HADMÉRNÖK

XII. Évfolyam 1. szám – 2017. március

AZ ELEKTRONIKAI HADVISELÉS JELENE ÉS LEHETSÉGES JÖVŐJE

TODAY'S ELECTRONIC WARFARE AND ITS POSSIBLE FUTURE

KOVÁCS László

(ORCID: 0000-0002-6403-0650)

kovacs.laszlo@uni-nke.hu

Absztrakt

Az ukrajnai válságban és az azt övező fegyveres konfliktusban, valamint a szíriai háborúban az elektronikai hadviselés hagyományos értelmezése újra előtérbe került. Jelen tanulmány azt a kérdés vizsgálja, hogy melyek azok az elektronikai hadviselési elvek, eljárások és eszközök, amelyek egy 21. századi, de hagyományos fegyverekkel vívott konfliktusban hatékonyan alkalmazhatóak az egyre inkább kibertéri műveletek előretörése mellett.

Kulcsszavak: *elektronikai hadviselés, kiberhadviselés, Ukrajna, Szíria*

Abstract

The pragmatic use of Electronic Warfare has emerged again in the Ukrainian crisis and in the Syrian war. This study focuses on the tactics, techniques and procedures of Electronic Warfare in a 21th Century's military crisis where the parties use conventional weaponry beside the emerging of operations in the cyber sphere.

Keywords: *electronic warfare, cyber warfare, Ukraine, Syria*

A kézirat benyújtásának dátuma (Date of the submission): 2017.01.31.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.02.17.)

BEVEZETÉS

Az elektronikai hadviselés mind eljárásaiban, mind eszközeiben komoly fejlődésen ment keresztül története során. Mint minden hadviselési elem, így az elektronikai eszközök felfedésére, az azokkal szembeni ellentevékenységre, illetve a saját elektronikai eszközök és rendszerek védelmére alkalmas megoldások folyamatosan alkalmazkodtak a korszak aktuális technikai és eljárásbeli kihívásaihoz. Ezek a kihívások elsőként technikai válaszokat igényeltek, de mindezek mellett megjelentek azok a kérdések is, amelyek elsősorban az eljárások és műveleti megoldások területén bekövetkező változásokat jelentették. A hagyományos nagyméretű fegyveres összecsapások helyett (leszámítva az olyan műveleteket, mint Irak 1992, vagy 2003) az aszimmetrikus, vagy a 2010-es években a hibrid hadviselési elvekhez kellett, illetve a legutóbbi időben csak kellett volna alkalmazkodnia az elektronikai hadviselésnek is.

A hidegháborút követő időszakban azonban a biztonságpolitikai szakértők egyöntetű véleménye alapján elterjedt nézet szerint, a nagy, hagyományos fegyveres konfliktusok (háborúk) esélye minimális volt. A nehéz fegyverzetű, ebből következően nehezen mozgó, lassan reagáló, hagyományos fegyveres erők ideje leáldozni látszott. Ugyanakkor Irak, Afganisztán, vagy éppen Líbia némileg ellentmondott ezeknek a megállapításoknak, hiszen például a 2003-as Öböl-háborúban a szövetséges erők igen komoly hagyományos légi-, illetve szárazföldi fegyverzettel vettek részt. Ez a vélekedés, valamint a nyugati országok folyamatos védelmi kiadásainak csökkenő tendenciája összességében negatívan hatott az egyébként is méregdrága – egyes elemzések szerint a légierő fejlesztési kiadásaival összemérhető –, olyan elektronikai hadviselés eszközrendszerek fejlesztésére, amelyek a hagyományos háborús műveletekben lennének alkalmazhatóak. Ez alól talán csak a légierő egyes eszközei és rendszerei voltak kivételek, hiszen a repülőgépek (elektronikai) önvédelmi berendezései komoly fejlődésen mentek keresztül. Ennek persze nagyon is nyomós oka volt, mégpedig az, hogy a légierő alkalmazási területein megkövetelt a maximális védelem az elektromágneses spektrumban is. Összességében megállapítható, hogy a szárazföldi erők klasszikus elektronikai hadviselési képességei, illetve azok fejlesztése számos országban messze elmaradt az elvárható szinttől.[1]

Mindezeken túl, az elmúlt évtizedben a számítógépek és számítógép-hálózatok katonai műveletekben való elterjedése, valamint a polgári számítógép-hálózatok célpontként való megjelenése egyre többször és egyre nagyobb átfedést jelent az elektronikai hadviselés, valamint a kibertérben folyó műveletek között.

Maga az elektronikai hadviselés – főleg annak eszközei és eljárásai – a legszenzitívebb, legtitkosabb tényezők minden ország hadseregén belül. Az általános elvek azonban nem titkosak, sőt számos publikációt találunk az elektronikai hadviselésről évtizedek óta.

Jelen írás arra keresi a választ, hogy hol történt képesség csökkenés, és hol történt esetleg képesség növekedés az elektronikai hadviselés területén az elmúlt időkben. Ugyanakkor az elemzés nem kíván teljes és átfogó képet adni a területről, de néhány tényező felvillantásával bepillantást kíván engedni az egyébként meglehetősen szenzitív és minden ország által rendkívül titkosan kezelt elektronikai hadviselés néhány konkrét jellemzőjébe.

[1] Ez alól az egyik kivétel a rádió távvezérelt improvizált robbanóeszközök elleni védelemben elengedhetetlen zavaró eszközök fejlesztése volt.

AZ ELEKTRONIKAI HADVISELÉS JELLEMZŐI

Az elektronikai hadviselés összetevői és feladatai

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.*" [1]

Ez a meglehetősen bonyolult és hosszú meghatározás azonban nem jelent mást, mint az elektromágneses spektrumban működő elektronikai eszközök működésének felderítését, az így megszerzett adatokból az elektronikai eszközök helyére, együttműködéseikre következtetések levonását, valamint a kisugárzások lehallgatásából információk megszerzését, az elektronikai eszközök működésének akadályozását, illetve nyilvánvalóan a saját elektronikai eszközeink védelmét. Az elektronikai hadviselés legfontosabb tartománya az elektromágneses spektrum, és mivel elektronikai eszközöket a hadseregek minden tevékenységük során használnak, így az elektronikai hadviselés jelen van a szárazföldi csapatok, a légierő, valamint a haditengerészet műveleteiben is. [2]

Hazánkban az elektronikai hadviselés külön dedikált doktrínával rendelkezik, amely szerint e tevékenység fogalma: „*olyan 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."* [3]

A fogalmi meghatározásokból is kitűnik, hogy az elektronikai hadviselés három nagy területre osztható: elektronikai támogatásra (angol terminológiában: Electronic Support Measures – ESM), elektronikai ellentevékenységre (Electronic Counter Measures – ECM)[2] és elektronikai védelemre (Electronic Protection – EP)[3]. Ugyanakkor a NATO elektronikai hadviseléssel foglalkozó doktrínájához hasonlóan a hazai szabályozási környezet is területekre és funkciókra osztja az elektronikai hadviselést, amely elektronikai támadás, elektronikai védelem és elektronikai megfigyelés területeket, valamint elektronikai támogatási, elektronikai ellentevékenységi és elektronikai védelmi funkciókat különböztet meg. [3]

Mindezekből a meghatározásokból le lehet vezetni az elektronikai hadviselés konkrét és kézzelfogható feladatait. Az elektronikai támogatás feladata alapvetően az elektromágneses spektrumban történő veszélyjelzés, az ISTAR (Intelligence Surveillance Target Acquisition Reconnaissance – felderítés és célazonosítás) képességekhez való hozzájárulás, valamint a SIGINT (Signals Intelligence – rádióelektronikai felderítés) tevékenység támogatása. Az elektronikai ellentevékenység hadviselési dimenziók szerinti feladata alapvetően két részre osztható: légierő-, valamint szárazföldi feladatok[4]. A légierő tevékenysége során az elektronikai hadviselés többek között a repülőgépek önvédelmi elektronikai hadviselési feladatait, kötelékoltalmazást (zavarást), az ellenséges légvédelem lefogását (SEAD -

[2] Az elektronikai ellentevékenységet egyre többször, főleg az amerikai terminológiában elektronikai támadásnak (EA - Electronic Attack) hívják.

