eredménye az, hogy nem csupán támogató funkcióként értelmezik az információs és kibertérműveleteket, hanem egyenrangú műveletekként.[19]

Ezért teljesen természetes, hogy Oroszország információs műveleteket alkalmazott Ukrajnában: az „Euromaidan" tüntetések kezdetétől a Krím annektálásáig és a kelet-ukrajnai hadműveletek dimenziójaként. És az sem meglepő, hogy az internet korszakában Moszkva hatékony taktikát dolgozott ki az információs hadviselés virtuális térben történő alkalmazására.[20]

Oroszország 2020-as nemzetbiztonsági stratégiája kimondja, hogy a „nacionalista, szeparatista, radikális vallások" veszélyt jelentenek a nemzetállamokra, és hogy most fokozódik a „globális információs harc". A dokumentum ennek a fenyegetésnek az ellensúlyozását javasolja az „igaz" információk terjesztését az orosz állampolgárok számára, többek között a közösségi médiát felölelő natív internetes platformok népszerűsítésével.[21]

Ami a kibertér (orosz felfogás szempontjából információs tér) fontosságát illeti, számos hivatalos dokumentum írja le a számítógépes hálózati műveleteket az orosz információbiztonság szerves részeként, többek között: az Orosz Föderáció információbiztonsági doktrínája, az Orosz Föderáció fegyveres erőinek információs térben végzett tevékenységével kapcsolatos koncepcionális nézetek és az Orosz Föderáció állampolitikájának alapelvei a nemzetközi információbiztonság területén.

[18] Margarita Levin Jaitner: Russian Information Warfare: Lessons from Ukraine. In Kenneth Geers (szerk.): *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn, NATO CCD COE, 2015. 87–94.
[19] Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus. 2018. 198.
[20] Jaitner (2015): i. m. 87–94.
[21] Az Orosz Föderáció Biztonsági Tanácsa. Стратегия национальной безопасности Российской Федерации до 2020 года. (Orosz Nemzeti Biztonsági Stratégia 2020).

Oroszországban a kiberbiztonság az információbiztonságnak van alárendelve, amely lehetővé teszi a nemzetbiztonsági tervezők számára, hogy mind a műszaki, mind a kognitív adatokat felügyeljék.

A konfliktusok tendenciája azt mutatja, hogy a polgári kommunikációs technológiának egyre nagyobb hatása van a konfliktusokban, és hogy az alacsony technológiájú, rögtönzött rendszerek ugyanolyan hatékonynak bizonyulnak, mint a csúcstechnológiájú katonai megfelelői. A kereskedelmi kommunikációs technológia konfliktusokban való elterjedésével és a katonai felszerelések nem állami szereplők általi használatával az РЭБ-nek egyre többféle fenyegetéssel kell szembenéznie, a legkülönfélébb technológiai szintektől. Az információs és kommunikációs technológiák konvergenciája a hadviselés formái határainak elmosódását eredményezi, ami nagyobb lehetőségeket és igényt kínál az РЭБ számára az információs térrel való együttműködésre.

Előfordulhat, hogy az РЭБ eszközeinek támogatnia kell a biztonsági műveleteket, továbbfejlesztett képességeket biztosítva számukra a mobiltelefonok és egyéb eszközök nyomon követésére, vagy más fenyegetések elleni védelemre. Új РЭБ-technológiákat fejlesztenek és a meglévő rendszereket adaptálják annak érdekében, hogy ellenintézkedéseket hozzanak egy kiszámíthatatlan világban, ahol a konfliktusok egyik napról a másikra változhatnak.[22]

Az orosz hadseregen belüli kutatók közötti diszkurzus is arra a következtetésre jutott, hogy a számítástechnika terén elért haladás a hadviselés új generációját hozta el, amelynek lényege a kibertérben elérendő abszolút információs fölény.[23] Nevezetesen: bármely kívánt befolyásolási zónán belül idetartoznak a technikai adatok és a kognitív információk, valamint a pszichológiai műveletek elleni támadás és védekezés egyaránt.

