INFORMATION OPERATIONS AND INFORMATION WARFARE

INFORMÁCIÓS MŰVELETEK ÉS INFORMÁCIÓS HADVISELÉS

PÁL Anita Brigitta[1]

Abstract

Information warfare has become crucial in the art of war and military practice of the 21st century. With the results of the fourth industrial revolution, our imagination of war and the primary goals set in warfare, have also changed. Information has become one of the biggest value before impact measurements. In part, disinformation and sabotage have also entered the arenas of the games in the art of war, controlled by algorithms. Parallel with technological development, information warfare has been redefined. Automated weapon systems, drones, firewalls, viruses, radars, and programs that can be used to influence the physical and virtual battlefield have become an essential part of cyber warfare. The current four-dimensional battlefield (air, land, water and space) is connected by the information battlefield.

Keywords

information warfare, virtual warfare, digital revolution, cyber warfare, military leadership, information operations

Absztrakt

Az információs hadviselés döntő jelentőségűvé vált a 21. század hadművészetében és katonai gyakorlatában. A negyedik ipari forradalom hozadékaival a háborúról alkotott képünk és a hadviselésben kitűzött elsődleges célok is megváltoztak. Az információ lett a legnagyobb érték a csapásmérések előtt. Részint a dezinformáció és a szabotálás is bekerült a játszmák színterei közé az algoritmusok által vezérelt harcok művészetében. A technológiai fejlődéssel párhuzamosan újra definiálták az információs hadviselést. A kiberhadviselés elengedhetetlen részévé váltak az automatizált fegyverrendszerek, a drónok, tűzfalak, vírusok, radarok, valamint az olyan programok, amelyekkel befolyásolni lehet mind a fizikai- mind a virtuális hadszínteret. A jelenkori négydimenziós hadszínteret (levegő, szárazföld, víz és űr) az információs hadszíntér kapcsolja össze.

Kulcsszavak

információs hadviselés, információs műveletek, virtuális hadviselés, digitális forradalom, kiberháború, katonai vezetés

[1] pal.anita@hm.gov.hu | ORCID: 0000-0003-4750-193X | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

GLOBALIZÁCIÓ

„Veszélyektől, vagy bántódástól mentes, zavartalan állapot. A biztonság fogalma mára általánosabb és összetettebb lett, és a biztonsági kockázatok elemzése során a terület specifikus sajátosságait is figyelembe kell venni. A biztonság megértése ma már sokkal összetettebb, mint korábban, és a különböző területeken alkalmazott biztonsági intézkedések és protokollok eltérőek lehetnek egymástól" [1]

A globalizáció folyamatai egy sor fenyegetéssel járulnak hozzá a biztonságpolitika és a nemzeti biztonsági stratégiák mihamarabbi integrációjához. A külpolitikán keresztül a védelempolitikáig, a legnagyobb kihívást szerintem az adat-, illetve az információbiztonság jelenti. Világunkat és egymáshoz való kapcsolódásunkat láthatatlan hálózatok sorai övezik. Világunk globalizációs folyamati között a technológiai fejlődés olyan ütemben halad, amit nem látott még a világ.

Az információs műveletekben meghatározó szerep jut a műveleti tervezések folyamatainak. Az információs technológia gyors fejlődése új szerepet határozott meg a katonai földrajz területén. Az állami vezetés művészetében a geopolitika és geostratégia fontos szerepet játszik, míg a földrajz a logisztika, térképészeti elemzés és műveleti tervezés szempontjából meghatározó tényező. Ugyanakkor a stratégiai földrajz, amely elsődlegesen határozza meg a nemzetvédelmi és a nemzeti biztonsági magatartást, súlya az idők folyamán csökkent. [2]

A globalizáció hatására a biztonság fogalma megváltozott, és már nem csak a területi érdekek mentén alakul. Az államoknak figyelmet kell fordítaniuk az összekapcsolódás és a kölcsönös függőség kérdéseire, nem csak a saját területükön zajló eseményekre koncentrálva. A belbiztonsági kérdések tekintetében a helyi konfliktusok mellett egyre fontosabbak a regionális és globális összefüggések, amelyek között a tömeges bevándorlás és a terrorizmus elleni harcok különösen kiemelkedőek.

Az információs technológia fejlődése számos új kihívást jelent a hadviselésben, amelyek tovább alakítják a korábbi területi határokat. A kiberháború és az információs hadviselés által teremtett új hadszínterek nem ragaszkodnak a hagyományos földrajzi határokhoz, és jelentősen átformálják a nemzetbiztonsági szemléletet. Az információs technológia fejlődése által az új hadszínterek (levegő, szárazföld, víz és űr) határai tovább bővültek és összemosódnak az információs hadszíntér határaival. Az egyre növekvő kibertér már teljes mértékben globálissá vált, és a szakértők egyetértenek abban, hogy a hagyományos, lineáris hadviselési formák kiegészítésére szükség van a nem lineáris konfliktusokkal keleten és nyugaton egyaránt. Azáltal, hogy a társadalmak közötti kapcsolatok dimenziói sokrétűvé váltak (politikai, gazdasági, infrastrukturális, média- és pszichológiai dimenziók), a nemzeti biztonság már nem csak határokkal határozható meg, és az ellenük irányuló támadások sem csak a terület elfoglalásával vagy megtartásával jellemezhetők. [3]

DIGITÁLIS FORRADALOM

Kereken fél évszázada hódít teret Moore törvénye, miszerint az integrált áramkörök összetettsége exponenciális teljesítménynövekedést mutat. A digitális forradalom, amit "harmadik és negyedik ipari forradalom" néven is ismerünk, az áttörést jelenti, amit a számítógépek és a digitalizáció hozott az élet számos területére a 20. század végétől kezdve.

Az integrált áramkörök és mikrocsipek feltalálása megnyitotta az utat a digitális fejlődés előtt. A technológiai eszközök teljesítményének folyamatosan növekedése lehetővé tette a termelés rugalmas automatizálását. Az internet, amely egy globális kommunikációs hálózatként működik, mára megszüntette a tér és idő korlátait.

Az informatikai forradalom, melyet a számítógép és a mikroprocesszorok bevezetése elindított, olyan mértékű hatást gyakorolt a társadalmi életre, hogy ma már az informatikai eszközök használata szinte mindenhol magától értetődőnek tekinthető - legyen szó munkahelyről, otthonról, vagy akár az oktatásról. Minden olyan digitális szolgáltatást amit ingyen használunk, ott gyakorlatilag mi magunk válunk áruvá a titkainkkal és az életünk privát részeivel fizetünk, amit aztán a mesterséges intelligencia által futatott algoritmusok fognak felhasználni, hogy még célozottabb reklámokat kaphassunk.

Az ún. „digitális javak", azaz a szoftverek és a „digitalizált információk" kiemelt jelentőséget kaptak. A digitális forradalom hatására ma már az állami és magánszféra egyaránt elkötelezett a digitális technológiák világa iránt, amelynek használatával egy sor előny és árnyoldal is társul.

Az egyre növekvő globális kibertér az új típusú fenyegetések egyre bővülő kínálatát nyújtja, valamint a nemzetközi és állami szinteken egyaránt új fajta szervezetek és kibervédelmi jogszabályok megszületését eredményezték.[4] Azonban nem szabad figyelmen kívül hagynunk, hogy a digitális javak jelentős előnyei alapvetően új szemléletet követelnek meg, amelynek eredményeként komoly jogi és szerzői jogi kihívásokat kell megoldani. [5]

Ha az információs műveletek során lehetőségünk van információs és vezetési előnyre szert tenni a ellenfelekkel szemben, akkor az újonnan létrejövő információk új módon való felhasználása hatékony eszköze lehet a katonai műveletek sikeres végrehajtásának.

Az információs kor és az XXI. század hadviselése szervesen összefonódik, amely megköveteli az információs műveletek elméleti és gyakorlati kérdéseinek fokozott figyelmét.[6] Ezek a műveletek természetes evolúciója során bonyolult, integrált és komplex katonai tevékenységekké válnak, amelyek az információs hadszíntéren megoldandó feladatokhoz különböző tudományterületeket ötvöznek.

A Magyar Honvédség vezetése is felismerte az információs műveletek fontosságát, aminek következményeként külön figyelemmel szenteltek egy fejezetet a MH Összhaderőnemi Doktrínájában, hasonlóan a NATO tagországokhoz. [7]

INFORMÁCIÓS MŰVELETEK HATÁSÁNAK KIHASZNÁLÁSA

Az információs kor és az információs társadalom fejlődésével olyan intellektuális és anyagi erőforrások váltak hozzáférhetővé, amelyek újraértelmezték a hadviselési stratégiákat. Az információs technikai és technológiai forradalom vívmányai gyökeres átalakítást hoztak mindazon elvek és eljárásokat illetően, amelyeket idáig vallottunk és alkalmaztunk a hadügy területén. A fejlődés során egyértelműen kirajzolódott, hogy a korszerű katonai műveletekben, az információ megléte és hiánya, döntő jelentőséggel bír. Az információ hatékony megszerzése és felhasználása komoly előnyöket biztosít a haderő számára, így mindkét fél nagy erőfeszítéseket tesz annak érdekében, hogy információs rendszerei hatékonyabban működjenek, és teljes mértékben kihasználják azok képességeit. E cél érdekében az

információ már nem csak a vezetés és fegyverirányítás során használatos, hanem mint egy nem-kinetikus energia alapú fegyver is alkalmazható. Az új kihívások számos magasabb követelményt állítanak a társadalom és a katonák számára. [8]

Az adat megőrzése és azok helyes felhasználása prioritássá válik olyan hierarchizált és kereszthivatkozásokat tartalmazó struktúrákban, amelyek lehetővé teszik, hogy az adatból információ, abból pedig bölcsesség alakuljon ki. Az internet sokrétű funkcionalitása nemcsak az információ megosztását és a közösségi média használatát teszi lehetővé, hanem egyben a pénzügyi csalások és a kiberbűnözés olyan platformjává vált, amelyet a hálózatba kapcsolt bűnözői csoportok és terrorista szervezetek is nagymértékben ki tudnak használni. [9]

Világunkban minden tevékenységünkkel szinte már adatot generálunk. Takács Gergely, a „Big Data (adatvezérelt) elemzési módszerek alkalmazása a nemzetbiztonsági szférában" című tanulmányának a bevezetésében úgy írja le a Big Data jelenségét, ami olyan exponenciális és folyamatosan keletkező adatok mennyiségét generálja, amelyeket a hagyományos eszközökkel már nem lehet menedzselni, feldolgozni vagy tárolni. Etikai szempontból ráadásul a rendszernek vannak hiányosságai. Stigmatizálás híján egy algoritmus nehezen tud különbséget tenni kódok és igazságok között.

A Big Data módszerek és technológiák lehetővé teszik a rendkívül nagy adatmennyiségek feldolgozását az adatkezelés és feldolgozás párhuzamosítása révén. Ennek lényege az olyan logikailag összekapcsolt géphálózatokon működő algoritmusok alkalmazása, melyek tér- és időbeli korlátok nélkül képesek tevékenykedni. Íly módon az előrejelző elemzések és a predektív analítika alapján hozzásegíthet a bűnmegelőzésben, vagy akár a terrorelhárításban is. [10]

A koalíciós műveletek tapasztalatainak értékelés során a NATO vezetői megállapították, hogy a győzelem elérése érdekében az információs műveletek növekvő jelentőséggel bírnak, míg a precíziós felderítés és fegyverek használata minden haderőnem számára létfontosságúvá vált. Az információs műveletek azonban stratégiai szinten is megnőtt jelentőségre tettek szert, és ezáltal az ezekre adott válaszok is hasonló komolysággal bírnak, különösen azok, amelyek számítógépes hálózatokat céloznak meg. Ezt jól példázza, hogy Oroszország néhány évvel ezelőtt figyelmeztette az Amerikai Egyesült Államokat, hogy a számítógépes hálózati támadásokat egyenértékűnek tekintik a nukleáris támadással, és ennek megfelelően válaszolnak majd rá.

„A katonai létesítményeknek tudomásul kellene venniük, hogy a csata harctere változik. Az információ, mint a konfliktusok és a verseny dimenziója, felcsigázta a jövőbeni nemzetbiztonsági szférák változatosságának palettáját. Legalább olyan fontos élenjárója, és legalább annyira egyenértékű, mint a levegő, a föld, a tenger és az űr dimenziója. Olyan elméletek kidolgozásához kezdtek, mely alátámasztja az Információs műveletek szellemi szükségességét, amely választ ad háborús kérdésekben napjaink digitális korában." [11]

Az új kor hadseregeinek lényeges jegyei közé tartoznak az automatizált irányítási funkciókkal ellátott, nagy pontosságú fegyverek, valamint hatékony felderítési, navigációs és információfeldolgozási módszerek, amelyek integrált alkalmazása már napjainkban is alapvető fontosságú az eredményes hadviseléshez.

Az aktív tevékenységek dinamikusan változó környezetében az információs fölény kialakítása és fenntartása létfontosságú a kitűzött célok eléréséhez. Ennek megfelelően, az információs műveletek (information operations) és az információs hadviselés (information

warfare) fogalmait használják annak érdekében, hogy meghatározzák azokat az eljárásokat, amelyek az információs fölény megteremtéséhez és megtartásához szükségesek.

INFORMÁCIÓS HADVISELÉS

„Az információs hadviselés az információs fölény elérése érdekében végrehajtott, a szemben álló fél információi, információalapú folyamatai, információs rendszerei és számítógépes hálózatai befolyásolására, illetve a saját információk, információalapú folyamatok, információs rendszerek és számítógépes hálózatok védelmére irányuló tevékenységek összessége.”[12]

Az információs hadviselés az ellenféllel szembeni információelőny megszerzése érdekében végrehajtott művelet. Ez abból áll, hogy ellenőrzik a saját információs terüket, megvédik a saját információkhoz való hozzáférést, miközben megszerzik és felhasználják az ellenfél információit, megsemmisítik az információs rendszereiket és megzavarják az információáramlást. Az információs hadviselés nem új jelenség, mégis innovatív elemeket tartalmaz a technológiai fejlődés hatása, amelynek eredményeként információkat terjesztenek gyorsabban és nagyobb léptékben.[13]

Az információs hadviselés önálló katonai fogalmaként az 1990-91-es Öböl-háborúk és az azt követő balkáni, majd afganisztáni konfliktusok során jelent meg először a hadviselés színterén. Később, az aszimmetrikus háború kapcsán, ahol kiderült, hogy a katonai és nem katonai szakterületek szoros kapcsolatban vannak egymással és több helyen átfedik egymást. Az éles háttér elmosódik a harctér és a hátország között. Továbbá a vezetékes és a vezeték nélküli, valamint űrkommunikációs hálózatokba kapcsolt, számítógép által vezérelt kritikus infrastruktúrák működésének korlátozása már nem csak kinetikus tűzeszközökkel (pusztító hatású légi, tüzérségi vagy rakétacsapásokkal) lehetséges, hanem nem kinetikus számítógép hálózati eszközökkel (korlátozó programokkal) is.

A hidegháború óta rendkívüli jelentősége van a technikai-hírszerzési és a technikai együttműködési rendszerek kapcsolata között, hogy ellenőrizni lehessen a szemben álló fél tevékenységét és kommunikációját. Az amerikai és brit szolgálatok kifejlesztették a tömeges lehallgatás képességét, amely lehetővé tette, hogy az Öböl-háború során először az információs hadviselés szabályai érvényesüljenek. Az újonnan megalakulkó információs háborúval, más néven vezetési háborúval (information war - command and control war), egy újszerű és teljesen eltérő módszer alakult ki a háború lefolytatására, amelyben az információs erőforrások használata kulcsfontosságúvá vált. Az úgynevezett információs hadviselés (information warfare) tartalmazza az integrált tudást tartalmazó információk megszerzését és felhasználását, valamint a küzdő felek is ezek védelme érdekében vívják meg a harcot.

Az enyhülő hidegháború és az atomerő visszaszorításával egyre fontosabbá váltak a hagyományos robbanóanyaggal felszerelt fegyverek, melyek fejlett irányítási rendszerekkel rendelkeznek, így nagy távolságról célzottan alkalmazhatóak. A rendszerek zavarása, befolyásolása vagy bénítása stratégiai előnyhöz vezethet valamelyik küzdő fél számára, mivel lehetővé teszi az érzékeny mélységi objektumok megsemmisítését. Ebben az összefüggésben azonban egy ország fegyveres agresszivitása korlátozottá válhat, mivel a saját területén lévő objektumok könnyen célpontjává válhatnak a korszerű repülő- és rakétatechnikai eszközöknek. A hidegháború alatt ez a tényező biztonsági szempontból is fontos volt, mivel elkerülte a közvetlen fegyveres konfliktus kialakulását a két nagyhatalom között és a jövőben is fontos visszatartó erőként szolgálhat. [14]

TERRORIZMUS

Az elmúlt évtizedek információs forradalma főként a csúcstechnológiával foglalkozó "infokommunikációs" szektorban tapasztalható. Az egyik ilyen példa a dróntechnológia gyors fejlődése, amely felveti a nemzetbiztonsági kockázatok és a drónok legitim felhasználásának kérdését. A terroristák gyakran használják a dróntechnológiát támadásokra, megfigyelésre, propagandavideók készítésére vagy zavarásra. Jelenleg 4 terrorszervezet rendelkezik azonosítható drónprogrammal: a Hezbollah, a Hamász, az Iszlám Állam és a Jabhat Fateh al-Sham.[15] Fontos kiemelni, hogy a terrorizmus növekedése szorosan összefügg a globalizáció és a technológiai fejlődés jelenségeivel. Az átfogó összekapcsolódásuk gyorsította az elektronikus pénzügyi átutalásokat, amelyek radikálisan átalakították a pénzügyi szektor működését, és hatással voltak a társadalmi tevékenységekre is. Az új technológiai vívmányok elterjedése széles körűvé vált, így az 1990-es évek posztindusztriális társadalmaiból az első információs társadalmak jöttek létre.

A terrorizmus elleni háború frontvonala nem mindig a háborús helyeken zajlik, hanem európa fővárosaiba, a szervereken, az összeköttetésekben. A modern harcmező mindent behálóz. Vagyis többé nem kell lövészárkokban megbújni meg bombákat kerülgetni. Minden generációnak megvan a maga hézaga amiből a következő nemzedék korrigálva a hiányosságokat prevenciós előnnyel indulhat neki a fejlesztéseknek. A cél mindig a rendszer biztonságos működésének biztosítása kell, hogy legyen.

Az új típusú katonai konfliktusok és háborúk ma már a világ szeme láttára zajlanak. Az elmúlt másfél évtizedben a katonai technológia folyamatos fejlesztése az idő és tér összesűrűsödéséhez vezetett, amelynek következtében a távoli akciók helyi hatásokat váltanak ki és fordítva. Az interdependens nemzetközi rendszer egy összekapcsolódott világrendet hozott létre, amelyben a helyi és regionális katonai fejlemények potenciálisan globális hatásúak lehetnek. A szakértők felismerték, hogy a világ bármely pontján kialakuló zűrzavar és konfliktus azonnal elérheti a globális közönséget, az információs technológia robbanásszerű terjedésének köszönhetően. A média fontossága nemcsak a nyugati nagyhatalmak és a feltörekvő államok (például Russia Today, Al Jazeera) számára nyilvánvaló, hanem a terrorista szervezetek (például ISIS) is teljes mértékben kihasználják azt. [16]

A nemzetközi kapcsolatok európai folyóiratában említést tesznek a paneladatok elemzése alapján arról, hogy a hazai terrortámadások és a belföldi és transznacionális terrorista szervezetek által észlelt fenyegetések fokozzák a katonai részvételt a politikában.

A terrortámadások és az erőszakkal való megfélemlítés lehetőséget biztosít a politikába való katonai beavatkozásra, az állami intézmények ellenőrzésének átvétele nélkül. Két olyan mechanizmust említ Vincenzo Bove, amelyek révén a terrorizmus befolyásolja a katonai részvételt a politikában: Amikor a terrorizmus elleni küzdelemhez és a nemzetbiztonság megerősítéséhez, valamint a fegyveres erők „bevonásához" a kormányzati hatóságoknak katonai szakértelemre van szükségük a politikához, és amikor az állam fegyveres szereplői kihasználják az információs előnyüket a civilekkel és a hatóságokkal szemben, hogy „belenyomják" magukat a politikai jelenlétbe és a politikaalkotásba.[17]

Azonban, ha az nemzetközi terrorizmus elleni küzdelemről van szó, akkor fel kell ismernünk, hogy a katonai erő alkalmazása csak egy, az összetett stratégiai eszközök között. A terrorizmus elleni küzdelem többdimenziós tevékenység, amelyet mind nemzeti, mind

nemzetközi szinten kellene összehangolni. Ideális esetben ez egy összehangolt válságreagálási stratégia lenne, amely politikai, gazdasági, diplomáciai, titkosszolgálati, adminisztratív, felderítő, rendőri és katonai megoldásokat kombinál. [18]

KIBERHÁBORÚ

A kiberhadviselés az állami szereplők által kezdeményezett kibertámadások összefoglaló neve, amelynek lényege, hogy az államok az információs technológiai fejlődést egyre gyakrabban használják fel a politikai és katonai előnyök elérésére. [19] A NATO a kiberhadviselést hadtudományi szempontból, az információs műveletek részének tekinti, amelyek célja az információs fölény elérése. Az ilyen műveletek lehetnek támadó jellegűek, amikor az ellenséges hálózatokra irányulnak, vagy védekezőek, amikor a saját rendszerek biztonságát kívánják megőrizni. Azonban fontos kiemelni, hogy a kiber-hadviselés nemzetközi jogi szempontból csak akkor értelmezhető, ha az elkövető állam kiléte egyértelműen azonosítható. [20]

Egy nemzetnek a kibertérben megnyilvánuló hatalmát a National Cyber Power Index összetett formula szerint értékeli. Olyan kritikus faktorokat vesz számításba, mint a belső csoportok megfigyelése, a nemzeti kiberbiztonsági erők megerősítése, a nemzetközi normák és szabályok kialakításában való részvétel és azok hatékony definiálása, az információs környezet szabályozása, a nemzetbiztonsági erők külföldi információgyűjtési képessége, az ellenséges kibertámadásokra való hatékony válaszlépés, valamint az ipar és a kereskedelem digitális növekedésének mértéke. [21]

A kibertér és az ehhez kapcsolódó új technológiák fontos területét képezik az információs hadviselésnek. A kiberháborús tevékenységek állhatnak kibertámadásokból, az ellenfél információs rendszereinek megsemmisítéséből, de magukban foglalhatnak úgynevezett társadalmi kibertámadásokat is, azáltal, hogy az emberek tudatában sajátos képet alkotnak meg a világról, összhangban az adott ország által folytatott információs háború céljaival. [22]

Az információs hadviselésnek azon vonatkozásai, amelyek a vezetési-fegyverirányítási és navigációs rendszerek megbontására és védelmére irányulnak, jelenleg az egyik leghatékonyabb hadviselési eljárások közé tartoznak. Az 1990-91-es Öböl-háború tapasztalatai egyértelműen igazolták a több hónapos légi és elektronikai csapások elsődleges célpontjainak - a tömegpusztító fegyvereken, repülőtereken és rakétakilövő-állásokon túl - az ellenséges felderítési (lokátor), kommunikációs és fegyverirányítási képességeinek bénítását. Az információs hadviselés másik jelentős elemének, a saját vezetési rendszer hatékony alkalmazásának köszönhetően, a szárazföldi hadműveletek során az ellenséges erők dezorganizációja, és nem pedig teljes megsemmisítése, segítette a szövetséges erőknek jelentős ellenállással szembeni sikerességüket.

Bár az Öböl-háború nem mutatta meg az információs hadviselés minden aspektusát, így például a polgári célú információs rendszerek zavarásának és bénításának gazdasági károkat okozó hatásait, vagy politikai instabilitást okozó képességeit, az elektronikus felderítésnek a siker döntő tényezőjeként bizonyult. Az elektronikai eszközökkel gyűjtött műholdas és egyéb felderítési információk hatalmas tömege egyértelműen gazdagította a hadművészet elméletét. Az elektronikai felderítés nélkülözhetetlen eleme a korszerű hadviselésnek, és bebizonyította, hogy az információs hadviselés eljárásai között az egyik legfontosabb.

Az információs hadviselés egy újfajta stratégia, amelynek célja azonos a hagyományos hadviseléssel - azaz a struktúrák megtörésével vagy megőrzésével - azonban módszerei és eszközei jelentős mértékben eltérnek a hagyományos hadviseléstől. Míg a hagyományos hadviselés főként a harcoló csapatok, a végrehajtó szakaszok, a műszaki zárrendszerek és a logisztikai bázisok megsemmisítésére összpontosít, addig az információs hadviselés elsődlegesen az alakulatok vezetési és irányítási rendszerének feltérképezésére, támadására, alkalmazására és védelmére irányul sajátos eszköz- és eljárásrendszerével.

A hagyományos és az információs hadviselés egymást kiegészítik és támogatják, azonban az információs hadviselés rendszere - mint a hadművészet egy része - fokozatosan előtérbe kerül és döntő tényezővé válik a háborúk eredményes megvívásában a társadalmak és haderők fejlődésével párhuzamosan.

„Az ellenség harcoló csapatainak pusztítása nélkül háborús körülmények között nem érhető el tartós siker. Az információs hadviselés alkalmazása azonban lehetővé teszi a győzelem kivívását lényegesen kevesebb erőforrás bevonásával, a veszteségek jelentős mérséklését, és a katonai helyzetnek a saját csapatok javára fordítását."[23]

INFORMÁCIÓS HADVISELÉS ÉS A KATONAI VEZETÉS ELMÉLETÉNEK KAPCSOLATA

Az ellenség információs hozzáférési lehetőségeinek megszüntetése önmagában csak korlátozott értékű, ha nem jár együtt a saját információs képességek kialakításának, továbbfejlesztésének és hatékony alkalmazásának szorgalmazásával. [24]

Az információs hadviselés a katonai vezetés elméletének gazdagító eleme, amelynek meghatározó területei az információfeldolgozási rendszerek fejlesztése és üzemeltetése. Az ilyen tevékenységek célja az ellenséges haderő információs folyamatainak támadása és a saját információs képességek védelme. Az információs hadviselés megköveteli a saját információs rendszer fejlesztésének és üzemeltetésének szigorú szabályozását, beleértve az információ típusát, tartalmát és formáját, az információ áramlását, feldolgozását és rendelkezésre bocsátását. A szervezetek az információs hadviselés módszereinek kidolgozásával gazdagítják a katonai vezetés elméletét, hogy hatékonyabban védelmezhessék és használhassák információs képességeiket.

Az összehangolt katonai informatikai rendszereknek képesnek kell lenniük az autonóm működésre, miközben együtt kell működniük a többnemzetiségű összhaderőnemi csoportosítás (CJTF-*Combined Joint Task Force*) más összetevőivel, hogy biztosítsák a művelet sikerét. Ezt az összehangolt rendszert "szövetségnek" nevezik, amely dinamikusan változik az információs környezet változásaihoz igazodva. Az együttműködő információs rendszerek által alkotott szövetségek összetétele nem állandó, és egy adott rendszernek más és más rendszerekkel kell interoperábilis módon együttműködnie a körülményeknek megfelelően. [25]

Specifikus szakértők képzése mellett helye lenne átfogó és központosított információbiztonsági rendszerek és berendezések folyamatos fejlesztésének és erősítésének, mely a szolidarizmus jegyében képesek azonnali végrehajtások megosztására és biztosítani tudják az összehangolt nemzetközi cselekvőképességet a reziliencia, a versenyképesség és a digitális autonómia megerősítése jegyében.

INFORMÁCIÓS HÁBORÚ ÉS AZ INTERNET KAPCSOLATA

Az Internet kibővíti az adatgyűjtés lehetőségeit és spektrumait, illetve az információvédelem és az információ megzavarásának lehetőségeit. Megkönnyíti az adott ország állampolgárainak és a nemzetközi közösség tagjainak a részvételt ebben a játszmában a világ bármely pontjában tekintettel a kommunikáció sebességére.

A közösségi oldalak értékes információforrást jelentenek azokról a célcsoportokról is, amelyeknek a félretájékoztatási szándék címezve van. Ennek megfelelően az Információs hadviselés felhasznál:

- úgynevezett trollgyárakat. Ezek szervezetek, akik a célnak megfelelően lobby kommenteket tesznek közzé hamis profilok felhasználásával a közösségi médiában.
- Felhasznál továbbá botokat. Ez egy úgynevezett automatizált hírlevélküldő program, ami bizonyos kulcsszó megjelenésekre generálja üzeneteit.
- Továbbá felhasznál hamis híreket a médiafelhasználók félrevezetésére/dezinformációjára.[26]

A médiahasználók az úgynevezett hagyományos média segítségével áldozatává válnak az internetes sebezhetőség széles spektrumának az információs háborúban. A propaganda kampányok és a dezinformációk számos médiaüzenetben kódolva vannak, beleértve a hagyományos- és a közösségi médiát is. A médiahasználók egyre inkább tudatában vannak ennek a dezinformációs tevékenységnek, amelyek a valóság felfogásának befolyásolására irányulnak.

Az orosz elképzelésekben az információs hadviselésnek két fő – egymást kiegészítő oldala – létezik: „az információs-technikai és az információs-pszichológiai hadviselés. Az információs-technikai hadviselés döntően a nyugati terminológia szerinti számítógéphálózati hadviselést és az elektronikai hadviselést foglalja magában, beleértve az információs rendszerek technikai eszközökkel történő támadását vagy védelmét. Az információs-pszichológiai hadviselés pedig a közvélemény és a tömegek tudatának befolyásolását, a kognitív folyamatok manipulálását, a politikai és katonai döntéshozatali folyamatok lassítását és bénítását, végül a kedvező politikai hatások kiváltását célozza.” [27]

Talán az Információ a legújabb harci dimenzió a fegyveres erők között. Sok elmélet szól arról, hogy egy információs korszak kezdetén vagyunk. Ugyan megváltoztak a harcászati eszközök, a végső cél ugyanaz maradt: meghódítani az ellenfelet. Az információs kor új lehetőségeket, és ezzel együtt új célpontokat is teremtett, ami megváltoztatja a 21. század háborúinak a harcmódját.

Például mi történik, amikor az új harcmező határvonalává az információ válik, amelyek alapján a parancsnokok meghozzák kritikus döntéseiket? György Gilder, a The Quantum Revolution in Economics and Technology szerzője elmondta: „a legértékesebb tőke napjainkban az emberi elme és a szellemi tőkéje.” [28]

Gordon Sullivan tábornok szerint „az információ, a győzelem valutája a hadszíntéren.”[29] Az információ értékes, de csak akkor hasznos, ha megfelelően kommunikáljuk. A hatékony kommunikáció nem csak azt jelenti, hogy az információhoz hozzáférünk, hanem azt is, hogy megosztjuk a megfelelő emberekkel. A kommunikáció fő célja az információ közzététele, amely meghatározza annak jelentőségét és értékét. [30]

Az információgyűjtés ma már nem csupán az általunk önkéntesen megadott információkból áll. Az internet világában nincsenek ingyenes dolgok - a meséktől kezdve az alkalmazásokon át a szolgáltatásokig mindenért valamilyen formában fizetünk, akár csak az adatainkkal is. A mobiltelefonok rögzítik az általunk felkeresett helyeket, keresési szokásainkat, míg a hűségkártyáink nyomon követik vásárlási szokásainkat. Mindennapi tevékenységeink során jelentős mennyiségű adatot termelünk, amelyek nagy része automatikusan felkerül a felhőbe. Az adatszerver tulajdonosa teljes hozzáférést biztosít az adatokhoz, amelyeket adatbrókerek harmadik felek részére el is adhatnak. [31]

Az elmúlt években bekövetkezett technológiai előrelépés lehetővé tette az információs hadviselés számos formájának alkalmazását, amelyek révén emberek milliói célponttá válhatnak valós időben, bármilyen nyelven és országhatártól függetlenül. A folyamatos technikai fejlődés - kiterjesztett és virtuális valóság technológiája, mesterséges intelligencia fejlesztések, propagandaterjesztés automatizált lehetőségei, úgynevezett personal management szoftverek - valószínűleg növelni fogja az információs technológiák szerepét a stratégiai célok eléréséhez szükséges versengésben. [32]

FELHASZNÁLT IRODALOM

[1] https://www.britannica.com/topic/security

[2] Szenes Zoltán: Katonai biztonság napjainkban. Új fenyegetések, új háborúk, új elméletek 70-104.old. https://m2.mtmt.hu/api/publication/3258112 Finszter G. Biztonsági kihívások a 21. században. (2017) ISBN:9786155680502

[3] U.o.

[4] Az EU Tanácsa: Kiberbiztonság Európában; Infojegyzet, 2016/44; Inforkörkép, 2018
https://www.parlament.hu/documents/10181/1789217/Infojegyzet_2019_49_Kiberhadviseles.pdf/11686cc6-54a5-8388-87db-54233ab8a32d?t=1573810309857 , ORSZÁGGYŰLÉS http://industry4.hu/hu/fogalomtar/digitalis-forradalom

[5] Global Terrorism Index 2020: A terrorizmus hatásának mérése. https://reliefweb.int/sites/reliefweb.int/files/resources/GTI-2020-web-2.pdf

[6] Dr. Haig Zsolt, Dr. Várhegyi István: A vezetési hadviselés alapjai http://www.bibl.u-szeged.hu/bibl/mil/konyvek/elmelet/info/h/haig2_i.html

[7] Dr. Haig Zsolt és Dr. Várhegyi István Információs műveletek: Információs korszak hadügyi forradalma és információs rendszerei, Zrínyi Miklós Nemzetvédelmi Egyetem 2004-es számú egyetemi jegyzet

[8] Takács Gergely: Big Data (adatvezérelt) elemzési módszerek alkalmazása a nemzetbiztonsági szférában, A Terrorelhárítási Központ Tudományos Tanácsának 2018/1- es számú folyóirata, 7. évfolyam 1. szám http://epa.oszk.hu/02900/02932/00016/pdf/EPA02932_terror_elharitas_2018_1.pdf

[9] U.o

[10] Wayne M. Hall, "Information Operations: Military Competition," Cyber Sword: The Professional Journal of Joint Information Operations 4, no. 1 (Spring 2000): 6. http://www.iwar.org.uk/iwar/resources/cybersword/Dragon_R_A_01.pdf

[11] Muha Lajos: Fogalmak és definíciók, 2004 [In.: Az informatikai biztonság kézikönyve (szerk.: Muha Lajos), Budapest: Verlag Dashöfer Szakkiadó, ISBN 963 9313 12 2]

[12] Defence Education Enhancement Programme (DEEP): Media, (Dis)Information and Security https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf
[13] Szabó András: Az információs hadviselés, Magyar Hadtudományi Szemle 1998 VIII. évfolyam 8. szám http://mhtt.eu/hadtudomany/1998/ht-1998-4-5.html
[14] Dr. Kis-Benedek József nyá. Ezredes: A nemzetközi terrorizmus jelenlegi tendenciái Európában, Felderítő Szemle , Katonai Nemzetbiztonsági Szolgálat XVIII. évfolyam 3. szám https://www.knbsz.gov.hu/hu/letoltes/fsz/2019-3.pdf
[15] Finszter G. Biztonsági kihívások a 21. században. (2017) ISBN:9786155680502 https://www.uni-nke.hu/document/uni-nke-hu/3.%20Szenes%20k%C3%B6nyv,%20k%C3%B6nyvr%C3%A9szlet.pdf
[16] Vincenzo Bove: Beyond coups: terrorism and military involvement in politics: European Journal of International Relations 2020, Vol. 26(1), DOI: 10.1177/1354066119866499 https://journals.sagepub.com/doi/pdf/10.1177/1354066119866499
[17] Dr. Szternák György, Dr. Szternák Nóra, Dr. Bolgár Judit: A terrorizmussal kapcsolatos kutatások legújabb eredményei. Felderítő Szemle , Katonai Nemzetbiztonsági Szolgálat 2005 IV. évfolyam 4. szám https://www.knbsz.gov.hu/hu/letoltes/fsz/2005-4.pdf
[18] Szathmáry Zoltán: Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban. PhD értekezés. https://pea.lib.pte.hu/bitstream/handle/pea/16033/szathmary-zoltan-tezis-hun-2013.pdf?sequence=2&isAllowed=y
[19] Berki Gábor: Kiberháborúk, kiberkonfliktusok. In: Pintér István (szerk.) A virtuális tér geopolitikája. Geopolitikai Tanács, 2016. 260–264. old. HU ISSN 1788-7895. ISBN 978-963-9816-34-3. https://mek.oszk.hu/16100/16182/16182.pdf
[20] Julia Voo, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, Anina Schwarzenbach: National Cyber Power Index (NCPI) 2020, Harward Kennedy School Belfer Center for Science and International Affairs, https://www.belfercenter.org/publication/national-cyber-power-index-2020
[21] Defence Education Enhancement Programme (DEEP): Media, (Dis)Information and Security https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf
[22] Szabó András: Az információs hadviselés, Magyar Hadtudományi Szemle 1998 VIII. évfolyam 8. szám http://mhtt.eu/hadtudomany/1998/ht-1998-4-5.html
[23] Marc Loi: New equipment gives Reserve MP Soldiers resources to succeedhttps://www.army.mil/article/97665/New_equipment_gives_Reserve_MP_Soldiers_resources_to_succeed
[24] Munk Sándor : Katonai informatikai rendszerek interoperabilitásának aktuális hadtudományi kérdései. MTA Doktori értekezés https://core.ac.uk/download/pdf/35134477.pdf
[25] NATO Standard AJP-6, Allied joit Doctrine for Communication and Informatin Systems, Edition A Version 1. 2017 https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDA_V1_E_2525.pdf

[26] Thomas Timothy L.: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? The Journal of Slavic Military Studies, 2014
[27] 3 Joint Pub 6-0, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations, 30 May 95, I-3 https://nsarchive.gwu.edu/sites/default/files/documents/5628050/Joint-Force-Joint-Pub-6-0-Doctrine-for-Command.pdf
[28] Kranzieritz Veronika Marketing információs rendszerek alkalmazhatósága a pszichológiai műveletek vezetés-irányítási folyamatában1 DOI 10.17047/HADTUD.2019.29.E.11 HADTUDOMÁNY, 2019. ÉVI ELEKTRONIKUS LAPSZÁM http://mhtt.eu/hadtudomany/2019/2019e/2019ekranzieritz.pdf
[29] Haig Zsolt: Információ – társadalom – biztonság. Budapest, NKE Szolgáltató Kft., 2015. 8., https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf
[30] Horváth-Sántha Hanga1 Milipol Asia Pacific 2019 – A délkelet-ázsiai térség legjelentősebb belügyi és biztonságpolitikai konferenciájának összefoglalója, Hadtudományi Szemle • 12. évfolyam (2019) 4. szám http://real.mtak.hu/109468/1/HSZ_2019_4_05-Horvath-Santha-45-60.pdf
[31] Fekete Csanád: Az információs hadviselés orosz koncepciójának fejlődése a hidegháború végét követően, Hadtudományi szemle 11. évf. 3. sz. (2018.)
[32] Erdész Viktor: A mesterséges intelligencia felhasználási lehetőségei a korszerű nemzetbiztonsági hírszerző elemzés-értékelésében, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola Doktori értekezés https://hdi.uni-nke.hu/document/hdi-uni-nke-hu/erdesz_viktor_ertekezes_tervezet.pdf