[3] Korábban az elektronikai védelmet elektronikai ellen-ellentevékenységnek (Electronic Counter-Counter Measures – ECCM) is nevezték.

[4] Természetesen ezek a dimenziók a haditengerészettel rendelkező országok esetében a tengeri dimenziót is jelentik.

Suppression on Enemy Air Defenses) valamint a szárazföldi (ide értve a légideszant, különleges műveleti, stb.) erők számára elektronikai támogatási feladatokat végez. [4] A szárazföldi feladatok során az elektronikai ellentevékenység feladatai lehetnek a szembenálló fél kommunikációs eszközeinek, radarjainak, vagy akár a navigációs eszközeinek zavarása vagy megtévesztése. Az elektronikai védelem feladata elsősorban a saját csapatok elektronikai eszközeinek a védelme, közvetlen vagy közvetett módon a csapatok oltalmazása, valamint az elmúlt időszakban kiemelt feladatként a vezeték nélküli távirányítással[5] működő improvizált robbanóeszközök zavarását (counter RC-IED).

Ezekből a feladatokból világosan látszik, hogy az elektronikai hadviselés rendkívül összetett, komplex feladatrendszerrel rendelkezik. Ezek a feladatok mindegyike hatalmas technikai eszközparkot feltételez úgy, hogy ezeknek a technikai eszközöknek és rendszereknek fejlettségben folyamatosan követniük kell a „másik oldal" technikai fejlődési trendjeit, hiszen anélkül rendkívül gyorsan devalválódnak, azaz korlátozottan vagy teljesen használhatatlanná válnak a saját oldali eszközök. Ennek megfelelően a terület tudományos igényű kutatása nélkülözhetetlen. Ezeket a kérdéseket természetesen hazánkban is kiemelt területként kezelik a tudományos kutatások és mind a hadtudományi mind a katonai műszaki kutatások egyik meghatározó irányaként definiálják. [5] [6]

Az elektronikai hadviselés a NATO szövetségi szintjén is jelen van. A NATO legfontosabb elektronikai hadviselési szerve a NATO Elektronikai Tanácsadó Testület (NATO Electronic Warfare Advisory Committee - NEWAC). Ez a szervezet felelős a NATO elektronikai hadviselési politikájának, doktrínájának, utasítási és ellenőrzési koncepcióinak kialakításáért, valamint az elektronikai hadviselési támogatás NATO-műveletekben való megjelenésének biztosításáért. [7]

Az elektronikai hadviselés története dióhéjban

Az elektronikai hadviselés, bár magával a hadviseléssel természetesen nem lehet egyidős, mégis viszonylag régen jelen van a fegyveres küzdelmekben. Amióta az első komolyabb elektronikai eszköz, nevezetesen a harctéri rádió megjelent a katonai műveletekben, azóta beszélhetünk annak felderítési, lehallgatási, később pedig zavarási igényéről.[6] A Marconi féle rádió volt az első olyan vezeték nélküli híradást megvalósító eszköz, amely forradalmasította a harctéri kommunikációt. Ugyanakkor az első elektronikai hadviselési elveknek megfelelő katonai tevékenység az 1905-ös japán-orosz háborúban jelent meg először.[7] [8]

Mind az 1. mind a 2. világháború hatalmas fejlődést hozott az elektronikai hadviselés területén. Az 1. világháborúban, majd a két háború közötti időszakban a rádiók lehallgatása, a kisugárzás helyének a meghatározása, valamint az üzenetek tartalmának a megfejtése volt a fő feladat[8].

---

[5] A vezeték nélküli távirányítású eszközök közül is elsősorban a rádióhullámok tartományában működő eszközök ellen lehet hatékony az elektronikai ellentevékenység.

[6] Ugyanakkor a vezeték nélküli kommunikáció megjelenése előtt a vezetékes híradást lehetővé tevő Morse távíró vonalak lehallgatása vagy akár annak rombolása volt az első, klasszikus „elektronikai hadviselési" eljárás. *„A közlemények egyszerű vezetékre való csatlakoztatással lehallgathatóvá váltak, amin a különféle rejtjelezési módszerek, kódtáblázatok és más eljárások némiképpen segíthettek. Egyszerűen megvalósítható volt a megtévesztő közlemények bejuttatása a hálózatba, hiszen az adókészülék helyére egy ugyanolyan készülékkel rácsatlakozva fizikailag helyettesíteni lehetett az igazi felhasználókat. A vezetékek elvágásával, a távíróoszlopok kidöntésével a vonalak fizikailag is könnyen támadhatóak voltak."* [9]

[7] A japán-orosz háborúban jelent meg először a szembenálló fél rádióinak lehallgatási igénye. [8] [10]

[8] Itt meg kell említeni Pokorny Hermann nevét, aki az Osztrák-Magyar Monarchia tisztjeként kiváló orosz nyelvtudása miatt először az orosz rádió-táviratok feldolgozását, majd később – 1916-ig – a rádiólehallgatás megszervezését is feladatul kapta. [11]

A 2. világháborúban az elektronikai eszközök, mint például a repülőgép-fedélzeti rádiók és radarok egyre gyorsuló ütemű elterjedése az elektronikai hadviselési eszközök és erők fejlődését is magával hozta.

Ezt követően a helyi háborúk – koreai háború, az arab-izraeli háborúk, a vietnámi háború, később az Öbölháború 1991-ben – a harctéren megszerzett tapasztalatokkal támasztották alá és erősítették meg azokat a véleményeket, melyek szerint az elektronikai hadviselés elengedhetetlen része a korszerű fegyveres küzdelemnek.

Nem túlzás azt állítani, hogy ezt követően az elektronikai eszközök robbanásszerűen nyertek teret a 20. század közepén a hadviselésben. Minden ország fegyveres ereje egyre több és egyre komplexebb elektronikai eszközt alkalmazott és alkalmaz ma is a vezetés és irányításra, a felderítésre és információszerzésre, a fegyverrendszerek vezérlésére, a kommunikációra, az adatátvitelre, vagy a navigációra. Mindezek mellett olyan eszközök jelentek meg, mint a pilóta nélküli repülőgépek (angol terminológiában: Unmanned Aerial Vehicle – UAV), vagy a szárazföldi robotok (angol terminológiában: Unmanned Ground Robot – UGR), amelyek már nem csak „egyszerű" felderítésre, hanem a fedélzeti fegyvereiknek köszönhetően nagyon gyakran csapásmérésre is alkalmasak. Ezek az eszközök feladataik ellátása során, bár már sokszor önálló döntéshozatalra is képesek, de mégis egyelőre alapvetően elektronikai eszközökkel történő irányításuk a döntő.

Ezek a változások az elektronikai hadviselés képességeinek fejlődését és alapvető változását igényelték, mind eszközrendszer, mind eljárások tekintetében. Ez a hidegháború befejeződéséig nyomon követhető is volt. Ezt követően azonban – ahogy arra később részletesen szó lesz –, az alapvető biztonságpolitikai enyhülés, valamint az olyan egyéb kihívásoknak – pl. terrorizmus, aszimmetrikus fenyegetések, stb. – köszönhetően nagyon sok ország fegyveres ereje nem fordított kellő figyelmet az elektronikai hadviselési eszközök, rendszerek és képességek fejlesztésére. Ez természetesen nem minden területre igaz, de pl. a szárazföldi csapatok elektronikai hadviselési képességeinek sokszor még a szinten tartása is elmaradt.

ELEKTRONIKAI HADVISELÉSI KÉPESSÉGEK

Elektronikai hadviselési képességvesztés: Egyesült Államok

A hidegháború utáni időszakban, azaz az elmúlt több mint 25 évben a nyugati nagyhatalmak közül sokan – és ezzel párhuzamosan a kisebb országok[9] is – mintha elfelejtették volna azt a tényt, hogy mind a hadsereg vezetése, mind az ahhoz elengedhetetlen kommunikáció és felderítés elektronikai eszközökre épülnek, és ezek az elektronikai eszközök, hasonlatosan a számítógépekhez, illetve a számítógép-hálózatokhoz sérülékenyek. Ráadásul ez a tény ma már egy bizonyos szintű függőséget is jelent az elektronikai rendszerekkel szemben. Ugyanakkor az ezeket lehallgatni, az ezekbe az elektronikai eszközökbe beavatkozni képes, vagy az ezeket zavarni tudó – elektronikai hadviselési – eszközöket és rendszereket nem, vagy csak alig fejlesztették.[10]

Ezt támasztják alá azok a nagyon súlyos megállapítások, amelyeket az Amerikai Egyesült Államok Védelmi Minisztériumának úgynevezett Védelmi Tudományos Testülete (Defense

[9] Az elmúlt időben hazai kutatók is utaltak erre a problémára Magyarország vonatkozásában. [12] [13]

[10] Ez természetesen nem jelenti azt, hogy ne történt volna elektronikai hadviselési eszközfejlesztés. De maga az elektronikai hadviselési képesség, amellyel egy-egy ország rendelkezik messze alul maradt attól a képességtől, amelyet a hidegháború utáni technikai és technológiai fejlődés megkövetelt, illetve prognosztizálható lett volna.

Science Board of Department of Defense - DSB)[11] 2015 nyarán született jelentésében tett. A DSB jelentése, amelyben a 21. század katonai tevékenységeit a komplex elektromágneses környezetben vizsgálják, leszögezi, hogy az Egyesült Államok nagyon komoly hiányosságokkal küzd az elektronikai hadviselés területén.[12] A tanulmány három fő okra vezeti vissza ezen hiányosságok meglétét, illetve azok kialakulását:

- a hidegháborút követő 25 évben az USA elhanyagolta az elektronikai hadviselés területét, amely elsősorban az elektromágneses spektrumban rejlő veszélyek negligálása miatt következett be;
- a második ok abban keresendő, hogy a fejlett szoftver vezérelt elektronikai eszközök kutatás-fejlesztése, azok előállítása már nem csak az USA privilégiuma, számos feltörekvő ország képes ma már ilyen high-tech elektronikai eszköz és rendszer gyártására;
- világossá vált, hogy a potenciális ellenfelek, amelyek folyamatosan figyelték az Egyesült Államok harctéri elektronikai dominanciáját, olyan eszközöket és rendszereket állítottak hadrendbe, amelyek ezt a dominanciát megtörik és ezzel az USA számára a lépéselőny megszűnik.

Mindezek alapján az elemzés három olyan területre mutat rá, amelyek elengedhetetlenül szükségesek ahhoz, hogy a feltárt hiányosságok megszüntethetőek legyenek. Az első: szükség van az elektromágneses spektrum dinamikus használatára. Ez jelenleg egy olyan technikai kihívás, amely megnehezíti a helyzetismeret kialakítását, a spektrum hatékony kihasználását, valamint a szembenálló fél spektrumhasználatának akadályozását. A második: el kell érni az elektronikai rendszerek közel valós idejű adaptációját. Az a sebesség, amellyel a korszerű digitális elektronikára épülő technológia a működési üzemmódjai között vált drámai módon megnőtt. Ehhez alkalmazkodnia kell az USA elektronikai hadviselési eszközeinek is. A harmadik terület: az Egyesült Államok nem engedheti meg magának, hogy alárendelt szerepet játsszon az elektronikai hadviselés bármely területéről legyen is szó. Ennek érdekében olyan nagyarányú elektronikai fejlesztések szükségesek, amelyeket nem, vagy csak nehezen tudnak követni a potenciális vetélytársak. Ez egyrészről technológiai fölényt eredményez, másrészt a harctéren elektronikai fölényt fog jelenteni. [15]

Ezeket a megállapításokat támasztja alá Laurie Buckhout, az Egyesült Államok Szárazföldi Erők korábbi elektronikai hadviselési főnökének nyilatkozata: "*A legnagyobb probléma az, hogy évtizedek óta nem harcoltunk úgy, hogy a kommunikációnkat zavarták volna, így nem tudjuk, mit kell tenni ilyen helyzetben. Ráadásul nem csak az eljárásaink hiányoznak ilyen esetekre, hanem kiképzésünk sincs a zavar alatt álló kommunikációs környezetben való tevékenységre*." [16]

Ugyanebből a nyilatkozatból az is világosan kiderül, hogy az Egyesült Államok szárazföldi hadereje (US Army) az elektronikai ellentevékenység (zavarás) terén is hiányosságokkal

[11] A DSB-t 1956-ban hozta létre az amerikai Védelmi Minisztérium azzal a céllal, hogy a Testület révén olyan tudományosan magalapozott tanácsokat biztosítsanak a fegyveres erők számára, amelyek alapján azok megfelelnek a változó világrend egyre nagyobb kihívást jelentő rakéta technológiájával, az információs hadviseléssel, a biológiai, kémiai és nukleáris fegyverekkel, valamint egyéb hidegháború fenyegetésekkel szemben. A testület munkájára napjainkban ugyanolyan szükség van, mint korábban, hiszen a fegyveres erőkkel szembeni kihívások a hidegháború elmúltával nem, hogy csökkentek volna, hanem éppen ellenkezőleg: drasztikusan nőttek. [14]

[12] A tanulmány több területen vizsgálta az elektronikai hadviselés műveleti támogatásban betöltött szerepét és jellemzőit: műholdas kommunikáció, harcászati kommunikáció, precíziós navigáció és felderítés. Ezt a négy tényezőt megvizsgálták a legjellemzőbb három műveleti formában: harcászati légiharc, haditengerészeti védelem, valamint szárazföldi harcászati műveletek. [15]

küzd. "*Nagyszerű rádióelektronikai felderítésünk*[13] *van, egész nap tudunk lehallgatást végezni, de egytized részben sem tudjuk őket zavarni, összehasonlítva azzal, amit ők*[14] *tudnak. Nagyon védtelenek a hálózataink az ő támadásaikkal szemben.*" [16]

Számos elemzés ezeknek a hiányosságoknak a kialakulását paradox módon éppen Irakra és Afganisztánra vezeti vissza. 1999 óta, azaz az afganisztáni műveletek megkezdése óta, az USA szárazföldi ereje alapvetően az itt, valamint később Irakban tapasztalt kihívásokra koncentrált. Ennek megfelelően a US Army jelenlegi elektronikai hadviselési eszközeinek, illetve képességeinek a jelentős része a gyorsreagálású képességek biztosítása érdekében született. [17] Ezek a képességek pedig mind minőségben, mind (eszköz) mennyiségben nagyon messze vannak attól, amelyet egy hagyományos háborúban a szárazföldi erőknek teljesíteniük kellene.

Az afganisztáni és iraki kihívásokra adandó válaszok ad-hoc fejlesztésekhez és beszerzésekhez vezettek. Többek között olyan eszközök beszerzése történt meg, mint pl. a C-12-es repülőgépé, amely az úgynevezett CEASAR[15] (Communications Electronic Attack with Surveillance and Reconnaissance – kommunikációs zavaró és felderítő) függeszthető elektronikai hadviselési konténert alkalmazza. Ugyanakkor ez a konténer is alapvetően a felkelők elleni műveletek céljából, a gyorsreagálású képességek biztosítása érdekében került alkalmazásra.

Hasonló fejlesztés a GATOR (Ground Auto Targeting Observation/Reactive – földi automatikus célmeghatározó/zavaró) elektronikai hadviselési rendszer. (1. kép) Ez szintén abból az igényből származtatható, hogy nagyon gyors iránymérés és helymeghatározás szükséges az RCIED-k elleni tevékenységek esetén. [17] Ugyanakkor a rendszer ennél szélesebb körű felhasználással rendelkezik – hiszen a zavaró képesség a szembenálló fél kommunikációs rendszerei ellen is alkalmazható lenne –, de a korlátozott számban rendelkezésre álló berendezések miatt a felhasználhatóság itt is erősen limitált. [16]

---

[13] Rádióelektronikai felderítés: SIGINT (Signals Intelligence): alapvetően passzív eljárásokra épülő, az elektromágnes spektrumban működő felderítési fajta. Két részre osztható: COMINT (Communication Intelligence), azaz kommunikációs felderítés (magyar terminológiában: rádiófelderítés), valamint ELINT (Electronic Intelligence), azaz nem kommunikációs felderítés (magyar terminológiában rádiótechnikai felderítés). [2]

[14] Az orosz fél.

[15] A CEASAR a C-12 Beechcraft King Air repülőgépre, mint hordozóra kifejlesztett elektronikai felderítő és zavaró konténer. Fő feladata a felkelők elleni műveletekben (counter-insurgencies operations) a kommunikáció felfedése és zavarása. A fejlesztést alapvetően az US Army gyorsreagálású erői (U.S. Army Quick Reaction Capability Effort) számára készítették. [18] A C-12-es repülőgép, mint hordozó ugyanakkor számos más feladatban is szerepet kapott már korábban is (pl. futárgép, felderítőgép, stb.), és erre a típusra épült RC-12N Guardrail Common Sensor típusnévvel gyártott SIGINT repülőgép, amely az afganisztáni műveletekben is részt vett 2015-ig. [19]

A CEASAR alapjaira épült a szintén a Raytheon cég által gyártott NERO (Networked Electronic Warfare, Remotely Operated – távirányítású, hálózati elektronikai hadviselési) rendszer, amely alapvetően a US Army MQ-1C Gray Eagle típusú pilóta nélküli repülőgépéhez készült konténer. Fő feladata a kommunikációs felderítés és zavarás. Ez a konténer nagy előrelépés a fejlesztésben, hiszen egy (közvetlen) kezelőt nem igénylő, és így pilóta nélküli repülőgépen is alkalmazható rendszert jelent. [20]

1. kép. A GATOR elektronikai hadviselési rendszer. [21]

Mindezekhez a technikai kérdésekhez hozzájárul az elektronikai hadviselési szakemberek helyzete is. Az egyébként is kevés létszámú elektronikai hadviselési tiszt és altiszt alapvetően elméleti képzésben részesült, ráadásul békebeosztásuk sokszor más, párhuzamos feladat ellátását is jelentette, így gyakorlatban, harci körülmények között is alkalmazható szakmai ismereteik erősen korlátozottak. [16]

A problémák és a hiányosságok felismerése megtörtént. Ennek megfelelően az olyan elektronikai hadviselési rendszerek, mint pl. a CEASAR, NERO, GATOR további fejlesztése mellett újabb elképzelések is születtek. Ilyen például az MFEW (Multifunctional Electronic Warfare – multifunkcionális elektronikai hadviselés) fejlesztése. Az MFEW olyan elektronikai ellentevékenységi képességekkel fog rendelkezni, amely a mobil telefonok zavarásától, a GPS rendszerek zavarásán át, a harctéri rádiórendszerek zavarásáig széles spektrumot fed le[16]. Ugyanakkor ennek rendszerbeállítása csak 2023-ban, a teljes műveleti képesség elérése pedig csak 2027-re várható. [16] [21]

[16] Az eredeti elképzelések szerint az MFEW nem csak elektronikai támadó (zavarási) hanem elektronikai támogatási (ESM) képességekkel is rendelkezik, valamint mind szárazföldi, mind légi komponense is van. A rendszer hálózatos kialakítású, valamint valós idejű át- és újraprogramozási (új feladatszabási) lehetőségekkel is bír. [21]

Elektronikai hadviselési képesség növekedés: Oroszország

Az ukrajnai konfliktus során az Egyesült Államok katonai kiképzői folyamatosan segítik az ukrán hadsereg felkészítését és kiképzését. E tevékenység során az amerikai fél is nagyon sok hasznos tapasztalatra tesz szert, mert számos olyan ukrán csapat vesz részt a kiképzéseken, akik korábban Kelet-Ukrajnában az orosz barát felkelők elleni műveletekben harcoltak.

Így az ukrán hadsereg harcban szerzett tapasztalatait az USA feldolgozza, amely során elemzi többek között az orosz elektronikai hadviselési eszközök fajtáit, működési filozófiájukat, képességeiket, valamint ezen eszközök hatótávolságát. Mindezt segíti az is, hogy bár az ukrán fél elektronikai hadviselési képességei messze alul múlják az orosz félét, mégis a korábban a Szovjetunió részeként kiképzést kapott idősebb katona generáció még – részben – emlékszik azokra az elvekre és eljárásokra, ahogy az orosz fél elektronikai hadviselése felépül és működik.

Az így kapott eredmények arra engednek következtetni, 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 zavaró, illetve egyéb szárazföldi elektronikai eszközök, valamint rádiólokációs zavaró képességeik fejlesztésére.

A fentiekből levonható további következtetés, hogy – hasonlóan az amerikai haderőhöz – az ukrán hadsereg elektronikai zavarás esetén történő feladatellátásra való felkészülése teljesen hiányzik. Ez visszavezethető az ukrán hadsereg ilyen típusú kiképzésének, szimulációs gyakorlatainak, valamint az ilyen helyzetek kezelésére megfelelő eljárásrend kidolgozásának és begyakorlásának a teljes hiányára. Ez azzal a következménnyel jár, hogy a nagyarányú elektronikai zavarás a vezetés (C2 – Command and Control) megbontását eredményezi, azaz végső soron a masszív elektronikai hadviselés vezetési fölényt eredményez.[17] A katonai vezetés technikai eszközeinek elektronikai zavarás miatti kiesését – akár átmenetileg is – polgári kommunikációs eszközökkel, pl. GSM telefonokkal történő helyettesítése, pótlása szintén nehéz feladat, mert a területen a polgári rendszerek, így a GSM rendszerek zavarása is folyik. Egy másik – nem kevésbé veszélyes – következmény, hogy a tüzérségi felderítő radarok zavarása miatt nem lehetséges a tüzérségi tűz kiváltási helyének a meghatározása, így nem lehetséges pontos válasz-tűzcsapást vezetni a szembenálló fél tüzérségi eszközeire. [16] [22]

A fentieken túl az elektronikai hadviselési eszközök nem kinetikus energiájú „fegyverek”, hatásaik nem látszanak a médiában, így például Ukrajna keleti részében is gyakorlatilag láthatatlanul, vagy csak az avatott szemek számára látható módon képesek tevékenységet folytatni. Ez óriási előny az orosz félnek, hiszen anélkül képes vezetési fölényt biztosítani, hogy a jelenlétére utaló áruló technikai eszközök explicit módon megjelennének a hírekben. „*Az ukrán erők félelmetes orosz elektronikai hadviselési képességekkel szemben küzdöttek, amely elemzők szerint még az amerikai szárazföldi erők számára is megdöbbentő. Az amerikai hadsereg is használ zavarást a felkelők kommunikációja ellen a levegőből és a*

[17] Az elektronikai hadviselés az információs műveletek (IO – Information Operations) egyik alap összetevője (katonai képességként értelmezett módon). Az információs műveletek kiemelt célja az információ fölény, és ezen keresztül a vezetési fölény kivívása. Ennek értelmében megállapítható, hogy az orosz fél az információs műveletek területén is kiemelkedő sikereket ér el azzal, hogy az elektronikai hadviselés révén vezetési fölényt biztosít a maga számára. A vezetési fölény többek között a harcban azért is bír nagy fontossággal, mert birtoklója számára biztosítja a kezdeményezés, valamint a harctéren való dominancia előnyét.

szárazföldről egyaránt, de ez csak korlátozottan áll rendelkezésre, és a zavaró rendszerek fejlesztése nem is várható 2023-ig." [16]

Mindezek alapján jelen írás néhány olyan orosz elektronikai hadviselési eszközt kíván bemutatni, amelyek fejlesztése az elmúlt évtizedben történt, és amelyek szerepet kaptak Kelet-Ukrajnában, vagy akár Szíriában.

Az első ilyen eszköz egy új elektronikai hadviselési helikopter: az Mi-8MTPR-1, amely fedélzetén a Rychag-AV nevű zavaró állomás helyezkedik el. Az állomás fő rendeltetése a radarok zavarása, valamint radar rávezetéssel rendelkező föld-levegő és levegő-levegő rakéták elleni tevékenység, alapvetően azok zavarása[18]. Az eszközt a moszkvai központú Kret[19] nevű orosz, rádióelektronikai ipari vállalati egyesülés gyártja és forgalmazza[20].

A Mi-8 helikopterre szerelt zavaró rendszer látható a Kret cég hivatalos weblapján közzétett képen (2. kép). Ezen azonban valószínűsíthetően csak a mikrohullámú tartomány egyik antennája látszik a törzs hátsó harmadában.

2. kép. A Mi-8MTPR1 helikopterre szerelt Rychag-AV a Kret hivatalos fényképén [23]

Ugyanakkor amennyiben a fedélzeti rendszer kommunikációs zavaró képességgel is rendelkezik, akkor az szükségessé teszi URH antennák alkalmazását is. Ez a teljes antenna rendszer a 3. sz. képen látható módon nézhet ki (egy másik típus esetében).

[18] A Kret cég hivatalos képein és filmjein az is látható, hogy az állomás valószínűleg infravörös hullámtartományban is képes zavarásra.

[19] Kret: http://oblik.msk.ru/en/

[20] A Kret cég 2015-ben 9 db Moszkva-1 elektronikai felderítő állomást, 10 db Rychag-AV helikopter fedélzeti zavaró állomást, 8 db Krasukha-2 és 15 Krasukha-4 elektronikai hadviselési komplexumot, valamint 20 Rtut-BM elektronikai felderítő és zavaró állomást szállított az orosz hadseregnek. [24]

3. kép. Az orosz légierő Mi-8 típusú helikopterre szerelt elektronikai hadviselési eszköze. [25]

Érdemes megjegyezni, hogy a korábban a Varsói Szerződés több tagországában, így Magyarországon is rendszeresített Mi-17PP elektronikai hadviselési helikopter, amely hasonló feladatokkal és hasonló rendeltetéssel bírt (URH zavarás), antenna rendszerének elhelyezése és kialakítása sok hasonlóságot mutatott a 3. számú képen látható eszközzel. (4. kép)

4. kép. Az 1990-es évek közepéig a Magyar Honvédségben (korábban Magyar Néphadseregben) rendszerbe állított Mi-17PP elektronikai hadviselési[21] helikopter. [26]

[21] Az akkori terminológia szerint az elektronikai hadviselés rádióelektronikai harc kifejezésként volt használatos.

A Rychag-AV zavaró állomásról – csakúgy, mint az többi orosz elektronikai hadviselési eszközről – meglehetősen kevés, és csak általános technikai információ érhető el nyílt és nem utolsósorban megbízható forrásból. Egyes források a Rychag-AV eszközt az 1970-es években gyártott Szmalta zavaró állomás utódjának tartják. Az elől 100 km-es zavarási hatótávolsággal rendelkezett, ezzel szemben ennél az állomásnál ezt már több száz kilométerre teszik[22]. Fázisrács-vezérelt antennájának köszönhetően egyszerre több célpont zavarását is el tudja végezni. Magát a zavaró állomást nem csak helikopter fedélzetére lehet elhelyezni, hanem akár haditengerészeti vagy szárazföldi platformokra is. A gyors jelfeldolgozásnak, illetve a fedélzeti adatbázisnak köszönhetően önvédelmi elektronikai hadviselési feladatokat is képes ellátni az állomás. [27]

Vladimir Mikheev a Kret vállalat egyik vezetőségi tanácsadójának nyilatkozata alapján ezt a rendszert 2017-ben a Rychag-AVM zavaró rendszer fogja követni, amely még nagyobb hatótávolsággal és megnövelt funkcionalitással fog rendelkezni. [24]

A következő bemutatni kívánt orosz elektronikai hadviselési eszköz, illetve eszközök a Kraszuha-2/4 elektronikai hadviselési komplexumok. A két egymást kiegészítő változatban gyártott és rendszerbe állított elektronikai hadviselési komplexum az 1RL269 Kraszuha-2 és az 1RL257 Kraszuha-4 típus nevet viselik. Ezeket az eszközöket a szintén a Kret vállalathoz tartozó Bryansk Electromechanical Plant nevű cég gyártja. (5. és 6. kép). [28]

5. kép. Kraszuha-2 elektronikai hadviselési komplexum. [29]

A Kraszuha-2/4 alapvető feladata az AWACS (Airborne Warning and Control System – fedélzeti korai előrejelző és vezetési rendszer) felderítése és zavarása 250-300 km-es hatótávolságig. A komplexumok további elektronikai ellentevékenységi feladatai lehetnek az olyan fedélzeti radarok zavarása, mint például az amerikai Joint STARS[23] repülőgépen lévő

[22] A Rychag-AV zavarási hatótávolságát a Kret cég hivatalos bemutató filmje földi célok ellen 50-200 km-ben, a légi célok ellen 300 km-ben, az egyidejűleg lefogható célok számát pedig maximum 8 db-ban adja meg. [30]

[23] A Joint STARS (E-8C) repülőgép fedélzetén elhelyezett SAR radarjával mind a légierő, mind a szárazföldi csapatok számára biztosít felderítési adatokat, valamint harcvezetési rendszerének köszönhetően célinformációkkal támogatja a támadó műveleteket. [31]

SAR (Synthetic Aperture Radar – szintetikus apertúrájú radar), vagy akár a pilóta nélküli repülőgépek zavarása (pl.: RQ-4 Global Hawk, MQ-1 Predator). A rendszer korlátozott mértékben, de képes műholdak zavarására (pl.: az USA Lacrosse és Onyx típusú műholdjai) is, valamint alkalmas radar rávezetésű rakéták zavarására és hamis cél imitációra. A komplexum olyan nagy fontosságú célok védelmét is feladatul kaphatja, mint pl. az Iskander (9K720 Iskander SRBM).[24]

6. kép. A Kraszuha-4 elektronikai hadviselési komplexum. [32]

Szintén érdemes megjegyezni, hogy a Kraszuha-4 állomás antennarendszere kísértetiesen hasonlít a korábban a Varsói Szerződés számos tagországában – így hazánkban is – az 1980-as években rendszeresített SZPN-30 repülőgép-fedélzeti rádiólokátor zavaró állomás antennáihoz[25].

[24] Iskander (9K720 Iskander SRBM): ballisztikus rakéta. (NATO kódneve SS-26 Stone) Alapvető rendeltetése a harcászati csapásmérés a nagyértékű és nagyfontosságú célokra. Hatótávolsága 500 km. Ebből következően ez a komplexum elsődleges cél lehet egy adott fegyveres konfliktusban, így a védelme kiemelt fontosságú. [33]

[25] Ugyanakkor a gyártó hivatalos videóin jól látszik, hogy az állomás elektronikai eszközei a kor színvonalának megfelelő, számítógép vezérlésű eszközök.

7. kép. Az SZPN-30 repülőgép-fedélzeti rádiólokátor zavaró komplexum. [34]

Az SZPN-30 fedélzeti rádiólokátor zavaró állomás fő feladata a 3 cm-es hullámtartományban működő repülőgép-fedélzeti radarok zavarása zajzavarral, illetve válasz-impulzus zavarral volt. Az állomás egyszerre 5 cél lefogására volt képes közel 300 km-es hatótávolságig.

Az orosz katonai intervenció Szíriában szükségszerűen a korszerű orosz haditechnikai eszközök bevetését is igényelte. Ennek egyik példája többek között a Kraszuha-4 alkalmazása a szíriai háborúban. Erről tanúskodik a szíriai Latakia mellett telepített állomásról készített kép. (8. kép).

A fenti eszközökön kívül is számos olyan elektronikai hadviselési berendezést fejlesztett vagy modernizált az orosz haderő[26], amelyek a hagyományos fegyveres konfliktusokban sikerrel alkalmazhatóak, de mindezek mellett rendelkeznek az olyan képességekkel is mint a korábban említett RC-IED-k elleni elektronikai ellentevékenység, illetve védelem. Ilyen eszköz például az Infauna K1Sh1 UNSh-12 elektronikai felderítő és zavaró állomás, amely egy BTR-80-as alvázon került elhelyezésre, vagy például a Tigr-M MKTK REI PP állomás, amely Tigr típusú terepjáró személygépkocsi alvázára szerelt Leer-2 típusú iránymérő és zavaró berendezést jelent. [36]

További hasonló elektronikai hadviselési berendezés az MTLBU[27] alvázra épített Borisoglebsk-2 nevű RH és URH frekvenciatartományban működő elektronikai felderítő és zavaró állomás. Ez az új állomás annak az elektronikai hadviselési fejlesztési programnak a

[26] Az orosz haderő modernizációja az említetteken kívül is számos haditechnikai eszközt érintett. Ilyenek például a korszerű páncélozott harcjárművek irányított rakéták elleni védelmét lehetővé tevő ellentevékenységi rendszerek (többek között a Drozd-2, Sthora-1, Arena, stb.) [39]

[27] Az MTLBU oroszul МТ–ЛБу – многоцелевой транспортёр легкобронированный универсальный, azaz többcélú könnyű páncélozott szállító járművek korábban a Magyar Néphadseregben, illetve a Magyar Honvédségben is rendszeresítve voltak. Többek között az R-330P zavaró állomás is ilyen hordozó eszközön került elhelyezésre.

része, amely az orosz hadsereg gépesített lövész dandárjainak ilyen irányú képességei növelését célozta 2014-től kezdődően. [37]

8. kép. Kraszuha-4 komplexum a szíriai Latakia[28] közelében. [35]

Meg kell jegyezni, hogy ezek az állomások – azaz az Infauna, a Tigr-M MKTK REI PP, illetve a Borisoglebsk-2 is – mindegyike harcászati szintű, nagy páncélvédettséggel rendelkező, és nagy terepjáró képességekkel bíró olyan eszköz, amelyek elsősorban gépesített lövész egységek és alegységek, illetve légideszant csapatok[29] támogatására kerülnek alkalmazásra. Ebből egyértelműen levezethető, hogy alkalmazásuk – rendeltetésüknek megfelelően –, leginkább hagyományos háborúban a legvalószínűbb. Ez pedig intő jel kell, hogy legyen a számunkra.

AZ ELEKTRONIKAI HADVISELÉS LEHETSÉGES JÖVŐJE

Az eddig bemutatottak alapján jól látszik, hogy az elektronikai hadviselésnek a sikeres harc megvívása érdekében eszközeiben és eljárásaiban is alkalmazkodnia kell (a fentiek alapján számos országban csak kellene) azokhoz a körülményekhez, amelyek a korszerű fegyveres küzdelmet jellemzik.

Az elektronikai hadviselés a 20. század kezdetétől a 21. század kezdetéig az elektromágneses spektrum minél hatékonyabb sajátoldali felhasználását, valamint a szembenálló fél spektrum használatának az akadályozását jelentette. A 21. század elejére azonban már az elektromágneses spektrumban is megjelent egy sor olyan technikai kihívás, amely komoly dilemma elé állította az elektronikai hadviselési szakembereket. Egyrészt a hatalmas ütemben fejlődő digitális technika és az általuk biztosított új kommunikációs

[28] Latakia városa mellett van az orosz légierő Szíriába települt erőinek egyik legfontosabb légibázisa. Ennek megfelelően természetesen szükséges a bázis, illetve az onnan felszálló repülőgépek védelme. Így a Kraszuha-4 telepítése nem meglepő. A zavaró állomás mellett Sz-300 légvédelmi rakétakomplexumokat is telepítettek a légibázis, illetve az innen nem messze lévő tengeri kikötő védelmi érdekében. [38]

[29] A légideszant csapatok orosz hivatalos megnevezése: ВДВ – Воздушно-десантные войска.

módok[30] jelentik ezt a kihívást, másrészt a korábban említett biztonságpolitikai változásokból eredő kihívások is megmaradtak, sőt fokozódtak. Az olyan fegyveres konfliktusokon kívül, mint például Irak vagy Afganisztán, az orosz-ukrán válság rávilágított, hogy a hagyományos háborús eszközkészletre továbbra is, de modernizált, a 21. század technikai színvonalát elérni képes módon, de szükség van, hiszen sok helyen (pl.: Oroszország, Kína) nem csak megmaradtak a hagyományos fegyverzettel rendelkező hadseregek, hanem ezek tudatos és tervszerű modernizációja miatt hatalmas potenciált jelentenek. Ennek megfelelően a jövőben az elektronikai hadviselésnek mind eszközeiben, mind eljárásaiban nem csak a gyorsreagálású képességek támogatására, nem csak békekikényszerítő és béketámogató műveletekben[31], hanem nagy intenzitású háborús műveletekre is készen kell állnia.

Mindezeken túl a látható és nem látható fény tartományában, technikai eszközökkel végzett információszerzési tevékenységek és ezzel együtt a képi felderítés (Imagery Intelligence – IMINT) hatalmas fejlődése is nyomon követhető az elmúlt 10-15 évben, amely egyrészt a képi felderítő szenzorok hordozóinak (pl. UAV-knek), másrészt maguknak a képalkotó szenzoroknak és eljárásoknak a fejlődése miatt következett be. Az elektronikai hadviselésnek pedig egyrészt erre a spektrumtartományra (a látható és nem látható fény tartományára), a képi felderítő eszközök adatátviteli, adatfeldolgozó, kommunikációs és vezérlő rendszerei elleni tevékenységre, valamint az ezeket az eszközöket hordozó berendezések (sok esetben az említett UAV-k) elleni harcra is fel kell készülnie.

Ugyanakkor a 20. század végén, a 21. század elején számos más, egészen új kihívás is jelen van. Az egyik ilyen kihívást a kibertér és az abban folyó tevékenységek és műveletek jelentik. A kibertér, valamint az elektromágneses spektrum és a kibertéri elektromágneses műveletek meghatározásai, valamint azok összefüggéseinek a feltárása megtörtént az elmúlt években. [40] [41] [42]

A kibertérben megjelenő új technológiák, valamint az új, egyre inkább mindennapos eljárások és szolgáltatások összessége az elektronikai hadviselés számára is több alternatív, de mindenképpen párhuzamos jövőt feltételez. Így a kibertéri elektronikai hadviselés szükségessége már ma jelen van a hadviselésben.[44] Az elektromágneses spektrum és a kibertér átfedése azt is jelenti, hogy az elektronikai hadviselésnek komoly szerepe lesz a számítógép-hálózati műveletekben[32] (pl. annak felderítési, információszerzési fázisában), mert ahogy korábban a katonai vezetés és irányítás a rádiókommunikációt, úgy ma a számítógép-hálózatokat használja alap képességként. Ennek megfelelően, ha a számítógép-hálózatok adatforgalma vezeték nélküli, azaz a rádióhullámok tartományára alapul (akár csak részben is), akkor abba az elektronikai hadviselés – megfelelő technikai eszközök megléte

[30] Olyan megoldások jelentek meg a digitális technikának köszönhetően, mint pl. a kiterjesztett spektrumú adásmódok, vagy például az SDR (Software Defined Radio – Szoftverrádió) technológia.

[31] Meg kell jegyezni, hogy az ilyen műveletekben megjelenő kihívások is komplexek. Új, nem hagyományos kommunikációs és vezetési eszközök jelennek meg az ilyen területeken (pl. a felkelők elleni műveletek), amely eszközök nem katonai, hanem polgári eszközöket, vagy azok bizonyos modifikációit jelentik. Ugyanakkor a nem hagyományos katonai műveletekben megjelennek a nem katonai ECM eszközök is (pl.: Irán által gyártott eszközök), amelyre az egyik legjobb példa Izrael 2006-os libanoni beavatkozása során történt. Ekkor a libanoni erők (elsősorban a Hezbollah), olyan elektronikai hadviselési eszközöket alkalmazott az izraeli hadsereggel szemben, amelyeket nagy valószínűséggel Iránban gyártottak. [43] Ebből levonhatjuk azt a következtetést, amelyet korábban az USA elektronikai hadviselési képességeinél említett DSB szintén elemzései eredményeként jelenített meg, hogy ma már nem csak fejlett országok privilégiuma a legkorszerűbb elektronikai hadviselési eszközök fejlesztése és gyártása.

[32] Számítógép-hálózati műveletek (Computer Network Operations CNO), amelyek az elektronikai hadviseléshez hasonlóan szintén az információs műveletek részét képezik, fő feladatuk a szembenálló fél számítógép-hálózatainak felderítése, onnan információk kinyerése, vagy akár annak működésbeli korlátozása, mindeközben a saját ilyen hálózatok működésének a biztosítása, védelme.

esetén – be tud avatkozni, onnan adatokat tud kinyerni, vagy akár működésében tudja azt akadályozni (pl. zavarással).

A kibertéri elektronikai hadviselési képességek mellett szükséges megőrizni és fejleszteni a hagyományos hadviselési elveknek megfelelő elektronikai hadviselési erőket és eszközöket, valamint az ehhez a képességekhez tartozó eljárásokat[33].[44]

Ennek megfelelően leegyszerűsítve azt is mondhatjuk, hogy az elektronikai hadviselés számára a célok hasonlóak, mint korábban, csak a tartomány (domain) bővült.

KÖVETKEZTETÉSEK

Az elektronikai hadviselés a hagyományos hadviselés összetevői közül napjaink és prognosztizálhatóan a jövő fegyveres konfliktusainak és háborúinak egyik meghatározó tényezője.

Az elmúlt évtizedek, valamint a közelmúlt háborúiban szerzett tapasztalatok arra engednek következtetni, hogy az elektromágneses spektrumban folyó küzdelem a hadviselés elengedhetetlen része. A vezetési fölény megszerzéséhez és így a siker kivívásához pedig szükség van az információs fölényre. Az ukrán konfliktus különösen élesen rávilágított arra a tényre, hogy napjainkban, legyen szó bár aszimmetrikus, vagy hibrid hadviselésről, a javarészt a hagyományos fizikai dimenzióban vívott fegyveres küzdelem lényeges összetevője az elektronikai hadviselés.

A nyugati országok, köztük az Egyesült Államok azonban leépítették, vagy nem az elvárható mértékben fejlesztették a szárazföldi erőik elektronikai hadviselési képességeit. Így az komoly képességvesztést eredményez számukra.

Az ukrajnai konfliktusban, illetve a szíriai háborúban megjelenő – az elmúlt másfél évtizedben hatalmas technikai fejlesztésen és korszerűsítéseken átesett – orosz elektronikai hadviselési eszközök és rendszerek, illetve az ezek által megtestesített képességek figyelmeztető jelzések a számunkra.

A jövő elektronikai hadviselése kettősséget mutat: megmaradnak a hagyományos fegyveres küzdelem során a szárazföldi erőket támogató, ott a vezetési fölény kialakításához nagymértékben hozzájáruló korszerű elektronikai hadviselési eszközök és rendszerek szükségessége, valamint a másik oldalról a kibertér elektromágneses műveleteire alkalmas elektronikai hadviselés eszközei, erői és képességei szintén jelen lesznek a hadseregek arzenáljaiban.

FELHASZNÁLT IRODALOM

[1] Magyar Honvédség Összhaderőnemi Doktrína 3. kiadás. MH Vezetési és Doktrinális Központ kiadványa, 2012.

[2] HAIG Zs., KOVÁCS L., VÁNYA L., VASS S., NÉMETH A.(szerk.): Elektronikai hadviselés. Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[3] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína, 2. kiadás, 2015.

[4] KOVÁCS L.: A légerő elektronikai hadviselése a terrorizmus elleni harcban. Repüléstudományi Közlemények. 20/1. 2008.

[33] Mindezeket ki kell egészíteni a korszerű elektronikai hadviselési elvek szerinti kiképzéssel és felkészítéssel, valamint a felmerülő új technikai igényeket tudományos alapossággal kell megjeleníteni és transzformálni az ipar (haditechnikai ipar) számára, ahhoz, hogy valóban megfelelő – a kihívásokra választ adni képes – elektronikai hadviselési eszközök kerüljenek gyártásra.

[5] BODA J., BOLDIZSÁR G., KOVÁCS L., OROSZ Z., PADÁNYI J., RESPERGER I., SZENES Z.: Fókusz és együttműködés: A hadtudomány kutatási feladatai. Honvédségi Szemle 144/3. 2016.

[6] BLESZITY J., FÖLDI L., HAIG Zs., NEMESLAKI A., RESTÁS Á.: Műszaki kutatások és hatékony kormányzás. Hadmérnök 11/3. 2016.

[7] Electronic Warfare; http://www.nato.int/cps/en/natohq/topics_80906.htm [1] (letöltve: 2016.12.18.)

[8] GORDON, D. E.: Electronic Warfare: Element of Strategy and Multiplier of Combat Power, Pergamon Press, New York, 1981.

[9] HAIG Zs., KOVÁCS L., MUNK S., VÁNYA L.: Az infokommunikációs technológia hatása a hadtudományokra. Nemzeti Közszolgálati Egyetem, Budapest, 2013.

[10] BOKOR I., PAPP I., VÁRHEGYI I.: Elektronikus hadviselés. Műszaki Könyvkiadó, Budapest 1992.

[11] BAKONYI P. (szerk.): Pokorny Hermann vezérezredes: Emlékeim. A láthatatlan hírszerző. Hadtörténelmi Levéltári Kiadványok. http://mek.oszk.hu/02000/02095/html/ (letöltve: 2017.01.05.)

[12] BALOGH P.: Az elektronikai támogatás és a SIGINT helyzete a Magyar Honvédségben. Felderítő Szemle 2013:(1), 2013.

[13] HORVÁTH J.: Elektronikai hadviselés a Magyar Honvédségben. Hadmérnök, 9/1. 2014. http://hadmernok.hu/141_17_horvathj.pdf (letöltve: 2017.01.05.)

[14] Defense Science Board: About DSB: http://www.acq.osd.mil/dsb/index.htm (letöltve: 2017.01.05.)

[15] Report of the Defense Science Board: Study on 21st Century Military Operations in a Complex Electromagnetic Environment, Washington D.C., 2015. http://www.acq.osd.mil/dsb/reports/DSB_SS13--EW_Study.pdf (letöltve: 2017.01.05.)

[16] GOULD, J.: Electronic Warfare: What US Army Can Learn From Ukraine, Defense News, 2015. augusztus 2. http://www.defensenews.com/story/defense/policy-budget/warfare/2015/08/02/us-army-ukraine-russia-electronic-warfare/30913397/ (letöltve: 2017.01.05.)

[17] ACKERMAN R. K.: Consolidation Is the Course for Army Electronic Warfare. Signal, 2013. április 1. http://www.afcea.org/content/?q=consolidation-%E2%80%A8the-course-army-%E2%80%A8electronic-warfare (letöltve: 2017.01.14.)

[18] NSWC Crane Electronic Warfare Center Fact Sheet. http://www.navsea.navy.mil/Portals/103/Documents/NSWC_Crane/EW%20Air%20Fact%20Sheet%20(no%20mark).pdf (letöltve: 2017.01.05.)

[19] United States Army Acquisiton Support Center: Guardrail Common Sensor (GR/CS). http://asc.army.mil/web/portfolio-item/guardrail-common-sensor-grcs/ (letöltve: 2017.01.05.)

[20] Raytheon News Release: Raytheon delivers electronic jamming capability for Gray Eagle UAS. http://investor.raytheon.com/phoenix.zhtml?c=84193&p=irol-newsArticle&ID=1819171 (letöltve: 2017.01.05.)

[21] Program Executive Office Intelligence Electronic Warfare & Sensors: Electronic Warfare & Cyber, Multi-Function Electronic Warfare – MFEW https://peoiews.army.mil/electronic-warfare-cyber (letöltve: 2017.01.05.)

[22] MCLEARY, P.: Russia's Winning the Electronic War. Foreign Policy, 2015. október 21. http://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/ (letöltve: 2017.01.05.)

[23] Kret News Release: http://oblik.msk.ru/en/news_and_media/ (letöltve: 2017.01.05.)

[24] Kret News Release: http://oblik.msk.ru/en/news/10246/ (letöltve: 2017.01.05.)

[25] VASILESCU, V.: Sistemul de bruiaj rusesc Richag-AV vs drona americana RQ-170 Sentinel. Ziarul de Garda, 2015. április 15. http://www.ziaruldegarda.ro/sistemul-de-bruiaj-rusesc-richag-av-vs-drona-americana-rq-170-sentinel/ (letöltve: 2017.01.05.)

[26] ILLÉS Z.: Mi-8 Hip, a forgószárnyas mindenes. http://www.hunaf.hu/rovatok/fegyverek/mi8/hip/ (letöltve: 2017.01.19.)

[27] Deagel: Rychag-AV. http://www.deagel.com/Ship-Protection-Systems/Richag-AV_a003124001.aspx (letöltve: 2017.01.05.)

[28] Kret: Kraszuha. http://www.kret.com/en/product/12/ (letöltve: 2015.11.14.)

[29] Defense Blog: New Russian Electronic Warfare System «Krasukha» at TVM-2014. http://defence-blog.com/news/new-russian-electronic-warfare-system-krasukha-at-tvm-2014.html (letöltve: 2017.01.05.)

[30] КРЭТ передал армии секретное оружие https://www.youtube.com/watch?v=wdzI1iK4xxI (letöltve: 2017.01.05.)

[31] US Air Force: Popular Fact Sheets: E-8C Joint Stars. http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104507/e-8c-joint-stars.aspx (letöltve: 2017.01.05.)

[32] Pakistan Defense: Russia Displays Innovative Asymmetric Counter Stealth Systems at MAKS-2015. http://defence.pk/threads/russia-displays-innovative-asymmetric-counter-stealth-systems-at-maks-2015.395964/ (letöltve: 2017.01.05.)

[33] GlobalSecurity.org: 9K720 Iskander-M (SS-26 Stone) http://www.globalsecurity.org/wmd/world/russia/ss-26.htm (letöltve: 2017.01.05.)

[34] Valka.cz: http://en.valka.cz/topic/view/38028/SOV-SPN-30-prostredek-REB (letöltve: 2017.01.05.)

[35] The Boresight Air Power Focus. http://theboresight.blogspot.hu/2016/07/the-end-of-primacy-russian-federation.html (letöltve: 2017.01.05.)

[36] Army Recognition: Army in the world - Russia Electronic Warfare units. http://www.armyrecognition.com/armies_in_the_world_analysis_focus/russian_airborn

e_troops_are_ready_to_use_electronic_warfare_ew_vehicles_infauna_and_leer-2_0410124.html (letöltve: 2017.01.05.)

[37] Kret News Release: http://rostec.ru/en/news/4516361 (letöltve: 2017.01.05.)

[38] BBC News: Syria conflict: Russia sends missile system to Tartus base. 2016. október 4. http://www.bbc.com/news/world-middle-east-37557138 (letöltve: 2017.01.05.)

[39] VÁNYA L.: Российские средства и способы радиоэлектронной борьбы в интересах защиты бронетанковых машин. Hadmérnök. 9/2 (2014). http://hadmernok.hu/142_32_vanyal.pdf (letöltve: 2017.01.05.)

[40] HAIG Zs.: Információ - társadalom – biztonság. NKE Szolgáltató Kft., Budapest, 2015.

[41] FM 3-38: Cyber Electromagnetic Activities. Headquarters Department of Army, 2014. https://fas.org/irp/doddir/army/fm3-38.pdf (letöltve: 2017.01.05.)

[42] POMERLEAU. M.: DoD could declare the spectrum a domain of warfare. Defense Systems, 2015. december 10. https://defensesystems.com/articles/2015/12/10/dod-could-declare-spectrum-an-operational-domain.aspx?s=ds_141215 (letöltve: 2017.01.05.)

[43] ESHEL, D.: Hezbollah's Intelligence War: Assessment of the Second Lebanon, Defense Update, 2007. http://defense-update.com/analysis/lebanon_war_1.htm (letöltve: 2017.01.05.)

[44] VÁNYA L.: Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre. Doktori (PhD) értekezés. ZMNE, Budapest, 2003. http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2003/vanya_laszlo.pdf (letöltve: 2017.01.05.)