Ivan Vorobjev vezérőrnagy és Valerij Kiselyov ezredes azt írta, hogy az információ „nemcsak a tűzerő, a támadás, a manőver kiegészítője, hanem mindezeket átalakítja és egyesíti".[24] Szergej Csekinov ezredes és Szergej Bogdanov altábornagy még ennél is tovább megy: „Ma az információs befolyás eszközei olyan tökéletesre lettek fejlesztve, hogy stratégiai feladatokat tudnak megoldani."[25]

Oroszország az ukrajnai válság során átfogó információs műveleti kampányt folytatott és folytat a közvélemény befolyásolásának és az információs tér megzavarásának érdekében. Az orosz információs műveletek egyértelmű célja volt, hogy befolyásolja, összezavarja és demoralizálja az állampolgárokat, narratívájában gyakran keveredtek az igaz és hamis információk, hogy elfogadhatónak tűnjenek és illeszkedjenek a „közönség" korábban létező világképéhez.

Oroszország jelentős erőfeszítéseket tett e kampány érdekében: a *Bellingcat* jelentése szerint az orosz trollok mintegy 65 ezer tweetet tettek közzé nagyjából 24 órával a Malaysia Airlines MH-17 lelövése után, Ukrajnát okolva a tragédiáért.[26]

[22] B. Van Niekerk – M. Maharaj: The Future Roles of Electronic Warfare in the Information Warfare Spectrum. *Journal of Information Warfare,* 8. (2009), 3. 1–13.
[23] Jaitner (2015): i. m. 88.
[24] I. Vorobyov – V. Kiseljov: Russian Military Theory: Past and Present. *Military Thought,* (2013), 3.
[25] Sergei G. Checkinov – Sergei A. Bogdanov: Asymmetrical Actions to Maintain Russia's Military Security. *Military Thought,* (2010), 1.
[26] Bellingcat Podcast: *MH-17, Episode 2 Guide: A Pack of Lies* (2019. július 24.).

A Krím annektálása során az orosz erők kilenc ukrán tévécsatornát kapcsoltak le a krími műsorszóró állomásokon, továbbá az ukrán csatornákat az orosz tévéadások váltották fel Donyeckben. Az orosz propaganda példái közé tartoznak azok a nyilatkozatok, miszerint a Krímben élő orosz etnikai lakosságot súlyos ultranacionalista fenyegetés érte, és tagadták, hogy Oroszország részt venne a krími eseményekben.[27]

Másrészről Oroszország РЭБ-eszközökkel is támogatta az információs műveleteit. Az ukrán hadügyminisztérium jelentései szerint Oroszország a Leer-3 rendszert használta az ukrán katonák demoralizálásának megkísérléséhez, fenyegető szöveges üzenetek küldésével közvetlenül személyes mobileszközeikre.[28]

Az orosz támadó kibertérműveletek Ukrajnában magukban foglalják a kémkedést, az információs műveletek támogatását és a fizikai hatások kiváltását is. Egy ilyen jellegű kampánynak az a célja, hogy széles körű zavart okozzon, információs előnyt szerezzen és demoralizálja az ukrán biztonsági erőket. Ez magában foglalja az elosztott túlterheléses támadásokat, a kormányzati weboldalak elérésének ellehetetlenítését, a mobilhálózatok megzavarását, a kormány szavazatszámláló rendszerébe való beavatkozást és az idegen zászló alatti műveleteket. Az ilyen jellegű műveletek együttesen támadják a kibertér három rétegét: a fizikai, a logikai és a kiberszemélyiség réteget.

Az ukrán hadügyminisztérium jelentése szerint az orosz erők képesek voltak távolról letiltani az orosz gyártmányú harcászati rádiókat, amelyeket az ukrán biztonsági erők használtak 2015-ben. Ezt úgy érték el, hogy a kibertéren keresztül kiiktatták a beágyazott hibamentes funkciókat.[29]

A fentin kívül a GRU, az orosz katonai hírszerző ügynökség állítólag számos más offenzív kibertérműveletet is szervezett Ukrajnában. Ez magában foglalta a 2015-ös nagy intenzitású, összehangolt támadásokat is, amelyek tönkretették a kormányzati információs rendszerek adatait, letiltották az ATM-eket és megzavarták a közlekedési rendszereket. Ennek csúcspontja volt az a nyilvánosan dokumentált számítógépes támadás egy elektronikai hálózat ellen, 2015. december 23-án, amelynek következtében áramkimaradás következett be,[30] mintegy 225 000 ukránt érintve.[31]

Ugyanakkor, az oroszok által vezetett információs műveletek Ukrajnában jóval a tárgyalt konfliktus előtt megkezdődtek. Az ukrán biztonsági szolgálat (SBU) figyelmeztetést adott ki, hogy a kormányzati szervereket és tisztviselőinek számítógépeit 2010 óta orosz kémkedésre szánt kártevők (különböző nevén „Snake", „Uroboros" vagy „Turla") célozták meg.[32]

Checkinov és Bogdanov rámutatnak – a Krím annektálása és Ukrajna jelenlegi destabilizálása következtében –, hogy az információk felhasználhatók a kormányzat

[27] Michael Kofman et al.: *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. Santa Monica, CA, RAND Corporation, 2017. 13.

