Kovács László

Az elektronikai hadviselés helye és szerepe a jövõ információs hadviselésében

A 21. század óriási kihívások elé állítja társadalmainkat. Az információs kor kihívása, illetve az annak megfelelés – a modern társadalmakat gyökeresen átalakítja. A tudásalapú társadalmaknak is nevezett információs társadalmakban az információ válik az egyik legfontosabb tényezõvé. A szerzõ a vezetési hadviselés definíciószerûen megfogalmazott tartalmi jellemzésén túl annak egyik alkotóelemét, az elektronikai hadviselést és annak, a vezetési hadviselésben, illetve ezen keresztül az információs hadviselésben elfoglalt helyét és szerepét mutatja be – nem konkrét hadseregekre és országokra lebontva, hanem általános érvényûen a jelen század kihívásainak tükrében, amelyre minden, sikereket elérni akaró hadseregnek fel kell készülnie.

Az információs társadalom természetesen a hadügyben is alapvetõ változásokat okoz. Megjelenik az információs hadviselés fogalma. Definíciószerûen megfogalmazva az információs hadviselés „*az információs háború és az információs hadjárat részeként és a valós hadmûveletek közvetlen támogatójaként, illetve azzal párhuzamosan folytatott és annak részben önálló elemeként – az információs fölény, információs felsõbbség, az információs uralom és az idõfölény, valamint a vezetési fölény kivívására irányuló, feszített szellemi és fizikai információs küzdelem, amelyet a szemben álló katonai felek (ellenoldali felek, ellenfelek, ellenségek) magasan képzett vezetõállománya [összhaderõnemi és haderõnemi parancsnokai és törzsei és e sajátos küzdelembe bevont szaktörzsei, szakharcászati területek és a mûveleteket kivitelezõ «információs harcosok» (Information Warriors)] folytatnak*”[1]. Ennél egy kissé egyszerûbben megfogalmazva: az információs hadviselés nem más, mint, „*mindazon, az információs fölény megszerzésére irányuló tevékenységek összessége, amelyek a saját információ, információalapú eljárások, információs rendszerek és számítógép-alapú rendszerek védelmére, ezek elõnyeinek kihasználására, illetve a szemben álló fél hasonló rendszereinek és képességeinek a csökkentésére irányulnak.*”[2]

A jövõ háborúit és fegyveres konfliktusait az fogja megnyerni, aki megszerzi a másik féllel szembeni információs fölényt. Az információs fölény birtokában képesek vagyunk „látni” az ellenséget, pontosan meg tudjuk határozni jelenlegi helyét, erõinek összetételét, vezetésének rendjét. Mindezek birtokában lehetõségünk van feltárni gyenge pontjait, és a szükséges erõkkel és eszközökkel csapást mérni ezekre a pontokra. Az információs hadviselés katonai mûveletekben a vezetési hadviselésen keresztül jelenik meg.

A vezetési hadviselés és alkotóelemei

Az információs hadviselés célja nem más, mint az információs fölény kivívása. Az információs fölény idõfölényt biztosít számunkra, amelynek birtokában lehetõvé válik, hogy megfelelõ módon elemezzük az ellenség tevékenységét, megtervezzük a hatékony válaszlépéseinket és ezek várható hatásait. Az idõfölény lehetõséget biztosít továbbá az alapos tervezés után arra, hogy a megfelelõ válaszlépéseket megtegyük, megelõzve az ellenséget, ezzel mintegy biztosítva a gyõzelmet.

Az információs hadviselés egy nagy, ország- vagy nemzetszintû össztársadalmi (kormányzati) tevékenység. Ennek katonai vetülete a vezetési hadviselés.

„A vezetési hadviselés – a felderítés által a híradás és az informatika kölcsönösen támogatott – pszichológiai mûveletek, katonai megtévesztés, hadmûveleti biztonság, fizikai megsemmisítés és elektronikai hadviselés

összehangolt alkalmazása egyrészt az ellenség vezetési lehetõségeinek csökkentése, befolyásolása, rombolása érdekében, másrészt a saját vezetési képességeinknek az ellenség hasonló tevékenységeivel szembeni védelme céljából."[3]

A vezetési hadviselést minden szintû katonai tevékenységben alkalmazzák. Típusát tekintve a vezetési hadviselés lehet támadó vagy védelmi jellegû.

A vezetési hadviselés célja – összhangban az információs hadviseléssel – az információs fölény megszerzése. Az információs fölény megszerzése azonban nem pusztán felderítõfeladat. A felderítési adatokat össze kell gyûjteni, össze kell hasonlítani, értékelni kell és végül döntéstámogató információt kell mindezekbõl elõállítani. Ezek után vagy ezekkel párhuzamosan el kell végezni a célok fontosság és értékesség szerinti osztályozását. A célok osztályozása és elosztása után következhet azok kemény, illetve puha módszerekkel történõ pusztítása, mûködésük és tevékenységük korlátozása, illetve lefogása.[4]

A kemény módszerek közé tartozik a *fizikai pusztítás,* mint a vezetési hadviselés öt alapelemének egyik igen fontos összetevõje.[5] A fizikai megsemmisítés az ellenséges erõk és eszközök pusztítása vagy semlegesítése érdekében a harci erõ alkalmazása, amely magában foglalja a földi, légi, szövetségi mûveletekben pedig a tengeri erõk közvetlen vagy közvetett tûzcsapásait, valamint a speciális erõ különbözõ közvetlen tevékenységeit.

A vezetési hadviselés nem nélkülözheti azt az erõt, amelyet a *pszichológiai hadviselés* rejt magában. A pszichológiai hadviselés magában foglalja többek között a kiválogatott, megtévesztõ információk és jelzések továbbítását az ellenség felé, ezáltal befolyásolva érzelmeiket, indítékaikat, következtetéseiket, amelyek hatással lehetnek további tevékenységükre és viselkedésükre.

A *hadmûveleti biztonság* a következõ elem, amely szerves részét képezi a vezetési hadviselésnek. A hadmûveleti biztonság a katonai mûveletekhez és egyéb tevékenységekhez kapcsolódó saját tevékenységek elemzésének folyamata, amely lehetõvé teszi az ellenséges felderítõ rendszerek megfigyelõtevékenységének azonosítását. A hadmûveleti biztonság lehetõséget teremt továbbá meghatározni mindazon jellemzõket, amelyeket az ellenséges felderítõ rendszer megszerezhet és azokat értelmezve vagy összeillesztve, számára hasznos, idõben releváns információt nyerhet. A hadmûveleti biztonság keretében kell kiválasztani és érvényesíteni mindazon biztonsági rendszabályokat, amelyekkel kiküszöbölhetõ vagy elfogadható szintre csökkenthetõ a saját tevékenységek sebezhetõsége az ellenséges felderítéssel szemben.

A *katonai megtévesztés és álcázás* szintén fontos szerepet játszik a vezetési hadviselés céljainak elérésében. A katonai megtévesztés azon tevékenységek végrehajtása, amellyel az ellenséges parancsnok szándékosan félrevezethetõ saját csapataink katonai képességeit, szándékait és mûveleteit illetõen. Ezáltal az ellenség olyan helyzetbe hozható, hogy saját tevékenységével hozzájárul feladataink sikeres teljesítéséhez.

Az elektronikai hadviselés az ötödik elem, amely elengedhetetlenül szükséges tényezõ a vezetési hadviselésben. Ma már a katonai vezetés nélkülözhetetlen részét képezik a modern kommunikációs, elektronikai és informatikai rendszerek. Ezek bénítása, lefogása illetve pusztítása az elektromágneses spektrum útján az a fõ feladat, minek sikeres teljesítésével az elektronikai hadviselés hozzájárul a vezetési hadviselés sikeréhez és végsõ soron a gyõzelemhez.

Az elektronikai hadviselés összetevõi

Az elektronikai hadviselés az elektromágneses spektrum teljes szélességét kihasználja feladatai elvégzésére. Teszi mindezt úgy, hogy az elektromágneses energiát felhasználva meghatározza, felderíti, csökkenti vagy megakadályozza az elektromágneses spektrum ellenség részérõl történõ felhasználását és biztosítja annak saját részrõl történõ minél hatékonyabb alkalmazását.

Az elektronikai hadviselés – ugyanúgy, mint a vezetési hadviselés többi eleme – szerves részét képezi minden hadmûveletnek, alkalmazása minden szinten elengedhetetlen.

Az elektronikai hadviselés három nagy – viszonylag jól elkülöníthetõ – területre osztható; az elektronikai támogatásra (Electronic Support Measures – ESM), elektronikai ellentevékenységre (Electronic Counter Measures – ECM) és elektronikai védelemre (Electronic Counter-Counter Measures – ECCM[6]).

Az elektronikai támogatás feladata a szándékos és nem szándékos elektromágneses kisugárzások felfedése, azonosítása és a kisugárzás irányának, illetve pontos földrajzi vagy térbeli helyének a meghatározása. Az így szerzett adatok egyrészt felderítési információvá alakíthatóak, másrészt kiindulópontját és alapját képezik a közvetlen fenyegetés felismerésének, ennélfogva az elektronikai támogatás biztosítja az elektronikai hadviselési erõk – és természetesen az összhaderõnemi csapatok vagy más fegyvernemek, szakcsapatok – mûveleteihez, a célzáshoz, a fenyegetés elhárításához és az erõk egyéb harcászati alkalmazásához szükséges információkat.

Az elektronikai ellentevékenység az elektronikai hadviselés azon területe, amely az elektromágneses energia és irányított energia felhasználásával csökkenti, semlegesíti vagy rombolja az ellenség elektronikai rendszereit, vezetési képességeit. Az elektronikai ellentevékenység – az elektronikai hadviseléshez hasonlóan – további három összetevõre bontható. Az elsõ összetevõ az *elektronikai zavarás* (Electronic Jamming). Az elektronikai zavarás sugárzott, visszasugárzott, vagy visszavert[7] elektromágneses energiával csökkenti a szemben álló fél elektronikai rendszereinek hatékonyságát. Második összetevõként értékelhetjük az *elektronikai megtévesztést* (Electronic Deception). Az elektronikai megtévesztés manipulációs, imitációs és szimulációs eszközökkel ad hamis képet a saját tevékenységünkrõl vagy csapatainkról. A harmadik összetevõ a *fizikai rombolás* (Physical Destruction). A fizikai rombolás során irányított energiájú fegyvereket, bombákat[8], lézerfegyvereket alkalmazva, az ellenség elektronikai készülékeit pusztítjuk.

Az elektronikai hadviselés harmadik nagy területe az *elektronikai védelem.* Ez az a terület, amely magában foglalja mindazon tevékenységeket, amelyekkel biztosítható az élõerõ és a technikai eszközök védelme bármilyen, a saját csapatok által keltett elektronikai behatással szemben vagy az ellenség elektronikai hadviselési tevékenységével szemben, amellyel csökkenteni, semlegesíteni vagy rombolni akarja a saját vezetési képességeinket. Ennek érdekében az elektronikai védelem szigorú rendszabályokat fogalmaz meg a saját elektronikai rendszereink felhasználásához, illetve alkalmaz minden olyan tevékenységet[9] és anyagot, amelyek csökkentik az ellenség elektronikai hadviselési rendszereinek hatását a saját csapatainkra.

A 21. század kihívásai az elektronikai hadviseléssel szemben és a lehetséges válaszok

Az információs korban kezdenek körvonalazódni az információs társadalmak, amelyek természetes módon átalakítják a fegyveres erõiket is. A fegyveres erõkben különlegesen fontos szerepet fognak kapni az információs hadviselésre felkészített speciális erõk. Ezen speciális erõk egyik alapvetõ pillérét – a fegyveres konfliktusokban és a nem háborús mûveletekben egyaránt – az elektronikai hadviselési csapatoknak kell alkotniuk. Ennek megfelelõen az elektronikai hadviselésnek és az elektronikai hadviselési csapatoknak is fel kell készülniük a várható kihívásokra. Nézzük, melyek azok a legmarkánsabb kihívások, amelyekkel az elektronikai hadviselés szembetalálhatja magát a jövõben!

Az elektronikai támogatásnak fel kell használnia az információs kor technikai vívmányait ahhoz, hogy feladatát el tudja látni, illetve hogy követni tudja a kommunikációs vagy akár a radartechnikában bevezetett és ma már általánossá vált forradalmian új technikai eszközöket és eljárásokat. A teljesség igénye nélkül néhány kihívás, amely óriási feladat elé állítja az elektronikai támogatást:

- megjelentek a kis valószínûsséggel felderíthetõ adásmódok (Low Probability of Interception – LPI), amelyek további térnyerése várható;
- a kriptográfia és az elektronikus kriptográfia óriási fejlõdésen ment keresztül az elmúlt ötven év során, amely gyakorlatilag már ma is lehetetlenné teszi, az elfogott titkosított elektronikus adások információtartalmának kinyerését;
- egyre szélesebb körben jelennek meg a frekvenciaugratásos vagy a kiterjesztett spektrumú kommunikációs rendszerek;
- a rádiólokátor-technika szintén jelentõs fejlõdésen ment keresztül, amely – a teljesség igénye nélkül – a CHIRP vagy a szekunder-radarrendszerekben követhetõ a leginkább nyomon;
- az elfogott elektromágneses jel kisugárzási helyének megállapítása, vagyis az iránymérés, a frekvenciaugratásos, illetve kiterjesztett spektrumú adások esetén igen nehéz.

Az elektronikai ellentevékenységnek a kommunikáció területén egészen a közelmúltig rövidhullámú és ultrarövidhullámú adásokkal kellett felvennie a harcot. Az ilyen kommunikációs adások zavarása óriási teljesítményû (esetenként több tízkW, vagy több százkW!) elektromágneses energiát használt. Megjelentek azonban már URH frekvencián is a csomagkapcsolt adások, a frekvenciaugratásos rádiórendszerek, a kiterjesztett spektrumú adások, amelyek felderítése is igen nehéz, nemhogy zavarása. A kommunikációs rendszerekben a fejlõdés további iránya a nagyfrekvenciás, mikrohullámú rendszerek felé vezet. További

térnyerése várható a cellásrádió rendszereknek[10], amelyek szintén megnehezítik az ellenük való elektronikai ténykedést. A megoldást a területre kijuttatott egyszeri felhasználású, intelligens zavaró adók jelenthetik. Más megoldás lehet a pilóta nélküli repülõeszközökön elhelyezett és az alkalmazás helyére ezzel kijuttatott kis méretû intelligens zavaróadók alkalmazása.

Az elektronikai ellentevékenységnek fel kell készülnie a navigációs rendszerek esetleges zavarására. Ma már egyre több fegyverirányítási rendszer – de itt megemlíthetjük gyakorlatilag az összes modern rádiókommunikációs rendszert is – mûholdas navigációt használ a helymeghatározásra vagy kommunikációs rendszerek esetében az együttfutás idõbeni szinkronizálására. Ezek zavarása óriási veszteséget lenne képes okozni a szemben álló félnek.

A nem kommunikációs rendszerek területén az elektronikai ellentevékenységnek hasonló kihívásokkal kell szembenéznie, mint az elektronikai támogatásnak. A rádiólokátor-rendszerek területén további fejlõdés várható a passzív radarok, a szekunderradarok, illetve a CHIRP-radarok területén.

Mindezeket egybevetve, meglátásom szerint az elektronikai ellentevékenység súlypontja a napjainkban alkalmazott elektronikai zavarásról egyre inkább az irányított energiájú fegyverekkel és bombákkal, illetve a lézerfegyverekkel végrehajtott fizikai pusztítás irányába helyezõdik át. Már napjainkban is hadmûveleti-harcászati szinten egy adott fegyveres konfliktusban több ezerre vagy akár több tízezerre is tehetõ a számítógépek által vezérelt elektronikai berendezések száma. Az információs technológia rohamos fejlõdése egyre újabb és újabb, mikroprocesszor alapú, integrált áramköri elemekre épülõ informatikai, számítástechnikai és kommunikációs berendezéseket nyújt a hadseregek számára feladatuk elvégzéséhez. Már ma is jellemzõ, de a jövõben még inkább az lesz, hogy a modern hadseregek (de ez igaz a társadalom többi területére is) nagymértékben függenek az általuk használt számítógépes rendszerektõl, hálózatoktól, elektronikai berendezésektõl és ezek megbízható mûködésétõl. Ez az a függõség, amit az impulzusfegyverek révén kihasználhatunk. Ha megkeressük a kulcsfontosságú számítógép-hálózatokat, kommunikációs berendezéseket, és ezeket impulzusfegyverekkel, impulzusbombákkal mûködésképtelenné tesszük, ha csak rövid idõre is, de óriási elõnyre tehetünk szert. Az ellenség nem tudja irányítani csapatait, nem tud felderíteni, nem „lát" a hadszíntéren, mindezek következményeként információs hátrányba kerül. Ez számunkra a siker záloga az információs hadviselésben.

A jövõ hadszínterén a jól felszerelt „digitális katona" vívja majd a harcot. Felszereléséhez olyan eszközök tartoznak majd, mint például a személyi kommunikációs és az egyéni harctéri azonosító berendezés, vagy a „body lan", amely egy olyan számítógépes rendszer, amely a katona testén elhelyezett különféle érzékelõk számítógépes és kommunikációs rendszerhez kapcsolódva, többek között reális képet ad a katona pillanatnyi fizikai állapotáról, de akár a katona sisakján elhelyezett videokamera képét is továbbíthatja a vezetési pontra. Mindezek célpontul fognak majd szolgálni az elektronikai ellentevékenység számára. Ha ezt a digitális katonát rávezetjük egy elektromágneses aknamezõre és ott nagyteljesítményû elektromágneses impulzusaknát robbantunk fel, akkor gyakorlatilag a katona összes elektronikai készüléke és berendezése használhatatlan lesz, a katona el lesz vágva a csapatától, a parancsnokától, és végsõ soron feladata elvégzésére válik alkalmatlanná.

A közelmúltban megjelent számítógép-hálózatok is mindinkább beépülnek napjaink és a jövõ hadviselésébe. Ez természetesen magával hozta azt is, hogy megjelent *a hálózati hadviselés* (Net Warfare). Jelenleg nincs döntés arról, és ennek megfelelõen nincs is olyan szervezet sem, amely a hálózati hadviselés támadó (Attack) oldalával foglalkozna. Véleményem szerint ezt az elektronikai ellentevékenységet ellátó (mint az elektronikai hadviselés támadó része) csapatoknak és szervezeteknek kell felvállalniuk mindaddig, amíg speciális, ezzel a szakterülettel foglalkozó szervezetek létre nem jönnek.

Az elektronikai védelemnek a mostaninál is lényegesebb szerepet kell, kapnia a 21. század elektronikai hadviselésében és ezen keresztül az információs hadviselésben. Az elektronikai rendszerek száma folyamatosan nõ, a felhasználható elektromágneses spektrum azonban változatlan marad. A jövõben a már napjainkban is igen komoly gondokat okozó elektromágneses kompatibilitás kérdésköre még nagyobb koordináló feladat elé állítja az elektronikai védelmet.

Az elektronikai védelemnek tovább kell kutatnia azokat az adásmódokat, amelyek felderítési valószínûsége a minimálisra csökkenthetõ, ezáltal a saját tevékenységünkrõl a lehetõ legkevesebb információt nyújtjuk az ellenségnek. Tovább kell kutatni és alkalmazni mindazon új anyagokat és technikákat, amelyek használatával a rádiólokációs visszaverõ felület csökkenthetõ, amely szintén kisebb információforrásként szolgál az ellenség számára.

Az eddig elmondottakból azonban adódik a kérdés: *milyen összetételû és szakképesítésû állomány kell a jövõ elektronikai hadviselési csapatai részére?* A válasz egyértelmû: a számítógépesítés és az informatikai rendszerek alkalmazása miatt egy kis létszámú, de jól képzett technikai fejlesztõ, kezelõ- és kiszolgálóállománnyal. Ez azt jelenti, hogy mérnöki képzettséggel kell rendelkeznie annak, aki az elektronikai hadviselési rendszereket kezeli, hiszen e nélkül elképzelhetetlen a bonyolult elektronikai és számítógépes rendszerek hatékony alkalmazása. Már kezelõi szinten is meg kell érteni mindazokat a tevékenységeket, amelyeket a szemben álló fél elektronikai hadviselése végez, és erre ki kell választani a megfelelõ ellenlépéseket. Ez az információs technika korában elképzelhetetlen mérnöki – informatikai, elektronikai, kommunikációs – tudás nélkül. Tehát ne féljünk kimondani: a jövõben az elektronikai hadviselési berendezések kezelõ-pultjainál felsõfokú végzettségû mérnökök fognak ülni, akik szaktudásuk révén hatékonyan lesznek képesek kezelni a technikai eszközöket.

*

Az információ az a szó, amely a leginkább meghatározza napjaink és a jövõ társadalmait és ezzel együtt a modern társadalmak hadseregeit is. Ma már információs hadviselésrõl beszélünk, amelyben a fõ cél az információs fölény megszerzése, és amely idõfölényt biztosít a számunkra. Ennek birtokában megszerezhetõ a gyõzelem a szemben álló fél felett. Ennek megfelelõen át fog alakulni a hadviselés jellege is. Az információs társadalmak elsõsorban urbánus társadalmak lesznek, kialakulnak a milliós és tízmilliós lakosú városok, amelyek szintén újfajta helyzet elé állítják a hadviselõ feleket.

Az információs kor forradalmian új technikai eszközöket is ad a hadseregek kezébe. Eddig még sohasem látott módon lehet megvívni a háborúkat az elektronikai eszközök, számítógépek, számítógépes hálózatok segítségével. A vezetési hadviselés az az új hadviselési forma, amely az információs hadviselés részeként, annak mintegy katonai vetületeként jellemzi ezt az újfajta hadviselést.

A tömeghadseregek felett eljárt az idõ. A jövõben már nem harckocsihadosztályok fognak szemben állni egymással a harcmezõn, hanem digitális katonák, akik az információs kor miden vívmányát kihasználják, hogy gyõzzenek. Elektrooptikai felderítõkészüléket alkalmaznak, digitális rádión kapják a parancsot a saját fejhallgatójukba, a sisakjukba szerelt videokamera képét valós idõben nyomon tudja követni a parancsnokuk. A testükön elhelyezett érzékelõk még a pillanatnyi fizikai és lelki állapotuk legfontosabb jellemzõit is továbbítják a vezetési pontokra.

A vezetési pontokon virtuálisan a harcmezõ egész képe megjelenik. A parancsnok azt a képet látja, amit a harctéren lévõ katona és anélkül hozhat döntéseket, hogy fizikailag ott kellene lennie. Mindez a döntéshozatali mechanizmus egy forradalmian új technikáját is hozza magával. Szintén az információs forradalom „termékei” az impulzusfegyverek, amelyek alkalmazása a komputerizált és elektronizált hadseregekkel szemben esetlegesen az egész konfliktus kimenetelét befolyásolhatja. Az információ – ez az a legfontosabb tényezõ vagy elem, amely nélkül társadalmaink és hadseregeink sem sikeresek, sem gyõztesek nem lehetnek.

FELHASZNÁLT IRODALOM

1. Dr. Várhegyi István–Dr. Makkay Imre: Az információs hadviselés alapjai; Egyetemi jegyzet, ZMNE, Budapest 2000.

2. Joint Pub 6–02, Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems, Joint Chiefs of Staff; 1 october 1996.

3. Dr. Haig Zsolt–Dr. Várhegyi István: A vezetési hadviselés alapjai; Egyetemi jegyzet, ZMNE, Budapest, 2000.

Dr. Várhegyi–Dr. Makkay: Az információs hadviselés alapjai; p.:165. [1.]

2

Joint Pub 6–02 p.: II–6 [2.]

3

Dr. Haig–Dr. Várhegyi: A vezetési hadviselés alapjai; p. 72. [3.]

4

Fontos célok (High Priority Targets – HPTs): midazon ellenséges célok összessége, amelyek pusztítása elsõdleges fontosságú a számunkra, pl.: tüzérség és a tüzérségi vezetési pontok, csapatvezetési pontok stb.

Nagy értékû célok (High Value Targets – HVTs): mindazon ellenséges célok összessége, amelyek pusztítása vagy lefogása jelentõs elõnyökkel jár számunkra, pl.: kommunikációs központok, C4I rendszerek stb.

Kemény módszerek (Hard Kill): fizikai pusztítás, rombolás útján akadályozzuk vagy korlátozzuk a mûködést, illetve tevékenységet.

Puha módszerek (Soft Kill): olyan, nem fizikai pusztítás útján végzett, tevékenység, amely lényegesen csökkenti a szemben álló fél képességeit pl.: elektronikai zavarás, lefogás stb.

5

Meglátásom szerint a jövõben – amellett, hogy komoly elõnyökre lehet szert tenni a modern hadviselési módokkal, a modern technikai eszközök alkalmazásával – nem mellõzhetjük majd azt az elrettentõ és valós erõt, amelyet a fizikai pusztítás eszközei képviselnek.

6

Az elektronikai védelem kifejezést napjainkban egyre többször Electronic Protection kifejezésként használják a nyugati szakirodalomban.

7

Különbséget kell tennünk a visszavert és a visszasugárzott elektromágneses energia között. A visszavert jel azt jelenti, amikor az ellenség által kibocsátott elektromágneses energiát szándékosan kihelyezett tárgyakról – például szögvisszaverõkrõl – az ellenség felé visszaverjük, álcázás vagy megtévesztés céljából. A visszasugárzás fogalma azt takarja, hogy az ellenség által kisugárzott elektromágneses jelet elfogjuk, analizáljuk, majd bizonyos változtatásokat eszközölve ebben – például hamis jelsorozatot belefûzve – visszasugározzuk az ellenség felé, amelyet az ellenség saját jelként értékel, és hamis információkhoz jut a saját csapatainkról vagy tevékenységünkrõl.

8

Irányított energiájú fegyverek közé tartoznak például az impulzusfegyverek és impulzusbombák. Az impulzusfegyverek nagyon rövid idõ alatt óriási energiájú – több gigaWatt – elektromágneses impulzus kibocsátására képesek. Ez az impulzus a félvezetõkben, mikroprocesszorokban, de gyakorlatilag az összes elektronikai készülékben túláramot hoz létre, amely elégeti a vezetõrétegeket, ezáltal használhatatlanná válik az adott alkatrész vagy esetleg az egész berendezés.

9

Olyan tevékenységek, mint például az elektronikai manõverezés térben és idõben vagy a különbözõ, kis valószínûséggel felderíthetõ adásmódok alkalmazása.

10

A cellásrádió rendszerek, akárcsak a polgári életben is használt GSM rendszerek, óriási mobilitást, és nagy elõnyöket adnak a felhasználóiknak. Ezek zavarhatóságára a kutatások már megkezdõdtek, és például a GSM rendszerek zavarása területén már ma is kézzelfogható eredmények vannak.