[28] Borys Krementskyi: Hybrid Warfare in Ukraine EW Domain. 2019. szeptember 12. 20.

[29] Trevithick (2019): i. m.

[30] DDOS támadás az áramellátó ellen az Ivano-Frankovszki körzetben. Pontosan egy évre rá, ugyanezzel a módszerrel, ugyanez megtörtént Kijev egyik északi kerületében, és párhuzamosan kiiktatták a nemzeti légitársaság (MAU) jegyeladási rendszerét.

[31] David E. Whitehead et al.: *Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies*. Power and Energy Automation Conference, Washington, 2017. március 21–23.

[32] InfoSecurity Magazine: *Snake Cyber-espionage Campaign Targetting Ukraine is Linked to Russia* (2014. március 14.).

dezorganizálására, a kormányellenes tüntetések megszervezésére, az ellenfelek megtévesztésére, a közvélemény befolyásolására és az ellenfél ellenállási akaratának csökkentésére. Továbbá kritikus fontosságú, hogy az ilyen tevékenységek a hagyományos katonai műveletek előtt megkezdődjenek.[33]

A fent említett kutatók ugyanakkor nem veszik figyelembe azt a kritikát, miszerint különbséget kell tenni a technikai és a kognitív adatok elleni támadások között. Az Orosz Föderáció következő nemzetbiztonsági stratégiájának tervezete is problematizálja a nyugati és orosz definíciós különbségeket.

5. Következtetések

A sikeres felderítés stratégiai hatással lehet. Háborús körülmények között közvetlenül kapcsolódhat az információs fölény megszerzésének vágyához a harctéren, és néha könnyen társítható a folyamatban lévő katonai műveletekhez.

A hadviselés során mindig szoros kapcsolat állt fenn az információs műveletek és a hagyományos katonai műveletek között. Krímben az események teljes menetét – a parlament átvételétől a vitatott népszavazásig és a Krím orosz annektálásáig – az információáramlás ellenőrzésének kifinomult módszertana támogatta. Az orosz műveletek kiterjedtek a kommunikáció teljes spektrumára mind a kinetikus, mind az információs térben (és kibertérben).

Oroszország magas szintű jártasságot mutatott az РЭБ, a kiber- és információs műveletek szinergikus alkalmazásában. Ez az elemzés Ukrajnára összpontosított, kiemelve Oroszország e több területre kiterjedő képességeinek alkalmazását az ukrán erőkkel kapcsolatos hírszerzéshez, a navigációs és kommunikációs rendszerek befolyásolásához, az ukrán katonák közvetlen támadásához a mobil hírközlés rejtett földrajzi elhelyezkedése révén, a kritikus nemzeti infrastruktúra letiltásához és a társadalmi és politikai kohézió aláásásához.

Ezeket a komplex, több területet átfogó képességeket, amelyek Oroszországnak meghatározó katonai előnyt biztosítottak az ukrajnai válság idején, később Szíriában továbbfejlesztették, és jelenleg is továbbfejlesztik aszimmetrikus válaszként a kifinomult nyugati katonai képességekre.

Felhasznált irodalom

Bellingcat Podcast: *MH-17, Episode 2 Guide: A Pack of Lies* (2019. július 24.). Online: www.bellingcat.com/resources/podcasts/2019/07/24/bellingcat-podcast-mh17-episode-2-guide-a-pack-of-lies/

Checkinov, Sergei G. – Sergei A. Bogdanov: Asymmetrical Actions to Maintain Russia's Military Security. *Military Thought,* (2010), 1.

[33] Sergei G. Checkinov – Sergei A. Bogdanov: The Art of War in the Early 21st Century: Issues and Opinions. *Military Thought,* 24. (2015), 11. 26–38.

Checkinov, Sergei G. – Sergei A. Bogdanov: 'The Art of War in the Early 21st Century: Issues and Opinions. *Military Thought,* 24. (2015), 11. 26–38.
Darczewska, Jolanta: Russia's Armed Forces on the Information War Front, Strategic Documents. *OSW Studies (Center for Eastern Studies),* (2016), 57. 1–50. Online: www.osw.waw.pl/sites/default/files/prace_57_ang_russias_armed_forces_net.pdf
Dévai Dóra: An Overview of the Development of the Russian Information Warfare Concept: Part 2. *Hadtudományi Szemle,* 13. (2020), 2. 5–12. Online: https://doi.org/10.32563/hsz.2020.2.1
Guzenko, V. F. – A. L. Moraresku: *Radioelektronnaia borba. Sovremennoe soderzhanie. Tematicheskiy Sbornik. Radioelektronnaia borba v vooruzhennykh silakh Rossiiskoi Federatsii.* Informatsionnyi Most, Moszkva, 2017. 14–15.
Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018.
Infosecurity Magazine: *Snake Cyber-Espionage Campaign Targetting Ukraine is Linked to Russia* (2014. március 11.). Online: www.infosecurity-magazine.com/news/snake-cyber-espionage-campaign-targetting-ukraine/
Jaitner, Margarita: Russian Information Warfare: Lessons from Ukraine. In Kenneth Geers (szerk.): *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallinn, NATO CCD COE, 2015. 87–94.
Krementskyi, Borys: *Hybrid Warfare in Ukraine EW Domain.* 2019. szeptember 12. Online: www.dsei.co.uk/__media/libraries/global-theatre/Borys-KREMENETSKYI.pdf
Kofman, Michael– Katya Migacheva – Brian Nichiporuk – Andrew Radin – Olesya Tkacheva – Jenny Oberholtzer: *Lessons from Russia's Operations in Crimea and Eastern Ukraine.* Santa Monica, CA, RAND Corporation, 2017. Online: https://doi.org/10.7249/RR1498
Kovács László. Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12. (2017), 1. 213–232. Online: https://doi.org/10.32567/hm.2017.1.17
Lapaiev, Yuir: Ukraine as Clandestine Testing Ground for Russian Electronic Warfare. *Eurasia Daily Monitor,* 15. (2018), 157. Online: https://jamestown.org/program/ukraine-as-clandestine-testing-ground-for-russian-electronic-warfare/
Magyar Honvédség Összhaderőnemi Doktrína 3. kiadás. MH Vezetési és Doktrinális Központ, 2012.
Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 2. kiadás. 2015.
McCrory, Duncan: Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States. *The RUSI Journal,* 165. (2020), 7. 34–44. Online: https://doi.org/10.1080/03071847.2021.1888654
McDermott, Roger N.: *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum.* Tallinn, International Centre for Defence and Security, 2017. Online: https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf
Military Encyclopaedia: Voennyi Entsiklopedicheskii Slovar. Moscow, Voennoe Izadatelstvo, 1984.
Naval Dictionary: Voenno-morskoi Slovar. Moscow, Voennoe Izadatelstvo, 1990.
Az Orosz Föderáció Biztonsági Tanácsa: Orosz Nemzeti Biztonsági Stratégia. 2021. Online: http://publication.pravo.gov.ru/Document/View/0001202107030001

Trevithick, Joseph: Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio "Virus". *The Drive,* 2019. október 30. Online: www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus

Tucker, Patrick: Exclusive: US Intelligence Officials and Satellite Photos Detail Russian Military Buildup on Crimea. *Defense One,* 2019. június 12. Online: www.defenseone.com/threats/2019/06/exclusive-satellite-photos-detail-russian-military-buildup-crimea/157642/

US Army Asymmetric Warfare Group: *Russian New Generation Warfare Handbook.* Version 1, 2016. Online: https://info.publicintelligence.net/AWG-RussianNewWarfareHandbook.pdf

Van Niekerk, B. – M. Maharaj: The Future Roles of Electronic Warfare in the Information Warfare Spectrum. *Journal of Information Warfare,* 8. (2009), 3. 1–13. Online: www.jstor.org/stable/26486763

Vorobyov, I. – V. Kiseljov: Russian Military Theory: Past and Present. *Military Thought,* (2013), 3.

Whitehead, David E. – Kevin Owens – Dennis Gammel – Jess Smith: *Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies.* Power and Energy Automation Conference, Washington, 2017. március 21–23. Online: https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdf