Haig Zsolt – Kovács László –
Ványa László – Vass Sándor

ELEKTRONIKAI HADVISELÉS

ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel

Haig Zsolt – Kovács László –
Ványa László – Vass Sándor

ELEKTRONIKAI HADVISELÉS

Nemzeti Közszolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar
Budapest, 2014

Nemzeti Közszolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar
Katonai Műszaki Doktori iskola

Szerzők:

Kiadja:

Olvasószerkesztés, tördelés: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt.

ISBN 978-615-5305-87-0

TARTALOMJEGYZÉK

3. FEJEZET

4. FEJEZET

5. FEJEZET

1. FEJEZET

Elektronikai hadviselés az információs műveletekben és a kibertéri műveletekben

1.1 Információs műveletek

1.1.1 Az információs hadszíntér megjelenése

Napjaink új típusú társadalmában a különféle információs tevékenységek az úgynevezett információs környezetben, vagy más kifejezéssel az információs színtéren zajlanak. Az információs környezet definíciójára többféle meghatározással is találkozhatunk, attól függően, hogy ki milyen szempontból vizsgálja azt, és mit tart fontosnak hangsúlyozni. Az USA összhaderőnemi információs műveletek doktrínája szerint *az információs környezet mindazon egyének, szervezetek és rendszerek összessége akik, és amelyek az információ gyűjtésével, feldolgozásával, szétosztásával foglalkoznak.*[1] A definíció szerint az információs környezet magába foglalja annak valamennyi szereplőjét és erőforrásait, illetve tevékenységeit és folyamatait.

Az információs környezetnek többféle szintje lehet. Témánk szempontjából ezek közül kettőt emelünk ki: a globális információs környezetet és a katonai információs környezetet. Az információs társadalom kibontakozásával kialakuló globális gazdaságot a globális információs környezet veszi körül. A fenti meghatározást alapul véve a globális információs környezet az információ világméretű gyűjtésével, feldolgozásával és elosztásával foglalkozó szereplők (egyének, szervezetek és rendszerek) összessége. Ennek a globális környezetnek a technikai-technológiai alapját az a globális információs infrastruktúra képezi, amely nem más, mint azoknak a vezetékes és vezeték nélküli távközlési rendszereknek, számítógép-hálózatoknak és egyéb információszerző, -feldolgozó és -szétosztó rendszereknek az összessége, amelyek a globális információcserét biztosítják. A globális információs környezetnek a világ minden érintett globális, regionális és nemzeti szerve, intézménye és rendszere részét képezi.

Az információs környezet megjelenése következtében, a katonai műveletek működési területei és tartományai tovább bővültek. A hadszíntér fizikai dimenziói kiegészülnek egy lényeges, nem földrajzi dimenzióval. A szárazföldi-, tengeri-, légi- és kozmikus hadszíntér mellett a hadviselés egy újabb tartománya jelent meg, amelyet katonai információs környezetnek, más szóval információs hadszíntérnek nevezünk.

[1] Joint Publication 3-13, Information Operations, 27 November 2012 by United States Government US Army, p. I-1. (fordították a szerzők)

Az információs hadszíntéren a szárazföldi-, légi-, tengeri- és kozmikus műveletek mellett, és azokkal szoros összhangban, egy újabb fajtájú katonai tevékenységet is folytatnak az egymással szembenálló felek az információ megszerzéséért, megtartásáért és hatékony felhasználásáért. E tevékenységeket összefoglalóan információs műveleteknek nevezik. Az információs hadszíntér kifejezésben az információs jelző azonban nemcsak az információs műveletekre utal. Azt is jelenti, hogy a hagyományos katonai műveleteket a korábbiaknál jelentősebben támogatják az információs korszak által biztosított infokommunikációs technológiák.[2] Ezáltal minőségileg új helyzet áll elő a katonai tevékenységek eddigi történetében, hiszen ha az egyik félnek egyre gyorsabban és pontosabban van lehetősége folyamatos információáramlással az adatok gyűjtésére, feldolgozására és továbbítására, miközben kihasználja, vagy megakadályozza az ellenség képességét ennek megtételére, akkor uralja az információs hadszínteret.[3]

Az információs hadszíntér a háborús szintér egyik speciális vetülete, amelyben az információs küzdelem az információ megszerzéséért és a szembenálló félnél hatékonyabb felhasználásáért folyik. Az információs hadszíntér minden olyan valós és virtuális teret, helyet, eszközt, rendszert magába foglal, ahol az információ megszerzésével, előállításával, feldolgozásával, felhasználásával, tárolásával és védelmével foglalkoznak. Az információs hadszíntér kiterjedésében rendszerint túlnő a valódi hadszíntéren, mivel a hadműveleti területen kívül magába foglalja a hátországi támogató katonai és polgári szervek infokommunikációs rendszereit és szervezeteit is.[4]

A jelenkor négydimenziós hadszínterét (levegő, szárazföld, víz és űr) az információs hadszíntér kapcsolja össze. Az információs hadszíntér dominanciája teszi lehetővé, hogy a parancsnok jobb rálátással rendelkezzen a műveletekre, és az erők hatékonyabban hajtsák végre feladataikat.

Napjainkra a fejlett infokommunikációs technológiával rendelkező haderőkben megvalósul a harcmező digitalizálása. Megjelennek a harctéri számítógépek összekapcsolásából kialakított harcászati internetnek *(Tactical Internet – TI)* nevezett hálózatok. A harcászati internet tulajdonképpen nem más, mint a számítógépek, digitális harcászati rádiók és routerek integrációja, amely a nyílt rendszerekből ismert protokollokat *(Transmission Protocol/Internet Protocol – TCP/IP)* alkalmazza. A harcászati internet egy olyan IP alapú hálózat, amely a felhasználók legalsó szintjétől a műveleti parancsnokig bezárólag mindenkinek lehetővé teszi a gyors adatátvitelt és adathozzáférést, ezáltal valósítva meg egy egységes információs rendszert.[5]

[2] Haig, Zs.; Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005. p. 156.

[3] Seiferth, G.: *Hatásalapú információs műveletek*. Nemzetvédelmi Egyetemi Közlemények, 9. évf. 4. sz., ZMNE, Budapest, 2005. pp. 17-23.

[4] Haig, Zs.; Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005. p. 157.

[5] Hóka, M.: *The Tactical Internet*. AARMS, Volume 2, Issue 2., MZNDU, Budapest, 2003. pp. 271-282.

A harctér digitalizálása a katonai számítógép-hálózatok megjelenése mellett azt is jelenti, hogy megjelennek az üzenetcsomagok továbbítására alkalmas, kis valószínűséggel felderíthető *(Low Probability of Intercept – LPI)* digitális híradó rendszerek. A digitális híradásra való áttérés lehetővé teszi a kapcsolóközpontok mellőzését, és az úgynevezett kapcsolásmentes összeköttetések megvalósítását. Ezen túlmenően a törzsekben digitális vezetéstechnikai és irodatechnikai eszközök alkalmazására térnek át. Megjelenik a digitális térkép és a térinformatikai *(Geographical Information System – GIS)* alapú tervezés. A harcparancsok digitális formában készülnek, sokszorosíthatók és továbbításuk az alárendelteknek egyidejűleg történhet.

A harcmező digitalizálásnak köszönhetően lehetővé válik a harcmező láthatóvá tétele. A harctéri vizualizáció *(Battlefield Visualization)* azt jelenti, hogy a digitális harcmezőről digitális álló és mozgó képeket, térképvázlatokat juttatnak a parancsnokok számítógépére, amelynek segítségével távolabbra, és a be nem látható területekre is képesek betekinteni. Ezáltal követni lehet az ellenség tartalékainak manővereit, valamint képesek folyamatosan figyelni a szemmel még nem látható, de például pilóta nélküli felderítő eszközökkel vagy harctéri szenzorokkal érzékelhető harctéri helyzetváltozásokat.[6]

1.1.2 Az információalapú hadviselési módok kialakulása

A történelem során a hadviselés jelentős változásokon ment keresztül mind a haderő struktúráját, létszámát, fegyverzetét illetően, mind pedig az alkalmazott harceljárások tekintetében. A hadviselési formák az évszázadokon keresztül fokozatosan fejlődtek, új technikai eszközök sora jelent meg a hadszíntéren, és ezek törvényszerűen magukkal hozták az új alkalmazási elvek megjelenését.

A katonai műveletek sikeres végrehajtását az egyre kifinomultabb infokommunikációs technológia, az információgyűjtő rendszerek, a vezetési-irányítási rendszerek és a fegyverrendszerek – beleértve a nem-halálos képességeket is – összekapcsolódása teszi lehetővé. A sikeres műveleteket az ellenség rendszerei megértésének jobb képessége támogatja. Az infokommunikációs technológia segít felismerni, hogy a szembenálló fél hogyan tevékenykedik, hol vannak a valódi sebezhető pontjai. Természetesen mindezek a másik félre is érvényesek, vagyis az infokommunikációs rendszereken alapuló tényezők ugyanúgy növelik az ellenség képességeit, mint a sajátjainkat.[7]

Napjaink katonai műveleteiben kiemelt jelentőséget kap a vezetési ciklusidő drasztikus csökkentése. A vezetési ciklus ideje az adott művelet végrehajtásához szükséges teljes időtartamot magában foglalja, amely tartalmazza: a célpont(ok) felderítését, azonosítását, adatainak feldolgozását, elemzését; a végrehajtó alakulat és fegyverrendszer

[6] Haig, Zs. – Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005. p. 159.

[7] Purdy, R. W. H.: *A hatásalapú műveletek áttétele a gyakorlatba*. Nemzetvédelmi Egyetemi Közlemények, 9. évf. 4. sz., ZMNE, Budapest, 2005. pp. 9-16.

kiválasztását; a döntés meghozatalát; a parancs kiadását; a feladat végrehajtását; és az eredmények ellenőrzését. A vezetési ciklus időtartamának gyorsuló ütemű csökkenése kölcsönös összefüggésben áll a hálózatos infokommunikációs eszközök mennyiségi és minőségi mutatóival. Ez azt jelenti, hogy a katonai műveletek felgyorsult üteme egyrészt megköveteli a gyors, pontos döntések meghozatalát, ami a hálózatba kapcsolt eszközök alkalmazásával érhető el. Másrészt az infokommunikációs technológia rohamos fejlődése, a számítási kapacitás, adatátviteli sebesség, adattárolási képesség növekedése lehetővé teszi a gyors és pontos adatszerzést, továbbítást, helyzetértékelést és objektív döntések meghozatalát.

A vezetési ciklusidő csökkentésére való törekvés szoros kapcsolatban van az információs fölény kialakításának képességével. Az információs fölény kivívása és megtartása merőben új típusú hadviselési elvek, formák, módok alkalmazását teszik szükségessé. Ezek az új elvek gyökeresen más aspektusból közelítik meg a katonai siker eléréséhez vezető utat. A háborúra, hadviselésre jellemző pusztítás, rombolás, emberi élet kioltása helyett a hatékonyság, az élőerő megóvása, a manipuláció, és a vezethetetlenség állapotának (káosz) előidézése a cél. Ez azt jelenti, hogy a katonai műveletekben az információalapú hadviselési módok egyre inkább előtérbe kerülnek, a végső sikert jelentősen befolyásoló szerepet kapnak.[8]

1.1.3 Az információs fölény

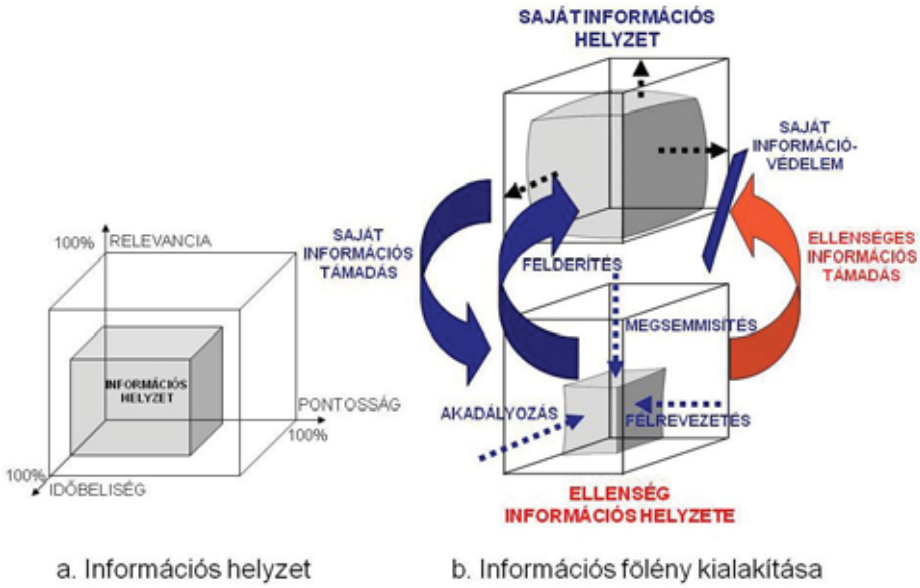
A korszerű katonai műveletekben – a célok elérése érdekében – a szembenálló felek minden támadó és védelmi eszközt és -módszert felhasználnak az információs képességeik kihasználására, és a másik fél lehetőségeinek csökkentésére.[9] A saját információs képességek erősítésének és az ellenség információs lehetőségei gyengítésének képessége a katonai műveletekben egy új típusú fölénytényezőben,[10] az információs fölényben nyilvánul meg.

Az információt minden esetben annak relevanciája, időbelisége és pontossága jellemzi. Az információs fölény kialakítására tett erőfeszítések azt célozzák, hogy ezek a tényezők közelítsenek a 100% irányába. Természetesen ezt a kívánt értéket soha nem lehet elérni, mivel azt minden esetben különböző korlátok akadályozzák. A katonai műveletekben a saját oldalon különböző információvédelmi intézkedésekkel arra törekszünk, hogy az információ ezen tulajdonságait közelítsük a felső határig. A szembenálló fél oldalán pedig különböző támadó információs képességekkel – például a vezetés-irányítási rendszer megsemmisítésével, működésének akadályozásával, félrevezetésével – próbáljuk az információ fentebb jelzett tulajdonságait lerontani. Mindezt szemlélteti a 1.1. ábra.

[8] Haig, Zs. – Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005. p. 168.

[9] Munk, S.: *Az információs fölényről*. Hadtudomány, XI. évf. 3. sz., 2001. pp. 43-52.

[10] A katonai műveletekben többféle fölénytényező ismert, mint például légi fölény, tengeri fölény, hadműveleti fölény.



1.1. ábra. **Az információs fölény értelmezése**[11]

Katonai értelmezés szerint az információs fölény a két szembenálló fél közötti relatív viszonyt jelenti, amely felhasználható a saját célok, érdekek másik félnél eredményesebb érvényesítésére. A fölény tehát tulajdonságok, képességek, lehetőségek közötti célorientált, helyzetfüggő, előnyös különbséget jelent. Az információs fölény szintjeit – a szembenálló felek képességei közötti különbség mértékét – tekintve lehet például előny, fölény, uralom, időbeni fennállása szerint pedig lehet állandó, tartós, ideiglenes és változó. Az információs fölény egyaránt jelentheti a szemben álló felek közötti viszonyt, valamint azt a helyzetet, amelyben ez a viszony fennáll. Ezek alapján az információs fölény az érintett felek információs képességei közötti, az adott fél számára hadműveleti eredményekben realizálható előnyös különbséget jelenti.[12]

Az információs fölény megléte napjaink információra alapozott katonai műveleteiben elsőrendű fontosságú. Aki ugyanis birtokolja az információs fölényt, az több, pontosabb és valós idejű információval rendelkezik, és felhasználva a korszerű katonai információs rendszereket, megalapozottabb, pontosabb, objektívebb döntéseket képes hozni, mint a másik fél. Az információs fölény birtokában lévő fél képes információs rendszereit és azok képességeit kihasználva hadműveleti fölényt elérni, és a helyzetet folyamatosan úgy alakítani, irányítani, hogy emellett az ellenséget megfossza ugyanezen képességeitől.

[11] Alberts, D. S. – Garstka, J. J. – Stein, F. P.: *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series, Washington, 1999. p. 34., p. 56. (a forrás alapján szerkesztették a szerzők)

[12] Munk, S.: *Az információs fölényről.* Hadtudomány, XI. évf. 3. sz., 2001. pp. 43-52.

Az információs fölény megléte a birtoklója számára a következőket jelenti:
- az információs technológia alkalmazása terén előnyben van a szembenálló féllel szemben, és ezt a fölényt folyamatosan képes növelni;
- a hálózatalapú műveleti képesség birtokában a saját döntési ciklus tudományra támaszkodó, megalapozottabb, gyorsabb és ennek következményeként hatékonyabb, mint a szembenálló fél hasonló vezetés-irányítási folyamata;
- többet tud a szembenálló félről, mint amit ő tud a saját erőiről;
- eredményesen tudja korlátozni a szemben álló fél vezetés-irányítási rendszereit, befolyásolni döntési folyamatait, miközben az ellenség hasonló tevékenységével szemben megfelelő védelemmel rendelkezik.[13]

Az információs fölény kivívásának és megtartásának három azonos fontosságú területe van. Mindenekelőtt az információs fölény alapját az adja, hogy elegendő, pontos és valós idejű információval kell rendelkeznünk a döntést befolyásoló tényezőkről, amelyek a katonai műveletekben három terület köré csoportosíthatók, úgymint: az ellenség helyzete, a saját kötelékek helyzete, valamint a harctéri környezet, ahol a katonai művelet zajlik. E három területről a felderítés és a saját erők jelentései alapján juthatunk információhoz.

Másodsorban ki kell építeni a saját hálózatalapú információs rendszereinket, amelyeket hatékonyan kell működtetni annak ellenére is, hogy a szembenálló fél komoly erőfeszítéseket tesz annak érdekében, hogy vagy magát az információ tartalmat, vagy az információs rendszereket, illetve a döntéshozó(ka)t megpróbálja korlátozni, összezavarni, és ezáltal egy számára kedvező helyzetet előidézni. Ez tehát azt jelenti, hogy megfelelő védelmi megoldásokat kell alkalmazni a saját információk és információs rendszerek megóvása érdekében.

Harmadrészt pedig rendelkeznünk kell mindazon képességekkel, amelyekkel befolyásolni tudjuk a szembenálló fél információit, információs rendszereit és folyamatait, valamint döntéshozóit. Ennek hatására kevesebb és pontatlanabb információ áll a szembenálló fél rendelkezésére a döntést befolyásoló tényezőkről, aminek következtében a parancsnok nem lesz képes objektív, valós idejű elhatározás meghozatalára.

Az információs fölény elérése és egy adott időszaknak megfelelő tartós érvényessége az információs uralom kivívásához vezet. Az információs fölény megléte nem folyamatos, állandó és változatlan. Egyenletesen fenntartani nem lehet, mivel az számos tényezőtől függ, és tartóssága (érvényessége) időszakonként változhat.

Az információs fölény csak akkor biztosít felhasználható előnyöket a saját fél számára, ha ez a fölény a döntésekben és a feladat végrehajtásban is érvényesül. Vagyis a végcél a vezetési ciklusban[14] jelentkező vezetési fölény elérése. A vezetési fölény azt jelenti,

[13] Várhegyi, I. – Makkay, I.: *Információs korszak, információs háború, biztonságkultúra*. OMIKK, Budapest, 2000. p. 158.

[14] A vezetési ciklus elemei az informálódás, helyzetértékelés, döntés és végrehajtás. Külföldi szakirodalmi megnevezése: *OODA Loop – Observation, Orient, Decide, Act Loop.*

hogy a korszerű, hálózatba kötött vezetés-irányítási rendszerek segítségével a parancsnok gyorsabban, megalapozottabban, a kialakult helyzet kezelésére több reális cselekvési változatot *(Course of Action)* figyelembe vevő döntést képes meghozni, mint az ellenség. Ennek következtében a saját vezetési ciklus az ellenség vezetési időciklusán belülre kerül, tehát gyorsabb lesz a saját információszerzés, helyzetértékelés, döntés és feladat végrehajtás, mint az ellenségé. Az időben meghozott helyes döntés hatására új helyzet áll elő harctéren, ami előnyös a vezetési fölényben lévő számára és hátrányos az ellenségre nézve. A vezetési fölény birtokosa a feladat végrehajtását korábban tudja megkezdeni, és így képes a kezdeményezést megragadni, valamint akaratát folyamatosan rákényszeríteni a szembenálló félre.

A saját vezetés-irányítási képességeink maximális kihasználása, és a szembenálló fél hasonló képességének részleges vagy teljes akadályozása jelentős erősokszorozó tényező, amely a katonai műveletek végrehajtásában nyilvánul meg. A saját erők pontos és hiteles információkon alapuló elhatározás alapján végzik feladataikat. Az elöljáró folyamatosan kapcsolatban van az alárendeltjeivel, akik a valós helyzetre reagáló feladataikat szervezetten képesek végrehajtani.

Ezzel szemben a másik fél folyamatos információhiányban szenved, így a parancsnok döntései pontatlan és csak valószínűsíthető információkon alapulnak. Az alárendeltjeivel való kapcsolattartás bizonytalan vagy lehetetlen, aminek következtében parancsait, intézkedéseit nem tudja lejuttatni a végrehajtói szintre, illetve azok képtelenek helyzetükről tájékoztatni az elöljárót. Ennek eredményeként a feladat végrehajtása irányíthatatlanná, kaotikussá válik. Mindezek alapján a – műveletek tervezése során alkalmazott – szembenálló felek közötti hagyományos erőviszony számvetés elveszti korábbi jelentőségét.[15]

1.1.4 Információs műveletek értelmezése, területei

Az információs társadalom működését befolyásoló tevékenységek elmélete szerint a társadalmakat fejletlen- (vagy kevésbé fejlett-) és fejlett-, vagy más szóval első- és másodfokú társadalmi-technológiai civilizációs fejlettségi szintre oszthatjuk. A fejlett, második fokozatú társadalmi rendszerek jogi és erkölcsi törvényekkel, szabályzókkal, szabványokkal irányítottan működnek. Amennyiben ez a magas fokú szervezettségi rend – valamilyen külső vagy belső negatív hatásoknál fogva – megszűnik, vagyis a törvények és szabályzók már nem képesek működni, akkor az érintett szervezeteknél és rendszereknél bekövetkezik a dereguláció, egy társadalmi-technológiai hanyatlás az első fokozatú civilizációs szervezettségi szintre, ahol a természet törvényei objektív módon – a káosz törvénye szerint – hatnak.

[15] Haig, Zs. – Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005. pp. 163-168.

Egy konfliktushelyzetben az alapvető cél saját oldalon a második fokozatú civilizációs rend fenntartása és az ellenfélnél az első fokozatú civilizációs rend ideiglenes kialakítása, vagyis irányíthatatlan helyzet, sajátos káoszrend előidézése.[16] E kettős célt, az információt magát, illetve az információt kezelő rendszerek működését saját oldalon pozitív, illetve az ellenfél oldalán negatív irányban befolyásoló, összehangolt információs tevékenységekkel lehet elérni. Katonai értelmezés szerint ezen összehangolt információs tevékenységeket információs műveleteknek nevezzük.

Az információs műveletek kezdeti jegyei az első Öböl-háborúban (1991) voltak felismerhetők, ahol a szövetséges erők sikerének döntő eleme volt az információs fölény, és vezetési fölény, amelyet multiszenzoros adatszerzéssel, adatfúziós feldolgozási technológiával, számítógép-hálózatokra alapozott harcvezetéssel, az ellenség vezetés-irányítási rendszereinek bénításával és félrevezetésével értek el. Mindezen tevékenységeket tervszerűen, egységes vezetés alatt végezték, ami az információs műveletek egyik alapvető elve.

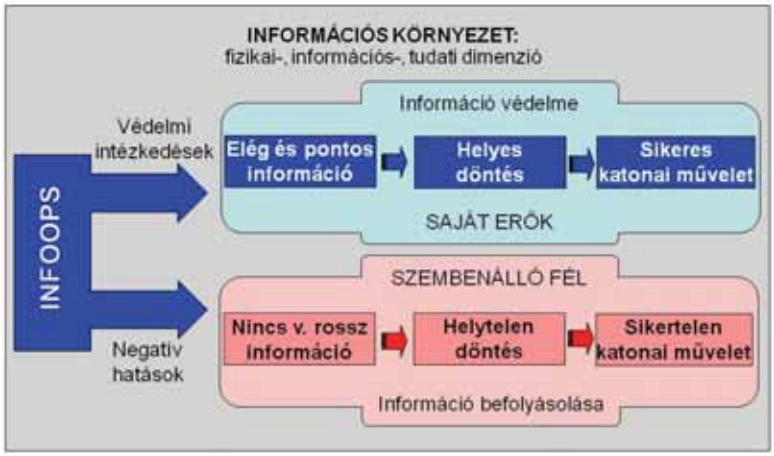
Napjainkban a hagyományos hadszíntereken folyó katonai műveletekkel együtt az információs hadszíntéren információs műveletek is zajlanak. Minden olyan tevékenységet az információs műveletek közé sorolhatunk, amelyek a szembenálló fél információs rendszereire, végső soron információira gyakorolnak olyan hatást, amelyekkel a saját döntéshozók a politikai, gazdasági és katonai célkitűzéseik elérése érdekében támogathatók, illetve amelyek biztosítják a saját információk és az információs rendszerekben rejlő képességek maximális kihasználását és megvédését. Az információs műveletek a már korábban is bemutatott három dimenzióban folynak, úgymint:

– a fizikai dimenzióban;
– az információs dimenzióban; és
– a kognitív (tudati) dimenzióban.

A fizikai dimenzióban jelentkező hatások az információs infrastruktúrák és infokommunikációs rendszerek elemei elleni fizikai támadásokat illetve ezek védelmét jelenti. *Az információs dimenzióban* folytatott információs műveleti tevékenységek az említett elektronikus információs folyamatoknak (például adatszerzés, adattárolás, adatfeldolgozás, kommunikáció) elektronikai úton való, korlátozó hatású támadását jelenti annak érdekében, hogy a célpontokat és azok működését pusztító, romboló fizikai ráhatás nélkül közvetlenül lehessen befolyásolni. Másrészről ide tartozik a szembenálló fél saját elektronikus információs folyamatainkra irányuló hasonló támadásának megakadályozása is. *A kognitív (tudati) dimenzióban* megvalósuló információs tevékenységek a szembenálló fél oldalán közvetlenül az emberi gondolkodást – észlelést, érzékelést, értelmezést, véleményt, vélekedést – veszik célba valós, csúsztatott vagy hamis információkkal, elektronikus és nyomtatott médiával vagy közvetlen beszéd formájában. Saját oldalon pedig az ellenség fenti tevékenységével szembeni védelmi megoldásokat soroljuk e dimenzióba. E dimenzióban a cél a döntéshozók közvetlen befolyásolása, ami egybeesik az információs műveletek információs fölényen keresztül elérni kívánt

[16] U.o. p. 180.

célkitűzésével, vagyis, hogy a döntéshozót olyan helyzetbe hozzuk, hogy saját oldalon optimális döntést hozhasson, másik oldalon pedig pontosan ellentétes hatást érjünk el, amely kihat a katonai műveletek sikerességére vagy sikertelenségére. (1.2. ábra)



1.2. ábra. **Az információs műveletek hatásmechanizmusa**[17]

A fentiek alapján megfogalmazhatjuk, hogy mit is értünk általánosságban információs műveletek alatt. Azért csak általánosságban adjuk meg az információs műveletek definícióját, mert a különböző országokban, katonai szövetségekben (például NATO), a haderőkben és azok doktrínáiban eltérő, különböző területeket jobban kihangsúlyozó vagy másokat háttérbe szorító megfogalmazásokkal, értelmezésekkel is találkozhatunk.

Az információs műveletek tehát a fizikai-, az információs- és a tudati dimenzióban érvényesülő, koordinált tevékenységeket jelentik, amelyek a szembenálló fél információira, információalapú folyamataira és infokommunikációs rendszereire gyakorolt ráhatásokkal képesek befolyásolni a döntéshozókat a politikai és katonai célkitűzéseik elérésében úgy, hogy emellett a saját hasonló folyamatokat és rendszereket hatékonyan kihasználják és megóvják. Az információs műveletek – az információs fölény és a befolyásoló képesség elérése valamint megtartása érdekében – minden szinten (például politikai, gazdasági, kulturális, katonai: hadászati, hadműveleti, harcászati) és minden időben (Béke, válság, háború) alkalmazott információs képességek közötti integráló, szinkronizáló és koordináló tevékenység.

Az információs műveletek célja az információs fölény, információs uralom, és végső soron a vezetési fölény kivívásával a befolyásoló képesség fenntartása, a saját oldali vezetési ciklus számára időcsökkentés, a szembenálló fél vezetési időciklusa tekintetében pedig időnövelés elérése érdekében.

[17] Haig, Zs. – Kovács, L. – Munk, S. – Ványa, L.: *Az infokommunikációs technológia hatása a haditudományokra*. Nemzeti Közszolgálati Egyetem, 2013. p. 83.

Az információs műveletek tehát nem más, mint a különböző elkülönülten is létező, komplex információs tevékenységek közötti integráló, szinkronizáló és koordináló tevékenység, amelynek szükségességét és létjogosultságát az összehangolt információs tevékenységek nagyságrendekkel növelhető hatékonysága adja. Az információs műveletek egymással összhangba hozott széles tevékenységi területen, számos – külön-külön is alkalmazható -információs vagy információalapú tevékenység révén érvényesülnek.

Az információs műveletekkel olyan újfajta eljárások jelennek meg a hadművészetben, amelyek ugyanarra a célra irányulnak, mint a hagyományos hadviselés, azonban módszerei és eszközei az esetek többségében jelentős mértékben eltérnek attól. Míg a hagyományos katonai műveletek alapvetően az ellenség tűzzel való pusztítására irányulnak, addig az információs műveletek elsősorban a szembenálló fél információinak és információs képességeinek, vezetés-irányítási rendszereinek felderítésére, működésük korlátozására, befolyásolására, illetve a saját hasonló képességek és rendszerek alkalmazására és védelmére törekszik a maga sajátos eszközrendszerével és módszereivel. Az ellenség harcoló csapatainak pusztítása nélkül háborús körülmények között nem érhető el tartós siker. Az információs műveletek alkalmazása azonban lényegesen kevesebb erőforrás bevonásával, és a veszteségek jelentős mérséklésével lehetővé teszi a győzelem kivívását. Az információs műveletek lényege éppen az, hogy elemeinek integrált, összehangolt alkalmazása döntő módon képes befolyásolni a fegyveres küzdelem kimenetelét, a katonai és politikai célok elérését.

Az információs műveletek a harc-hadműveleti támogatás körébe tartoznak. Ezek a műveletek a 21. századi teljes katonai műveleti spektrum – például konfliktus, válság, háború, békekikényszerítés, béketeremtés, békefenntartás, békemegőrzés, stabilizáció – minden fázisában megtalálhatók. Az alkalmazott információalapú tevékenységek köre, intenzitásuk és időtartamuk mindenkor a kialakult helyzettől és a feladattól függ.[18]

Mint arra már korábban utaltunk, az információs műveletek a már korábban is létező, és a katonai műveletekben alkalmazott információs tevékenységek közötti összhangot teremti meg. Ennélfogva összetevőit is ezek alkotják, kiegészülve olyan új képességekkel, amelyek csak az információtechnológia fejlődésével, illetve harctéren való megjelenésével egy időben jelenhettek meg (például a számítógép-hálózatok harctéri alkalmazása). Mint ahogy azt már a definíciónál is jeleztük, ugyanazon indokok alapján itt sem adható egy egzakt felsorolás az információs műveletek területeit illetően. Általánosságban az információs műveleteket alkotó elemek közé az alábbiak sorolhatók:

- a műveleti biztonság *(Operation Security – OPSEC)*;
- a katonai megtévesztés *(Military Deception – MILDEC)*;
- a pszichológiai műveletek *(Psychological Operations – PSYOPS)*;
- a fizikai pusztítás *(Physical Destruction – PD)*;
- az elektronikai hadviselés (*Electronic Warfare – EW)*; és
- a számítógép-hálózati műveletek *(Computer Network Operations – CNO)*.

[18] Haig, Zs. – Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005. pp. 181-185.

Az információs műveletek kapcsolódó elemei közé sorolhatjuk a civil-katonai együttműködést *(Civil-Military Cooperations – CIMIC)* és a tömegtájékoztatást *(Public Information – PI)*. A hatékony információs műveletek végrehajtásának alapját mindenesetben a hálózatos infokommunikációs technológián alapuló saját vezetés-irányítási rendszerek és az összadatforrású felderítés adja.

A területek egyenként is alkalmasak arra, hogy a fizikai-, az információs- vagy a tudati dimenzióban hatást gyakoroljanak az információra, információs rendszerekre, valamint információs folyamatokra, és ennek következtében befolyásolják a döntéshozókat a saját és a szembenálló fél oldalán egyaránt. Az információs műveletekben azonban mindezeket egy közös cél érdekében integrálva, szinkronizálva, nagyságrendekkel nagyobb hatékonyságot érhetünk el. Ez az egységes vezetés-irányítás alatt megvalósuló összehangolt alkalmazás adja az információs műveletek lényegét.

Az információs műveletek lényegi összefüggései szinte minden haderőben – ahol alkalmazzák ezt az új típusú hatásalapú műveleti felfogást – megegyeznek. Ugyanakkor több országban (szövetségben) eltérőek lehetnek a kategorizálások.

Az információs műveletek doktrinálisan elsőként az USA haderő doktrináiban jelentek meg. Ebben nincs semmi meglepő, hisz az Egyesült Államok hadereje volt az, amelynek technikai és technológiai fejlettsége lehetővé tette a legkorszerűbb elvek elsőként való kipróbálását, és ennek megfelelően először szerzett tapasztalatokat e területen. A vezetés-irányítási rendszerek elleni összehangolt tevékenység igénye már a ‚80-as években megjelent, azóta pedig az e tevékenységekkel foglalkozó haderőnemi és összhaderőnemi doktrínák folyamatosan fejlődtek. Az USA jelenleg érvényben lévő összhaderőnemi információs műveletek doktrínája az alábbiakban határozza meg az információs műveleteket: *„A katonai műveletek során folytatott tevékenység, amely a többi műveletekkel összehangolt információalapú képességek integrált alkalmazását jelenti, az ellenség vagy a potenciális szembenálló fél döntéshozatali folyamatának befolyásolása, megzavarása, lerontása, vagy korlátozása, illetve a saját döntéshozatali folyamat védelme érdekében."*[19]

A definícióban előtérbe kerül az információs tevékenységek közötti koordináló, integráló funkció úgy, hogy emellett hangsúlyozza a különböző másfajta katonai műveletekkel való szoros összhangot. Kiemeli, hogy az információs műveletek a szembenálló fél és a saját döntési folyamatra kívánnak hatást gyakorolni.

A NATO információs műveletekkel foglalkozó irányelveit először 1998-ban adták ki, amelyet 2002-ben, 2005-ben, majd 2007-ben vizsgáltak felül és dolgoztak át.[20] 2009-ben jelent meg a NATO információs műveletek doktrínája, amely egységes keretbe foglalja a NATO elveket. A doktrína meghatározása szerint: *„Az információs műveletek képesség egy olyan katonai funkció, amely koordinálja a katonai információs tevékenységeket, illetve azzal kapcsolatos tanácsokat ad abból a célból, hogy megfelelő hatást gyakoroljon a szembenálló fél, a lehetséges szembenálló fél, és az Észak Atlanti Tanács (North Atlantic*

[19] Joint Publication 3-13, Information Operations, 27 November 2012, by United States Government US Army. p. GL-3. (fordították a szerzők)

[20] MC 422/3 NATO Military Policy on Information Operations

Council – NAC) által jóváhagyott felek akaratára, helyzetmegértési folyamatára és képességeire, és ezáltal támogassa a Szövetség missziós célkitűzéseit. Az információs tevékenységek hatást gyakorolnak az információra és/vagy az információs rendszerekre. Azokat bármely szereplők végrehajthatják, és védelmi rendszabályokat is tartalmaznak."[21]

A NATO doktrína meghatározza azokat a tevékenységi területeket, amelyeken keresztül az információs műveletek megvalósulnak. Ezek az alábbiak:

– a szembenálló fél, valamint az NAC által jóváhagyott felek érzékelési képességének, magatartásának, viselkedésének megváltoztatására, befolyásolására vagy megerősítésére irányuló információs tevékenységek;
– a Szövetség információs környezetben való manőverszabadságának megőrzésére és megóvására irányuló információs tevékenységek, amelyek biztosítják a Szövetség döntéshozóit és döntéshozatali folyamatait támogató adatok és információk védelmét;
– a vezetési funkciók és képességek elleni tevékenységek, amelyek hatást gyakorolnak a szembenálló felet és más, a NAC által jóváhagyott felet támogató mindazon adatokra és információkra, amelyeket a vezetési és irányítási-, felderítő-, megfigyelő- és célfelderítő-, valamint fegyverrendszerekben használnak.

Ezek kibontásaként a doktrína felsorolja mindazon képességeket, eszközöket és eljárásokat, amelyeket az információs célkitűzések elérésében alkalmaz. Ezek az alábbiak:

– pszichológiai műveletek *(Psychological Operations – PSYOPS)*;
– megjelenés, viselkedés, arculat *(Presence, Posture and Profile – PPP)*;
– műveleti biztonság *(Operation Security – OPSEC)*;
– információbiztonság *(Information Security – INFOSEC)*;
– megtévesztés *(Deception – DEC)*;
– elektronikai hadviselés *(Electronic Warfare – EW)*;
– fizikai pusztítás *(Physical Destruction – PD)*;
– kulcsfontosságú vezetőkkel kapcsolatos tevékenység *(Key Leader Engagement – KLE)*;
– számítógép-hálózati műveletek *(Computer Network Operations – CNO)*;
– civil-katonai együttműködés *(Civil-Military Cooperations – CIMIC)*.

A képességeken, eszközökön és eljárásokon túl kiemeli a kapcsolatot a közügyekkel (nyilvánossággal, tömegtájékoztatással).[22]

Mint látható a NATO doktrína fokozott hangsúlyt fektet az információs műveletek lényegi elemére: a különböző katonai információs tevékenységek koordinálására, szinkronizálására. Az információs műveletek összehangolt alkalmazása során a befolyásoló tevékenységek, az ellentevékenységek és a védelmi tevékenységek közötti szoros kapcsolat kialakítására helyeződik a hangsúly. Ennek eredményeként a felsorolt képességek,

[21] AJP-3.10 Allied Joint Doctrine for Information Operations, 2009. p. 1-3. (fordították a szerzők)
[22] U.o. pp. 1-8. – 1-13.

eszközök és eljárások koordinációjának fő célja a különböző célcsoportok (saját erők, szembenálló fél és más NAC által elfogadott felek) akaratának, megértésének és képességének *(will, understanding and capabilities)* befolyásolása.

A Magyar Honvédségben (MH) az információs műveletek elvei 2002-ben, az MH Összhaderőnemi Doktrína első kiadásában jelentek meg először. A doktrína 2007-ben átdolgozott 2. kiadása a korábbinál bővebb tartalommal foglalkozik e kérdéssel. A 2012-ben megjelent 3. kiadás szerint az információs műveletek „a *műveleti (hadműveleti, harc-) támogatás fajtája. Olyan funkció, mely a katonai információs tevékenységet koordinálja, illetve azzal kapcsolatos tanácsot ad abból a célból, hogy a kívánt hatást gyakorolja az ellenfél, a lehetséges ellenfél döntéseire és képességeire azért, hogy a küldetést, parancsnoki szándékot támogassa. Az információs műveletek olyan cselekmények, melyek célja, hogy hatást gyakoroljanak az információkra és/vagy az információs rendszerekre, úgy, hogy emellett a saját hasonló rendszereket hatékonyan kihasználják és megóvják. Alapvető fajtái a védelmi és a támadó információs műveletek."*[23] A doktrína megfogalmazása alapján az információs műveletek célja: *„az információs fölény, végső soron a vezetési fölény elérésével a hadműveleti előny megszerzése, ezáltal biztosítva az információs fölény birtokosa számára azt, hogy a vezetési rendszereit és azok képességeit kihasználva hadműveleti előnyre tegyen szert, vagy a hadműveletet úgy vezesse és irányítsa, hogy az ellenséget megfossza a képességeitől."*[24]

Az információs műveletek képességeit, eljárásait, eszközeit és technikáit az MH Összhaderőnemi műveleti doktrína ismerteti. E szerint az információs műveletekben az információs fölény és a befolyásoló képesség elérése és megtartása az alábbi területek összehangolt alkalmazásával érhető el:

- lélektani műveletek;
- megjelenés, viselkedés és arculat;
- műveleti biztonság;
- információbiztonság;
- katonai megtévesztés;
- elektronikai hadviselés;
- fizikai megsemmisítés
- kulcsfontosságú személyekkel kapcsolatos tevékenységek; és
- számítógépes hálózati műveletek.[25]

Mint látható az MH doktrináiban foglaltak is többnyire összhangban vannak az információs műveletek általános elméleti összefüggéseivel, és több területen kapcsolódnak más haderők és különösen a NATO doktrináihoz.

Összességében megállapítható, hogy az információs műveletek a fenti képességek alkalmazásával nagymértékben lehetővé teszik a hagyományosnak tekinthető erők és

[23] Magyar Honvédség Összhaderőnemi Doktrína 3. kiadás, 2012, MH kiadvány, p. M1-8.
[24] U.o. p. 4-7.
[25] Magyar Honvédség Összhaderőnemi Műveleti Doktrína 1. kiadás, 2013, MH kiadvány, pp. 1-19. – 1-21.

eszközök gazdaságos felhasználását. Ez azt jelenti, hogy a különböző koordinált információs tevékenységekkel kivívott információs fölény adott esetben kevesebb repülőgép, tüzérségi eszköz, harckocsi, légvédelmi eszköz bevetését teszi szükségessé. Mindez annak köszönhető, hogy egyrészt a saját információs képességeink – a pontos összadatforrású felderítés és az alkalmazott védelmi eljárások, rendszabályok következtében – maximálisan kihasználhatók, a saját vezetési ciklusunk ideje jelentősen lerövidül, másrészt a szembenálló fél hasonló képességei – az alkalmazott befolyásoló jellegű információs műveletek eredményeként – korlátozottakká válnak, vezetési ciklusuk ideje jelentősen megnövekszik. Ebben a helyzetben a szembenálló fél képtelen megfelelően irányítani alárendeltjeit, pontosan meghatározni számukra a harcfeladatokat, tehát a vezetési folyamatban káosz jelentkezik, bekövetkezik a „vezethetetlenség" állapota.[26]

E helyen nem részletezzük az információs műveletek minden egyes összetevőjét. Erre vonatkozóan bővebb információk találhatók a vonatkozó szakirodalomban.[27] Az azonban jól látható, hogy a jelen jegyzet témáját adó elektronikai hadviselés fontos részterületét adja az információs műveleteknek.

1.2 Kibertéri műveletek

1.2.1 A kibertér katonai értelmezése

Az információs hadszíntéren zajló információalapú tevékenységek, így az információs műveletek a céljaik elérése érdekében fizikai-, információs- és tudati (kognitív) dimenzióban fejtik ki hatásaikat. A fizikai dimenzióban az információs környezet és a fizikai világ átfedi egymást. Itt zajlanak a katonai műveletek (például szárazföldi, légi, tengeri), és itt működnek a különböző infokommunikációs rendszerek és hálózatok. Magába foglalja a számítógépeket, távközlési rendszereket, adatátviteli eszközöket és a támogató infrastruktúrákat. Az információs dimenzióban zajlanak az információs folyamatok, mint például az információ gyűjtése, feldolgozása, tárolása, megjelenítése, átvitele és védelme. Itt történik meg az automatizált döntéshozatal és a parancsnok intézkedéseinek eljuttatása az alárendelteknek. A tudati (kognitív) dimenzió felöleli a döntéshozók és a személyi állomány értelmezési folyamatát, gondolatalkotó tevékenységét, itt hozza meg a parancsnok a döntését.[28]

Civil terminológia szerint a kibertér az elektronikus kommunikációs eszközök és rendszerek (például számítógép-hálózatok, telefonvonalak, műholdas rendszerek) és a rajtuk található szolgáltatások, információk alkotta virtuális tér vagy világ összefoglaló

[26] Haig, Zs. – Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005. p. 194.
[27] Haig, Zs. – Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005.
[28] Joint Publication 3-13, Information Operations, 27 November 2012, by United States Government US Armys. pp. I-2. – I-3.

neve. A kibertér meghatározásával kapcsolatban – civil értelmezés szerint – általánosan elterjedt nézet, hogy az a számítógép-hálózatokkal és az internettel van összefüggésben.

A kibertér katonai értelmezése azonban kiterjeszti ezt a dimenziót, és nemcsak a számítógép-hálózatok működési környezetét érti alatta. Az USA Vezérkari Főnökök Egyesített Bizottságának elnöke által 2006-ban kiadott dokumentuma[29] szerint *„a kibertér egy olyan tartomány, ahol hálózatos rendszerekben és fizikai infrastruktúrákban működő elektronikai eszközöket és az elektromágneses spektrumot használják fel az adatok tárolására, cseréjére és módosítására."*[30] Később az USA Védelmi Minisztériuma módosította e meghatározást, mely szerint a kibertér *„az információs környezetben, az egymással kölcsönös függőségben lévő információs infrastruktúrák hálózata által létrehozott globális tartomány, amely magában foglalja az internetet, a távközlési hálózatokat, a számítógépes rendszereket, valamint a beépített feldolgozó és vezérlő elemeket."*[31]

Az MH Kibervédelmi szakmai koncepciójának definíciója szerint a *„kibertér az elektromágneses spektrum használatával meghatározható, dinamikusan változó tartomány, mely az összekapcsolt hálózatok, eszközök és kiegészítő fizikai infrastruktúrák közötti adatok kezelésére szolgál."*[32]

Mint látható mindegyik idézett fogalom alkalmas lehet a kibertér meghatározására. Míg az első és a harmadik definíció hangsúlyozza a kibertérben zajló folyamatokat, addig a második az abban működő eszközökre fókuszál. Az első és harmadik definíció a hálózatos rendszerek működési tartományára az elektromágneses spektrumot határozza meg, az utóbbi meghatározás viszont nem hangsúlyozza ki a hálózati kapcsolat közegét. A hálózatban lévő különböző infokommunikációs eszközök különböző vezetékes kapcsolaton keresztül, illetve az elektromágneses spektrumot felhasználva csatlakozhatnak egymáshoz. A katonai műveletekben is az állandó helyű (stacioner) rendszerek elterjedt hálózati összeköttetési formája a vezetékes kapcsolat, azon belül is a leginkább elterjedőben lévő optikai kábeles csatlakozás. Harcászati-hadműveleti szinten azonban a műveletet végrehajtó manőverező erőknek nincs lehetőségük a vezetékes technológia használatára. A kapcsolattartásra, a számítógép-hálózatok kialakítására ekkor az elektromágneses spektrumban működő eszközöket kell alkalmazni.[33]

Ezek alapján teljességgel elfogadhatjuk az USA Nemzetvédelmi Egyetem professzorának, Daniel Kuehl-nek a definícióját, amely szerint *„a kibertér egy olyan dinamikusan változó műveleti tartomány, amelynek egyedi és megkülönböztető jellegzetessége, hogy ott az egymással hálózatba kapcsolt infokommunikációs rendszerekben és a kapcsolódó infrastruk-*

[29] National Military Strategy for Cyberspace Operations

[30] Fahrenkrug, D. T.: *Cyberspace Defined*. (Letöltve: 2014.03.09.) http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm (fordították a szerzők)

[31] Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms 2010. p. 64.

[32] 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról. Hivatalos Értesítő, a Magyar Közlöny melléklete, 2013. 48. sz., Magyar Közlöny Lap- és Könyvkiadó, 2013. pp. 13873-13882.

[33] Lásd harcászati internet *(Tactical Internet)* koncepció.

túrákban az információ létrehozását, tárolását, módosítását, cseréjét és felhasználását végző elektronikai- és elektromágneses spektrumot használó eszközök működnek."[34]

A definíciók alapján egyértelműen kijelenthetjük, hogy a kibertérnek fontos jellemzője, hogy abban az elektromágneses spektrumot felhasználva és/vagy vezetékes kapcsolaton keresztül hálózatba kötött infokommunikációs rendszerek működnek, amelyek különböző elektronikus információkezelési folyamatokat (például elektronikai úton végrehajtott adatszerzés, adatfeldolgozás, adattárolás, kommunikáció) végeznek. A harctéren a különböző hálózatba kapcsolt infokommunikációs rendszerek az információs hadszíntér azon tartományát használják, amelyben e rendszerek működnek, léteznek (fizikai dimenzióban), a különböző elektronikus információs folyamatok zajlanak (információs dimenzióban), valamint az e rendszerek elleni tevékenység és a védelem megvalósul (fizikai- és információs dimenzióban). Ebből következően tehát a kibertér az információs hadszíntér fizikai- és információs dimenziójában értelmezhető.

Napjainkban a harctéren elektronikai eszközökből (például rádiók, radarok, navigációs eszközök, harctéri azonosító berendezések) és számítógépekből olyan hálózatokat hoznak létre, ahol igen nehéz különválasztani egymástól a rendszert alkotó komponenseket. Ezeket a hálózatokat olyan komplex rendszerként lehet értelmezni, amelyeknek közös műveleti környezetük van. A harctéren ezek a hálózatos rendszerek kisebb részben vezetékes kapcsolatokat használnak, nagyobb részben viszont – többnyire mobil rendszerekként – az elektromágneses energiát használják fel az adatok, információk megszerzésére, továbbítására. A kibertér katonai értelmezésében tehát helyet kap az elektromágneses spektrum, és ezzel párhuzamosan a vezetékes hálózatok jelentette virtuális tér is. Mivel a vezetékes hálózatokhoz való hozzáférés kívülről korlátozott, ezért azon hálózatos rendszerek elleni tevékenység lehet sikeres, amelyek az elektromágneses spektrumot használják, mivel azon keresztül lehet felderíteni és támadni azokat.[35]

Meg kell azonban jegyezni, hogy a harctéren jelenleg még nem minden elektromágneses spektrumban működő eszköz van hálózatba kapcsolva, léteznek önállóan működő elektronikai eszközök is (például önállóan működő felügyelet nélküli szenzorok, egyszeri felhasználású zavaróeszközök, rádió távirányítású eszközök[36]). Így tehát a kibertér nem azonosítható teljes mértékben az elektromágneses spektrum felhasználásával, az csak a hálózatos elektronikai rendszerekre értelmezhető. Egyértelműen megfigyelhető azonban a hálózatosítás irányába való elmozdulás. Egyre több – korábban önálló, független – rendszer működik hálózatos környezetben. Jó példa erre a korábban említett harcászati internet koncepciója, vagy a hálózatos harctéri szenzorrendszerek. Ennek következtében

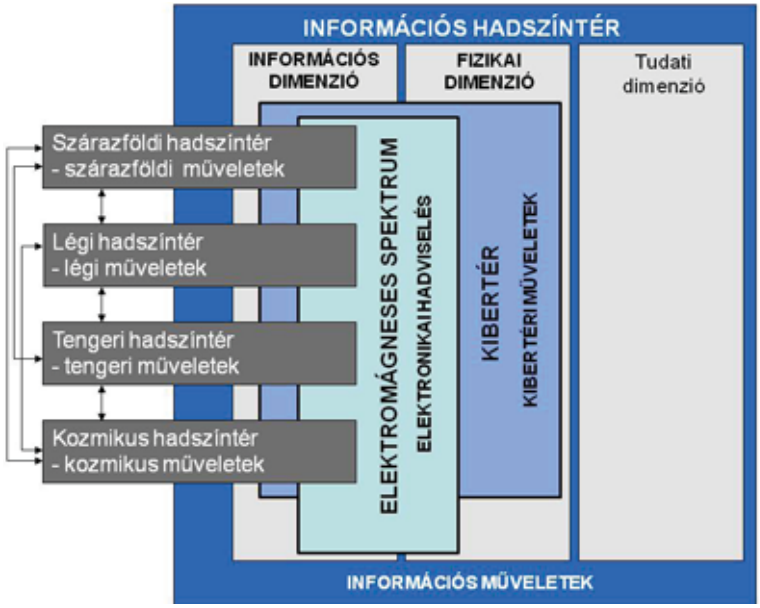
[34] Kuehl, D.: *From Cyberspace to Cyberpower: Defining the Problem*. In: Cyberpower and National Security. ed. Kramer, F. D. et al., Potomac Books Inc. pp. 24-43, 2009. p. 28. (fordították a szerzők)

[35] Haig, Zs. – Várhegyi, I.: *A cybertér és a cyberhadviselés értelmezése*. Hadtudomány, elektronikus szám, 2008, ISSN 1215-4121, pp. 1-12. http://mhtt.eu/hadtudomany/2008/2008_elektronikus/ 2008_e_2.pdf (Letöltve: 2014.03.09.)

[36] Például rádió távirányítású házi készítésű robbanóeszközök *(Radio Controlled Improvised Explosion Devices – RC-IED).*

közeledik egymáshoz e két tartomány, konvergencia figyelhető meg az elektromágneses spektrum és kibertér között.

A kibertér a katonai műveleteknek a földi-, légi-, tengeri- és kozmikus színtereivel hasonlatos, azzal egyenértékű, de azokat átfogó tartománya. Mint ahogy a tengeri hadszíntér jellemezhető a vízfelszínen vagy a víz alatt folytatott műveletekkel, vagy a légi hadszíntér a levegőben folytatott harctevékenységgel, ugyanúgy jellemezhető a kibertér is a vezetékes kommunikációs közeget és/vagy az elektromágneses spektrumot felhasználó hálózatba kötött elektronikai rendszerekkel. A leírtakat összefoglalóan szemlélteti az 1.3. ábra.



1.3. ábra. **A kibertér értelmezése**[37]

Az internet sebezhetősége ismert tény. Az információs társadalomban igen sok szolgáltatás és információs rendszer (köztük számos kritikus információs infrastruktúra) használja az internetet. Ezért az internetnek – mint önmagában is kritikus infrastruktúrának – a biztonsága nemzetbiztonsági szempontból rendkívül fontos kérdés, melyet a kritikus információs infrastruktúrák védelmének megszervezése során figyelembe kell venni. Ugyanakkor egy országban számos olyan hálózatos rendszer is működik, amelyek nem csatlakoznak az internethez. A katonai vezetés-irányítási *(Command and Control – C2)* rendszerek többsége ilyen elszigetelt, zárt hálózatokként működnek, közvetlenül

[37] Haig, Zs. – Kovács, L. – Munk, S. – Ványa, L.: *Az infokommunikációs technológia hatása a hadtudományokra*. Nemzeti Közszolgálati Egyetem, 2013. p. 58. (a forrás alapján szerkesztették a szerzők)

nem kapcsolódnak a világhálóhoz. Tehát ha csökkenteni akarjuk az ellenség vezetési-irányítási képességeit, akkor ezeket a hálózatokat a kibertérben elektronikai úton, az elektromágneses tartományban lehet támadni.[38] Ez a megállapítás viszont is igaz. Ha a saját hálózatainkat meg akarjuk védeni, a működőképességét fenn kívánjuk tartani, akkor azt jó eséllyel tudjuk megtenni a vezetékes hálózatok vonatkozásában. A vezeték nélküli hálózatok védelmére viszont olyan eszközöket, eljárásokat és módszereket kell alkalmazni, amelyeket az elektromágneses spektrumban tudunk megvalósítani. Ezek a kibertérben folyó támadó és védelmi tevékenységek a kibertéri műveletekben *(Cyberspace Operations)* zajlanak.

1.2.2 A kibertéri műveletek értelmezése

A kibertérben folyó műveletek során a hálózatos képességek saját oldalon való kialakítása, fenntartása, illetve a szembenálló fél oldalán való gyengítése, lerontása döntő fontosságú. A kibertérben folyó tevékenységek során a cél a kiberfölény megszerzése és megtartása. A kiberfölény az információs fölény azon részét képezi, amelyet a különböző hálózatba kötött elektronikai eszközökkel, rendszerekkel és számítógépekkel tudunk elérni, és amelynek következtében a saját erők cselekvési szabadsága jelentős mértékben megnő. A kiberfölény kivívásának és megtartásának három egyenrangú és egymással szoros kapcsolatban lévő eleme különböztethető meg:

- a különböző hálózatba szervezett elektronikai eszközökkel, infokommunikációs rendszerekkel az információ biztosítása a kialakult és a várható helyzetről;
- a szembenálló fél hálózatos elektronikai eszközei, infokommunikációs rendszerei működésének korlátozása, akadályozása;
- a saját információs képességek kihasználása és megóvása a szembenálló fél elektronikus úton végrehajtott különböző támadásaival szemben.

Az információ biztosítása a kialakult és a várható helyzetről egyrészt a szembenálló fél elektronikai rendszereinek, számítógép-hálózatainak felderítését, másrészt a saját erők helyzetéről szóló információk elektronikus feldolgozását, tárolását és továbbítását, harmadrészt pedig a harctéri környezetről szóló adatok (például terepviszonyok, időjárás) elektronikai rendszerekkel, eszközökkel való megszerzését, feldolgozását,[39] továbbítását jelenti.

A szembenálló fél hálózatos elektronikai eszközei, infokommunikációs rendszerei működésének korlátozása, akadályozása alatt egyrészt az elektronikai hadviselés keretében végrehajtott ellentevékenységi módszereket értjük, mint például elektronikai zavaró eszközökkel az ellenséges híradás megbontása, légvédelmi radarrendszerek zavarása,

[38] Fahrenkrug, D. T.: *Cyberspace Defined*. (Letöltve: 2014.03.09.) http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm

[39] Például meteorológiai lokátorokkal adatok megszerzése, digitális térképi információk feldolgozása térinformatikai módszerekkel.

különböző elektronikai megtévesztő tevékenységek folytatása, vagy nagy energiájú impulzus fegyverekkel (e-bomba) az ellenséges elektronikai eszközök, számítógépek tönkretétele. Másrészt a számítógép-hálózati műveletek keretében az ellenséges számítógép-hálózatokba való behatolást, és ennek következtében például adatbázisok tönkretételét, módosítását, programfutási hibák előidézését jelenti.

A saját információs képességek kihasználása és megóvása a szembenálló fél elektronikus úton végrehajtott különböző támadásaival szemben magába foglalja a saját hálózatos infokommunikációs rendszereinkben rejlő lehetőségek maximális kihasználását, vagyis a hálózatalapú műveleti képességek kialakítását és fenntartását, illetve e rendszereink elektronikai- és számítógép-hálózati védelmét.

A kiberfölény fentiek szerinti értelmezése az információs fölényhez kapcsolódik, annak azon részét képezi, amelyet a kibertérben lehet kivívni, és amelynek elérését a harctéren alkalmazott hálózatba kötött elektronikai berendezések és infokommunikációs rendszerek kihasználása, sajátoldali védelme és ellenség oldali támadása biztosítja. Kiberfölény nélkül a teljes információs fölény nem vívható ki és nem tartható meg. A kiberfölény kivívására irányuló képességek megteremtése döntő fontosságú napjaink katonai műveleteiben.[40]

Mint ahogy a kiberfölényt az információs fölény részeként értelmezzük, úgy annak kivívása az információs műveleteken belül folytatott kibertéri műveletekkel valósítható meg. Tekintettel a kibertér katonai értelmezésére, a kibertérben folytatott műveletek közé sorolhatjuk például a számítógép-hálózatok feltérképezését, azokba való bejutást és az adatbázisok tönkretételét, a szerverek túlterhelését, a távközlési hálózatok lehallgatását, zavarását és a navigációs rendszerek elleni elektronikai ellentevékenység különböző formáit is. A felsorolt kibertéri tevékenységek csak néhány kiragadott példa arról a széles palettáról, amelyek támadó céllal alkalmazhatók a szembenálló fél hálózatos elektronikai rendszerei és számítógép-hálózatai ellen, illetve védelmi jelleggel a saját hasonló rendszereink megóvása érdekében.

A kibertéri műveletek célja a kiberfölény kivívása és fenntartása, egyfelől a saját oldali hálózatalapú elektronikus információszerző, -továbbító, -feldolgozó rendszerek védelmével, másfelől a szembenálló fél hasonló rendszerei működésének zavarásával, korlátozásával, lefogásával, vagy akár elektronikus úton történő megsemmisítésével.

Mint azt korábban említettük, nem minden elektronikai eszköz működik hálózatban. Ebből következően az elektronikai hadviselésnek csak azon tevékenységeit soroljuk a kibertéri műveletek területei közé, amelyeket a hálózatos elektronikai rendszerekkel szemben vagy saját oldalon azok védelmére alkalmaznak. Mint ahogy az információs műveletek alapját képezik a katonai információs rendszerek, illetve az összadatforrású felderítés, úgy a kibertéri műveletek alapját is a hálózatokra épülő elektronikus információs rendszerek, és a különböző szenzorhálózatokra épülő elektronikai felderítés képezi. Itt is különbséget kell azonban tennünk a hálózatba kapcsolt eszközök elektronikai

[40] Haig, Zs. – Várhegyi, I.: *A cybertér és a cyberhadviselés értelmezése*. Hadtudomány, elektronikus szám, 2008, ISSN 1215-4121, pp. 1-12. http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf (Letöltve: 2014.03.09.)

felderítése és az elektromágneses spektrumot felhasználó, autonóm módon működő eszközök elektronikai felderítése között. Míg az előző része a kibertéri műveleteknek, az utóbbi eszközök felderítése – bár az elektromágneses spektrumban történik – nem az. Mindezekre tekintettel a kibertéri műveletek területei közé – az elektronikai hadviselésre és az elektronikai felderítésre vonatkozó hálózatos megkötéseket figyelembe véve – az alábbiakat soroljuk:

- számítógép-hálózati műveletek;
- elektronikai hadviselés;
- elektronikai felderítés.

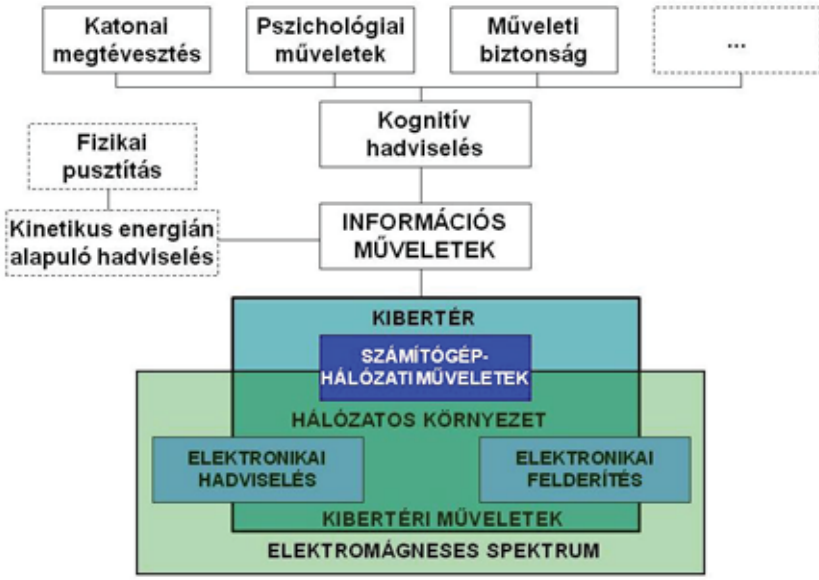
Ki kell hangsúlyoznunk, tehát, hogy míg a számítógép-hálózati műveletek teljes körűen beletartoznak a kibertéri műveletekbe, addig az elektronikai felderítés és az elektronikai hadviselés csak a hálózatos infokommunikációs környezetben értelmezhetők a kibertéri műveletek területeiként. (1.4. ábra)

A számítógép-hálózati műveletek egyrészt a szembenálló fél hálózatba kötött informatikai rendszerei működésének befolyásolására, lerontására, lehetetlenné tételére irányul, másrészt viszont a saját hasonló rendszerek működésének fenntartására törekszik a számítógép-hálózati ellentevékenység és a számítógép-hálózati védelem eszközeivel és módszereivel. A számítógép-hálózati műveletek magukba foglalják:

- a számítógépes hálózatok struktúrájának feltérképezését;
- a forgalmi jellemzőik alapján a hierarchikus és működési sajátosságok feltárását;
- a hálózaton folytatott adatáramlás tartalmának regisztrálását;
- a hálózatokban folyó megtévesztő, zavaró tevékenységet;
- a célobjektumok program-, és adattartalmának megváltoztatását, megsemmisítését; valamint
- a szembenálló fél hasonló tevékenysége elleni védelmet.

A számítógép-hálózati támadás szoftveres vagy hardveres úton való behatolást jelent a szembenálló fél számítógép-hálózataiba, azzal a céllal, hogy tönkretegyük, módosítsuk, manipuláljuk, vagy hozzáférhetetlenné tegyük az adatbázisaiban tárolt adatokat, információkat, illetve magát a hálózatot vagy annak egyes elemeit. A támadás a számítógép-hálózati elemekben való fizikai károkozást is jelentheti, amelyet a szoftverek módosításával vagy manipulációjával lehet elérni.

A számítógép-hálózati támadás eszközei közé tartoznak a különböző kártékony, rosszindulatú programok, melyeket malware-eknek *(Malicious Software)* nevezünk. A malware azon szoftverek gyűjtőneve, amelyek közös jellemzője, hogy anélkül jutnak a rendszerbe, hogy arra a felhasználó engedélyt adott volna. Ezek közé sorolhatóak többek között: a vírusok, a programférgek, a trójai programok, a rootkitek, a böngésző eltérítők, a backdoor programok, a keyloggerek, a spam proxyk, a spyware és az adware programok, és a sort még folytathatnánk. A rosszindulatú szoftverek módosíthatják a programokat, erőforrásokat foglalhatnak le, adatokat törölhetnek, módosíthatnak, hardverhibát eredményezhetnek, eltávolításuk pedig megfelelő eszközöket, időt és energiát, egyes esetekben pedig különleges szakértelmet igényelhet.



1.4. ábra. **Kibertéri műveletek értelmezési tartománya és területei**[41]

A rosszindulatú szoftverek – ötvözve azok alkalmazásának különböző módszereivel – lehetővé teszik a hálózatba való behatolást, működésének akadályozását, megbontását, illetve az adatokhoz való hozzáférést. A támadóknak számos támadási módszert és eszközt kell kombinálniuk, hogy kikerüljék mindazokat a védelmi eljárásokat, amelyeket a hálózatok biztonsága érdekében alkalmaznak. A hálózatok támadására nagyon sokféle módszer létezik,[42] így a támadóknak csak a megfelelő szakértelemre van szükségük, hogy a támadás eszközeit a megfelelő eljárásokkal kombinálják.

A számítógép-hálózati védelem a saját számítógép-hálózat megóvását jelenti a jogosulatlan hozzáféréssel és behatolással szemben, amelyet abból a célból hajtanak végre, hogy megszerezzék az adatbázisokban tárolt adatokat illetve, hogy szándékosan lerontsák, működésképtelenné tegyék infokommunikációs rendszerünket. A számítógép-hálózatok védelmének megvalósítása lehet passzív és aktív. A passzív védelmi módszerek és eszközök lehetnek: a tűzfalak; a vírusirtók; a hozzáférés szabályozás, valamint a behatolás detektálás és adaptív válaszlépések. Az aktív védelem módszerei közé sorolhatók a megelőző támadások, az ellentámadások és az aktív megtévesztés.[43]

41 Bourque, J.: *The Language of Engagement and the Influence Objective*. The Journal of Electronic Defense, Vol. 30. No.11., 2007. pp. 30-35. (a forrás alapján szerkesztették a szerzők)

42 Például Sniffing, Spoofing, Session Hijacking, Spamming, Man-in-the-Middle Attack és a leggyakrabban alkalmazott túlterheléses támadás *(Distributed Denial of Service – DDoS).*

43 Holdaway, E. J.: *Active Computer Network Defense: An Assessment*. Air Command and Staff College. Maxwell Air Force Base, Alabama, 2001. pp. 11-26.

A kibertéri műveletek során alkalmazott számítógép-hálózati védelem felsorolt módszereinek és eszközeinek együttes és komplex alkalmazása növeli a számítógép-hálózatok biztonságát. Eredményes védelem alkalmazása esetén biztosítható a számítógépes rendszerben tárolt adatok esetében a bizalmasság, titkosság (lehallgatás elleni védelem); a sértetlenség (adatok törlése, módosítása elleni védelem); illetve a számítógépes rendszer által ellátott funkciók esetében a rendelkezésre állás (szolgáltatás működésének megakadályozása elleni védelem).

Az elektronikai felderítés céljára alkalmazott technikai eszközök képesek a teljes frekvenciaspektrumban adatokat gyűjteni, azokat akár automatikusan is a fúziós technológián alapuló adatfeldolgozó központokba továbbítani, ahol értékes felderítési információkat lehet nyerni belőlük.

A felderítés természetesen nem minden esetben épül az elektronikai eszközökkel végzett adatszerzésre, de mindegyikben megtalálhatók adatszerzési- vagy adattovábbítási-, és feldolgozási szinteken az elektronikus eszközök. Az összadatforrású felderítés adatfúziós technológiája biztosítja a különböző érzékelési tartományú szenzorok által szerzett adatok összegyűjtését, feldolgozását, összegzését és az eredmények szétosztását. Ezáltal a felderítési információk hitelesebbé válnak, és így például az ellenséges megtévesztés, félrevezetés hatékonysága jelentősen csökkenthető, mivel a korábbi egyforrású felderítés helyett egy adott célobjektumról több forrásból (például radar felderítéssel, képi felderítéssel, rádiófelderítéssel) szerezhetők adatok. Az elektronikai felderítésről bővebben a 2. fejezetben lesz szó.

Az elektronikai hadviselést a következő alfejezetben, illetve a következő fejezetekben részletesen tárgyaljuk.

A kibertéri műveleti erőkhöz és eszközökhöz tartoznak az elektronikai hadviselési erők és eszközök továbbá azok az új, kibontakozó és gyorsan fejlődő hálózati támadó és védelmi erők és eszközök, amelyeket a számítógép-hálózati műveletek keretében alkalmaznak, továbbá ide sorolhatjuk az elektronikai felderítést végző erőket és eszközöket is. Ezen erők és eszközök hatékonyságát nagyságrendekkel növelik azok hálózatba szervezése, aminek következtében működésük egységes adatbázis alapján, az összadatforrású felderítés (adatfúzió) nyújtotta előnyöket kihasználva valósul meg.

Összegzésként megállapíthatjuk, hogy az elektronikai hadviselés részét képezi az információs hadszíntéren folyó információs műveleteknek, és azon belül az információs hadszíntér részeként megjelenő kibertérben folyó kibertéri műveleteknek is.

1.3 Az elektronikai hadviselés fogalma, területei

1.3.1 Az elektronikai hadviselés fogalma, értelmezése

Napjainkba a korszerű haderő hatékonysága jelentős mértékben az *elektromágneses spektrum, tágabb értelemben a teljes frekvenciaspektrum* használatán alapul. A vezetési és irányítási rendszerek tevékenységében, valamint a védelmi és a támadó fegyverek irányításának általános eljárási rendjében jelentős szerepe van a frekvenciaspektrum megha-

tározott részeinek.[44] A katonai erők széles körűen alkalmazzák a teljes frekvenciaspektrumot a híradás, a fegyverrendszerek irányítása, a felderítés és megfigyelés, a navigáció, a kisugárzó munkahelyek és az erők megóvása érdekében. Az e területeken alkalmazott elektronikai eszközök jelentősen növelik a csapatok alkalmazási lehetőségeit, a fegyverrendszerek hatékonyságát, és a technikai eszközök és az élőerő túlélőképességét. Ebből következően a katonai műveleteket irányító parancsnokok kiemelt figyelmet kell, hogy fordítsanak a felelősségi- és hadműveleti körzetükben a frekvenciaspektrum felhasználására.

A hadszíntéren – amely a frekvenciaspektrumban végzett műveletek szempontjából *elektronikus harcmezőnek* is nevezhető – számtalan különböző típusú és rendeltetésű elektronikai eszköz található. Ezek az eszközök egyfajta osztályozás szerint a következők lehetnek:

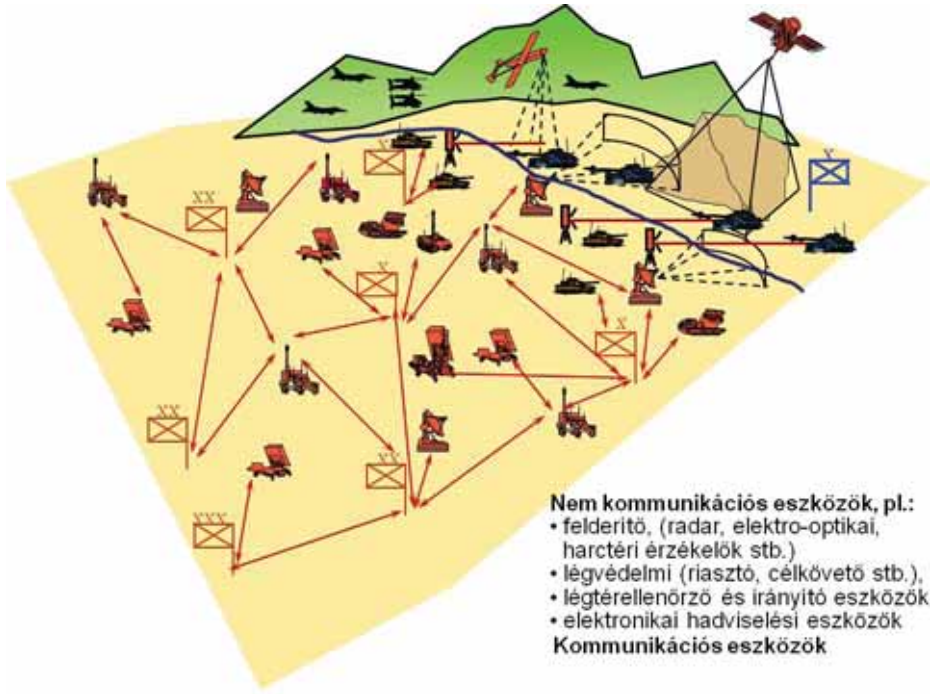
- nem kommunikációs eszközök:
  - felderítő eszközök, melyek minden forrásból biztosítják az adatok megszerzését a harctéren;
  - légvédelmi eszközök, melyek biztosítják a légtér ellenőrzését, a célkövetést és célmegjelölést, valamint a légvédelmi rakéta komplexumok célokra történő rávezetését;
  - légi irányító eszközök, melyek biztosítják a repülőgépek légtérben történő irányítását, navigálását;
  - elektronikai hadviselési eszközök, melyek az ellenség katonai információs rendszereiben működő elektronikai eszközök célmegjelölését, zavarását, megtévesztését és pusztítását, vagy rongálását biztosítják;
- kommunikációs eszközök, amely a harctéren a legnagyobb számban használt elektronikai eszközcsoport. Ezek az eszközök az elöljáró, alárendeltek, szomszédok közötti összeköttetést, az adatok, információk különböző formátumban való továbbítását biztosítják. (1.5. ábra)

Ezek az eszközök ugyanazon környezetben, többnyire az *elektromágneses környezetben (Electromagnetic environment)* működnek. Ez az elektromágneses környezet a fegyveres küzdelem elektronikai színtere, ahol a szemben álló felek elektronikai eszközei egyidejű tevékenységet folytatnak.

Az elektromágneses környezet összetevői:

- frekvenciaspektrum;
- elektronikai eszközök technikai paraméterei (például üzemi frekvencia, sávszélesség, moduláció, teljesítmény, érzékenység, impulzus paraméterek, átviteli sebesség, antenna paraméterek);
- tér;
- idő.

[44] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 3.



1.5. ábra. **Elektronikus harcmező**[45]

A frekvenciaspektrum feletti uralom megszerzése és fenntartása a haderő egyik kulcsfontosságú célja, amelyben a parancsnok rendelkezésére álló elsődleges eszköz az elektronikai hadviselés. Az elektronikai hadviselés olyan harci képességeket foglal magában, amelyek kiegészítik más fegyverrendszerek hatását.[46]

Az MH Összhaderőnemi Doktrína definíciója alapján: „A*z 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.”*[47]

Az MH Összhaderőnemi Műveleti Doktrína szerint *„Az elektronikai hadviselés az elektromágneses spektrum felhasználására irányuló katonai tevékenység, amely magában foglalja: az elektromágneses kisugárzások kutatását, felfedését és azonosítását, az elektromág-*

[45] Szerkesztették a szerzők.

[46] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 3.

[47] Magyar Honvédség Összhaderőnemi Doktrína 3. kiadás, 2012, MH kiadvány, p. M1-3.

neses – ezen belül az irányított – energia alkalmazását, abból a célból, hogy csökkentse vagy megakadályozza az elektromágneses spektrum ellenséges felhasználását, egyúttal biztosítsa hatékony használatát a saját erők számára."[48]

Végül az érvényben lévő MH Összhaderőnemi Elektronikai Hadviselés Doktrína a következőképpen határozza meg az elektronikai hadviselést. *„az EM (elektromágneses) spektrumot hasznosító azon katonai tevékenység, amely magában foglalja az elektromágneses kisugárzások kutatását, felfedését és azonosítását, az irányított energiát is beleértve az elektromágneses energia felhasználását abból a célból, hogy megakadályozza vagy korlátozza az ellenség részéről az EM spektrum hatékony használatát, és lehetővé tegye annak a saját csapatok általi használhatóságát."*[49]

Látható, hogy a különböző szintű doktrínák meghatározásaiban nincsenek lényegi eltérések. A doktrínák szerinti definíciók azonban nem tartalmazzák a mechanikus rezgések tartományát, azaz az akusztikus hullámtartományt, ami nélkülözhetetlen például a harctéri szeizmikus érzékelők, a víz alatti hidroakusztikus eszközök, vagy akár az akusztikus lehallgatás, illetve az ultrahangtartomány speciális eszközei számára. A későbbiekre tekintettel a fogalomban tehát az elektromágneses spektrum helyett a teljes frekvenciaspektrum kifejezést alkalmazzuk.

Az elektronikai hadviselés a harcképességet jelentősen befolyásoló tényező. Fontossága abból adódik, hogy feltárja az ellenség gyenge pontjait, védi a saját cselekvési szabadságot, növeli a saját elektronikai rendszerek biztonságát és csökkenti a sebezhetőségüket.

Az elektronikai hadviselés szerves része mindenfajta katonai műveletnek és egyike az információs műveletek elemeinek. Az elektronikai hadviselés elősegíti az értékelő és döntéshozó folyamatot, hozzájárul a műveletek szervezéséhez és a harc-, hadművelet irányításhoz, óvja a csapatokat az ellenséges tevékenységektől, és biztosítja az elektronikai eszközeink működését a saját csapatok kisugárzó eszközeinek nem szándékos elektromágneses interferenciái mellett is.[50] Az elektronikai hadviselés – a parancsnok elhatározásától függően – lehet folyamatos, vagy időben korlátozott. Az elektronikai hadviselési tevékenység hatása lehet ideiglenes vagy végleges.

A katonai műveletekben az elektronikai hadviselés alkalmazása az alábbi feladatcsoportba sorolható:

- a saját vezetési és irányítási-, valamint más elektronikai rendszerek számára a frekvenciaspektrumhoz való hozzáférés, védelem és felhasználás biztosítása;
- a hasonló ellenséges rendszerek számára a frekvenciaspektrumhoz való hozzáférés, védelem és felhasználás akadályozása;
- adott terület, csapatok, illetve harceszközök (platformok) védelme;
- információval hozzájárulás az Egységes Felderítő Információgyűjtő Rendszerhez *(Intelligence, Surveillance, Target Acquisition and Reconnaissance – ISTAR)*;

[48] Magyar Honvédség Összhaderőnemi Műveleti Doktrína 1. kiadás, 2013, MH kiadvány, p. M1-2.

[49] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 5.

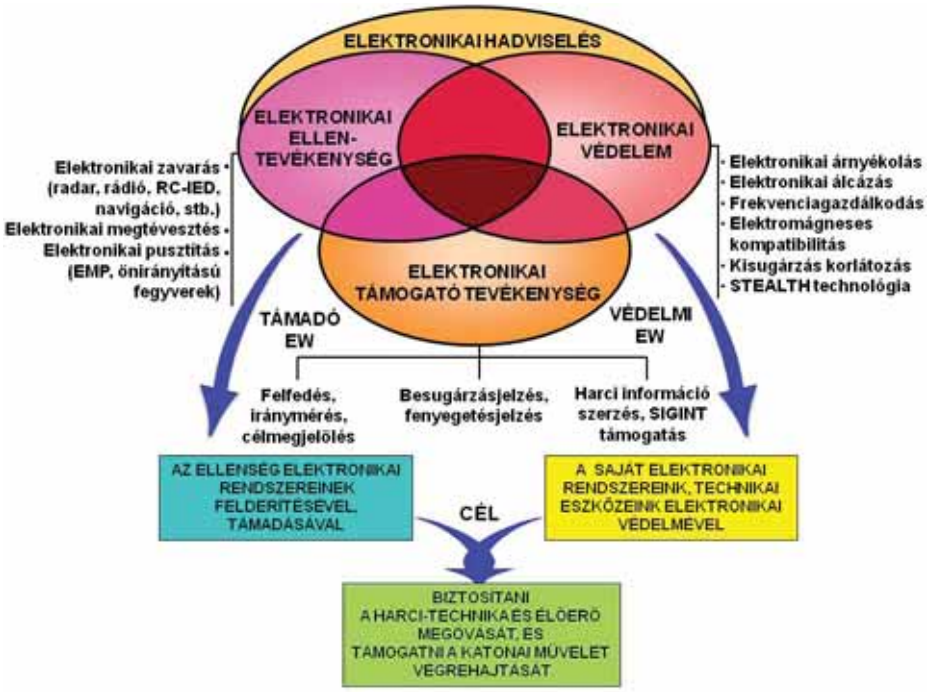
[50] Haig, Zs. – Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005.

– a támadó és védelmi műveletek támogatása, beleértve az ellenséges légvédelem lefogását *(Suppression of Enemy Air Defence – SEAD)*, és az információs műveleteket is.[51]

1.3.2 Az elektronikai hadviselés területei

Az elektronikai hadviselés három egymást kiegészítő, valamint egymást részben átfedő területre osztható, úgymint:

– elektronikai támogató tevékenység *(Electronic Support Measures – ESM)*;
– elektronikai ellentevékenység *(Electronic Counter Measures – ECM)*; és az
– elektronikai védelem *(Electronic Protection – EP)*. (1.6. ábra)



1.6. ábra. **Az elektronikai hadviselés területei**[52]

Az elektronikai hadviselés egy olyan *kétoldalú tevékenység*, melynek alapvető célja az ellenség katonai információs rendszereinek elektronikai úton való támadása, illetve

[51] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 6.
[52] Szerkesztették a szerzők.

a saját hasonló rendszerek működésének biztosítása, az élőerő és a csapatok megóvása. Eszerint az elektronikai hadviselésnek van egy *támadó (offenzív)* és egy *védelmi (defenzív)* oldala.

A támadó oldal az elektronikai hadviselés olyan alkalmazását jelenti, mely lehetetlenné teszi vagy akadályozza az ellenség elektronikai eszközeinek hatékony alkalmazását. Ide tartozik az elektronikai ellentevékenység és az e tevékenység számára célinformációkat biztosító elektronikai támogató tevékenység.

A védelmi elektronikai hadviselés körébe tartoznak azok a tevékenységek és rendszabályok, melyek elősegítik a frekvenciaspektrum hatékony felhasználását. Mivel a parancsnokok a katonai műveletek során nagymértékben alapoznak a vezetést, irányítást kiszolgáló elektronikai eszközökre, ezért a defenzív elektronikai hadviselés elsődleges feladata védeni ezen eszközöket a felderítés, helymeghatározás, azonosítás és elektronikai úton végrehajtott támadásokkal szemben. Ugyanakkor a saját elektronikai eszközökre jelentős hatással lehetnek a saját csapataink által véletlenül, vagy akaratukon kívül generált nem szándékos zavarok is, melyek kiküszöbölése szintén a defenzív oldal feladata. A frekvenciaspektrum általunk történő felhasználásának biztosításában az elektronikai hadviselés mindhárom területe részt vesz.

Az elektronikai hadviselést – mint a frekvenciaspektrum feletti uralom megszerzésének alapvető módszerét, tevékenységét és eszközét –, illetve annak egyes területeit az elektronikai hadviselés szakcsapatok végzik, más területeit viszont minden haderőnem, fegyvernem és szakcsapat végrehajtja. Az elektronikai hadviselés magába foglal *aktív* (érzékelhető) és *passzív* (rejtett, nem érzékelhető) tevékenységeket. Az elektronikai támogatás passzív, az elektronikai ellentevékenység és az elektronikai védelem mindkettő lehet.[53]

Az elektronikai hadviselést – időtartam szerint – rendszeresen, folyamatosan, illetve időszakosan folytatják. Az elektronikai védelem és az elektronikai támogatás rendszeres, minden időben (békében, válsághelyzetben, háborús tevékenységben, nem háborús tevékenységben) folyamatosan végzendő és végezhető tevékenységi forma. Az elektronikai ellentevékenység ezzel szemben csak meghatározott időszakokban, a katonai műveletek időszakainak megfelelően, időszakosan folytatott tevékenység.

1.3.2.1 Elektronikai támogató tevékenység

„Az elektronikai támogatás az elektronikai hadviselés azon területe, amely az ellenség helyzetére vonatkozó tájékozottság és a fenyegetés késedelem nélküli felismerése céljából magában foglalja az elektromágneses kisugárzások kutatását, felfedését és azonosítását, valamint a kisugárzók helyének meghatározását."[54]

Az elektronikai támogató tevékenység hasonlóan az elektronikai úton végzett felderítéshez az ellenség által használt elektromágneses- és más fizikai rezgéstartományokból

[53] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 5.
[54] U.o. p. 6.

nyeri ki információit, vagyis az elektromágneses és más kisugárzások jeleinek érzékelésével, azonosításával és azok felhasználásával kapcsolatos tevékenység. Az elektronikai támogatás fontos információkkal szolgál arról, hogyan használja az ellenség a teljes frekvenciaspektrumot. Az elektronikai támogatás érzékeli, azonosítja és felhasználja az ellenség szándékos (például rádióadás) és a nem szándékos (például hajtómű gázok infravörös tartományú) kisugárzásait.

A rádiófrekvenciás tartományban végzett elektronikai támogató tevékenységnek gyakorlatilag azonosak a feladatai a rádióelektronikai felderítéssel *(Signal Intelligence – SIGINT)*, de feladatait a közvetlen harcoló parancsnok követelményei alapján végzi. Az alapvető különbséget a rádióelektronikai felderítés és az elektronikai támogatás között az határozza meg, hogy a megszerzett információt mire használják. Az elektronikai támogatás *harci információkat* szolgáltat, melyeket fel lehet használni elektronikai ellentevékenységhez, tüzérségi tűz-, vagy repülő csapások kiváltásához, a csapatok manőveréhez, vagy a veszély elhárításához. Mindezt a vett információ rövid idejű analizálása és feldolgozása, valamint viszonylagosan rövid érvényességi ideje teszi lehetővé. A rádióelektronikai felderítés ugyanakkor *felderítési információkat* továbbít az összfegyvernemi törzs felé a parancsnoki döntéstámogatás céljából.[55]

Az elektronikai támogató tevékenység egy adott műveleti környezetben szinkronizálja és integrálja a különböző érzékelőket, elektronikai eszközöket és folyamatokat annak érdekében, hogy ezáltal csökkentse az ellenséggel, a környezettel, az idővel, és a tereppel kapcsolatos bizonytalanságot. Az elektronikai támogatással szerzett adatok hozzájárulhatnak a SIGINT-hez és más elektronikai úton végzett felderítő tevékenységhez, valamint célmegjelölési információt biztosítanak az elektronikai vagy fizikai támadás számára.[56]

Az elektronikai támogatás minden időben, így béke, válság és háború esetén egyaránt folytatott tevékenység, amely békeidőben alapvetően az elektronikai hadviselés hadműveleti adatbázisának feltöltésére irányul. A legtöbb elektronikai támogató tevékenység hadműveleti és harcászati szinten, napszaktól, időjárástól függetlenül hozzájárul a nagy hatótávolságú információgyűjtő rendszerek működéséhez.

Az elektronikai támogató tevékenység információt biztosít:

- az elektronikai ellentevékenységhez;
- az elektronikai védelem megszervezéséhez;
- az önvédelmi tevékenységek megszervezéséhez;
- a fegyverrendszerek célmegjelöléséhez;
- az elektronikai hadviselési adatbázis létrehozásához és aktualizálásához;
- a más forrásból származó felderítési információk megerősítéséhez; valamint
- az információs műveletek támogatásához.[57]

[55] Haig, Zs. – Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005.

[56] Joint Publication 3-13.1, Electronic Warfare, 08 February 2012 , by United States Government US Army p. I-6.

[57] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, pp. 6-7.

Az elektronikai támogatás által gyűjtött információkat elsősorban a közvetlen fenyegetés azonnali felismerésére, illetve célmegjelölésre alkalmazzák, ezenkívül hozzájárulhat az adott törzs felderítő adatgyűjtéséhez.

Az elektronikai támogató tevékenység *fenyegetést jelző funkciója* azt jelenti, hogy speciális elektronikai eszközök érzékelik a tér különböző irányaiból érkező elektromágneses és más tartományú hullámokat, értékelik azokat, döntenek arról, hogy milyen típusú fenyegetés érte az oltalmazott objektumot, és az eredményről jelzést küldenek a kezelőknek, valamint az önvédelmi rendszert vezérlő automatika felé. E funkcióra jó példa a repülőgépek önvédelmi elektronikai rendszereinek fenyegetettség jelző alrendszere, amely képes a repülőgép ellen indított önirányítású (például radar-, infra-, lézervezérlésű) rakéták közeledését érzékelni, kijelezni, riasztani, és automatikus működés esetén az elhárító eszközöket (például radarzavaró, infracsapda) működésbe hozni. Az elektronikai támogató tevékenységet, a harci technikai eszközök és földi létesítmények önvédelme érdekében együtt alkalmazzák más szenzorokkal és az ellentevékenységi rendszerekkel. Ez különösen igaz a repülőterekre, kommunikációs és logisztikai központokra, hajókra, repülőgépekre és helikopterekre, valamint a földi erők harcjárműveire, újabban pedig a földi és légi robotokra is.

Az elektronikai támogatás *célmegjelölő funkciója* azt jelenti, hogy az elektronikai ellentevékenység hatékony végrehajtásához biztosítja a célpontok felfedését, azonosítását, és elhelyezkedésük meghatározását. A hatékony zavarás kiváltásához elengedhetetlenek azok az elektronikus céladatok (például frekvencia, üzemmód, sávszélesség, impulzus paraméterek), melyeket az elektronikai támogató rendszerek nyújtanak az elektronikai zavaró eszközök számára. Az elektronikai támogató tevékenység iránymérő eszközei elegendő pontossággal rendelkezhetnek ahhoz, hogy a modern irányított, vagy hagyományos fegyverek alkalmazásához célmegjelölési adatokat biztosítsanak. Ahol ez nem lehetséges – például a földi közvetett irányzású fegyvereknél – az iránymérési pontosság gyakran elegendő más felderítő, megfigyelő és célmegjelölő rendszerek tájékoztatására.[58]

1.3.2.2 Elektronikai ellentevékenység

„Az elektronikai ellentevékenység az elektronikai hadviselés azon területe, amely magába foglalja az elektromágneses és egyéb irányított energiák kisugárzását abból a célból, hogy megakadályozza vagy csökkentse az elektromágneses spektrum ellenség által való hatékony használatát."[59]

Az elektronikai ellentevékenység az elektronikai hadviselés *támadó oldala*, ami abban nyilvánul meg, hogy minden olyan eszközt, eljárást és módszert felhasznál, amely az elektromágneses és irányított energiák felhasználásával képes megakadályozni az ellen-

[58] Haig, Zs. – Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005. p. 223.

[59] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 7.

séges elektronikai eszközök és rendszerek rendeltetésszerű működését (jelek vételét, feldolgozását), illetve rövidebb vagy hosszabb időre, esetleg véglegesen működésképtelenné tenni ezen eszközöket. Ugyanakkor egyes elektronikai ellentevékenységi módszerek alkalmasak védelmi természetű funkciók ellátására is. Az elektronikai ellentevékenység erőket és eszközöket oltalmazó módszerei komoly mértékben csökkenteni tudják az ellenség célfelderítésének, a fegyverek felderítő-, célkövető- és rávezető rendszerének hatékonyságát, ezáltal hozzájárulnak a harci technikai eszközök és a csapatok túlélőképességének növeléséhez.

Az új technológiák megjelenésével az elektronikai ellentevékenység túlmutat a tradicionális zavaráson és megtévesztésen. Az *irányított energiájú fegyverek (Directed Energy Weapons – DEW)* új rongáló és pusztító dimenziót jelentenek az elektronikai harctéren, megkövetelve ezek körültekintő alkalmazását.[60]

Az elektronikai ellentevékenységnek három területe van:

- elektronikai zavarás *(Electronic Jamming)*;
- elektronikai pusztítás *(Electronic Neutralization)*; és az
- elektronikai megtévesztés *(Electronic Deception)*.

„Az elektronikai zavarás az elektromágneses energiának szándékos kisugárzása, visszasugárzása vagy visszatükrözése azzal a céllal, hogy korlátozza vagy megakadályozza az ellenség által használt elektronikai eszközök, berendezések vagy rendszerek rendeltetésszerű működését."[61]

A fogalom alapján látható, hogy az elektronikai zavarás mind aktív (zavarójelet kisugárzó, vagy visszasugárzó), mind passzív (elektromágneses hullámokat visszaverő) eszközökkel megvalósítható. Az elektronikai zavarás nem öncélú tevékenység, ezért azt a támadó jellegű információs műveletek elveinek megfelelően minden esetben össze kell hangolni valamennyi más harcászati-hadműveleti tevékenységgel, különösen a tűzcsapással és a csapatok manővereivel.

Az elektronikai zavarás hatékony eszköz a parancsnok kezében az ellenség vezetésének és fegyverei irányításának megbontására, ugyanakkor veszélyeket is hordoz a zavarást végrehajtó erőkre nézve. Mivel a zavarás könnyen felfedhető, ezért a zavarforrás behatárolható, a helye meghatározható, ami lehetőséget teremt az eszközök megsemmisítésére. Ezen túlmenően a zavarás nem szándékos interferenciákat okozhat a saját elektronikai rendszerekben. Ezért a zavarási paramétereket minden esetben egyeztetni kell a *Korlátozott Frekvenciák Jegyzékével (Restricted Frequency List – RFL).* Az elektronikai zavarás hatással lehet a saját tevékenységekre is, ezért más erők és eszközök alkalmazási elvei, és rendszabályai korlátozhatják hatékony végrehajtását. Ugyanakkor a zavarás az erők, eszközök alkalmazására vonatkozó szabályokra való tekintet nélkül alkalmazható ab-

[60] Haig, Zs. – Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005. p. 223.

[61] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 7.

ban az esetben, ha az önvédelmet biztosítja. Mindezek a körülmények az elektronikai zavarás vonatkozásában körültekintő tervezést, engedélyezést, szervezést és végrehajtást követelnek.[62]

„Az elektronikai pusztítás elektromágneses és egyéb irányított energiák, valamint önrávezetésű fegyverek alkalmazása az ellenség elektromágneses spektrumhasználaton alapuló rendszereinek időleges, vagy tartós rombolása céljából."[63]

Az irányított energiájú fegyverek elegendő nagyságú energiát képesek sugározni a célobjektumok felé, hogy azok kezelő állományát harcképtelenné, eszközeit pedig használhatatlanná tegyék. Irányított energiájú eszközök közé tartoznak például a nagy energiájú rádiófrekvenciás sugárforrások, az „impulzusbombák", és az „akusztikus zaklatás" eszközei. Az irányított energiájú eszközök alkalmazása kockázatot jelenthet a saját csapatokra, ezért ezeket fokozott körültekintéssel kell alkalmazni, használatukat a zavaráshoz hasonlóan koordinálni kell.

Az önrávezetésű fegyvereknél az irányítás összes eleme a fegyver (például rakéta) fedélzetén helyezkedik el. Az irányításhoz szükséges irányító jeleket maga a cél szolgáltatja. A fegyver fedélzetén elhelyezett érzékelő elemek (önrávezető fej) követik a célt, és ahhoz viszonyítva meghatározzák a találkozáshoz szükséges röppályát. Attól függően, hogy az irányítási alapjelek meghatározásához szükséges energiaforrás (információforrás) honnan és hogyan származik, megkülönböztetünk aktív-, félaktív- és passzív önrávezetésű fegyvereket.

Az elektronikai megtévesztés az elektromágneses energia szándékos kisugárzása, átalakítása, visszasugárzása, elnyelése vagy visszatükrözése azzal a céllal, hogy megtévessze, félrevezesse, összezavarja, és eredeti szándékától eltérítse az ellenséget, vagy annak elektronikai rendszereit.[64]

Az elektronikai megtévesztés az elektronikai kisugárzások manipulálásával, torzításával, vagy meghamisításával éri el, hogy az ellenség saját érdekeivel ellentétesen tevékenykedjen. A hatékony elektronikai megtévesztés feltétele egyrészt, hogy az ellenségnek érzékelnie kell a megtévesztő jeleket, másrészt pedig e tevékenységeknek – hogy az ellenség ne fedezze fel a félrevezetést – valóságosnak kell látszaniuk. Ennek érdekében az elektronikai megtévesztés részletes és alapos tervezést, koordinációt és végrehajtást igényel. Az elektronikai megtévesztés része a katonai megtévesztésnek, így az elektronikai megtévesztés feladatait be kell dolgozni a katonai megtévesztési tervbe.[65]

[62] Haig, Zs. – Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005. p. 224.

[63] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 8.

[64] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 7.

[65] Haig, Zs. – Várhegyi, I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005. p. 225.

1.3.2.3 Elektronikai védelem

Az elektronikai védelem az elektronikai hadviselés azon területe, amely biztosítja az elektromágneses spektrum saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok által okozott nem szándékos (kölcsönös) rádiózavarok előfordulása ellenére.[66]

Az elektronikai védelem lehetetlenné teszi, vagy csökkenti az ellenségnek a frekvencia spektrum feletti fölény, és uralom megszerzésére irányuló törekvéseit. Az elektronikai védelmi tevékenységek védelmi természetűek és többet jelentenek, mint az elektronikai rendszerekbe tervezett és beépített technikai lehetőségek összessége. Az elektronikai védelem egyfajta parancsnoki felelősség, mely a következőket jelenti:

- passzív és aktív rendszabályok meghatározását az elektronikai eszközök és rendszerek számára, valamint – a csapatok és harci-technikai eszközök alkalmazási elveivel összhangban – e rendszabályok bevezetésére vonatkozó irányelvek meghatározását;
- kiképzésen keresztül magas fokú jártasság kifejlesztését, amely biztosítja a csapatok, technikai eszközök harcászati követelményeknek megfelelő alkalmazását az ellenséges elektronikai hadviselési környezetben. Az elektronikai védelem a *felderítés* és az *elektronikai ellentevékenység* – ezen belül a *saját nem szándékos interferenciák* – megakadályozására irányuló *aktív* és *passzív* tevékenységek, módszerek és rendszabályok alkalmazását, bevezetését jelenti.

A passzív elektronikai védelem az ellenség számára nem érzékelhető rendszabályok alkalmazását jelenti – úgy, mint a technikai eszközök üzemmódjaival, működési módjaival és technikai jellemzőivel való manőverezés –, amelyekkel biztosítható, hogy a saját csapatok hatékonyan használják fel az elektromágneses- és más spektrumot.

Az elektronikai védelem aktív rendszabályait – a frekvenciák, az adóberendezések paramétereinek megváltoztatását – az ellenség is érzékeli. Ezekkel a rendszabályokkal – például spektrumkiterjesztés, kaotikus vagy periodikus frekvenciaváltás, modulációs módok-, kimenő teljesítmény megváltoztatása – biztosítani lehet a frekvenciaspektrum saját csapatok által történő hatékony felhasználását.

Az elektronikai hadviselés egyes területeinek részletes kifejtésére a következő fejezetekben kerül sor.

1.3.3 Az elektronikai hadviselés kapcsolatrendszere

Az elektronikai hadviselés területei szoros kapcsolatban állnak egymással, a felderítéssel, valamint magával a harctevékenységgel. Ez a kapcsolat egyrészt adatok, célmegjelölési információk átadása formájában valósul meg, másrészt pedig azáltal, hogy az egyes te-

[66] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 8.

rületeken végzett tevékenységek hatásukban egy másik terület célkitűzéseinek elérését is szolgálják. Ennélfogva az elektronikai hadviselés külső és belső kapcsolatrendszerrel rendelkezik. A *külső kapcsolatrendszert* a felderítés és az elektronikai hadviselés integrációja, egységes vezetés szerinti végrehajtása, vagyis az integrált felderítés és elektronikai hadviselés *(Intelligence and Electronic Warfare – IEW)* jelenti, a *belső kapcsolatrendszert* pedig az elektronikai hadviselés három területének egymáshoz való viszonya adja.

1.3.3.1 Integrált felderítés és elektronikai hadviselés

Napjainkban az ellenség, a terep, az időjárás és egyéb – a harcot befolyásoló – objektív tényezők felderítése elsősorban technikai úton valósul meg. Ennek igazolására elég csak arra gondolni, hogy a harctéren milyen nagyszámú különböző rendeltetésű és fajtájú technikai felderítőeszköz található. (A bővebb kifejtést lásd a 3. fejezetben.) Ezen kívül az úgynevezett emberi erővel végzett felderítés *(Human Intelligence – HUMINT)* is alapvetően technikai eszközöket használ az adatok megszerzésére. Ennek megfelelően igényként jelentkezik, hogy az így megszerzett adatokat adott szinteken, egy helyen kell összegezni, kiértékelni, egyeztetni, korrelálni és a felhasználók számára hozzáférhetővé tenni.

Ezt az igényt elégíti ki az adatfúziós technológián alapuló úgynevezett *összadatforrású felderítés,* mely biztosítja a felderítő adatszerző és más fajtájú információszerző rendszerek és eszközök által nagy mennyiségben és sebességgel ontott felderítő nyersadatok, mintavételezett jelek, jelzések, nyílt vagy rejtett üzenetek, mint primer információk összegyűjtését, feldolgozását és az eredmények szétosztását. (A bővebb kifejtést lásd a 3. fejezetben.)

Az elektronikai hadviselésnek igen jelentős a célinformáció igénye, melyet egyrészt az elektronikai támogató tevékenység biztosít rövid érvényességű, gyors, és nem részletes kiértékelésű úgynevezett *harci információk* formájában. Másrészt az általános felderítő tevékenység során megszerzett és értékelt *felderítési információk* biztosítják az elektronikai helyzet adatbázis folyamatos karbantartását. A hatékony tűztámogatáshoz szintén elengedhetetlenek a pontos célmegjelölési adatok, melyeknek struktúrája hasonló az előbb említett elektronikai hadviselési célinformációkhoz. Kézenfekvő tehát, hogy az elektronikai hadviselés számára szükséges célinformációk biztosítása céljából egyrészt az elektronikai támogatás harci információit beintegrálják az összadatforrású felderítés adatfúziós feldolgozó rendszerébe, másrészt ugyanezen rendszerből elérhetővé válnak számára a már előbb említett kiértékelt felderítési információk.

A felderítési információk az ellenségről rendelkezésre álló valamennyi adat részletes feldolgozásának eredményeként jönnek létre, melyek az ellenség összetételére, felépítésére, szándékára, elhelyezkedésére, mozgásának irányára és sebességére, valamint harci készenlétére vonatkoznak. A gyors adatfeldolgozás, az időben történő jelentés és a felderítési adatok gyors eljuttatása a felhasználóhoz igen fontos a csapatok közvetlen harcérintkezésben vívott harcának tervezése, irányítása és támogatása szempontjából.

Ezzel szemben a *harci információk* olyan gyors kiértékelésű adatok értelmezett összessége, melyeket a harcoló csapatok, és a különböző adatszerző eszközök gyűjtenek,

és amelyek közvetlenül felhasználhatók a célpontok megsemmisítéséhez és az elektronikai hadviseléshez. Az ilyen típusú adatok gyorsan elavuló jellegük, vagy a helyzetre gyakorolt kritikus hatásuk miatt azonnali válaszintézkedéseket követelnek. Ugyanakkor a harci információkból - amennyiben azok részletes mélyértékelésre, további feldolgozásra kerülnek – előállíthatók felderítési információk. Ebből következően megállapítható, hogy mind a harci információhoz, mind a felderítési információkhoz ugyanazon adatszerző eszközökkel lehet jutni.

Az előzőekben felsorolt igények kielégítése céljából, valamint a párhuzamos tevékenységek kiküszöbölése érdekében a felderítést, az elektronikai hadviselést és a célok meghatározását azonos elvek és egységes vezetés alapján, úgynevezett *integrált felderítő és elektronikai hadviselés* struktúrában hajtják végre.

Az integrált felderítési és elektronikai hadviselési feladatok négy fő terület köré csoportosíthatók, úgymint:

- a helyzetértékelés;
- a célpontok meghatározása;
- az ellenséges felderítés elhárítása; és
- az elektronikai hadviselés.

Mind a négy feladat jól körülhatárolható, önállóan is végrehajtható, azonban egymáshoz való viszonyuk, az adatok felhasználhatósága, illetve a több feladatra alkalmazható eszközök miatt ezek *egységes tervezése, szervezése és irányítása* szükségszerű és elengedhetetlen.

Az elektronikai hadviselés sikeres végrehajtása érdekében a fenyegetésjelzéshez és a célmegjelöléshez speciális felderítést – elektronikai támogató tevékenységet – kell folytatni, amelynek során harci információkhoz jutunk. Hasonló sajátosságokkal rendelkezik a manőver és a tűztámogató tevékenység is. Az elektronikai hadviselés akkor a leghatékonyabb, ha integrálják, illetve együttesen alkalmazzák a tűzcsapásokkal és a manőverekkel. Az említett integrált alkalmazás tervezése során olyan felderítési információkra van szükség, melyek lehetővé teszik a parancsnok rendelkezésére álló tevékenységi formák eredményességének összevetését.

A felderítés – és ezen belül különösen a technikai eszközökkel végzett felderítés – biztosítja az ellenség *elektronikai harcrendjének (Electronic Order of Battle – EOB)* felvázolását. Az elektronikai harcrend ismerete alapvetően fontos az elektronikai hadviselés megvívása érdekében. Az erre vonatkozó információk tájékoztatnak a kommunikációs és nem-kommunikációs jellegű eszközök paramétereiről, az adók típusáról és rendeltetéséről, modulációjáról, csatornaképzési lehetőségeiről, impulzus időtartamáról, impulzus ismétlődési frekvenciájáról, sávszélességéről, a hozzá kapcsolódó fegyverrendszerekről és a kisugárzás egyéb jellemző adatairól. Ezek az adatok elősegítik az ellenség elektronikai harcrendjének modellezését. A technikai adatok ismeretében pontosabban fel lehet mérni:

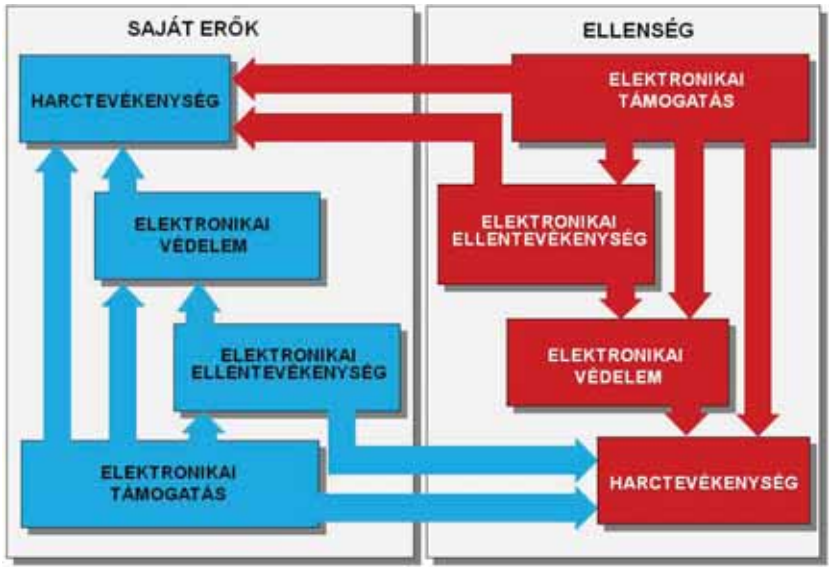
- az ellenség elektronikai rendszereinek az elektronikai ellentevékenységgel és a megtévesztéssel szembeni sebezhetőségét;
- könnyebben végrehajtható az eszközök figyelése és iránymérése az elektronikai felderítés eredményes végrehajtása érdekében; és

– az ellenség elektronikai hadviselési képességeire vonatkozó adatokkal támogatni lehet a saját csapatok elektronikai védelmi feladatainak végrehajtását.

Az integrált felderítő és elektronikai hadviselési erők és eszközök részét képezik az összfegyvernemi köteléknek. Feladatuk, hogy olyan pontos, időszerű és hatékony felderítési-, ellenséges felderítés elhárítási adatokat és elektronikai hadviselési támogatást nyújtsanak a parancsnoknak, melyek a sikeres harctevékenység megtervezéséhez, irányításához és végrehajtásához szükségesek. Az integrált felderítő és elektronikai hadviselési rendszerbe ténylegesen beletartozik minden szinten az összes olyan eszköz, részleg és szervezet, mely alkalmas az adatok gyűjtésére és feldolgozására, a felderítési információk elosztására, az ellenséges felderítés elhárítására, valamint az elektronikai hadviselés irányítására és végrehajtására. Az egyes szinteken meglévő integrált felderítő és elektronikai hadviselési eszközök szoros kapcsolatban vannak más, magasabb és alacsonyabb vezetési szinteken, valamint a szomszédoknál rendelkezésre álló eszközökkel, és így egységes, integrált és összefüggő felderítő és elektronikai hadviselési struktúrát alkotnak.

1.3.3.2 Az elektronikai hadviselés belső kapcsolatrendszere

Az elektronikai hadviselés belső kapcsolatrendszere az elektronikai támogató tevékenység, az elektronikai ellentevékenység és az elektronikai védelem egymáshoz való viszonyát jelenti. (1.7. ábra)



1.7. ábra. **Az elektronikai hadviselés belső kapcsolatrendszere**[67]

[67] Szerkesztették a szerzők.

Az elektronikai támogatás alapfunkcióját tekintve is a másik két terület tevékenységét támogatja veszélyjelzésekkel, a fenyegetések felismerésével, illetve célmegjelölési adatok biztosításával.

Az elektronikai támogatás a harchelyzet változását, az ellenséges harceszközök tevékenységét, a kommunikációs és nem-kommunikációs eszközök működését érzékeli, vagyis magából a harctevékenységből szerzi az információit. Az így megszerzett információkkal támogatja az elektronikai ellentevékenységet, az elektronikai védelmet, illetve a saját harctevékenységet.

Az elektronikai ellentevékenység számára biztosítja mindazon célmegjelölési információkat, melyek elengedhetetlenek a hatékony elektronikai zavarás, elektronikai megtévesztés és elektronikai pusztítás számára. Ezek az adatok a célobjektumok üzemi paramétereire (például frekvencia, üzemmód, modulációs mód, antenna paraméterek) és elhelyezkedésére vonatkoznak.

Az elektronikai védelem számára veszélyjelzésekkel (radar-, infrabesugárzás jelzés, rakétaindítás jelzés), a fenyegetések felismerésével biztosítja mindazon valós idejű, azonnali beavatkozást igénylő adatokat, melyek alapján a harci-technikai eszközök képesek elhárítani a rájuk leselkedő veszélyeket, melyek az ellenség általi célmegvilágításból, célmegjelölésből, önrávezetésű fegyverek alkalmazásából és az elektronikai zavarásból származnak.

Az elektronikai támogató tevékenység a fentieken kívül egyaránt támogatja a helyzetértékelést és a célpontok kijelölését, meghatározását is, és így közvetlenül a harctevékenységet is befolyásolja azáltal, hogy a parancsnok számára a harc vezetéséhez közvetlenül felhasználható és az összadatforrású felderítő rendszerbe integrálható harci információt biztosít.

Az elektronikai ellentevékenység az elektronikai támogató tevékenység által nyújtott célinformációk alapján lerontja az ellenség katonai információs rendszereinek hatékonyságát, csökkenti vezetési lehetőségeit, működésképtelenné teszi fontosabb harci-technikai eszközeit, megtéveszti felderítő és információs rendszereit. Az elektronikai támogató tevékenység fenyegetésjelző információi alapján pedig képes önvédelmi célú elektronikai ellentevékenységet folytatni (például aktív és passzív zavarással, infracsapdák alkalmazásával). Mindezek jelentős hatással vannak az ellenség harctevékenységére, és nagymértékben képesek befolyásolni a harctéren kialakult helyzetet.

Az elektronikai ellentevékenység – mint ahogy az a következő fejezetekből is látható lesz – az alkalmazott eljárásaival nagymértékben hozzájárul a hatékony elektronikai védelem megvalósításához is.

Az elektronikai ellentevékenység azáltal, hogy megtéveszti az ellenséges felderítő rendszereket, megnehezíti, lehetetlenné teszi azok működését és a felderítési adatok továbbítását, közvetlenül hozzájárul az elektronikai védelem egyik területének – az ellenséges felderítés elleni tevékenység – megvalósításához. Ezen túlmenően közvetve az elektronikai védelem másik területének – az elektronikai ellentevékenység elleni védelem – sikeréhez is hozzájárul, hiszen az ellenségnek az elektronikai zavaráshoz célmegjelölési adatokra (elektronikai támogató tevékenységre) van szüksége. Tehát amennyiben az előzőekben említett módon képesek vagyunk akadályozni, hogy az ellenség ezen

adatokat megszerezze, akkor közvetve csökkenthetjük például elektronikai zavaró tevékenységének hatékonyságát is.

Az elektronikai védelem azáltal, hogy csökkenti az ellenség felderítő és elektronikai ellentevékenységi lehetőségeit, minimálisra csökkenti a saját kisugárzó eszközök által keltett nem szándékos zavarokat, jelentősen hozzájárul a saját csapatok élőerejének és harci-technikai eszközeinek megóvásához, és így nagymértékben hatással van a saját harctevékenység sikerére.

Természetesen az ellenség hasonló módszerekkel törekszik a saját harctevékenységének elektronikai hadviselési támogatására, így a szembenálló felek között feszített küzdelem folyik az elektronikus harcmezőn.

1.3.4 Az elektronikai hadviselés alapelvei

Az elektronikai hadviselés megtervezésének és végrehajtásának hatékonyságát a következő alapelvek határozzák meg:

- felderítő támogatás;
- folyamatosság;
- rugalmasság, alkalmazkodó képesség;
- mozgékonyság;
- tűz, manőver és az elektronikai hadviselés egysége (összehangolása);
- erőforrások célirányos alkalmazása. (1.8. ábra)

1.8. ábra. **Az elektronikai hadviselés alapelvei**[68]

A felderítő támogatás elvének érvényre juttatása elengedhetetlen a sikeres elektronikai hadviselés érdekében. A sikeres elektronikai ellentevékenység és az elektronikai védelem megtervezése és végrehajtása alapvetően függ az elektronikai felderítés adatainak

[68] Szerkesztették a szerzők.

minőségétől és időszerűségétől. Az elektronikai támogató tevékenységet kiegészítő összes lehetséges felderítő adatforrás segíti meghatározni az ellenség sebezhető pontjait, kiválasztani a célokat és a prioritásokat, valamint értékelni a végrehajtott tevékenység hatékonyságát. Az elektronikai támogató tevékenységek és a felderítés összesítik és pontosítják a különböző ismérveket, azonosítják a célpontokat; meghatározzák a célpontok hadműveleti hovatartozását, fontosságát, sebezhetőségét, és ha lehetséges pontosítják a helyüket; valamint technikai és iránymérési adatokat biztosítanak a zavaráshoz és megtévesztéshez.

A folyamatosság azt jelenti, hogy a hatékonyság érdekében az elektronikai hadviselési eszközöket, meghatározott prioritások figyelembevételével, szünet nélkül kell alkalmazni. A harci veszteségek, az eszközök üzemképtelenné válása, a vezetés és irányítás romlása, vagy megszűnése és helyváltoztatása szükségessé teheti a prioritások gyakori felülvizsgálatát.

Az elektronikai hadviselési tevékenységek folyamatossága biztosítható:

- előzetes tervezéssel és a lehetséges céllista előkészítésével;
- a nagy fontosságú célok elleni tevékenység dublírozásával;
- a zavaróadók lépcsőzetes áttelepítésének megtervezésével;
- a zavarás irányítását biztosító összeköttetések dublírozásával;
- a frekvencia listák előkészítésével;
- a legbonyolultabb körülmények közötti kiképzéssel;
- több zavaróadó grafikon szerint váltakozó működéssel;
- légi zavaróeszközök alkalmazásával.

A rugalmasság, alkalmazkodóképesség elve szerint az elektronikai hadviselési szervezeteket úgy kell létrehozni, hogy azok rugalmasan alkalmazhatók legyenek mind harcászati, mind hadműveleti szinten. A rugalmasság biztosítja a parancsnok számára, hogy nem várt események esetén készen álljon az elektronikai hadviselési erők átszervezésére. Az erők rugalmas alkalmazása biztosítható, ha a tervezés során minden lehetőséget figyelembe veszünk. Ez megköveteli, hogy a feladatot tervező törzsek ismerjék az elektronikai hadviselési eszközök lehetőségeit annak érdekében, hogy a feladatnak megfelelően képesek legyenek átcsoportosításuk megszervezésére. A rugalmasság elve ezen kívül lehetővé teszi, hogy a csak szükségszerűen meglévő elektronikai hadviselési eszközökből szükségtelen tartalékok képzése.

A mozgékonyság (mobilitás) elve fokozottan érvényes napjaink nagy intenzitású hadviselési formáiban. Egy rendszer túlélőképességét és azt a képességét, hogy folyamatos támogatást biztosítson a gyakran változó hadműveletekben, alapvetően a mobilitási képessége biztosítja. Ebből következik, hogy az elektronikai hadviselési rendszereknek hasonló, vagy nagyobb mobilitással kell rendelkezniük, mint az általuk támogatott parancsnokság. Figyelembe véve azt a tényt, hogy a nagyteljesítményű elektronikai ellentevékenységi eszközök könnyen felderíthetők és így nagymértékben sebezhetők, ezért ezen eszközök nagyfokú mobilitása túlélőképességüket is biztosítja.

A tűz-, manőver- és az elektronikai hadviselés egységének (összehangolásának) elvét már az előzőekben is érintettük. Az elektronikai hadviselés – mint a harctámogatás egyik

fajtája – fontos részét képezi a katonai műveleteknek, és azon belül az információs műveleteknek. A támadó jellegű információs műveletek szerint az ellenséges vezetési rendszerekben akkor lehet a legnagyobb károkat okozni, ha azok támadására komplex módon kerül sor. Ennélfogva ahhoz, hogy kihasználjuk az elektronikai támogató tevékenység és az elektronikai ellentevékenység maximális lehetőségeit, tevékenységüket összehangoltan kell tervezni és végrehajtani a tűzcsapásokkal és a csapatok manővereivel. Mindez a tervezés során kidolgozott egységes céllista alapján történik.

Az erőforrások célirányos alkalmazásának elve azt jelenti, hogy a harc-, hadművelet célkitűzéseivel összhangban, az ellenség azon elektronikai objektumait kell felderíteni, zavarni, megtéveszteni és pusztítani, amelyek kiesése vagy működésképtelensége a legérzékenyebben érinti a vezetés megvalósításában, illetve a fegyverrendszerek irányításában. Az elektronikai hadviselési erők, eszközök viszonylagos alacsony mértéke, összehasonlítva a harcterületen elhelyezkedő lehetséges célpontok nagy számával, megköveteli az erőforrások maximális kihasználását. A csapatok alkalmazása során arra kell tehát törekedni, hogy a hadművelet főirányában kiválasztott elektronikai célobjektumok megsemmisítésére, illetve zavarására összpontosítsuk a rendelkezésre álló erőket és eszközöket. Az előzőekből következően tehát az elektronikai hadviselési csapatok sohasem alkalmazhatók tartalékként.

A következő fejezetekben részletesen tárgyaljuk az elektronikai hadviselés egyes összetevőit.

2. FEJEZET

Az elektronikai hadviselés fizikai alapjai

A további fejezetekben leírtak könnyebb megértése céljából e fejezetben röviden összefoglaljuk az elektronikai hadviselés színteréül szolgáló környezet néhány alapfogalmát, felosztását, matematikai összefüggését, úgymint:

- a frekvenciaspektrum felosztását;
- az elektromágneses hullámok jellemzőit és terjedésének alapjait;
- a főbb antenna típusokat és jellemzőiket;
- a modulációs módokat;
- az elektronikai zavarás alapvető matematikai összefüggéseit.

2.1 A frekvenciaspektrum felosztása

A frekvenciaspektrum a rezgések teljes tartományát magába foglalja. Fizikai tulajdonságait tekintve alapvetően az alábbi három fő részre osztható:

- a mechanikai rezgések tartománya;
- az elektromágneses rezgések tartománya;
- a részecskesugárzások tartománya.

Általánosan frekvenciának nevezzük az egy másodperc alatti rezgések számát, hullámhossznak pedig az egy rezgés időtartama alatt megtett utat.

A frekvencia és a hullámhossz, valamint az adott közegbeli terjedési sebesség között a következő összefüggés írható fel:

$$f = \frac{c}{\lambda} \tag{2.1.}$$

ahol: f – a frekvencia [Hz];
λ – a hullámhossz [m];
c – a hullám terjedési sebessége az adott közegben [m/s].

2.1.1 A mechanikus rezgések tartománya

A bennünket körülvevő világban zajló folyamatok, változások nagy része a köznapi értelemben is megfogható légnemű, szilárd, vagy folyékony közegben mechanikus rezgések formájában zajlik. Az anyag vagy tér állapotában keletkező zavarok tovaterjedését az anyagban, illetve a térben hullámnak nevezzük. A rugalmas hullám a rugalmas közeg mechanikai deformációinak tovaterjedése. Azokat a külső testeket, amelyek létrehoz-

zák ezeket a zavarokat, *hullámforrásnak* hívjuk. A hullámok és a részecskék rendezett mozgása között az a legfontosabb különbség, hogy a hullámok terjedését nem kíséri az anyag áramlása, hanem a hullámok terjedése során az egyre távolabbi közegrészecskék rezgése gerjesztődik.

A rugalmas hullám *longitudinális*, ha a közeg részecskéinek rezgése párhuzamos a hullám terjedésének irányával. Gázokban és folyadékokban csakis ilyen hullámok jöhetnek létre. Ezekben az esetekben a közeg *térfogati rugalmassága* kap szerepet, vagyis az adott anyag részecskéinek elmozdulásával összhangban annak sűrűsödése-ritkulása terjed tovább.

A rugalmas hullám *transzverzális*, ha a közeg részecskéinek rezgése merőleges a hullám terjedési irányára. Transzverzális hullám csak olyan közegben jön létre, amelynek az alakja rugalmas, vagyis csak a szilárd testekben. A folyadékok felületén terjedő hullámok egy időben longitudinális és transzverzális rezgést is végeznek, mivel kialakulásukban a nehézségi erő és felületi feszültség is szerepet játszik.[69]

A mechanikus rezgések tartománya az elektronikai hadviselés szempontjából azért fontos terület, mert ebbe a fizikai tartományba esik a mechanikus gépek és berendezések, harcjárművek, lőfegyverek működése során létrejövő rezgések, amelyek nem elektromágneses kisugárzások, vagy részecskesugárzások. Az emberi érzékelés olyan fontos szervei, mint a hallás és a tapintás (rezgésérzékelés) is ebben a tartományban működnek.

A fizikai testek működése, mozgása közben keletkező rezgések (hangok) a közvetítő közegek útján igen nagy távolságokra képesek eljutni, így alkalmasak arra, hogy felfedjük a létezésüket, mozgásukat, és sok egyéb más jellemzőjüket, vagyis információkat gyűjtsünk.

A gyakorlati életben a mechanikus rezgések tartományát többféleképpen is felosztathatjuk. Az emberi hallást a középpontba emelve a frekvencia szerinti felosztásban ezek a rezgések lehetnek például:

- infrahangok;
- hallható hangok;
- és ultrahangok.

A hordozó közeg szerinti felosztás szerint a mechanikai rezgéseket felosztathatjuk:

- akusztikai hullámokra (a levegőben, gázokban terjedő rezgések);
- hidroakusztikai hullámokra (a folyadékokban, számunkra elsősorban vízben terjedő rezgések);
- és szeizmikus hullámokra (a szilárd anyagokban terjedő rezgések).

Ez utóbbi felosztás számunkra célszerűbb, mert a katonai alkalmazási területeket sokkal pontosabban fedi le, mint a frekvencia szerinti felosztás.

[69] Holics, L. szerk.: *Fizika*. Műszaki Könyvkiadó, Budapest, 1986. pp. 352-354.

2.1.1.1 Akusztikai hullámok

Jelen csoportosításban az akusztikai hullámok tartománya alatt azokat a mechanikus rezgéseket értjük, amelyek a levegőben, illetve gázokban terjednek. Ebben a tartományban az emberi füllel, vagy műszeres eszközökkel folytathatunk hangfelderítést, különféle hanggenerátorokkal, pirotechnikai eszközökkel imitálhatunk hangforrásokat, zaklathatjuk a szemben álló felet, vagy irányított energiájú hangimpulzus fegyverrel támadhatjuk az élőerőt. Ennek részletes megvalósítását az adott felderítés, illetve ellentevékenység fejezet tárgyalja.

Az akusztikai hullámok fizikai jellemzői közül legfontosabb paramétereik a frekvencia, a terjedési sebesség, és a hangnyomás. Az emberi hallóképességet alapul véve frekvencia szerint megkülönböztetünk infrahangokat (f < 20 Hz), hallható hangokat (20 Hz < f < 20 kHz) és ultrahangokat (f > 20 kHz). Az állatok – például a kutya, vagy a denevér – sokkal szélesebb frekvenciatartományban is képesek a hanghullámok érzékelésére, sőt mint tudjuk a denevérek az általuk kibocsátott ultrahangokkal térképezik fel a környezetüket és tájékozódnak abban repülés közben.

A hang terjedési sebessége vákuumban a közvetítő közeg hiányában nulla. 0 °C-os, normális nyomású és nedvességű levegőben 331,5 m/s. A pontos értéke szinte független a nyomástól, alig függ a nedvességtől, a hőmérsékletfüggésre pedig jó közelítéssel fennáll:

$$c = c_0\sqrt{1+\frac{t}{273}} \text{ (levegőben } c_0\text{=331,5 m/s)}^{70} \qquad (2.2.)$$

Az akusztikai hullámok a levegőben frekvenciájuktól függően különböző csillapítást szenvednek el a terjedés során. Heves robbanásból származó hang terjedési sebessége a forrás közelében a normális érték többszöröse is lehet a kialakuló nagy hőmérsékleti és nyomásviszonyok miatt.

A szilárd testekben terjedő hang sebessége erősen függ az anyagminőségtől, a hullám jellegétől (longitudinális vagy transzverzális), a test alakjától (nagy tömegű test vagy vékony rúd), rugalmasságától és sok más tényezőtől is. Mérések szerint például ólomban 1300 m/s, vasban 5000 m/s, lucfenyőben pedig a szálak hosszirányában különösen nagy, 5300 m/s.

2.1.1.2 Hidroakusztikai hullámok

Általánosságban a folyadékok belsejében terjedő hangok sebessége nagyobb, mint a gázokban mérhető sebesség. A vízben terjedő akusztikus hullámokat hidroakusztikus rezgéseknek nevezzük. Például 0 °C-os desztillált vízben, normális nyomáson c = 1444 m/s, a sós tengervízben valamivel több és a mélységgel növekszik, mivel a nyomás miatt a részecskék egymáshoz mért közelsége csökken.

[70] Holics, L. szerk.: *Fizika*. Műszaki Könyvkiadó, Budapest, 1986. p. 401.

A hidroakusztikai tartományban mérhető jelek frekvenciája zömében a néhány száz Hz alatti tartományba esik, mivel a magasabb frekvenciákon a közeg csillapítása egyre nagyobb. A gyakorlatban tengeralattjárók kommunikációjára, illetve a legszélesebb alkalmazási körét tekintve víz alatti felderítésre, hang alapján való azonosításra, akadályok észlelésére használható a hidrolokáció. A víz alatti mikrofonokat hidrofonoknak, az akusztikus mérő berendezéseket szonároknak nevezik. Módszerét tekintve lehet aktív vagy passzív eljárásról beszélni.

2.1.1.3 A szeizmikus hullámok

A Föld belsejében terjedő mechanikai rezgéseket szeizmikus rezgéseknek nevezik. Igen nagy távolságokra képesek terjedni, így nagy erejű robbantások, atomkísérletek gyakorlatilag az egész bolygón érzékelhetők. A földrengések észlelésére használatos szeizmográfokkal azonos elven a katonai tevékenységek is megfigyelhetők. Jellemzően alacsony frekvenciatartományú rezgésekről van szó.

Katonai alkalmazásban felügyelet nélküli, úgynevezett harctéri szenzorok egyik érzékelőeleme a szeizmikus érzékelő, amelyet a Földbe leszúrva, leásva hoznak szoros kapcsolatba a közeggel. Érzékenységük jóval alacsonyabb a tudományos célú mérőkészülékeknél, de néhány száz méteres hatókörzetük elégséges az elhaladó katonák, kerekes és lánctalpas járművek, észlelésére, kategorizálására, megszámlálására.

2.1.2 A rádióhullámok tartományába eső elektromágneses hullámok jellemzése és terjedésük

Elektromágneses hullámnak nevezzük a dielektrikumban terjedő, időben változó, egymással kölcsönhatásban lévő elektromos (E) és mágneses (H) erőteret.

Az elektromágneses hullámok keletkezése visszavezethető az elektronok mozgására.

Az elektromágneses hullámok lehetnek természetes és mesterséges eredetűek. A természetes hullámok a Naptól, a kozmoszból, távoli égitestekről érkeznek, vagy éppen Földünk légkörében keletkeznek. A mesterséges elektromágneses hullámokat speciálisan e célra készített berendezésekkel állítják elő.

Az elektromágneses hullámot valamilyen sugárforrás állítja elő, és az a kisugárzóról (antennáról) leszakadva a szabad térben egyenes vonalban terjed. A szabadon terjedő elektromágneses hullámban mind a villamos tér, mind a mágneses tér transzverzális, vagyis a terjedés irányára merőleges, síkban változik. Az E és H síkja egymásra és az energia terjedés irányára is merőleges.

Az *elektromágneses hullám polarizációját* az elektromos erőtér helyzete határozza meg. Vagyis, attól függően beszélünk vízszintes-, vagy függőleges polarizációról, hogy az elektromágneses hullám két energiahordozó komponenséből az elektromos erőtér függőleges vagy vízszintes helyzetet foglal el. Ezt a polarizációs fajtát lineáris polarizációnak nevezzük. Lehetséges olyan eset, hogy a vektor hossza állandó marad, de a vektor iránya valamilyen körfrekvenciával forog, ilyenkor cirkuláris vagy körkörös polarizáci-

óról beszélünk. Ha a rádióhullám elektromos terének vektorai mind a hosszuk, mind az irányuk szerint szabálytalan változást mutatnak, akkor a rádióhullám elliptikusan polarizált. A polarizációs síkot alapvetően az adóantenna alakítja ki, de az ionoszféra akár egyik pillanatról a másikra megváltoztathatja azt akár 180°-kal is. Az ionoszféra okozta polarizációs sík változása különösen napkeltekor és napnyugtakor észlelhető.

Az elektromágneses hullámok fizikai viselkedésüket tekintve hasonlatosak a mindennapjainkban szemmel is jól megfigyelhető fénytani jelenségekhez, így viselkedésük sok esetben analógiát mutat a fénnyel. Ennek az az alapvető oka, hogy a fény is elektromágneses hullám, de több is annál. A fény kettős természetű, egyrészt hullámfizikai, másrészt részecskefizikai tulajdonságokkal bír.

Az elektromágneses hullámok visszaverődésének vizsgálatakor maradéktalanul felhasználhatjuk a fényvisszaverődésre vonatkozó szabályokat, miszerint a beeső sugár, a beesési merőleges és a visszavert sugár, illetve a megtört sugár egy síkban van, valamint a beesési szög és a visszaverődés szöge egyenlő egymással. Visszaverődést okozhat például a talaj, a tereptárgyak, az ionoszféra rétegek, a tengervíz. Általános szabályként leszögezhető, hogy visszaverődés csak akkor jön létre, ha a visszaverő felület megegyezik vagy nagyobb a hullámhossznál.

2.1. táblázat. **Az elektromágneses hullámok felosztása**[71]

Megnevezés		Hullámhossz		Frekvencia
Kozmikus sugárzás		$2 \cdot 10^{-16}$ m - 10^{-12} m		$1{,}5 \cdot 10^{15}$ GHz - $3 \cdot 10^{11}$ GHz
Gamma sugarak		10^{-12} m - $3 \cdot 10^{-12}$ m		$3 \cdot 10^{11}$ GHz - 10^{11} GHz
Röntgen sugarak		$3 \cdot 10^{-12}$ m - $0{,}3 \cdot 10^{-6}$ m		10^{11} GHz - 10^{6} GHz
Ultraibolya sugarak		$0{,}3 \cdot 10^{-6}$ m - $0{,}38 \cdot 10^{-6}$ m		10^{6} GHz - $7{,}9 \cdot 10^{5}$ GHz
Fénysugarak	lila	$0{,}42 \cdot 10^{-6}$ m		
	sötétkék	$0{,}45 \cdot 10^{-6}$ m		
	világoskék	$0{,}49 \cdot 10^{-6}$ m		
	zöld	$0{,}52 \cdot 10^{-6}$ m		
	sárga	$0{,}58 \cdot 10^{-6}$ m		
	narancs	$0{,}63 \cdot 10^{-6}$ m		
	piros	$0{,}7 \cdot 10^{-6}$ m		
Infravörös sugarak	közeli	$0{,}76 - 1{,}6 \cdot 10^{-6}$ m		$3{,}84 \cdot 10^{5}$ GHz
	közbeeső	$1{,}6 - 5 \cdot 10^{-6}$ m		
	távoli	$5 - 500 \cdot 10^{-6}$ m		
Rádióhullámok	Milliméteres	10^{-3} m = 1mm - 10^{-2} m = 10 mm		300 GHz - 30 GHz
	Centiméteres	10^{-2} m = 10 mm - 10^{-1} m = 10 cm		30 GHz - 3 GHz
	Deciméteres	10^{-1} m = 10 cm - 1m		3 GHz - 300 MHz
	URH	1 m - 10 m		300 MHz - 30 MHz
	RH	10 m - 100 m		30 MHz - 3 MHz
	KH	100 m - 10^{3} m = 1km		3 MHz - 300 kHz
	HH	LF	10^{3} m - 10^{4} m = 10 km	300 kHz - 30 kHz
		VLF	10^{4} m - 1000 m = 100 km	30 kHz - 3 kHz
		ELF	10^{5} m - 10^{7} m = 10000 km	3 kHz - 30 Hz

[71] forrás jelölés / saját szerkesztés hiányzik

Közeghatárhoz érve bizonyos körülmények között a beeső hullám egy része behatolhat az új közegbe, más része pedig visszaverődik, a visszavert hullám ilyen esetekben gyengébb a beeső hullámnál. A beeső és visszavert hullámok térerősségeinek hányadosa a visszaverődési tényező, amelyik jellemző erre a gyengülésre. A visszaverődési tényező értékét különböző közegekre és hullámokra diagramban szokás megadni.

Az elektromágneses hullámokat frekvenciájuk, vagy hullámhosszuk szerint különböztetjük meg egymástól és az egyes tartományokat általában külön névvel is ellátják.

2.2. táblázat. **A rádióhullámok felosztása, magyar és angol nyelvű elnevezései**[72]

Hullámhossz szerint		Frekvenciasáv szerint			Hullámsáv	Frekvenciasáv
Megnevezés	Jelölés	Magyar megnevezés	Angol megnevezés	Jelölés		
Rendkívül hosszú hullámok	RHH	Rendkívül kis frekvencia	Extremely Low Frequency	ELF	100 km felett	3 kHz alatt
Igen hosszú hullámok	IHH	Nagyon kis frekvencia	Very Low Frequency	VLF	100 km - 10 km	3 kHz - 30 kHz
Hosszú hullámok	HH	Kis frekvencia	Low Frequency	LF	10 km -1 km	30 kHz - 300 kHz
Középhullámok	KH	Közepes frekvencia	Medium Frequency	MF	1 km - 100 m	300 kHz - 3 MHz
Rövid hullámok	RH	Magas frekvencia	High Frequency	HF	100 m - 10 m	3 MHz - 30 MHz
Ultrarövid hullámok	URH	Igen magas frekvencia	Very High Frequency	VHF	10 m - 1 m	30 MHz-300MHz
Deciméteres hullámok	DMH	Ultra magas frekvencia	Ultra High Frequency	UHF	1 m - 1dm	300 MHz - 3 GHz
Centiméteres hullámok	CMH	Szuper magas frekvencia	Super High Frequency	SHF	1 dm - 1 cm	3 GHz - 30 GHz
Milliméteres hullámok	MMH	Rendkívül magas frekvencia	Extremely High Frequency	EHF	1 cm - 1 mm	30 GHz - 300 GHz
Mikrohullámok	µH	-	-	-	1 mm alatt	300 GHz felett

2.1.2.1 A rádióláthatóság

A Föld görbültsége és a légkör hullámtörési tulajdonságai hatást gyakorolnak a rádióhullámok terjedésére. A rádiófelderítési és zavarási feladatok során figyelembe kell venni a terepviszonyokat, illetve az adott frekvenciatartományra jellemző terjedési tulajdonságokat, mivel a reális feladatszabás egyik alapfeltétele ezek ismerete. Tudnunk kell, hogy mikor, milyen elméleti hatótávolságokkal számolhatunk, mivel az eszközök képességeit a fizikai törvényszerűségek határozzák meg.

[72] forrás jelölés / saját szerkesztés hiányzik

Elméletileg, a szabad térben, homogén hullámterjedési közegben a rádióhullámok egyenes vonalban terjednek. A Föld felszínén elhelyezett adóberendezésekből kisugárzott energia azonban hullámtartományonként (frekvenciánként) más-más terjedési tulajdonságokat mutatnak. A tapasztalat azt mutatja, hogy a hullámok az egyenes láthatósági vonal alá, tehát nagyobb távolságokra is képesek eljutni az elhajlás, a diffrakció útján. Az elhajlás annál kevésbé érvényesül, minél magasabb a jel frekvenciája. A mikrohullámoknál egyáltalán nem, az ultrarövid hullámoknál pedig csak az alsó tartományokban lép fel a hullámlehajlás jelensége. Ezekben a magasabb frekvenciatartományokban magas antennatornyok alkalmazásával növelik a rádióhorizont határát.

Levezethető, hogy ha a hullám csak egyenes vonalban terjedne, akkor az optikai látóhatár az alábbi összefüggéssel írható le:

$$D_0 = 3{,}56\sqrt{h} \tag{2.3.}$$

ahol: D_0 – az optikai látóhatár [km];
h – az antenna föld feletti magassága [m].

Figyelembe véve, hogy a földsugarat a valóságos 6370 km helyett 4/3-os földsugár tényezővel szorozzák a mérsékelt égövi régióban és így 8500 km-el számolunk a továbbiakban, tehát az optikai látóhatár képletünk emiatt tehát $D_0 = 4{,}12\sqrt{h}$ alakot vesz fel. A gyakorlatban az adó és a vevőantenna is valamely adott magasságban üzemel, ezért a kettőjükre számított elméleti láthatósági távolság képlete így módosul:

$$D_0 = 4{,}12(\sqrt{h_1} + \sqrt{h_2}) \tag{2.4.}$$

ahol: D_0 – az optikai látóhatár [km];
h_1 és h_2 – az adó és vevőantenna magassága [m].

Egyre hosszabb hullámok esetén a rádióhullámok diffrakció útján a fenti képlet által meghatározott távolságon túlra is eljutnak. Ennek mértékét alapvetően a hullámhossz és a földfelület vezetőképessége befolyásolja. A vezetőképesség tengervíz esetén megfelel a tökéletesen vezető földnek, erősen abszorbeáló föld lehet a száraz, homokos talaj.[73]

2.1.2.2 A rádióhullámok terjedési sajátosságai

Hullámterjedés szempontjából a Föld és légköre különbözőképpen viselkedik. Ha a Föld felől közelítve vizsgáljuk a rétegeket, akkor azok rendszere a következő:

- neutroszféra;
- ionoszféra;
- magnetoszféra.

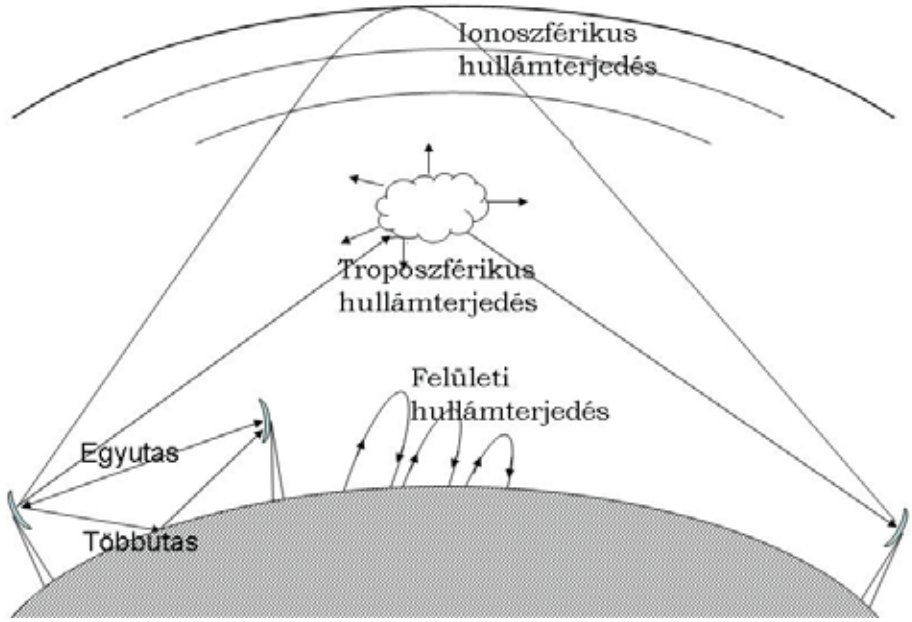
[73] Istvánffy, E.: *Tápvonalak, antennák és hullámterjedés*. Tankönyvkiadó, Budapest, 1984. pp. 584-588.

A *neutroszféra* a Föld felületéhez legközelebbi nagy réteg, amelynek a hullámterjedésben jelenleg csak korlátozott jelentősége van, elsősorban az úgynevezett tropo-scatter összeköttetéseknél használják. Az elektromágneses hullámok terjedése szempontjából az *ionoszféra* a legjelentősebb réteg, amely a neutroszféra és a magnetoszféra között található. Legjelentősebb a kb. 70–1000 km-ig terjedő vastagsága.

A napsugárzás a Föld felé haladva az egyre sűrűsödő légrétegeket ionizálva egyre több fotonját elveszíti, tehát van olyan légköri magasság, ahol a legsűrűbb az ionizáció. Az ionizáció következtében több réteg alakul ki, amelyek magassága, sűrűsége, határfrekvenciája a naptevékenység, napszak, évszak függvényében változik.

A rétegek vastagsága, ionizáltsági foka, magassága statisztikailag, sok év mérései alapján prognosztizálhatók, így az összeköttetések tervezésénél alapadatokként szolgálhatnak. Az évszak, napszak, valamint az összeköttetés paraméterei függvényében a rövidhullámú tartományban bonyolult számítási-prognosztizálási eljárással kell a frekvenciatervet elkészíteni, aminek részletes leírására jelen jegyzet keretein belül nincs mód.

A hullámterjedés többféle mechanizmus útján valósul meg, amelyek elsősorban a frekvenciától, az antennák fajtájától és a légkör állapotától függenek. (2.1. ábra)



2.1. ábra. **A főbb hullámterjedési módok**[74]

[74] Géher, K. főszerk.: *Híradástechnika*. 2. kiadás. Műszaki Könyvkiadó, Budapest, 2000. p. 107. (a forrás alapján szerkesztették a szerzők)

Így a hullámterjedés módjai lehetnek:
- közvetlen;
- reflektált;
- felületi;
- diffrakciós;
- troposzférikus szórással megvalósuló;
- ionoszférikus.[75]

A *közvetlen hullámterjedés* esetén a hullámvezető közeget áram- és töltésmentesnek feltételezzük, ideális dielektrikumnak tekintjük.

A részletes levezetést mellőzve, a szabadtéri csillapításra az alábbi összefüggés érvényes:

$$a_0[dB] = 20\log\frac{4\pi d}{\lambda} - 20\log\sqrt{G_a G_v} \tag{2.5.}$$

ahol: d – az adó-, és a vevőantenna közötti távolság [m];
λ – a hullámhossz [m];
G_a, G_v – az adó-, és vevőantenna nyeresége viszonyszámban.

Ha az antennanyereség dB-ben adott, akkor a képlet az alábbi alakra módosul:

$$a_0[dB] = 20\log\frac{4\pi d}{\lambda} - (G_a^{dB} + G_v^{dB}),\ dB \tag{2.6.}$$

ahol: d – az adó-, és a vevőantenna közötti távolság [m];
λ – a hullámhossz [m];
G_a, G_v – az adó-, és vevőantenna nyeresége [dB].[76]

Erre az összefüggésre gyors becsléseknél támaszkodhatunk, mivel azok a fizikai peremfeltételek, amelyekből kiindultunk, csak igen ritkán fordulnak elő a gyakorlatban. Általában a terjedési úton akadályok találhatók, a szakaszcsillapítást sok egyéb tényező is befolyásolja, mint például a Föld görbülete nem elhanyagolható, a talaj vezetőképessége változik a Föld más régióiban. A matematikai kiinduláshoz azonban az összefüggés korrekt.

Ha az antennák hatásaitól eltekintünk, és csak a szabad tér csillapítását kívánjuk megbecsülni, akkor jól használható összefüggés az alábbi is:

$$a_0 = 32{,}4 + 20\log d + 20\log f \tag{2.7.}$$

ahol: d – az adó-, és a vevőantenna közötti távolság [km];
f – az üzemi frekvencia [MHz].

[75] Istvánffy, E.: *Tápvonalak, antennák és hullámterjedés*. Tankönyvkiadó, Budapest, 1984. pp. 577-620.
[76] U.o. pp. 578-579.

A közvetlen hullám terjedésekor még egy fontos fizikai hatás fellép, amit hullámelhajlásnak, refrakciónak nevezünk. Ennek oka az, hogy a vákuumban való egyenes vonalú hullámterjedéssel szemben a földi légkörben a rádió- és optikai hullámok a levegő változó törésmutatója miatt elhajlanak. A levegő törésmutató indexét empirikusan, a meteorológiai tényezőkkel kifejezve kapjuk az alábbi összefüggést:

$$N = 77{,}6\frac{p}{T} + 3{,}73 \cdot 10^5 \frac{e}{T^2} \qquad (2.8.)$$

ahol: p – a légnyomás [mbar];
e – a vízgőz parciális nyomása [mbar];
T – levegő hőmérséklete [K].

Gyakorlati mérések eredményeit statisztikailag feldolgozva a levegő törésmutató-indexére a mérsékelt égövön a tengerszint feletti magasság függvényében az alábbi összefüggést kapták:

$$N(h) = 315\exp(-0{,}136h) \qquad (2.9.)$$

ahol: h – a magasság [m].

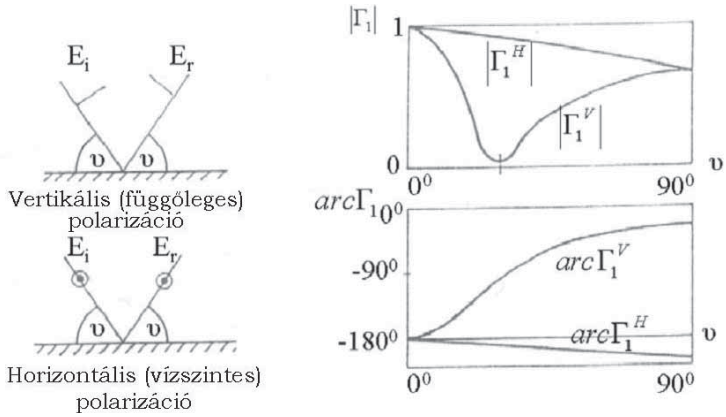
A törésmutató változása miatt a rádióhullámok a standard atmoszférában a Föld felé hajlanak. A gyakorlati számítások során azonban nem ezt a kényelmetlenül használható görbült hullám utat alkalmazzák, hanem az R_0 = 6370 km nagyságú tényleges földsugár helyett egy korrigált, úgynevezett effektív földsugarat használnak, $R_{eff} = kR_0$ amely értéke R_{eff}= 8500 km. A k értéke nálunk 4/3, de a világ más tájain a helytől függően más és más lehet.[77]

A földi rádiórendszerek működésekor egy további fizikai jelenség, a talajreflexió is fellép. A rádióhullámok talajról való visszaverődését a veszteséges dielektrikumról reflektálódó síkhullámok törvényei alapján kell vizsgálni. A síkhullámnak az e_r permittivitású és s vezetőképességű, végtelen kiterjedésű féltérről való visszaverődésekor a reflektált (E_r) és a beeső (E_i) térerősség közötti kapcsolatot a következő definíció szerinti földreflexiós tényező adja meg:

$$\Gamma_f = \frac{E_r}{E_i} \qquad (2.10.)$$

A 2.2. ábrán a horizontális és a vertikális hullám polarizációra vonatkozó reflexiós tényezőt ábrázoljuk a beesési szög függvényében.

[77] Géher, K. főszerk.: Híradástechnika. 2. kiadás. Műszaki Könyvkiadó, Budapest, 2000. p. 109.



2.2. ábra. **A földreflexiós tényező a beesési szögek függvényében**[78]

A görbékről leolvasható az a sajátosság, hogy kis beesési szögeknél ($<5^0$) a polarizációtól függetlenül, tetszőleges frekvencián a reflexiós tényező –1 értékű. A vertikális polarizáció esetén a földreflexiós tényezőnek minimuma van. Az ehhez tartozó szögértéket ideális dielektrikum esetén Brewster-szögnek, veszteségesnél pedig pseudo-Brewster-szögnek nevezik.

A gyakorlatban elsősorban az URH és mikrohullámú, látóhatáron belüli összeköttetések, valamint mobil rendszerek esetén lép fel a *kétutas terjedés* jelensége. Ennek lényege, hogy az adó és vevőpont között a direkt úton kívül egy földről visszavert hullám is megjelenik, így a vevőben a két jel eredője érkezik be.

A kétutas terjedés szakaszcsillapítása a levezetés mellőzésével:

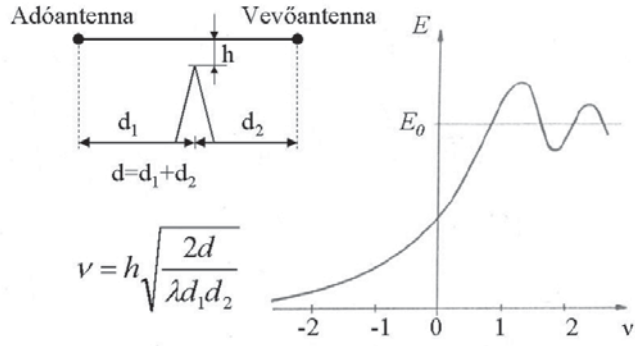
$$A_{sz} = 20\lg\left(\frac{r^2}{h_T h_R}\right) - G_T - G_R \qquad (2.11.)$$

ahol: r – az adó- és vevőpont távolsága [m];
h_T – az adóantenna magassága [m];
h_R – a vevőantenna magassága [m];
G_T, G_R – az adó- és vevőantennák nyeresége [dB].[79]

Ha a szabadtérben terjedő hullám útjában akadály van, akkor a geometriai optika szerint az „árnyákban lévő antenna” helyére nem jut energia. A valóságban azt tapasztaljuk, hogy bizonyos határok között így is van összeköttetés. A magyarázat abban áll, hogy a hullámoptika Huygens elve szerint az adóantennából kiinduló hullámfrontot másodlagos Huygens-forrásnak kell tekinteni és minden elemének a sugárzását a vevőantenna felé fázishelyesen kell összegezni.

[78] Géher, K. főszerk.: *Híradástechnika*. 2. kiadás. Műszaki Könyvkiadó, Budapest, 2000. p. 109.
[79] Istvánffy, E.: *Tápvonalak, antennák és hullámterjedés*. Tankönyvkiadó, Budapest, 1984. pp. 596-597.

A terepakadályokat általában késélmodellel írják le. A késél diffrakciós modellnél a vételi térerősség változása a késél elhelyezkedése és relatív magassága függvénye, amelynek jellegét a 2.3. ábrán megfigyelhetjük.



2.3. ábra. **A térerősség változása a késél paraméterei függvényében**[80]

A *diffrakciós terjedési* modellek a domborzat kiemelkedéseit egy, vagy több késélakadállyá transzformálják át és különböző algoritmikus eljárásokkal egy domináns késélt hoznak létre, amelyre a csillapítási számítások már elvégezhetők. Ilyen többszörös késél diffrakciós modellek a szakirodalomban Bullington, Epstein-Peterson, Japán-, és Deygout modell néven váltak ismertté. A különböző célokra a gyakorlatban más-más módszert célszerű alkalmazni. Interferencia számításához például a Deygout, a hasznos jel meghatározásához az Epstein-Peterson modell adja a valóságban mérhető értékekhez legközelebb álló adatokat.

A hullámterjedés egy másik fajtája a *felületi hullámú terjedés***,** amely a jól vezető föld és a levegő határfelülete mentén alakul ki a hullámhosszhoz képest kis antennamagasságok esetén, mivel a közvetlen és a reflektált hullámok kioltják egymást. A talaj általában néhány kHz-től néhány MHz-ig jó vezetőképességű közeg, így ebben a frekvenciasávban elsődleges terjedési módnak a felületi hullámú terjedés tekinthető. A gyakorlatban használt szakasztávolság néhány száz km. A talaj és a levegő határfelületén haladó felületi hullám elektromos erővonalai vertikális polarizációra – a talaj véges vezetőképessége miatt – a haladás irányában megdőlnek.

A felületi hullámok csillapodása horizontális polarizációra jelentős, ezért a vertikális polarizáció használatos.

A felületi hullámok nagy előnye, hogy a talaj és a levegő átmenetén terjedve, a talaj görbületét követve, nagy távolságokra, a látóhatáron túlra is képesek eljutni.

[80] Géher, K. főszerk.: *Híradástechnika*. 2. kiadás. Műszaki Könyvkiadó, Budapest, 2000. p. 111.

A felületi hullámterjedés térerőssége:

$$E_0 = \sqrt{\frac{P_A G_A 30}{d}} \tag{2.12.}$$

Körsugárzó monopól antenna esetén az alábbi összefüggéssel adható meg:

$$E_0 = 300 \frac{\sqrt{P_A}}{d} \tag{2.13.}$$

ahol: P_A – az adó teljesítmény [kW];
d – a távolság [km].

A hírközlési eszközök egy része a *troposzférikus szórás* fizikai jelenségét kihasználva működik. A földi légkör törésmutatója, mint azt korábban már leírtuk, szabályosan változik. Emellett persze mindig előfordulnak diszkontinuitások, amelynek oka a levegő páratartalmának, hőmérsékletének és nyomásának hely szerinti gyors változása. Ezek a változások nem jelentősek, de ha nagy az adóteljesítmény, akkor jelentős szórt teljesítmények jöhetnek létre.

A troposzférikus összeköttetések létrehozására a 200 MHz – 10 GHz frekvenciatartomány alkalmas. A frekvencia csökkentésének az alkalmazott nagy nyereségű antennák fizikai méretei szabnak határt, nagyobb frekvenciákon pedig a szakaszcsillapítás nő meg. Az összeköttetések tipikus távolsága néhány száz km. A vételi térerősség jelentős mértékben ingadozik, tehát a stabil összeköttetés létrehozásához igen nagy adóteljesítmény szükséges.

A troposzférikus szórás a 10 km alatti rétegekben alakul ki. Létrejöttének általános feltétele, hogy az adó- és vevőantenna sugárnyalábja egy közös, úgynevezett szórótérfogatot hozzon létre.[81]

A rövidhullámú frekvenciatartomány jellegzetes hullámterjedési módja az *ionoszférikus hullámterjedés*. A földfelszín felett 40-100 km magasságban elhelyezkedő ionoszférában nagyszámú ionizált gázrészecske van. Az ionizációt a Nap ibolyán túli és részecskesugárzása, valamint a légkörbe jutó meteoritok ionizáló hatása okozza. A Nap jelentős ionizációs hatása szorosan összefügg a naptevékenységgel.

Az ionoszférát rétegekre bontják, amelyet a térfogategységre eső szabad elektronok számával jellemeznek. Az elektronsűrűség helyi maximumai alapján D, E és F rétegeket különböztetünk meg. Az F réteg napközben további rétegekre, az F_1 és F_2 rétegre oszlik. Éjszaka csak a D és F rétegek jelentkeznek.

A rádióhullámok a közeg törésmutatójának változása miatt az ionoszférikus rétegről reflektálódnak.

Minden réteghez tartozik egy maximális frekvencia, amely a rétegről még éppen visszaverődik, és ezt a réteg kritikus frekvenciájának nevezzük. A réteg határfrekvenciá-

[81] Istvánffy, E.: *Tápvonalak, antennák és hullámterjedés*. Tankönyvkiadó, Budapest, 1984. pp. 615-617.

jának annak rádióhullámnak a frekvenciáját nevezzük, amely az ionoszférikus rétegről 50% valószínűséggel verődik vissza. Ferdeszögű beesésnél az *fc* kritikus frekvenciánál nagyobb frekvenciájú jelek is visszaverődnek és ekkor a maximális frekvencia (MUF) és a kritikus frekvencia közötti kapcsolatot a Y beesési szöggel az MUF = *fc*/*sin*Y összefüggés adja meg.[82]

2.1.3 Az optikai sávú elektromágneses hullámok tulajdonságai

A fény elektromágneses hullám, amely egyrészt hullám, másrészt részecskefizikai tulajdonságokkal is rendelkezik, egyes jelenségeit csak a hullámfizika, más jelenségeit csak a részecskefizika törvényszerűségei alapján lehet megmagyarázni. A részecskéket a kvantummechanika a fény kvantumainak, fotonoknak nevezi. A fotonok olyan részecskék, amelyek nyugalmi tömege zérus, üres térben pedig fénysebességgel mozognak.

A köznapi szóhasználatban a fény: emberi szemmel érzékelhető elektromágneses sugárzás. Tágabb értelemben beleérthető az ennél nagyobb (infravörös) és kisebb hullámhosszú (ultraibolya) sugárzás is.

A fény tulajdonságait meghatározó három fő szempont:

- intenzitás vagy amplitúdó, amelyet az ember fényerőként, fényességként érzékel;
- frekvencia (és ezzel összefüggésben a hullámhossz), amelyet az ember színként érzékel; és
- polarizáció, azaz az elektromágneses rezgés iránya, ezt az átlagember normál körülmények között nem érzékeli, de például bizonyos rovarok igen.

A fény az elektromágneses spektrum része, melynek frekvenciája $7{,}5 \cdot 10^{14}$ Hz és $3{,}8 \cdot 10^{14}$ Hz közé esik. A sebesség (c), a frekvencia (f vagy ν) és a hullámhossz (λ) között a (2.1.) már korábban is megismert kapcsolat áll fenn. Terjedési sebessége vákuumban:

$$c_0 = \frac{1}{\sqrt{\mu_0 \varepsilon_0}} \tag{2.14}$$

ahol: c_0 – a fény terjedés sebessége [m/s];
μ_0 – a vákuum mágneses permeabilitása;
ε_0 – a vákuum dielektromos állandója.

Értéke minden vonatkoztatási rendszerben: 299 792 458 m/s. Bármely más közegben a terjedési sebesség ennél csak kisebb lehet. Értékét a közeg abszolút törésmutatójából lehet meghatározni:

$$n = \frac{c}{v} = \sqrt{\varepsilon_r \mu_r} \tag{2.15.}$$

[82] U.o. pp. 602-614.

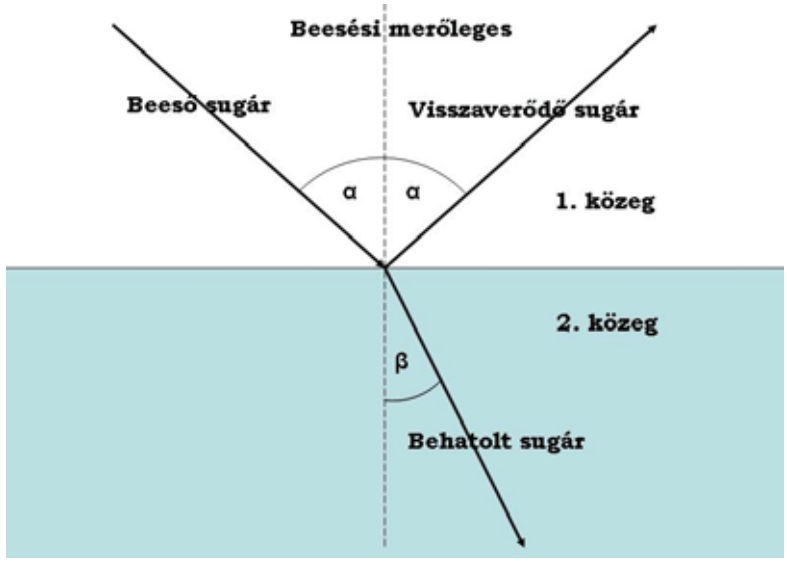
ahol: n – az adott közeg abszolút törésmutatója;
v – az adott közegbeli sebesség;
ε_r – az adott közeg vákuumra vonatkoztatott relatív dielektromos állandója;
μ_r – az adott közeg vákuumra vonatkoztatott relatív mágneses permeabilitása.

Ha az elektromágneses hullám egyik közegből egy másik közegbe lép, a határára érve irányváltoztatást szenved, amit hullámtörésnek nevezünk. Mértékét a két közegbeli terjedési sebesség aránya határozza meg. A második közegnek az elsőre vonatkoztatott relatív törésmutatója a hullám két közegbeli v_1, illetve v_2 terjedési sebességének a hányadosa:

$$n_{21} = \frac{v_1}{v_2} = \frac{n_2}{n_1} \tag{2.16.}$$

ahol: n_1, n_2 – az első, illetve a második közeg abszolút törésmutatója.

Ha az elektromágneses hullám tehát két különböző közeg határára ér, akkor ott részben visszaverődik, részben megtörik. A hullámok terjedési irányát a 2.4. ábra mutatja.



2.4. ábra. **Az elektromágneses hullámok visszaverődése és törése közeghatáron**[83]

E hullámterjedési jelenség legfontosabb jellemzői:
- a beeső sugár és a beesési merőleges közötti szög egyenlő a visszavert sugár szögével;
- a beeső sugár, a beesési merőleges és a visszavert sugár egy síkben vannak;

[83] Szerkesztették a szerzők.

– a beesési szög (α) szinuszának és a törési szög (β) szinuszának aránya a közegekben mért terjedési sebességek arányával egyenlő, amely a törésmutatókkal is kifejezhető:

$$\frac{\sin\alpha}{\sin\beta} = \frac{v_1}{v_2} = \frac{n_2}{n_1} = n_{21} \qquad (2.17.)$$

ahol: n_{21} – második közeg relatív törésmutatója az első közegre vonatkoztatva.[84]

Ezen jelenségek ismerete az elektronikai hadviselésben, a szögvisszaverők, dielektromos lencsék működésének megértéséhez szükségesek.

Mivel a fény sebessége vákuumban állandó, a látható fényt a hullámhosszával is jellemezhetjük. Kb. 400 nm és 800 nm közé esik a látható fény hullámhossza.

A fény az emberi szem retinájának érzékelőit, az úgynevezett csapokat és pálcikákat ingerli, mely ingerek elektromos impulzusokként terjednek az idegekben, a látóidegen végighaladva az agyban keltenek világosságérzetet.

Hogy az elektromágneses hullámok spektrumának éppen ezt a kis részét látjuk, valószínűleg a légkör sugárzáselnyelése miatt van így. Az elektromágneses hullámok jelentős részét ugyanis a légkör elnyeli, így azok nem érik el a Föld felszínét. Két „ablak" azonban nyílik a világűrre. Az egyik a rádióhullámok tartománya, a másik pedig a látható fényé. A rádióhullámokkal az a probléma, hogy a földfelszínen lévő kisebb tárgyak, illetve a víz igen csekély hatással vannak rá, leginkább magas fémtartalmú anyagokkal fogható fel. A másik ablak tartományának sugarai viszont – azaz ami végül az evolúció során láthatóvá lett – igen kis tárgyak felületéről is egyszerű szabályokat követve verődnek vissza és ráadásul az anyagtól függően általában igen jellegzetes visszaverődési színképet produkálnak, így az ezt érzékelni képes élőlények jól hasznosítható képet kapnak a környezetükről.

A lézer egy olyan fényforrás, amely stimulált emissziót használ egybefüggő fénysugár létrehozására. Neve az angol *Light Amplification by Stimulated Emission of Radiation* (fényerősítés a sugárzás gerjesztett emissziójával) kifejezés rövidítése, a *laser* magyarosításából származik. Az első lézert az amerikai Theodore H. Maiman fejlesztette ki 1960-ban.

A lézerfény tulajdonságai:

– a létrejött fény időben és térben koherens, a lézer által kibocsátott hullámok fázisa a sugár minden keresztmetszeténél azonos;
– a lézernyaláb keskeny és nagyon kis széttartású nyaláb, a lézerfény nagyrészt párhuzamos fénysugarakból áll, nagyon kis szóródási szöggel, ezzel nagy energiasűrűség érhető el szűk sugárban, a sugár által megtett távolságtól függetlenül;
– a lézerek energiája kis térrészben koncentrálódik, a lézerfény teljesítménysűrűsége a megszokott fényforrásokénak sokszorosa lehet;
– a lézer által kibocsátott hullámok mágneses mezejének iránya állandó;
– a lézerek fénye egyszínű, a lézersugár egy olyan elektromágneses hullám, amely közel egyetlen hullámhosszú összetevőből áll.

[84] Holics, L. szerk.: *Fizika*. Műszaki Könyvkiadó, Budapest, 1986. pp. 372-374.

A lézeres átvitelt alkalmazó adó-vevő párokat pont-pont közötti adatátvitelre használhatjuk. E kommunikáció napjainkban teljesen digitális, a lézerfény irányított energiakoncentrációja nagyobb távolság (akár 5 km) áthidalását teszi lehetővé.

Az illetéktelen lehallgatás, illetve külső zavarás ellen viszonylag védett. Az időjárási viszonyok azonban befolyásolják fény terjedését, így az eső, a köd, a légköri szennyeződések zavarként jelentkeznek, amik a kommunikációt akár teljesen blokkolhatják.

A lézerfényt azonban nem csak a szabad térben, hanem úgynevezett optikai szálban is lehet vezetni, így lézeres adatátvitel felhasználható lokális hálózatok, telefonközpontok összekötésére, valamint internetszolgáltatók adatátviteli gerincének kiépítéséhez és videó rendszereket összefogó kommunikációs hálózat központi gerincének telepítéséhez. A megvalósított adatátviteli sebesség jelenleg 1 és 10 Gbps között a leggyakoribb. A technológia folyamatos fejlődést mutat, így a maximálisan elérhető adatátviteli sebesség az előbbieket valószínűleg már meghaladja. Magyarország rendkívül fejlett hagyományokkal rendelkezik lézerfejlesztés terén, a magyar lézeres szakembereket világszerte elismerik.

Az infravörös sugarak a látható fény és a milliméteres hullámok között helyezkednek el a mikrométeres hullámtartományban. A –273,16 °C hőmérséklet felett minden test infravörös, szemmel nem látható sugárzást bocsát ki. Az infravörös tartományt a katonai alkalmazások széles körben alkalmazzák úgy mérési, érzékelési, mint hírközlési célokra. A méréstechnikai felhasználás során a testek által kibocsátott hőt a háttér hősugárzásával, vagy referencia hőmérsékletet biztosító anyag hőmérsékletével (például folyékony nitrogénnel) hasonlítják össze. Az érzékelő fejek, pelengátorok és képalkotó eszközök által szolgáltatott jeleket erősítés, jelfeldolgozás után egy vezérlőrendszerbe juttatják, vagy valamilyen monitoron teszik láthatóvá.

A hírközlési alkalmazásokban infravörös sugarakat kibocsátó sugárzók és érzékelők veszik át az adó-, és vevőantennák szerepét. Széles körben alkalmazzák távirányítókban is, mert zárt helyen meglehetősen zavarvédett, optikai álcázás után nincs nemkívánatos melléksugárzása.

Az infravörös sugárzást alkalmazó berendezéseket két nagy csoportba sorolhatjuk: az aktív és passzív eszközök csoportjába. Az aktív infravörös berendezések működtetéséhez infravörös megvilágító eszközök, reflektorok és megfelelő vevőberendezések szükségesek. A reflektor által megvilágított testekről visszaverődött hősugárzást veszi a vevő, és azt használja fel a rendeltetésének megfelelően.

Előnye, hogy érzéketlenebb vevőeszközökkel is jó eredmény érhető el, járulékos modulációkkal pedig a szándékos zavarok elleni védettségi jellemzők javíthatók. Hátránya, hogy a megvilágító sugárforrások intenzív áruló tényezők. Aktív infra reflektorok találhatók a harcjárművek éjjellátó rendszereiben, amely a kezelők éjszakai tevékenységét, a jármű vezetését, és a tájékozódást biztosítják a terepen.

A passzív infravörös berendezésekben nem alkalmaznak külön megvilágítást, hanem azt használják ki, hogy a testek a háttér környezetüktől eltérő intenzitású – következésképpen eltérő hullámhosszúságú – hősugarakat bocsátanak ki. A passzív infravörös berendezésekhez tartoznak a hőpelengátorok, az éjjellátó eszközök, foton sokszorozós éjszakai távcsövek, infra fényképező-, és videorendszerek.

Az infravörös sugárzás mértékét a sugárzási intenzitás jellemzi:

$$I = \varepsilon\sigma T^4 S / \Pi \qquad (2.18.)$$

ahol: ε – a sugárzási együttható, amely például repülőgép hajtóművek esetén 0,8-0,9. A gázturbinák kiáramló gázsugarára ε =0,2;
σ – a Stephan-Boltzmann állandó;
T – a hajtómű, a gázsugár, vagy adott test hőmérséklete [K];
S – a hatásos sugárzó felület nagysága a megfigyelés irányában.

Az összefüggésből látható, hogy az infravörös sugárzás intenzitását a hőmérséklet befolyásolja a legjobban, mivel annak negyedik hatványa szerint változik az intenzitás.[85]

Egy repülőgép hajtómű alkatrészeinek hőmérséklete 500-1200 K között van, a kiáramló gázsugár mintegy 900 K, utánégető üzemmódban elérheti az 1700 K hőmérsékletet. A Holizin-Wien-féle eltolódási törvénynek megfelelően a repülőgépek infravörös kisugárzásának hullámtartománya a 2,4-6,4 μm közé esik, utánégető alkalmazása esetén pedig 1,7-6,4 μm közé.

2.2 Az antennák

A különféle elektromágneses hullámok kisugárzására és vételére az elektronikai berendezések antennái szolgálnak.

Számtalan, különféle típusú, szerkezetű és felépítésű antenna ismeretes, amelyek típusának kiválasztásától és alkalmazásától nagymértékben függ az adott berendezés hatékony működése.

Az antennák alkalmazásánál figyelembe kell venni egyrészt például a hullámterjedés sajátosságait, a meteorológiai viszonyokat, a terepviszonyokat, a környezetben lévő zavaró objektumokat, az adás és vételi pont távolságát, irányát, másrészt az antennával kapcsolatos tényezőket, mint az antenna típusát, illesztését, hatásos magasságát, a sugárzás vagy a vétel irányát, a berendezés frekvencia tartományát, az adó teljesítményét, a vevő érzékenységét, az üzemeltetési feltételeket, illetve más körülményeket. Az esetek többségében kompromisszumos változatot kell elfogadni, mivel főleg mobil eszközök esetében általában nem lehetséges az elvileg optimális feltételek betartása a gyakorlatban.

Az antenna mérete, formája, illesztése szoros összefüggésben van a kisugárzandó vagy venni kívánt elektromágneses energia hullámhosszával. Ebből logikusan következik, hogy a hullámhossz függvényében különféle méretű és típusú antennák biztosítják az optimális adás-vételt. Mivel a katonai gyakorlatban a berendezések nem egy adott frekvencián, hanem egy viszonylag széles frekvenciasávon dolgoznak, ez rendkívül sokméretű antenna alkalmazását tenné szükségessé. Így gyakorlatilag néhány típust választanak ki, ezekkel szerelik fel a berendezéseket, és hangoló elemekkel biztosítják a helyes illesztést, az optimálishoz közel álló kisugárzást és vételt.

[85] Levityin, I. B.: *Infravörös sugárzástechnika*. Műszaki Könyvkiadó, Budapest, 1962. pp. 14-16.

Az elektronikai hadviselés fő területeiből kiindulva – elektronikai támogatás, elektronikai ellentevékenység, elektronikai védelem – meghatározhatók az antennával szemben támasztott követelmények.

Az elektronikai támogatás területén az antennáknak napszaktól, évszaktól, terepviszonyoktól függetlenül biztosítaniuk kell az ellenséges elektronikai berendezések teljes frekvencia tartományában a legkedvezőbb vételi lehetőséget.

Az elektronikai ellentevékenység területén dolgozó zavaró adók antennáinak a kisugárzott energia maximális mennyiségét kell az ellenséges vevőberendezések felé irányítaniuk, a saját eszközök lényeges zavarása nélkül.

Az elektronikai védelem területén a saját elektronikai eszközök antennáinak biztosítaniuk kell az ellenséges elektronikai eszközök zavarásának kiszűrését.

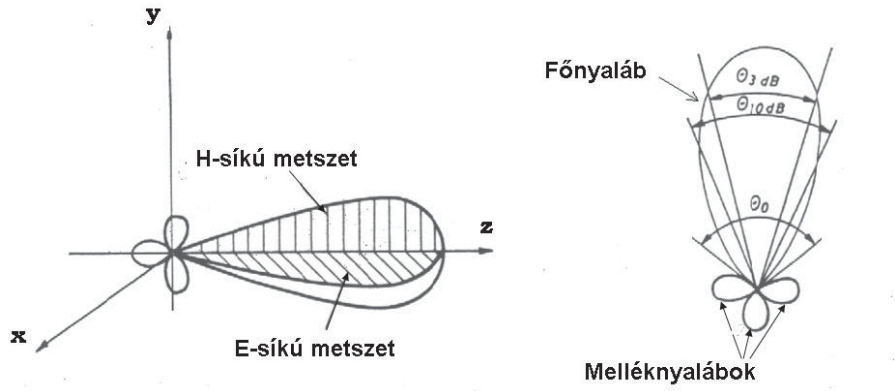
Az antennák helyes kiválasztása és a velük való manőverezés, telepítésük és alkalmazásuk nagymértékben befolyásolja az elektronikai eszközök és rendszerek hatékonyságát. Ezek alapján az antennákat többféle szempont szerint osztályozhatjuk.

Az antennák *üzemi hullámsávja* szerint beszélhetünk hosszú-, közép-, rövid-, ultrarövid hullámú, illetve mikrohullámú antennákról. Attól függően, hogy az antenna a *frekvenciasáv* mekkora részét képes átfogni megkülönböztethetünk normál- és szélessávú antennákat.

Irányítottság szerint az antennák lehetnek körkörösen sugárzók és irányítottak. Az irányított antenna is lehet tűsugárzó, legyező sugárzó, koszekáns iránykarakterisztikát létrehozó antenna. Az antennák *táplálása* lehet szimmetrikus vagy aszimmetrikus. *Árameloszlás szerint* meg lehet különböztetni állóhullámú vagy rezonáns antennát, illetve haladóhullámú antennát. Állóhullámú antennák esetében az antenna egyes pontjaiban az áram, illetve a feszültség értékei időben változnak, de az áram és a feszültség minimum és maximum helye változatlan. Haladóhullámú antennák közé sorolhatjuk azokat az antennákat, amelyeken sugárzás közben állandó minimum és maximum helyek nem találhatók, rajta haladó hullám van. Méreteik az üzemi hullámhossz többszörösét is elérik, és az adóval, illetve vevővel ellentétes oldalukon meghatározott értékű ohmos ellenállással vannak lezárva.

Az egyes frekvencia tartományokban alkalmazott antennák méretei lényegesen eltérnek egymástól, kivitelezésük alakja pedig jelentősen befolyásolja az *iránykarakterisztikájukat, irányhatásukat és nyereségüket.*

A gyakorlatban az antennák távoltere érdekes számunkra, tehát az iránykarakterisztika is a távoltérre vonatkozik. Az iránykarakterisztika az antenna által létrehozott térerősség térbeli eloszlásának leírására szolgál. A gyakorlatban az antennák háromdimenziós iránykarakterisztikái helyett azok síkmetszeteit szokták ábrázolni. A leginkább használatos a vízszintes és a függőleges síkok metszete. (2.5. ábra.)



2.5. ábra. **Az antenna iránykarakterisztika térbeli és síkbeli ábrázolása**[86]

Az antennák irányítottságát jellemző úgynevezett irányélességi szöget a félteljesítményű pontok ($\theta_{-3\ dB}$) közötti szög nagyságával szokták megadni. Mikrohullámú antennáknál szokásos még a $\theta_{-10\ dB}$-es pontok közötti szög, valamint a főnyaláb melletti első nullairányok θ_0 közötti kúpszög megadása is.

A normalizált iránykarakterisztika egyes térbeli pontjainak értékét a különböző térszögeken mért térerősség és a fő sugárzási irányban előállított maximális térerősség hányadosa adja meg. A fősugárzási irányban tehát az értéke mindig egy, valamennyi további irányban ennél csak kisebb lehet. A nagy teljesítménykülönbségek kényelmesebb ábrázolása céljából a logaritmikus feszültség-, vagy teljesítményskálázást alkalmazzák.

Van az antennaelméletben egy matematikai absztrakció, egy elvi antennakonstrukció, az izotróp sugárzó. Ennek az a jellegzetessége, hogy a fizikai mérete nulla, tehát pontszerű, az iránykarakterisztikája a térben szabályos gömb alakú, vagyis a tér minden irányában ugyanakkora térerősséget létesít.

Az egyes antennák abban is eltérnek egymástól, hogy egyesek körsugárzók, vagyis az adóból felvett energiát egy bizonyos sík mentén tekintve minden irányába egyenletesen sugározzák ki, míg mások csak a tér bizonyos irányaiban sugároznak (irányított antennák).

Az *antennanyereség* a főirányban kisugárzott teljesítménysűrűség és az azonos bemenő teljesítményű izotróp antenna teljesítménysűrűségének hányadosa:

$$G = \frac{S_{\max}}{S_0} \tag{2.19.}$$

ahol:

$$S_0 = \frac{P_{be}}{4\Pi r^2} \tag{2.20.}$$

[86] Géher, K. főszerk.: *Híradástechnika*. 2. kiadás. Műszaki Könyvkiadó, Budapest, 2000. p. 105.

A nyereség tehát függ az antenna veszteségétől. Az izotróp antenna hatásfoka 100%, de valamennyi gyakorlatban megépített antenna hatásfoka kisebb, mint 100%. A hatásfok tehát:

$$\eta = \frac{G}{D} = \frac{P_t}{P_{be}} \tag{2.21.}$$

Az antennák fontos paramétere a hatásos felületük, amelyet az alábbi összefüggés ad:

$$A_R = \frac{G\lambda^2}{4\Pi} \tag{2.22.}$$

ahol: λ – a hullámhossz [m].[87]

Amennyiben az összeköttetést csak egy meghatározott irányban kell fenntartani, akkor az irányított antennák alkalmazása az adó és a vevő oldalon is előnyöket biztosít. Irányított antenna esetén azonos betáplált teljesítmény mellett, az energia egy irányba koncentrálása miatt nagyobb a létrehozott térerő, mint körsugárzó esetén.

Az üzemi frekvenciatartományoknak megfelelően vannak jellegzetes antennakonstrukciók és vannak általános típusok, amelyek csak méretükben különböznek egymástól.

A hosszú-, és középhullámú rádiófrekvenciás tartományban dipólantennákat, haladóhullámú antennákat alkalmaznak. Jellemzőjük, hogy a megvalósításhoz igen nagy fizikai méretekre van szükség, ezért aktív elemként hatalmas tornyokat, vagy tornyok között kifeszített huzalokat használnak.

A rövidhullámú frekvenciatartomány jellegzetes konstrukciói a dipólok, szélessávú dipólok, sarokdipólok, haladóhullámú antennák, rombuszantennák, botantennák, keretantennák. Különleges műsorszórási célra készítenek rövidhullámú logaritmikus-periodikus antennát is, amely toronyra szerelve forgatható is lehet.[88]

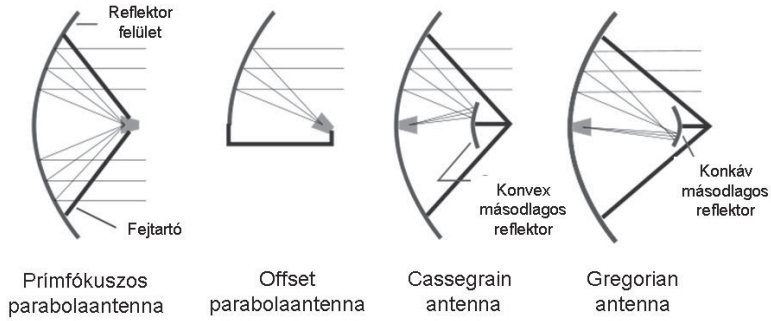
2.6. ábra. **A Yagi és a logaritmikus-periodikus antenna[89]**

87 Géher, K. főszerk.: *Híradástechnika*. 2. kiadás. Műszaki Könyvkiadó, Budapest, 2000. pp. 104-106.

88 Istvánffy, E.: *Tápvonalak, antennák és hullámterjedés*. Tankönyvkiadó, Budapest, 1984. pp. 309-333.

89 http://www.dnjradio.com///images/sy4.jpg?osCsid=0a0cc1a017e479f98bee2001185d17f3 http://www.arbenelux.com/images/ETS_LogPer.jpg (Letöltve: 2014. 02. 06.)

Az alacsony és magas ultrarövid-hullámú frekvenciatartományban kb. 1 GHz-ig bezárólag dipólantennákat, Yagi-antennákat, logaritmikus-periodikus antennákat (2.6. ábra), tárcsás-kúpos antennákat, helix-antennákat, illetve az ezekből felépített csoportantennákat használják. Lényeges műszaki tulajdonságuk, hogy szimmetrikus, vagy aszimmetrikus, koaxiális táplálásúak. A kis fizikai méretek, a stabil konstrukció, a jó sugárzási paraméterek miatt az utóbbi időben széles körben terjednek a nyomtatott, vagy más néven microstrip antennák.



2.7. ábra. **A parabola antennák táplálásának különféle fajtái**[90]

3 GHz fölött az antennák tervezésekor a fizikai méreteket meghatározó hullámhossz olyan kicsi, hogy már például egy félhullámú dipól kivitelezése a tápvezetékhez képest gondot okoz. 1,5-2 GHz felett megváltozik a hullámvezetés fizikai módja is. A kábelek helyett csőtápvonalakon továbbítják az elektromágneses energiát. Ebben a tartományban a csőtápvonalak szétnyitásából származtatott tölcsérsugárzók a legjellegzetesebb konstrukciók. Attól függően, hogy milyen a tölcsérsugárzó által megvilágított fémfelület, megkülönböztethetünk egyszerű tölcsérantennákat, parabolaantennákat, Cassegrain-antennákat. Attól függően, hogy a parabolafelület mely szakaszát világítják meg, lehet prímfókuszos és offset parabolákról beszélni. A Cassegrain-antennák esetén a sugárzó előbb egy hiperbola felületet világít meg, majd az sugározza be a parabolafelületet. (2.7. ábra – előző oldalon)

2.3 Modulációs módok

Az információ továbbítására szolgáló vivőhullámok valamely fizikai paraméterének szisztematikus megváltoztatását *modulációnak* nevezzük. Egy szinuszos vivőhullámú modulált jel általános matematikai leírása az alábbi módon adható meg:

[90] http://commons.wikimedia.org/wiki/File:Parabolic_antenna_types2.svg (Letöltve: 2014. 02. 14.) (a forrás alapján szerkesztették a szerzők)

$$s_v(t) = a(t)\cos[\Theta(t)] \tag{2.23.}$$

ahol: $s_v(t)$ – a szinuszos vivőhullámú modulált jel t időpillanatban felvett értéke;
$a(t)$ – a vivő pillanatnyi – a t időpillanatban felvett – amplitúdója;
$\Theta(t)$ – a vivő pillanatnyi – a t időpillanatban felvett – fázisa.

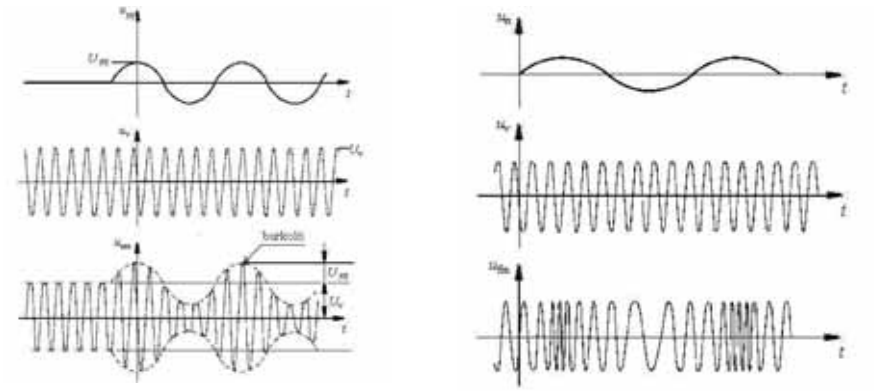
A vivőhullámnak mind az amplitúdója, mind a fázisa, akár mindkettő is változtatható. Aszerint, hogy melyiket változtatjuk, annak megfelelően amplitúdó-, vagy szögmodulációról beszélünk. Az amplitúdómoduláció során kapott kimenő jel lehet kétoldalsávos *(Amplitude Modulation Double Sideband – AM-DSB),* kétoldalsávos elnyomott vivőjű *(Amplitude Modulation Double Sideband Suppressed Carrier – AM-DSB/SC),* vagy egyoldalsávos elnyomott vivőjű (*Amplitude Modulation Single Sideband Suppressed Carrier – AM-SSB/SC).*

Amplitúdó moduláció esetén a moduláló jel csúcsértékének (U_m) és a vivőfrekvenciás jel csúcsértékének (U_v) a hányadosát modulációs mélységnek nevezzük, m-el jelöljük és százalékban adjuk meg:

$$m = U_m / U_v \times 100\% \tag{2.24.}$$

A moduláló jel (U_m) amplitúdójának változásakor változik a modulált jel (U_{am}) burkológörbéjének amplitúdója, a moduláló jel frekvenciájának változásakor pedig a burkológörbe frekvenciája, vagyis az eljárás mind a moduláló jel amplitúdó, mind a frekvencia információ pillanatnyi értékének átvitelére alkalmas.

A szögmodulált jelek lehetnek frekvencia- (FM), vagy fázismoduláltak (PM), mivel a moduláló jel közvetlen lineáris kapcsolatban lehet mind a pillanatnyi frekvenciával, mind a pillanatnyi fázisszöggel.



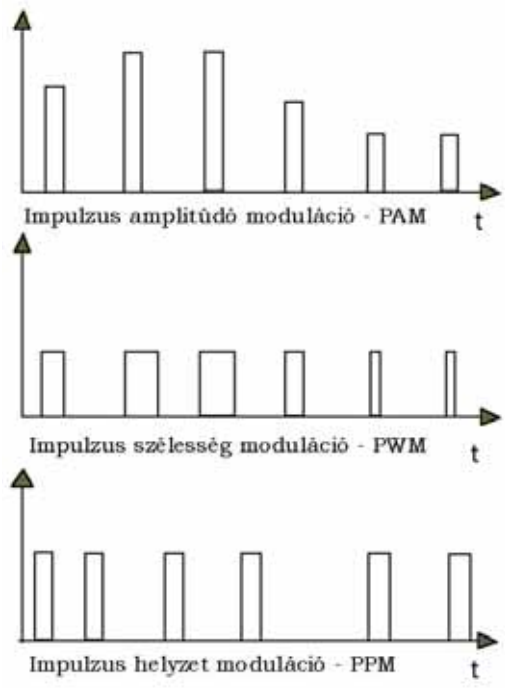
2.8. ábra. **A kétoldalsávos amplitúdómoduláció (AM-DSB) hullámformája (balra) és a frekvenciamodulált jel (FM) (jobbra)[91]**

[91] http://wiki.ham.hu/index.php/Oldals%C3%A1v (Letöltve: 2014.02.06.)

A frekvenciamoduláció esetén a modulált jel U_{fm} amplitúdója állandó, frekvenciája pedig a moduláló jel pillanatértékétől függ. A 2.8. ábrán jobbra, a moduláló jel amplitúdójának növekedésekor a modulált jel frekvenciája nő, a moduláló jel frekvenciájának változása pedig azt határozza meg, hogy a modulált jel frekvenciája milyen ütemben változzon. A moduláló jel maximális értékéhez a legnagyobb frekvencia kitérés tartozik, ezt frekvencia löketnek hívjuk. Jele: Δf. A frekvenciamodulált jelhez tartozó modulációs index a frekvencialöket (Δf) és a moduláló jel frekvenciájának (f_m) a hányadosa:

$$m = \Delta f / f_m \qquad (2.25.)$$

A frekvenciamodulált jel is egy adott szélességű frekvenciasávot foglal el a frekvenciatartományból. Ez a sávszélesség az úgynevezett modulációs indextől függ. Keskeny sávú frekvenciamodulációnál *(Narrow Band Frequency Modulation – NBFM)* $m < 1$, ekkor a sávszélesség $B = 2 f_m$, azaz a moduláló jel legnagyobb frekvenciájának kétszerese, széles sávú frekvenciamodulációnál *(Wide Band Frequency Modulation – WBFM)* $m > 1$, és a sávszélesség $B = 2 \Delta f$, azaz a löket kétszerese.[92]



2.9. ábra. **Digitális alapsávi modulációs eljárások**[93]

[92] Géher, K. főszerk.: *Híradástechnika*. 2. kiadás. Műszaki Könyvkiadó, Budapest, 2000. pp. 126-136.

[93] Szerkesztették a szerzők.

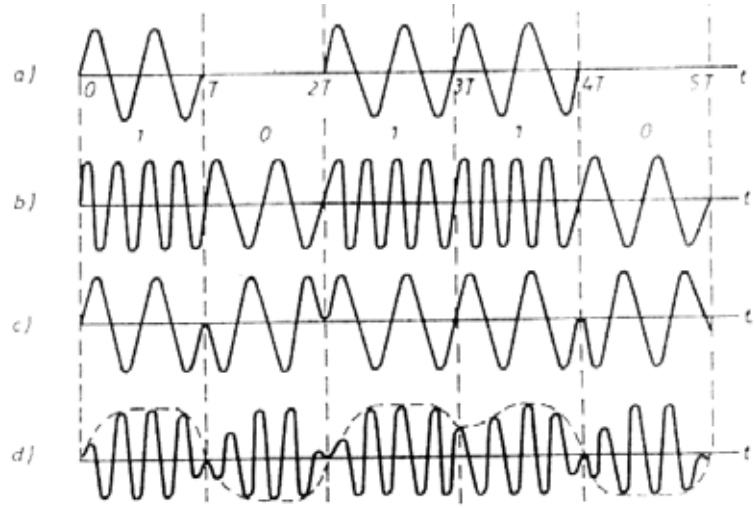
A digitális információk átvitelére szolgáló modulációs rendszereket két csoportba soroljuk:

– digitális alapsávi modulációs rendszerek;
– digitális vivős modulációs rendszerek.

Mivel most a moduláló jel nem analóg, hanem digitális, ezért itt nem az alakhű jelátvitel a fontos, hanem az, hogy az átvitt jelből a vevőoldalon minél kisebb hibavalószínűséggel lehessen visszanyerni az eredeti digitális adatokat.

A *digitális alapsávi moduláció* esetén a digitális információt az impulzusnak akár az amplitúdója, az időtartama, vagy akár a helyzete is hordozhatja. Ezeket az impulzusvivőjű rendszereket éppen ezért impulzusamplitúdó-modulációnak *(Pulse Amplitude Modulation – PAM)*, impulzus szélesség modulációnak (*Pulse Width Modulation – PWM),* illetve impulzushelyzet-modulációnak *(Pulse Position Modulation – PPM)* nevezzük. (2.9. ábra)

A *digitális vivős modulációs rendszerek* alkalmasak arra, hogy egy sávátereszto jellegű csatornán bináris adatokat vigyünk át. A 2.10. ábrán láthatók a bináris jellel modulált vivő jellegzetes hullámalakjai.



2.10. ábra. **Bináris jellel modulált vivőhullám képe**[94]
a) ASK; *b)* FSK *c)* PSK; *d)* AM-DSB

Az *a)* sorban látható a kétállapotú amplitúdómoduláció hullámformája, alatta pedig a bináris jelsorozat 0-1 értékei. Logikai 1-nél a vivőhullámot „bekapcsoljuk", 0-nál pedig ki, vagyis ott nem lesz kisugárzás. Ezt a modulációs módot amplitúdó billentyűzésnek *(Amplitude Shift Keying – ASK)* hívják.

[94] Géher, K. főszerk.: *Híradástechnika*. 2. kiadás. Műszaki Könyvkiadó, Budapest, 2000. p. 145.

A *b)* sorban látható jel vivőfrekvenciája logikai 1-nél f_1, logikai 0-nál pedig f_2 értéket vesz fel. Ezt szokás frekvenciabillentyűzésnek *(Frequency Shift Keying – FSK)* hívni.

A *c)* sorban látható esetben a szinuszos vivőnek csak a fázisa tolódik el ugrásszerűen a moduláció hatására, mind az amplitúdó, mind a frekvencia eközben változatlan marad. Ezt az eljárást fázisbillentyűzésnek *(Phase Shift Keying – PSK)* nevezzük.

Az utolsó (d) sorban a szinuszos vivőhullámot egy előzőleg „simított" pulzus amplitúdó modulált jellel moduláljuk. Ennek az eljárásnak az az előnye, hogy ez igényli a legkisebb sávszélességet.

A katonai rádiós hírközlési rendszerekben a negyvenes évek óta kiemelkedő jelentőségre tettek szert a kiterjesztett (szórt) spektrumú vezeték nélküli technológiák *(Spread Spectrum Technologies – SST).* A kiterjesztett spektrumú átviteli rendszerek alapvető jellemzője, hogy a bennük alkalmazott speciális csatornakódolási (modulációs) eljárások következtében a csatorna által felhasznált teljes sávszélesség, B (Hz) nagyobb, néha nagyságrendekkel nagyobb, mint a hagyományos modulációs rendszerekkel létrehozott jelek sávszélessége azonos R_b (bit/s) sebességű alapsávi forgalom esetén. Az ilyen rendszerek legfontosabb paramétere az ún. sávszélesítési tényező $ST=B/R_b$. A kiterjesztett spektrumú jelekben rejlő nagy redundancia még abban az esetben is elfogadható átviteli minőséget jelent, ha az átviteli csatornában a normál Gauss-zajon kívül jelentős, szándékos, additív zavar, vagy csatorna interferencia van.

A kiterjesztett spektrumú rendszerek másik fontos tulajdonsága az álvéletlen (pseudo random) jelleg, ami azt jelenti, hogy az átviteli csatornában folyó kommunikáció a rendszeren kívüli megfigyelő számára nagy sávszélességű, zaj jellegű véletlen folyamatnak tűnik. A rendszeren belüli alkalmazók – ismerve a csatornakódolás szabályosságát – dekódolni tudják az átküldött információt.

A rendszerben az átvitel során energianyereség (EG) keletkezik, ami azt jelenti, hogy adott hasznos jelteljesítmény (S) és zavaró teljesítmény (J) mellett a vevő demodulátorában a jel-zavar viszony ($(SJR)_d$) nagyobb, mint a csatorna jel-zaj viszonya ($(SJR)_{cs}$) és a két mennyiség hányadosa az energianyereségi tényező:

$$EG = \frac{(SJR)_d}{(SJR)_{cs}} \tag{2.26.}$$

ami tipikusan azonos a sávszélesítési tényezővel (ST). Mivel az adott teljesítményű kiterjesztett spektrumú jel sávszélessége nagy, a teljesítmény spektrális sűrűsége alacsony, így mód van arra, hogy a jelet a háttérzaj szintje alá csökkentsük.

A spektrum kiterjesztésének öt elve ismert:

Fázisugratásos vagy direkt szekvenciális (Direct-Sequence – DS) az a rendszer, ahol az adóból kisugárzott vivőhullám fázisát változtatjuk egy álvéletlen kódsorozat szerint (PSK moduláció). Ezt úgy oldják meg, hogy az eredeti digitális modulált jelet egy álvéletlen – legtöbbször bináris – kódsorozattal szorozzák meg. A kapott jel sávszélessége jelentősen megnő. A vevőben az eredeti jelet úgy kapjuk vissza, hogy a vett jelet újra ezzel a kódsorozattal szorozzuk meg, így a hasznos jel visszakerül az eredeti sávjába. Fontos feltétel, hogy a szorzójel frekvenciája legalább egy nagyságrenddel nagyobb legyen az eredeti digitális jel alapfrekvenciájánál.

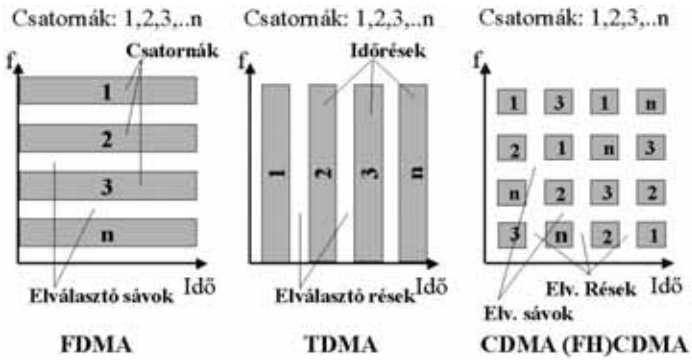
Frekvenciaugratásos (Frequency Hopping – FH) az a rendszer, ahol az adó frekvenciáját változtatjuk ugrásszerűen egy – az adóban és a vevőben egyaránt ismert – álvéletlen kódsorozat szerint. A frekvenciákat mindkét helyen egy előre meghatározott készletből választjuk ki, és az adó és vevő szinkronban fut. Lassú frekvenciaugratás esetén az ugratás ideje hosszabb a szimbólumidőnél, gyors frekvenciaugratás esetén viszont a vivő frekvenciája egy szimbólumidő alatt többször is változhat.

Időugratásos (Time-Hopping – TH) az a rendszer, ahol az adó az időtengelynek csak bizonyos időréseit használja fel adásra, és ezeket az időréseket az adó és a vevő is egy mindkét helyen ismert álvéletlen kód alapján választja ki. A vevő itt is követi az adót, de most időben és csak akkor lesz aktív, amikor az időrés számára ki van jelölve. Így is lehetőség van az aktív zavarok elhárítására.

A pulzus-FM, vagy Chirp-SST eljárás során a jel frekvenciáját adott f_1 és f_2 frekvenciákkal határolt frekvenciasávban lineárisan, vagy meghatározott függvény szerint változtatjuk. A változás adott T idő alatt történik. A vétel általában illesztett szűrőjű vevővel történik, ami a hasznos jel sajátosságai miatt a vivő-típusú interferáló jeleket (moduláció nélküli kisugárzásokat) erősen elnyomja.

Az ötödik eljárás az úgynevezett hibrid *(Hybrid SST)* rendszer, amely a DS, az FH, a TH, vagy a Chirp-SST eljárások kombinációjaként állítható elő.

Az eddig kialakult és leggyakoribbnak tekinthető a többszörös frekvencia hozzáférésű rendszer *(Frequency Division Multiple Access – FDMA),* a többszörös idő hozzáférésű rendszer *(Time Division Multiple Access – TDMA)* mellett a kiterjesztett spektrumú rendszerek a kódosztásos többszörös hozzáférési technikát *(Code Division Multiple Access – CDMA)* nyújtják. Az FH-CDMA eljárás esetén az egymástól független csatornákhoz, illetve tagállomásokhoz a rendelkezésre álló diszkrét frekvenciák készletéből más-más kombinációk, illetve az ennek megfelelő más-más kódok tartoznak. A kódokat álvéletlen zaj *(Pseudo Noise – PN)* generátorok hozzák létre. Az FDMA, TDMA és a CDMA többszörös csatorna hozzáférési elveket a 2.11. ábrán láthatjuk.



2.11. ábra. **A többszörös csatorna hozzáférések fajtái**[95]

[95] http://www.itu.int/osg/spuold/ni/images/codedivision.gif (a forrás alapján szerkesztették a szerzők)

Az elektronikai hadviselés szempontjából a kiterjesztett spektrumú rendszereknek speciális jelentőségük van. Igen jó felderítés elleni védelemmel és zavarállósággal rendelkeznek. A zajszint alatti jeleket a panoráma, pásztázó típusú felderítő vevők nem érzékelik, így a zavaráshoz szükséges célmegjelölés sem lehetséges a hagyományos módon. A keskeny-, de a szélessávú zavarokkal szemben is jó zavarvédelmet biztosítanak, hiszen a vett jelnek a vételi kódsorozattal való beszorzása a helyes szekvenciákat kiemeli, a zavarokat pedig szétszórja. A frekvenciaugratásos rendszerek felderítése új típusú, tárolós, ún. vízesés diagramot használó felderítő vevőkkel lehetséges, amíg a számuk nem túl nagy. Ma már a gyors iránymérésük is megoldott. A lefogásuk azonban továbbra is gondot jelent, mivel a szélessávú zavarás hatékonysága alacsony és a frekvenciakészlet (illetve az idő) több mint ötven százalékában ki kellene ütni a vett jeleket ahhoz, hogy a zavarás a kódjavító algoritmusok és hibajavító eljárások ellenére hatásos legyen.

2.4 Az elektronikai hadviselésben használt alapvető matematikai összefüggések

2.4.1 A decibelre (dB) épülő számolási rend

Mielőtt azonban továbblépnénk, álljunk meg egy pillanatra a számításoknál alkalmazott egységeknél. A rádiótechnikában szokásos számításokat nem a fizikai mennyiségek alapmértékegységeivel, hanem azok úgynevezett logaritmikus alakjával szokás végezni. Bevezették a dB-t (olvasva decibel), a tízes logaritmus alapú viszonyítási rendszert, amely definíciója szerint: A[dB]=10log$A$[lin]. Vagyis, valamely A arányténvező dB-ben úgy kapható meg, hogy az A arány lineáris egységének vesszük a tízes alapú logaritmusát, és azt megszorozzuk tízzel. Tehát például a kétszeres viszony 3 dB-t, a tízszeres 10 dB-t, a százszoros 20 dB-t, a századrész –20 dB-t jelent.

Megállapodás szerint a teljesítmény alapegységének, a számítási alapot képező 0 dB-nek az 1 mW-ot veszik, és ehhez képest számítanak tovább minden teljesítményértéket. Vagyis az 1 mW az 0 dBm, a 2 mW az 3 dBm, a 10 mW az 10 dBm, az 1 W az 30 dBm, és így tovább. A dB utáni „m” a mW-ra utal. Ez a számítási eljárás a logaritmusokkal végzett számítások azon előnyét használja, hogy a szorzások, osztások leegyszerűsödnek összeadásokká és kivonásokká. A gyakorlati számítások során alkalmazott táblázatok, mérési eredmények általában már eleve dB-ben adják meg az adatokat, így feltétlenül ezt célszerű alkalmazni.

Vegyünk egy gyakorlati példát. Legyen egy adó teljesítménye P_a = 1 W, az adóantenna nyeresége 10-szeres, a terjedési úton a kisugárzott jel csillapodjon a 10^{-10}-ed részére, az atmoszférikus csillapítás (táblázati adat) legyen 3 dB, a vevőantenna legyen izotróp sugárzó. Kérdés, mekkora a vett jel teljesítménye a vevő bemenetén? Látható, hogy a vegyes mértékrendszer igen megnehezíti a számítást, ezért célszerű áttérni a logaritmikus dB skálára. Az adó teljesítménye P_a[dB] = 10log1000 [mW] = +30 dBm. Az adóantenna nyeresége 10 dB, a szakaszcsillapítás 100 dB, az atmoszférikus csillapítás 3 dB, a vevőantenna nyeresége 0 dB.

A vett teljesítmény: P_v[dB] = +30 dBm + 10 dB – 100 dB – 3dB + 0 dB = –63 dBm, ami 0,5 nW. Fontos megjegyezni, hogy a számítás során minden olyan tényezőt, amely erősítés, vagy forrásteljesítmény szerepet játszik, azt pozitív előjellel, és minden csillapítás jellegű tényezőt negatív előjellel kell figyelembe venni.

2.4.2 Az elektromos térerősség

A gyakorlati életben a tér egy adott pontjában, a rádiócsatornában a két antenna között, a teljesítmény dBm-ben való jellemzése nem célszerű, mivel ott a mérőantennában indukálódott feszültségnek világosabb fizikai tartalma van. A tér egy adott pontjában adott frekvencián mérhető villamos térerősséget szokták használni, amely általában az adóberendezésektől távolabb mérve mV/m, mV/m, tartományba esik. A mikrohullámú berendezéseket kivéve, a rádiófrekvenciás vevőberendezések érzékenységét is mV-ban adják meg. Az érzékenység definíció szerint az a minimális bemeneti jelfeszültség, amely a vevőberendezés kimenetén az előírt jel/zaj viszonyt létrehozza.

Gyakran megeshet, hogy át kell tudnunk térni a mV/m térerősségről a dBm-re.

Ezt az alábbi összefüggés segítségével tehetjük meg (levezetés nélkül):

$$P = -77 + 20\log(E) - 20\log(f) \tag{2.27.}$$

ahol: P – a jel teljesítmény [dBm];
E – az elektromos térerősség [mV/m];
f – frekvencia [MHz].

Az összefüggés dBm-ről mV/m-re való átszámításhoz átalakítva:

$$E = 10^{(P+77+20\log(f)/20)} \tag{2.28.}$$

2.4.3 A rádiócsatorna

Legyen szó akár rádió összeköttetésről, rádiólokációról, jelfelderítésről, vagy zavarásról, alap építőkőnek tekinthető az úgynevezett rádiócsatorna leírása.

A rádiócsatorna egy jelforrást, egy vevőberendezést és a közöttük lévő átviteli utat, a hullámterjedési közeget foglalja magába. A jelforrás fizikailag lehet egy rádióadó, egy lokátor berendezés, egy izotróp sugárzó (elméleti, gömbfelületen egyenletesen sugárzó pontszerű antenna), vagy egy repülőgép felülete, amelyről a visszaverődött elektromágneses energiát tekintjük jelforrásnak. A vevőberendezést általában egy térbeli szelekciót megvalósító antenna és maga a vevőkészülék képezi.

Rendszertechnikai szempontból *a rádiócsatorna bemenete az adóberendezés kimeneténél* kezdődik, amelynek legfontosabb jellemzője a frekvencia, a kimenő teljesítmény és egyes esetekben az üzemmód, vagy más szóval a modulációs mód. Ezután következik az antenna, az átviteli közeg, amely hullámterjedési, csillapítási és más fizikai hatásokkal befolyásolja az elektromágneses energia vételi pontba jutását. Fontos paraméterei az

átviteli szakasz fizikai hossza, a terjedési út domborzati viszonyai, az évszak, napszak, időjárási tényezők. A rendszer másik végén található a vevőantenna, és az *a vevőberendezés*, amelynek *bemenetéig tart* a matematikai értelemben vett *rádiócsatorna*.

Tehát a rádiócsatorna az adóantenna bemenete és a vevőantenna kimenete közötti kétkapu. A kétkapu csillapítását szakaszcsillapításnak nevezzük, és az alábbi módon határozzuk meg:

$$a_{sz} = 10 \lg \frac{P_{be}}{P_R} \qquad (2.29.)$$

ahol: P_{be} – az antennába betáplált hatásos teljesítmény;
P_R – a vevőantenna által leadott hatásos teljesítmény.

A szakaszcsillapítást elsősorban a korábban már áttekintett antennák paraméterei, az adó és vevő közötti közeg hullámterjedési tulajdonságai határozzák meg. Ennek megfelelően a szakaszcsillapítás egy elméleti szabadtéri csillapításból (a_0), a polarizációs csillapításból (a_p), a reflexiós csillapításból (a_r) és az ún. többletcsillapításból (a_t) tevődik össze.

$$a_{sz} = a_0 + a_p + a_r + a_t \qquad (2.30.)$$

A *szabadtéri csillapítást* az egyes hullámterjedési módokra egyenként tárgyaljuk. A *polarizációs csillapítás* oka az, hogy adott antennák csak adott polarizációjú jelek vételére alkalmasak, tehát ha mást veszünk vele, a hatásfoka romlik. A csillapítás mértékét a 2.3. táblázatban foglaltuk össze.

A *reflexiós csillapítást* a berendezések, kábeleik és antennáik illesztetlenségéből adódó reflexiók okozzák. A *többletcsillapításhoz* számítunk minden egyéb járulékos csillapítást. Ilyen lehet például az eső, sűrű hóesés okozta ideiglenesen fellépő, akár igen nagy értékű légköri csillapítás is.

Adóoldal / Vevőoldal	Függőleges	Vízszintes	Jobbra forgó körpolarizált	Balra forgó körpolarizált	Jobbra 45°-ban álló, lineáris	Balra 45°-ban álló, lineáris
Függőleges	0 dB	∞	3 dB	3 dB	3 dB	3 dB
Vízszintes	∞	0 dB	3 dB	3 dB	3 dB	3 dB
Jobbra forgó körpolarizált	3 dB	3 dB	0 dB	∞	3 dB	3 dB
Balra forgó körpolarizált	3 dB	3 dB	∞	0 dB	3 dB	3 dB
Jobbra 45°-ban álló, lineáris	3 dB	3 dB	3 dB	3 dB	0 dB	∞
Balra 45°-ban álló, lineáris	3 dB	3 dB	3 dB	3 dB	∞	0 dB

2.3. táblázat. **A polarizációs csillapítás mértéke a lehetséges kombinációk esetén**[96]

[96] Forrás megjelölés / szerzők saját szerkesztése megjelölés hiányzik!!!!

2.4.4 A jelek energiaviszonyainak leírása rádiólokáció esetén

A rádiólokáció (*RADio Detection And Ranging – RADAR*) olyan műszaki eljárás, amely a rádióhullámok terjedése révén céltárgyak felderítésére, jellemzőik (például helyzetük, mozgásuk, méretük, alakjuk) meghatározására alkalmas. A rádiólokátor konstrukciók a legszélesebb felosztás szerint lehetnek primer, vagy szekunder lokátorok.

A *primer lokátorok* esetén egy adóberendezés által előállított jelet kisugárzunk a térbe és az ott található reflektáló tárgy, objektum által visszavert jelet veszi a vevőantennánk. Ilyen eszközök például a légtérfelderítő, meteorológiai lokátorok.

A *szekunder lokátorok* letapogató jelét a célobjektumban üzemelő vevőkészülék veszi, feldolgozza, majd a kialakított válaszjelet egy aktív adóberendezéssel visszasugározza. Ezt az elvet alkalmazzák a saját-ellenség felismerő rendszerek, valamint a polgári és katonai légi forgalom repülésirányító rendszerében is, ahol a földi radar kérdező jelére egy fedélzet transzponder válaszol.

Attól függően, hogy a lokátor adója és vevőberendezése egy helyen települ, vagy egymástól távol, beszélhetünk monosztatikus, illetve bisztatikus elrendezésről.

A monosztatikus elrendezésű lokátor elméleti hatótávolsága (levezetés nélkül):

$$R_{\max} = \sqrt[4]{\frac{\sigma_c}{4\Pi}\frac{P_a}{P_{v\min}}\frac{A_v^2}{\lambda^2}} \tag{2.31.}$$

ahol: R_{max} – az elméleti hatótávolság;
s_c – a légicél hatásos keresztmetszete;
P_a – a lokátor adóteljesítménye;
P_{vmin} – a lokátor vevőjének adott detekciós valószínűséghez tartozó minimális bemenő teljesítmény;
A_v – hatásos antennafelület, és az adásra ugyanazt az antennát használjuk, mint a vételre;
λ – üzemi hullámhossz.[97]

Az összefüggésből látható, hogy a hatótávolság kétszeres növeléséhez a teljesítményt a 16-szorosára kellene növelni, mert közöttük negyedik hatvány szerinti összefüggés van. A vett teljesítmény:

$$P_v = \frac{P_a \sigma_c}{4\Pi R^4}\frac{A_v}{\lambda^2} \tag{2.32.}$$

Aktív válaszadóval felszerelt céltárgy esetén a hatótávolság:

$$R_{ct} = \sqrt{\frac{P_c}{P_{v\,min}}}\frac{\sqrt{A_c A_v}}{\lambda^2} \tag{2.33.}$$

[97] Ferenczi, G. – Szűcs, P. – Balog, K.: *Rádiólokáció alapjai*. Bolyai János Katonai Műszaki Főiskola, Budapest, 1998. p. 50.

ahol: P_c – a céltárgyról kisugárzott válaszjel teljesítménye;
A_c – a céltárgyra telepített adóantenna hatásos felülete;
A_v – a vevőantenna hatásos felülete.

2.4.5 A rádiózavarás alapvető matematikai összefüggései

Az elektronikai zavarás távolsága több tényezőtől is függ. Ilyenek lehetnek:
- a zavarandó összeköttetés adójának teljesítménye;
- az adó által használt antenna nyeresége a vevőberendezés irányában;
- a vevő érzékenysége;
- az alkalmazott üzemmód (zavarállóság, jelfeldolgozási eljárás);
- a zavaró berendezés teljesítménye;
- a zavaró állomás antennájának nyeresége a lefogandó vevő irányában;
- a zavarandó összeköttetés távolsága és az azon fellépő szakaszcsillapítás;
- a zavaró adó és a lefogandó vevő távolsága, az azon fellépő szakaszcsillapítás;
- a hullámterjedést befolyásoló tényezők;
- az üzemi frekvencia;
- a zavaró adó által létrehozott zavarjel üzemmódja (moduláció típusa).

A gyakorlati számítások során ennyi tényezőt egzakt módon nem lehet figyelembe venni, ami tehát bizonyos fizikai tényezők elhanyagolását, leegyszerűsítését jelenti. A korszerű számítástechnikai eszközök segítségével a számítások precizitása fokozható, így például az összeköttetési és zavarási szakaszokon fellépő szakaszcsillapítások pontosításával. A korábbi elhanyagolások helyett például a terep által okozott diffrakciós terjedést modellezve a valós energiaviszonyok is jól közelíthetők.

A rádiózavarás számítási eljárásaiban két alapvető kérdésre keressük a választ. Adott műszaki paraméterekkel rendelkező konfiguráció esetén mekkora az összeköttetés lefogásához minimálisan szükséges zavarteljesítmény, és adott teljesítményviszonyok mellett mekkora a lefogási zóna távolsága? A továbbiakban ezt fogjuk áttekinteni.

A rádióeszközöket akkor lehet lefogni – rendeltetésszerű működésüket az előírt mértékben akadályozni –, ha a vevőberendezésük bemenetére az adott üzemmód mellett a lefogáshoz minimálisan szükséges zavarjelnél nagyobbat juttatunk. A lefogás bekövetkezésekor a bemeneten fellépő zavarjel és hasznos jel teljesítményének minimális arányát lefogási tényezőnek nevezzük:

$$K_{zmin} = \frac{P_z}{P_j} \tag{2.34.}$$

A zavarás hatékonynak számít, ha a vevő bemenetén nagyobb zavar/jel viszonyt tudunk létrehozni, mint $K_{z\,min}$. Minél kisebb ez az arányszám, annál könnyebb energetikailag a hatékony zavarást létrehozni. Azt a területet, térrészt, ahol $K > K_{z\,min}$ lefogási zónának, ahol pedig $K < K_{z\,min}$, azt le nem fogott zónának nevezzük. A zónahatár azon a térbeli felületen foglal helyet, ahol $K = K_{z\,min}$.

Ha $K_{z\,min}$ ismert, és adottak az állomások technikai, valamint elhelyezkedési paraméterei, akkor az effektív lefogáshoz szükséges minimális zavaró teljesítmény az alábbi összefüggéssel határozható meg:

$$P_{z\,min} = K_{z\,min} \frac{P_j G_j D_z^2 \Delta f_z}{G_z D_j^2 \Delta f_v \vartheta_z} \tag{2.35.}$$

ahol: $P_{z\,min}$ – a hatékony zavaráshoz szükséges minimális teljesítmény;
$K_{z\,min}$ – lefogási tényező;
P_j – a lefogandó összeköttetésben dolgozó adó teljesítménye;
G_j – a lefogandó összeköttetésben dolgozó adóantenna nyeresége a vevőkészüléke irányában;
G_z – a zavaró állomás antennájának nyeresége a vevő irányában;
D_z – a zavaró állomás és a vevő közötti távolság;
D_j – a lefogandó összeköttetésben dolgozó adó és vevő közötti távolság;
Δf_z – a zavarjel sávszélessége;
Δf_v – a vevőkészülék vételi sávszélessége;
ϑ_z – polarizációs egyeztetési tényező.

A rádióösszeköttetés lefogási távolsága matematikai átrendezéssel egyszerűen kapható:

$$D_z = D_j \sqrt{\frac{P_z G_z \Delta f_v \vartheta_z}{P_j G_j \Delta f_z K_z}} \tag{2.36.}$$

A gyök alatti mennyiséget a zavaró konfiguráció energetikai potenciáljának nevezzük. Jelöljük β-val. Ha $\beta < 1$, akkor a zavaró állomás energetikai potenciálja kisebb, mint a rádióösszeköttetésé és ekkor a zavarási zóna egy olyan kör alakú zóna belsejében lesz, amelynek a sugara R_z:

$$R_z = D_{zj} \frac{\beta}{1-\beta^2} \tag{2.37.}$$

ahol: D_{zj} – a zavarandó adó és a zavaró adó közötti távolság.

A lefogási zóna középpontja a zavarandó adóval ellentétes oldalon van, a zavaró adótól d_z távolságra:

$$d_z = R_z \beta \tag{2.38.}$$

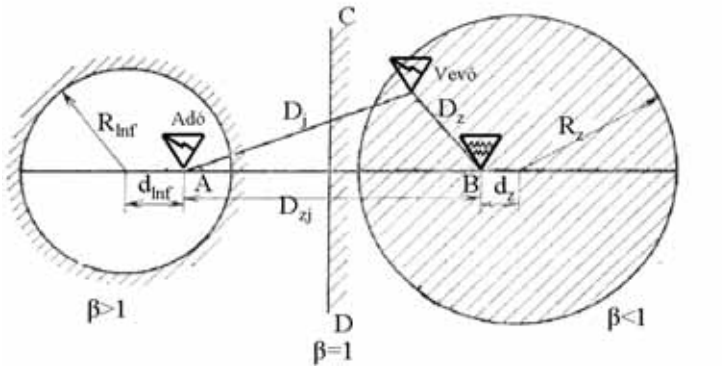
Amikor $\beta > 1$, vagyis a zavaró állomás energetikai potenciálja nagyobb, mint a híradó összeköttetésé, akkor a lefogható zóna az egész környezet lesz, kivéve a lefogandó adó körüli kör alakú területet. A le nem fogható zóna sugara R_{lnf}:

$$R_{\ln f} = D_{zj} \frac{\beta}{\beta^2 - 1} \tag{2.39.}$$

A zóna középpontja szintén eltolódik, méghozzá a zavaró adó irányával ellentétes irányba $d_{\ln f}$ távolságra:

$$d_{\ln f} = \frac{R_{\ln f}}{\beta} \tag{2.40.}$$

Amennyiben a $\beta = 1$, akkor a lefogási zóna határa egy egyenes, amely a lefogandó és a zavaró adó között féltávolságon helyezkedik el. A három esetet a 2.12. ábrán együtt láthatjuk.

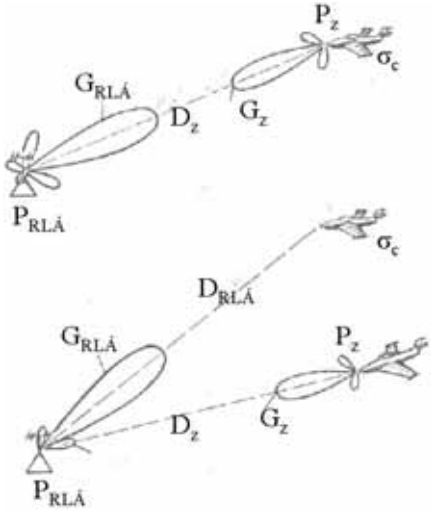


2.12. ábra. **A lefogási zóna alakulása a b energetikai potenciál függvényében**[98]

2.4.6 A rádiólokációs zavarás alapvető matematikai összefüggései

A rádiólokációs eszközök zavarásának két alapesetét különböztetjük meg. Az első esetben a zavaró adó a célrepülőn helyezkedik el, a második esetben a zavarást egy másik repülőgép fedélzeti berendezése állítja elő (2.13. ábra). Ilyen eset a kísérő elektronikai zavaró repülőgépek alkalmazásakor fordul elő. Az alapvető különbség a földi lokátor fő-, vagy melléknyalábon való lefogásában van.

[98] Palij, A. I.: *Radioelektronnaja Borba*. Voennoje Izdatyelsztvo, Moszkva, 1989. p. 54.



2.13. ábra. **A rádiólokációs lefogás alapesetei**[99]

Az első esetben a zavarjel és a céljel aránya a lokátor vevőjének bemenetén:

$$K = (\frac{P_{zav}}{P_{jel}})_b = \frac{P_z G_z 4\Pi D_z^2 \Delta f_v \vartheta_z}{P_{RLÁ} G_{RLÁ} \sigma_c \Delta f_z} \qquad (2.41.)$$

ahol: P_{zav} – a zavaró adó teljesítménye a vevő bemenetén;
P_{jel} – a célról visszavert jel teljesítmény a vevő bemenetén;
P_z – a zavaró adó teljesítménye;
G_z – a zavaró adó antennanyeresége;
D_z – a zavaró adó és a lefogandó lokátor közötti távolság;
Δf_v – a lokátor vevő sávszélessége;
ϑ_z – a céljel és a zavaró jel közötti polarizációs egyeztetési tényező;
$P_{RLÁ}$ – a lokátor teljesítménye;
$G_{RLÁ}$ – a lokátor antennájának nyeresége;
σ_c – a cél hatásos keresztmetszete, amelyet a zavarral el akarunk fedni;
Δf_z – a zavarjel sávszélessége.

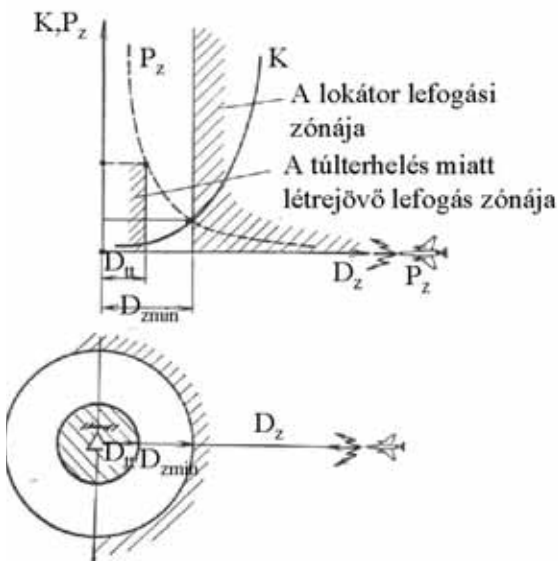
A zavarjel és a célról visszavert jel aránya fogja meghatározni, hogy a zavarás hatékony lesz, vagy sem.

A zavaró repülőgép távolról közeledik a lefogandó rádiólokátor felé (2.14. ábra). A zavarjel és a céljel aránya a közeledés mértékében egyre csökken, mivel a zavarjel azonos kisugárzott teljesítmény mellett csak a távolság négyzetével növekszik a lokátor vevőjében, a visszavert hasznos céljel pedig a távolság negyedik hatványa szerint. Ösz-

[99] U.o. p. 55. (a forrás alapján szerkesztették a szerzők)

szességében a hányadosuk négyzetesen csökken. Azt a távolságot átlépve, ahol a zavarjel és a hasznos céljel aránya egyenlő lesz a lefogási tényezővel, a céljel intenzívebb lesz, mint a zavar, és ezért a lefogás már nem lesz hatékony. A repülőgép további közeledése esetén a vevőberendezés bemenetét olyan intenzitású zavar éri, hogy az túlterhelődik, és a rendeltetésszerű működésre alkalmatlanná válik. Ezt a távolságot a zavarási zóna közeli határának nevezzük.[100]

Ha tehát a zavaró repülőgép a *Dzk* zavarási zóna külső határánál nagyobb távolságra, vagy a *Dzb* zavarási zóna belső határán belül tartózkodik, akkor a lefogás megvalósul.



2.14. ábra. **A zavarási zónahatárok kialakulása fedélzeti zavaró eszköz esetén**[101]

A zavarási zóna külső határa az alábbi összefüggéssel határozható meg:

$$D_{z\,min} = \sqrt{\frac{K_z P_{RLÁ} G_{RLÁ} \sigma_c \Delta f_z}{4\Pi P_Z G_Z \Delta f_v \vartheta_z}} \qquad (2.42.)$$

Kifejezhető a K_z zavarási tényezőhöz tartozó minimális zavarteljesítmény, amelynél nagyobb teljesítményű zavar kisugárzásakor adott távolságon a zavar hatékonynak minősül:

$$P_z = \frac{K_z P_{RLÁ} G_{RLÁ} \sigma_c \Delta f}{4\Pi G_z^2 \Delta f_z \vartheta_z} \qquad (2.43.)$$

[100] Palij, A. I.: *Radioelektronnaja Borba*. Voennoje Izdatyelsztvo, Moszkva, 1989. p. 55.
[101] Palij, A. I.: *Radioelektronnaja Borba*. Voennoje Izdatyelsztvo, Moszkva, 1989. p. 56.

Abban az esetben, ha a zavarral oltalmazandó cél és a zavaró repülőgép nem ugyanaz, akkor a zavarási tényező az alábbi módon írható fel:

$$K = \frac{P_z G_z D_{RLÁ}^4 4\Pi \Delta f_v \vartheta_z}{P_{RLÁ} G_{RLÁ} D_z^2 \sigma_c \Delta f_z} \tag{2.44.}$$

Fontos kérdés lehet, hogy a zavaró repülőgép és a zavarandó lokátor milyen távolságra helyezkedhet el egymástól, figyelembe véve a rádiólokátor és a célrepülő távolságát.

A lefogandó lokátor és a zavaróállomás között megengedhető legnagyobb távolság, ahol még teljesül a minimális lefogási tényező elérése:

$$D_{z\,max} = D_{RLÁ}^2 \sqrt{\frac{P_z G_z 4\Pi \Delta f_v \vartheta_z}{P_{RLÁ} G_{RLÁ} K_z \sigma_c \Delta f_c}} \tag{2.45.}$$

A másik fontos kérdés, hogy mekkora lesz a rádiólokátor minimális hatótávolsága zavarviszonyok között, vagyis mekkora az a távolság, ameddig a célok rejtve maradnak a zavarok mögött:

$$D_{RLÁ\,\min} = \sqrt[4]{\frac{P_{RLÁ} G_{RLÁ} \sigma_c K_z \Delta f_z D_z}{P_z G_z 4\Pi \Delta f_v \vartheta_z}} \tag{2.46.}$$

Természetesen ezek a számítások mindig egy pillanatnyi állapotra, pillanatnyi légi helyzetre vonatkoznak. Ha a célok elmozdulnak, akkor a rádiólokátor már más szög alatt láthatja a célt és a zavaróállomást, ami nem csak azt jelenti, hogy az antennája iránykarakterisztikájának más pontjait kell számításba venni, hanem azt is, hogy a célról lehet, hogy teljesen más szintű visszavert jelet kapunk. A lefogás például akkor lesz a leghatékonyabb, amikor a rádiólokátor főnyalábja a zavaróállomás felé mutat, ugyanekkor a cél pedig egy nullhely irányába esik. Ugyanakkor nem túl nagy elmozdulással létrejöhet olyan helyzet, amikor a zavaróadó esik nullairányba és a céljel a főnyaláb irányába.

A rádiólokáció szüntelen fejlődése és az egyre kifinomultabb zavarvédelmi technikái mind jobban megnehezítik a válaszimpulzus, vagy az egyszerű zajzavarás hatásos létrehozását. Az impulzusról-impulzusra áthangoló lokátorok, az impulzus-kompressziós jelfeldolgozás, az adaptív zavarcsökkentő antennarendszerek, valamint a digitális vezérlésű, fázisrács antennák alkalmazása komoly kihívást jelent a rádiólokátorok elleni elektronikai ellentevékenység számára.

Éppen ezért a lokátorokkal vívott harcban, egyes esetekben a megoldást valószínűleg nem is a zavarokkal való lefogás jelenti majd, hanem az elektronikai csapásmérés, vagy az önrávezető-fejes, lokátor elleni rakéták alkalmazása (AMR, HARM).

3. FEJEZET

Elektronikai felderítés és elektronikai támogatás

Napjainkban, a hadviselésben is – csakúgy, mint az élet más területein – az információ és a tudás válik az egyik legfontosabb, gyakran kulcsfontosságú tényezővé.

Az információszerzés egyik alapvető módja a felderítés, amely egyidős a háborúval és a különböző katonai tevékenységekkel. Az egymással szembenálló felek mindenkor törekedtek arra, hogy a legtöbb és a lehető leghitelesebb információt gyűjtsék be a másik fél erejéről, várható tevékenységéről. Napjainkban e célra a legkülönfélébb módszereket és technikai eszközöket használják fel, melyek jelentősen megnövelik, megsokszorozzák az emberi érzékelés határait. A felderítés céljára alkalmazott technikai eszközök képesek a teljes frekvenciaspektrumban (az elektromágneses tartományban, a fizikai rezgések– és egyéb más tartományokban) adatokat gyűjteni, azokat akár automatikusan is feldolgozó központokba továbbítani, ahol hozzáadott értékkel megnövelt felderítési információkat képezünk ezekből.

Napjainkban fontos szerep jut tehát az információnak, amelynek ma elsősorban nem a megszerzése a nehéz feladat, hanem sokkal inkább a megszerzett, és a jelentős mennyiségben rendelkezésre álló adattömeg feldolgozása jelent óriási nehézségeket. Ez olyannyira komoly probléma, hogy a hagyományos adatfeldolgozás már nem képes lépést tartani az adat mennyiségének robbanásszerű növekedésével, ezáltal maga a megszerzett adat felhasználhatósága, majd a kiértékelt információ felhasználásának a hatékonysága csökken, súlyosabb esetben akár káoszhoz, az adott vezetési rendszer teljes megbénulásához vezethet.

Ugyanakkor pont az elektronikai felderítés – pontosabban fogalmazva az elektronikai eszközökkel végzett adat- és információszerző tevékenység – területén az elmúlt években olyan kihívások jelentek meg, amelyek nagyon nagy mértékben megnehezítik ezt a fajta tevékenységet. Ilyen kihívások például (a teljesség igénye nélkül): az eddig hagyományosnak tekinthető AM, FM, PM adásmódok mellett megjelenő, kis valószínűséggel felderíthető adásmódok *(Low Probability of Interception – LPI),* az automatikus összeköttetés biztosítás *(Automatic Link Establishment – ALE),* a jobb minőségű összeköttetés *(Link Quality Analysis – LQA)*, az ezeket a technológiákat is magába integráló szoftver rádió rendszerek *(Software Defined Radio – SDR)*, az álcázás tökélesedése (festékkel, álcahálóval, speciális forma vagy alak kiképzéssel, STEALTH technológiával).

Mindezekből világosan kitűnik, hogy az elektronikai felderítésnek, illetve az elektronikai hadviselés elektronikai támogatás részének mind technikai eszközökben, mind eljárásbeli megoldások területén alkalmazkodnia kell ezen kihívásokhoz.

Jelen fejezet a felderítéssel kapcsolatos általános fogalmak bemutatása után az elektronikai felderítés módszereinek és eszközeinek bemutatásán keresztül az elektronikai támogatás jellemzését tűzi ki célul.

3.1 A felderítéssel kapcsolatos alapfogalmak, tevékenységek

A magyar terminológia az általános értelemben vett *felderítés* kifejezést használja az információ-szerzési eljárásokkal összefüggésben. Az angol terminológiában gyakran találkozunk az Intelligence, Surveillance és Reconnaissance kifejezésekkel. Az *Intelligence* kifejezés bár gyakran fordítjuk felderítésnek, mégis inkább a hírszerzés fogalmat, a *Surveillance* a megfigyelést vagy felügyeletet, a *Reconnaissance* pedig a klasszikus felderítést takarja. Ezzel összefüggésben a szintek is viszonylag jól elkülöníthetőek. Az eljárásbeli változásokra jellemző, hogy például az USA, ma már a világ számos helyén – jellemzően a potenciális válsághelyeken – folyamatos hírszerzést *(Intelligence)* végez. Ez az alap- és kiinduló adatok megszerzése után felügyeletet *(Surveillance)* jelent, amely a bekövetkezett esetleges változások hatására kényszeríti ki csak a (harcászati) felderítést *(Reconnaissance)*.

A felderítés – és így az elektronikai felderítés is – azonban nem pusztán csak adat- vagy információszerző tevékenységet takar. Az adatok, információk megszerzését és összegyűjtését követően azok feldolgozása, elemzése, értékelése, majd az eredmények felhasználókhoz való eljuttatása következik.

Megvizsgálva a különböző felderítő nemek tevékenységét, megállapítható, hogy a felderítésnek a következő alapvető céljai vannak:

- támogatni a parancsnokot;
- segíteni a célok kijelölését, azonosítását és megjelölését;
- a tervezés és végrehajtás során védelmet nyújtani az ellenséges megtévesztéssel szemben;
- hatékony módon hozzájárulni a műveletek sikeréhez, és a műveletek átszervezéséhez a bekövetkezett változások függvényében.[102]

3.1.1 A felderítés alapelvei

A felderítés megszervezését és végrehajtását nyolc alapelv határozza meg.
A centralizált irányítás: A felderítő tevékenységet a felderítő törzstől kiindulva központilag kell irányítani az indokolatlan duplikáció elkerülése, valamint a kölcsönös támogatás biztosítása, az összes adatforrás hatékony, gazdaságos felhasználása érdekében.

[102] Kovács, L.: *Az elektronikai felderítés korszerű eszközei, rendszerei és azok alkalmazhatósága a Magyar Honvédségben*. Doktori (PhD) értekezés, ZMNE, Budapest, 2003. p. 38.

Az időszerűség: A legpontosabb és legmegbízhatóbb információ is hasznavehetetlenné válhat, ha túlságosan későn érkezik a felhasználóhoz. Ugyanezen ok miatt, a feladatszabás rendszerének késedelem nélkül tükröznie kell a helyzet minden jelentős változását.

A szisztematikus kihasználás: A módszeres feladatszabáson keresztül – képességeik és korlátaik alapos ismerete alapján – szisztematikusan ki kell használni az adatforrások és adatszerző szervek tevékenységét.

Az objektivitás: El kell kerülni minden kísértést a megszerzett információk torzítására, hogy azok jobban illeszkedjenek az előzetes elképzelésekhez.

Elérhetőség: A szükséges információknak minden esetben rendelkezésre kell állniuk a felderítő törzs és a felhasználók számára. A felderítő törzsnek fel kell dolgoznia valamennyi információt és felderítési adatot, beleértve a korábban szerzett információkkal történő összevetésüket is. Nincs értéke annak a felderítési adatnak, melyek nem jutnak el, vagy nem válnak hozzáférhetővé azok számára, akiknek szükségük van rá.

Érzékenység: A felderítő törzsnek minden időben érzékenyen reagálnia kell a parancsnok által megfogalmazott felderítési követelményekre.

A források védelme: Megfelelő védelmet kell biztosítani minden adatforrás számára.

Folyamatos felülvizsgálat (ellenőrzés): Folyamatosan felül kell vizsgálni a felderítési adatokat és szükség szerint pontosítani kell azokat, figyelembe véve minden új információt és összevetni azokat a már ismert adatokkal.

3.1.2 A felderítés formái

A felderítésnek két alapvető formája van:
- alapvető felderítés;
- aktuális felderítés.

Az alapvető felderítés minden területre kiterjedő felderítés, mely hivatkozási alapként szolgál a tervezéshez, illetve az elkövetkező információk és felderítési adatok értékeléséhez.[103]

Az alapvető felderítés minden aktuális felderítési feladat háttéranyagát szolgáltatja, mely felhasználható a hadművelet (harc) megtervezése során, az újonnan szerzett információk és felderítési adatok értékelésének összehasonlító alapadataként.

Az aktuális felderítés az aktuális helyzetet tükröző, hadászati, vagy harcászati felderítő tevékenység.

Az aktuális felderítés a konkrét helyzettel, vagy eseményekkel kapcsolatban az adott időben megszerzett felderítési adat.

[103] AAP-6 NATO Glossary of Terms and Definition, NATO Standardization Agency, Brussels, 2006. p. 46.

3.1.3 Felderítési fogalmak, kategóriák

3.1.3.1 Adat

Az adat, mint fogalom meghatározásához nagyon sok definíciót találunk, amelyek a felhasználás szempontjából próbálják meg körülírni a fogalmat. A katonai téren használt meghatározások is sokfélék, ám ennek ellenére vizsgáljuk meg katonai-műszaki oldalról az adatot, mint fogalmat.

Néhány megfogalmazás katonai-műszaki szemszögből:

– az információ alapösszetevője, digitális (számszerű) vagy karakter (betű, írásjel) jellegű hordozója;
– valamely vizsgálat, kísérlet, mintavétel eredményeként megállapított olyan tény, ismeret, amelynek további feldolgozásával tanulmányozható a vizsgált jelenség; végső soron elősegítheti a döntés meghozatalát;
– az elhatározás alapjául szolgáló számszerű, vagy számszerűsített mutató, jellemző tényező. Lehet állandó vagy változó. Az elsődleges adatokat nyers adatoknak vagy kiírandó adatoknak is nevezik. Ezeket az adatfeldolgozás (információfeldolgozás) folyamán összesítik, tömörítik, vagyis magasabb értékű információkat állítanak elő belőlük. Az adat jelentését gyakran a számítógépes adatokra redukálják.

3.1.3.2 Információ

Hasonlatosan az adathoz, az *információ,* mint fogalom meghatározására is számtalan definíciót találunk, annak függvényében hol és mire használják a fogalmat. Ennek megfelelően a filozófia az anyagi világ leképeződését az agyban tartja információnak, míg az informatika adatok halmazaként jeleníti meg ugyanezt. Az információt az különbözteti meg az adattól, hogy ennek jelentése van, míg az adat egyedül csak puszta tény. A sok meghatározás ellenére egy sem nevezhető ki hivatalos definíciónak.

A NATO-ban elfogadott terminológia szerint az információ:

Információnak nevezzük a bármilyen formában megjelenő feldolgozatlan adatokat, melyek felhasználhatók a felderítési adatok létrehozására.[104]

Az AJP-2 meghatározása szerint az információ: az önálló adatból, illetve önálló adatok sorozatából, vagy csoportjából áll, melyet egy bizonyos szenzor érzékelt, és erről a szenzorról valamilyen módon begyűjtésre került. Az információ a tér és az idő egy meghatározott pontján létező, illetve létezett dolgok pillanatnyi helyzetére vonatkozó

[104] AAP-6 NATO Glossary of Terms and Definition, NATO Standardization Agency, Brussels, 2006. p. 132.

állítás, mely természetéből adódóan egyértelmű, vonatkozhat a múlt (történeti információ), illetve a jelen (aktuális információ) eseményeire.[105]

3.1.3.3 Tudás

Az adat, információ, tudás összefüggő hármas fogalomrendszert alkotnak.
Azonban hasonlatosan az adathoz és az információhoz, a tudásnak sincs egységesen elfogadott, egyszerű, jól körülhatárolt és letisztázott definíciója. A következő meghatározás is csak azokat a jellegzetességeket emeli ki, amelyek alapján a tudásról beszélünk. Tehát a tudás:

„Körülhatárolt tapasztalatok, értékek és kontextuális információk heterogén és folyton változó keveréke; szakértelem, amely keretet ad új tapasztalatok, információk elbírálásához és elsajátításához, s a tudással rendelkezők elméjében keletkezik és hasznosul."[106]

3.1.3.4 Felderítési adat

Felderítési adatnak nevezzük azt a végterméket, melyet az információk feldolgozása során nyerünk, általában a már meglévő, vagy új felderítési adatokkal összefüggésben. Az AAP-6 megfogalmazása szerint a felderítési adat nem más, mint:

„Az a termék, mely más nemzetek, ellenséges, illetve potenciálisan ellenséges erők, vagy folyamatban lévő, illetve potenciális műveletek részeiről, területeiről rendelkezésre álló információ feldolgozásának eredménye."[107]

Az információ abban az esetben bír jelentős értékkel, amikor valamilyen következtetést lehet levonni belőle. Ez abban az esetben fordulhat elő, ha az adott információ, egy már korábban beszerzettel hozható összefüggésbe, illetve ha a felhasználó, a már meglévő tapasztalatai alapján mérlegeli azt. A szenzor által gyűjtött adat önmagában nem sok mindenre használható. Amikor azonban begyűjtik a szenzorról, és szükség szerint átalakítják, információvá válik. Az információ önmagában csak egy tény, illetve tények sorozata. Amikor azonban összevetésre kerül másik, már ismert információval, illetve a korábbi tapasztalatok fényében kerül vizsgálatra, akkor olyan új tények előállítását eredményezheti, amit már felderítési adatnak nevezünk. A felderítési adat abban különbözik az információtól, hogy mivel szubjektív ítéletalkotási folyamat eredménye, ezért nem magától értetődő, tehát vitatható. Az információ felderítési adattá alakításának eredője az a folyamat (elemzés), melynek során az elemző az információ-csoportokat összeveti, illetve az információt a meglévő adatbázisok ismeretében megítéli, és következtetéseket von le.

[105] AJP-2.0 Szövetséges Összhaderőnemi Felderítő, Felderítés elleni védelem, és Biztonsági Doktrína, NATO HQ, Brüsszel, 2002, p. 24.
[106] Davenport, T.H. – Pusak, L.: *Tudásmenedzsment*, Kossuth, Budapest, 2000. p. 18.
[107] AAP-6 NATO Glossary of Terms and Definition, NATO Standardization Agency, Brussels, 2006. p. 132.

A folyamat a következő részekből áll: adatok gyűjtése, érték meghatározás, elemzés, integráció, interpretáció.

Az adatok gyűjtése: Az adatok gyűjtése a rögzítés rutinfeladata, valamennyi beérkezett információ rögzítését és csoportosítását jelenti.

Érték meghatározás: Az érték meghatározása az adatforrások megbízhatóságának és az általuk szolgáltatott információk hitelességének megállapítását jelenti.

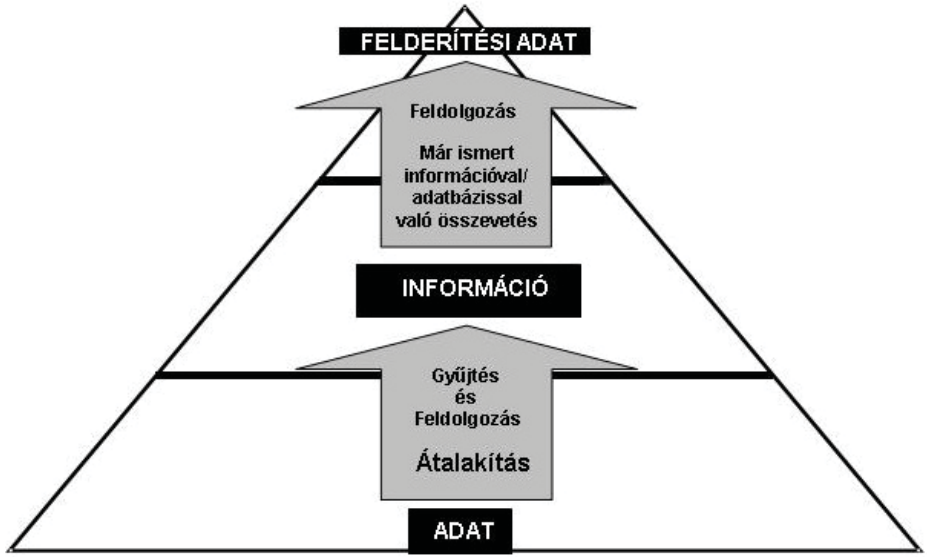
Elemzés: Az elemzés magában foglalja az információk, vagy felderítési adatok fontos tényeinek megállapítását, azok összehasonlítását a már meglévő ismeretekkel és a következtetések levonását.

Integráció: Az integráció az elemzett információk és felderítési adatok összevonását jelenti az ismeretanyag fontos jellegzetességeinek feltárása érdekében.

Interpretáció: Az interpretáció az elemzett információk és felderítési adatok jelentőségének megítélését jelenti, a meglévő ismeretek összessége tekintetében.

A fogalom alkalmazható sokkal általánosabb értelmében is, vagyis a nyers adatok értelmezhetőbb formába történő lefordítására (például, a fényképek elemzése).

Az adat, információ, felderítési adat kapcsolatát mutatja be a 3.1. ábra.



3.1. ábra. **Adat, információ és felderítési adat kapcsolat**[108]

Az egyes szinteken belül valamennyi felderítési adat besorolható az alábbi három típus valamelyikébe:

[108] AJP-2.0 Szövetséges Összhaderőnemi Felderítő, Felderítés elleni védelem, és Biztonsági Doktrína, NATO HQ, Brüsszel, 2002, p. 11. (a forrás alapján szerkesztették a szerzők)

Felderítési alapadatok: Egy adott témában rendelkezésre álló, békében és a műveletek folyamán folyamatosan frissített, adatbázisokban nyilvántartott háttéranyagok összessége. Elsődlegesen ez az adatcsoport használható fel a műveletek kezdetekor az alaphelyzet felvázolására, illetve a változatlan tény- és statisztikai adatok, úgymint a műveleti terület terep- és időjárási adatai, támpontot nyújthatnak az adott művelet végrehajtása során felmerülő új felderítési igények kielégítéshez. A felderítési alapadatok fogalma a következő: *„Olyan, bármely tárgyban rendelkezésre álló felderítési adat, mely a tervezés során referencia anyagként, illetve a beérkezett további információ, illetve felderítési adat feldolgozásának alapjául szolgálhat."*[109]

Aktuális felderítési adat: Az éppen folyamatban lévő műveletekkel kapcsolatos felderítési igények kielégítésére előállított, az adott művelet végrehajtásának idejében bekövetkező eseményekre vonatkozó felderítési adat. Meghatározása: *„Az aktuális helyzetet, akár stratégiai akár harcászati szinten megjelenítő felderítési adat."*[110]

Célfelderítési adat: „Az a felderítési adat, mely egyes célok, illetve célcsoportok elemeit, és azok helyét, sebezhetőségét, valamint relatív fontosságát megadja."[111] A célfelderítés biztosítja a célkijelölés folyamatához szükséges céladatokat. Ez a folyamat biztosítja a tűztámogató rendszerek leghatékonyabb felhasználását.

Harci információ: A harci információ olyan feldolgozatlan adat, melyet közvetlenül a harcoló csapatok parancsnokai gyűjtenek, akiknek gyorsan változó helyzetük, vagy a harctevékenység miatt nincs lehetőségük, hogy a felhasználó felderítési igényeinek megfelelő felderítési adatokat biztosítsanak.

Felderítés objektumai: Az ellenség vagy szembenálló fél mindazon erői, szervezetei, eszközei, műszaki berendezései, valamint azok a tereptárgyak és hadszíntéri objektumok, amelyek a saját csapatok számára veszélyt, akadályt jelentenek a feladatok végrehajtása során, vagy katonai jelentőségük van, és ezért a saját csapatok tevékenységük folyamán birtokba vehetik őket.

Korreláció: Felderítési értelmezésben, az a folyamat, melyben egy adott kérdésre, vagy tárgyra egymástól független megfigyelésekből származó adatokat kapcsolatba hoznak és kombinálnak azzal a céllal, hogy növeljék az információ megbízhatóságát és hitelességét.[112]

Fúzió: Felderítési értelemben, a különböző forrásokból és adatszerző szervektől érkezett információk és/vagy felderítési adatok összefüggő képpé történő egyesítése. A folyamatot követően az egyes részinformációk eredete nem állapítható meg.[113]

[109] AAP-6 NATO Glossary of Terms and Definition, NATO Standardization Agency, Brussels, 2006. p. 85.
[110] U.o. p. 67.
[111] U.o. p. 198.
[112] U.o. p. 201.
U.o. p. 343.
[113] U.o. p. 122.

3.1.4 A felderítés szintjei

A keletkezett adat felhasználását tekintve a felderítés három szintje különböztethető meg:

Stratégiai felderítés: „A nemzeti és nemzetközi szintű politikai irányelvek, illetve katonai tervek készítéséhez szükséges felderítés."[114] Ez a legmagasabb szintű felderítési adat a nemzetek kormányai által támasztott, a nemzeti és nemzetközi katonai, diplomáciai, politikai és gazdasági ügyek teljes spektrumát átfogó követelmények kielégítése érdekében, a lehető legszélesebb körből beszerzett információból kerül előállításra.

Hadműveleti felderítés: „A hadműveleti szintű tevékenység tervezéséhez, végrehajtásához szükséges felderítés."[115] Még konkrétabb megfogalmazásban; egy adott hadműveleti területen, az összhaderőnemi parancsnokság által vezetett hadműveletek tervezéséhez, végrehajtásához, valamint támogatásához szükséges felderítési adatok/felderítő tevékenység. Azon felderítési adatok összessége, melyet a hadszíntér földrajzi területén állítottak elő.

Harcászati felderítés: „A harcászati tevékenység tervezéséhez és végrehajtásához szükséges felderítési adat/tevékenység."[116] Az adott kötelék felelősségi körzetén belül előállított, a kötelék parancsnoksága és alárendeltjei által felhasznált felderítési adat.

3.1.5 A felderítés adatforrásai

A felderítési adat előállításához szükséges információt „adatforrások" és „adatszolgáltatók" gyűjtik be. A Felderítési ciklus részét képező Irányítás és Adatgyűjtés funkciójának megértése érdekében szükséges e két fogalom értelmezése:

Adatforrás: „A felderítés fogalomkörében, olyan személy, vagy tárgy, akitől, illetve amiről információ szerezhető be."[117] Az adatforrás begyűjtheti az információt véletlenszerűen, mint például egy a kávéházban véletlenül meghallott beszélgetés során, vagy kifejezett igényt is kielégíthet, mint például amikor a kamera a pilóta nélküli felderítő repülőgép *(Unmanned Aerial Vehicle – UAV)* programozott útja során rögzíti a képeket. Az információ elsődlegesen az adatforrástól ered. Az adatforrás önmaga is birtokában lehet az információnak, illetve tevékenysége demonstrálhatja az információ létét. Az adatgyűjtő az a személy, illetve rendszer mely az adatforrástól megszerzi az információt. Az adatforrás nem képes az információ feldolgozására, egyedül annak formai változására lehet hatással. Ilyen formai változás lehet a kapcsolattartó személy által végzett fordítás egyik nyelvről a másikra, vagy például a kép műhold általi digitális jellé alakítása.

[114] AAP-6 NATO Glossary of Terms and Definition, NATO Standardization Agency, Brussels, 2006. p. 234.
[115] U.o. p. 111.
[116] U.o. p. 76.
[117] U.o. p. 98.

Adatszolgáltató: „A felderítés fogalomkörében az a szervezet, vagy személy, aki (ami) az információ gyűjtésében és/vagy feldolgozásában vesz részt."[118] Az adatszolgáltató képes lehet az információ gyűjtésére és feldolgozására is. Egyszerűbb esetben azonban csak gyűjteni képes az információt és feldolgozásra át kell, hogy adja egy másik adatszolgáltatónak. Az adatszolgáltatók skálájának egyik végpontja például a keresztútnál ellenséges tevékenységet jelentő csapatfelderítő részleg. A másik végpont az a nagy kormányhivatal, mely információit a források széles skálájától szerzi be, és hatalmas feldolgozói kapacitást igénybe véve nemzeti stratégiai felderítési adatot állít elő.

Mielőtt rátérnénk a felderítés folyamatának ismertetésére és elemzésére, meg kell határozni azokat a felderítési *adatforrásokat*[119] vagy *adatszolgáltatókat*,[120] amelyek a felderítési adat előállításához szükséges információkat megszerzik. Meg kell jegyezni, hogy a Magyar Honvédség Összhaderőnemi Doktrína korábbi kiadása *információszerzők* kifejezésben definiálta mindezeket a következőképpen:

„Információszerzőnek tekinthető az a természetes személy, vagy szervezet, amelyik információt tud szolgáltatni. Az információszerzés lehet véletlen, vagy erre a célra ideiglenesen, illetve állandó jelleggel létrehozott és ilyen feladattal megbízott személy, szervezet által végzett tervszerű tevékenység."[121] Ez a meghatározás nagyon hasonló az adatforrás meghatározásához, ezért a továbbiakban az adatforrás fogalmat használom.

Az adatforrások több csoportra bonthatók. Függően az adatforrás fizikai, illetve technikai jellemzőitől többféle adatforrás típus csoportot különböztethetünk meg.

A Magyar Honvédség Összhaderőnemi Doktrína az adatforrásokat az általuk használt eljárások (módok) alapján osztályozza. Ennek alapján a megkülönböztethetünk:

- emberi erővel folytatott felderítést *(Human Intelligence – HUMINT);*
- képfelderítést *(Imagery Intelligence – IMINT)*;
- rádióelektronikai felderítést *(Signal Intelligence – SIGINT)*;
- hangfelderítést *(Acoustic Intelligence – ACINT)*;
- kisugárzás és jelfelderítést *(Measurements Intelligence – MASINT)*;
- radarfelderítés *(Radar Intelligence – RADINT)*;
- technikai felderítést *(Technical Intelligence – TECHINT)*;
- nyílt források felhasználásával folytatott felderítést *(Open Source Intelligence – OSINT)*;
- az ellenség felderítését elhárító tevékenység és a saját csapatok védelmét *(Counterintelligence and Force Protection – CI/FP)*.

[118] AAP-6 NATO Glossary of Terms and Definition, NATO Standardization Agency, Brussels, 2006. p. 154.

[119] Az adatforrás az a személy vagy tárgy, akitől vagy amitől információ szerezhető be. Az adatforrás nem végez adatfeldolgozást, de annak formai átalakítása – például a pilóta nélküli repülőgép fedélzetén elhelyezett kamera digitalizálja a látott képet – lehetséges.

[120] Az adatszolgáltató nemcsak az adatokat gyűjti, hanem azokat adott esetben fel is dolgozza.

[121] Magyar Honvédség Összhaderőnemi Doktrína, 2002. MH kiadvány, p. 23.

Tartalmukat tekintve ezek az adatszerző eljárások a következők:

HUMINT: bármely, emberi adatforrástól, illetve bármilyen adatszolgáltatótól származó felderítési adat.

IMINT: a fotografikus, radar, elektrooptikai, infravörös, hő, illetve multispektrális érzékelők által vett jelekből képzett képanyagból állít elő adatot.

SIGINT: kommunikációs felderítésre *(Communication Intelligence – COMINT)*, vagy más néven rádiófelderítésre, amely a szembenálló fél kommunikációs rendszereinek lehallgatásával szerez információt; illetve elektronikai felderítésre *(Electronic Intelligence – ELINT)*, vagy más néven rádiótechnikai felderítésre osztható, amely a kisugárzott elektromágneses jelek elemzéséből szolgáltat adatot.

ACINT: az akusztikai rezgések tartományból származó adatokat állít elő.

MASINT: a különböző tartományokban műszeres mérésekkel állít elő adatot.

RADINT: rádiólokációs technikával végzett felderítésből állít elő adatokat.

TECHINT: az eszközök technikai paramétereit felderítve állít elő adatot.

OSINT: a széles körben hozzáférhető nyílt adatforrások, például rádió-, televízióadás, újság, könyv felhasználásával állít elő adatot.

A felderítési adatforrásokat elemezve látható, hogy természetesen nem mindegyik épül elsősorban az elektronikai eszközökkel végzett adatszerzésre, de mindegyikben megtalálhatók vagy adatszerzési, vagy adattovábbítási és feldolgozási szinteken az elektronikus eszközök.

Mindezek alapján tehát szükséges megfogalmazni, hogy mit értünk *elektronikai felderítés* alatt. Az eddigiekből következően, az elektronikai felderítés fogalma alatt az elektronikai eszközökkel, különböző hullámtartományokban végzett adatszerzést és ezen adatok feldolgozását értjük, amely megjelenhet több adatforrás típus esetében is.

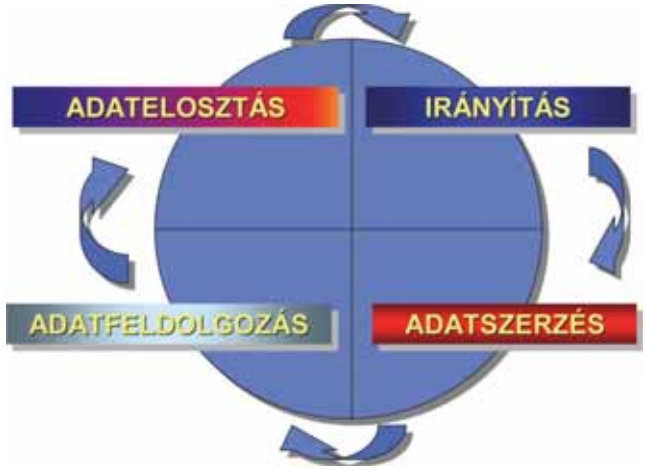
3.1.6 A felderítési ciklus

A felderítés ciklusa olyan fogalom, melyet a parancsnok hadműveleti feladatai tervező és végrehajtó tevékenységének támogatásához szükséges felderítés gondolkodási és tevékenységi rendjének leírására alkalmazunk. A folyamat ciklikus jellegű, mivel az időszerűség és a parancsnok igényei folyamatos teljesítésének érdekében a felderítő tevékenységet folyamatosan újra értékelni és pontosítani kell.

A ciklus négy alapvető fázisra osztható:

- irányítás;
- adatszerzés;
- adatfeldolgozás;[122]
- elosztás (az adatok jelentése).

[122] Az amerikai rendszerben az adatfeldolgozást két lépésre osztják: feldolgozásra és jelentésre. Ennek megfelelően az USA felderítési ciklus öt elemből áll.



3.2. ábra. **A felderítési ciklus**[123]

3.1.6.1 A felderítés irányítása

Az adatgyűjtés irányítását az adatgyűjtést irányító és elosztó részleg végzi az összesített értékelő részleg támogatásával. Ez egy kellő időben, megfelelő hatékonysággal történő meghatározása a felderítési követelményeknek, és feladatszabás az adatszerző ügynökségeknek a kívánt információ megszerzésére. Az adatgyűjtés komplex irányításának a legfontosabb célja, hogy a korlátozott mennyiségben rendelkezésre álló felderítési erőforrások biztosítsák a parancsnok által elsődlegesen meghatározott felderítési igényeket.

Az adatgyűjtés megtervezésének speciális lépései és követelményei, melyek biztosítják az optimális eredményt a következők:

- ha egy felderítési kérelem beérkezik először is meg kell vizsgáltatni az összesített értékelő részleggel, hogy van-e az adattárában olyan adat, mely megfelel a kérelemnek;
- folyamatosan aktualizáljuk az összesített értékelő részleg által biztosított esemény vázlatot és a terepben, időjárásban és az ellenség helyzetében bekövetkezett változásokat;
- az adatgyűjtési terv elkészítése mely logikus és rendezett formában biztosítja az információk gyűjtését és jelentését;
- minden helyzetben vegye figyelembe az adatgyűjtéshez rendelkezésre álló erőket, azok lehetőségeit és korlátait;
- maximalizálja a többcsatornás tevékenységeket, nagy hangsúlyt fektessen a különböző figyelmeztetésekre, az adatgyűjtés kiterjesztésére és a bizonyításra;
- a tevékenység folyamatosságának biztosítása;

[123] Szerkesztették a szerzők.

– biztosítani, hogy az adatszerző csapatokat és ügynökségeket speciális feladatra és követelmények alapján alkalmazzák;
– az elöljáró törzsektől kérni kell az információt, illetve annak megerősítését;
– biztosítani kell, hogy az adatgyűjtésre vonatkozó követelmények feleljenek meg a prioritási sorrendnek és időszerűek legyenek;
– biztosítani kell a kérés teljesítéséhez a szükséges időmennyiséget.

Mindezekkel az adatgyűjtés tervezését befolyásoló tényezőkkel minden vezetési szinten számolni kell.

Ezen követelmények megvalósulása és az adatgyűjtést irányító és elosztó részleg feladataiból adódik az *adatgyűjtési (felderítő) terv***.**

Az *adatgyűjtési terv* egy olyan dinamikus eszköz, melyet arra használnak, hogy koordinálják és egyesítsék az összes adatszerző alakulat és ügynökség erőfeszítését. Miután az adatgyűjtés folyamatos tervezést igényel teljesen új adatgyűjtési terv ritkán készül, kivéve, ha egy alakulat először lép harcba, vagy egy új hadműveleti szakaszba. Az adatgyűjtési tervet folyamatosan felül kell vizsgálni, ha szükséges. Kivitelezésében ez egy tábla, ahol az új belépőket felírják, és az idejétmúltakat letörlik.

Mivel az információs követelmények sokkal összetettebbek a magasabb vezetési szinteken, így az adatgyűjtési terv sokkal bővebb és formálisabb. Ugyanakkor, az adatgyűjtés tervezése minden szinten alapvetően egy szellemi tevékenység, tekintet nélkül az alkalmazott formátumra, mely csak egy javasolt változat. Nem pótolhatja a gondolkodást, viszont azért készítik, mert segíti az adatgyűjtés megtervezését és felügyeletét, és biztosítja a folyamatos adatcserét a harctevékenységet irányító központtal.

Az adatgyűjtési terv elkészítésének nincs egy meghatározott formátuma. El lehet készíteni egy egyszerű papírlapra, lehet hosszú és részletes terv, vagy lehet egy gondolatsor. Bár az adatgyűjtést irányító kialakíthatja az adatgyűjtésre vonatkozó elméletét fejben is, de az írásos terv megkönnyíti az adatgyűjtést, és jobban kizárja a szubjektív tévedések lehetőségét. Az írásos terv, ha nem is formális, lehetővé teszi az események követését, tehát ajánlott. Az adatgyűjtési terv típusa és elkészítési módja függ a szervezet nagyságától, a feladattól és a kidolgozók döntésétől.

3.1.6.2 Adatszerzés[124]

A felderítési ciklus második lépése az adatgyűjtés, amely az „*adatforrások adatgyűjtő szervek általi kiaknázása, valamint a megszerzett információ eljuttatása a felderítési adat előállítása szempontjából megfelelő feldolgozó egységhez.*”[125] Az adatszerzés az a folyamat, mely során a parancsnok – a felderítési ciklus irányítási szakaszában meghatározott –

[124] AJP-2.0 Szövetséges Összhaderőnemi Felderítő, Felderítés elleni védelem, és Biztonsági Doktrína, NATO HQ, Brüsszel, 2002, p. 22.
[125] AAP-6 NATO Glossary of Terms and Definition, NATO Standardization Agency, Brussels, 2006. p. 235.

információs és felderítési adatigényének kielégítése érdekében a szükséges információ és felderítési adat begyűjtésre kerül.

Az adatgyűjtés folyamata két részre osztható:

– az adatforrások kiaknázása adatgyűjtő szervek által, valamint az adatforrások és adatszolgáltatók felderítő törzsek általi felhasználása;
– az adatforrások és adatszolgáltatók által begyűjtött információ időbeli eljuttatása a felderítési ciklus következő fázisába, ahol az információból előállításra kerül a felderítési adat.

3.1.6.3 Feldolgozás[126]

Az *adatfeldolgozás* alapvetően a megszerzett információk felderítési és céladattá való alakítását jelenti. Az előzőekben megállapítottam, hogy a digitális technika alkalmazása, illetve a megváltozott körülmények – gyorsan lezajló tevékenységek, nagy területen való elszórt kis csoportok akciói, dinamikusan változó helyzetek – miatt a különböző adatforrások információinak nemcsak megszerzése, de felderítési adattá való átalakítása is jelentős kihívás elé állítja az adatfeldolgozást. Mindezek megoldási módjaival a későbbiekben e fejezeten belül részletesebben kívánunk foglalkozni, ezért itt csak a folyamat vázlatos ismertetését tesszük meg. Így tehát az adatfeldolgozás során a következő feladatok kerülnek végrehajtásra:

– *előkészítő szakasz:*
  - felderítő adatbázis elkészítése, folyamatos karbantartása;
  - a felderítési napló vezetése;
  - a harcrendre vonatkozó adatok összegyűjtése, értékelése;
  - a harcterület felderítő előkészítése során készült jelentések feldolgozása;
  - elektronikai helyzetvázlat elkészítése;
– *feldolgozó szakasz:*
  - adatok és információk vétele;
  - értékelés pontosság és megbízhatóság szerint;
  - felderítő adatbázisok és tárak aktualizálása;
  - az ellenség várható cselekvési formáinak megállapítása;
  - céladatok kialakítása;
  - adatgyűjtési terv ellenőrzése;
  - felderítő jelentések elkészítése.

A feldolgozás az információ és felderítési adat előállítása során több ponton is folyik. A skála egyik végpontján az a feldolgozási folyamat áll, ami az adatgyűjtő szerven belül megy végbe, ennek során többnyire nem történik más, mint a nyers adatot érthető formátumúvá alakítják. A felderítési adat előállítási folyamatának másik véglete, mi-

[126] Kovács, L.: *Az elektronikai felderítés korszerű eszközei, rendszerei és azok alkalmazhatósága a Magyar Honvédségben*. Doktori (PhD) értekezés, ZMNE, Budapest, 2003. p. 43.

kor a parancsnoki vonalon továbbított felderítési adatot a stratégiai (hadászati) szinten elemzik. A feldolgozási folyamat minden egyes szintjén olyan új tényekkel vetik egybe az információt/felderítési adatot, mely az előző szinten nem állt rendelkezésre, ezáltal téve lehetővé új felderítési adat kikövetkeztetését.[127]

A feldolgozás során az adatokat csoportosítják. A csoportosítás: *„A felderítési cikluson belül a feldolgozási folyamat egyik eleme, mely során az egymással összefüggő információ elemek, vagy felderítési adatok összekapcsolása az események leírását adja, ezzel segítve elő a további feldolgozást."*[128] A gyakorlatban ez a folyamat a felderítés valamennyi szintjén a beérkező jelentések vételéből, csoportosításából és nyilvántartásba vételéből álló tevékenység.

Ezt az adatfeldolgozási fázist követi az értékelés, amely *„a felderítési cikluson belül a feldolgozási folyamat azon eleme, mely során felbecslésre kerül az információt szolgáltató forrás megbízhatósága, valamint az információ hitelessége."*[129]. Az értékelés annak meghatározása, mennyire megbízható az információ forrása, valamint mennyi a valószínűsége annak, hogy az általa szolgáltatott információ igaz. A beérkező információ nem kezelhető névértékén. Egy információ megbízhatatlanságának, illetve pontatlanságának több oka is lehet, beleértve a megtévesztést is. A feldolgozási folyamat Értékelő része során minden egyes információ, illetve felderítési adat egy olyan alfanumerikus minősítést kap, mely megmutatja annak megbízhatóságát.

3.1. táblázat. **A forrás megbízhatóságára, valamint az információ hitelességére vonatkozó elfogadott szabványos minősítési fokozatok[130]**

Forrás megbízhatósága		Információ hitelessége	
A	Teljesen megbízható	1	Más forrás is megerősítette
B	Rendszerint megbízható	2	Valószínűleg igaz
C	Inkább megbízható	3	Feltételezhetően igaz
D	Rendszerint nem megbízható	4	Kétséges
E	Megbízhatatlan	5	Valószínűtlen
F	Meghízhatósága nem értékelhető	6	Hitelessége nem megbecsülhető

Az adatfeldolgozás következő állomása az elemzés és összegzés. Az elemzés és az összegzés külön került meghatározásra: *„A felderítési cikluson belül a feldolgozási folyamat azon eleme, mely során további kiértékelést igénylő lényeges tények azonosítása érdekében az információ felülvizsgálatra kerül."*[131] *„A felderítési cikluson belül a feldolgozási folyamat*

[127] AJP-2.0 Szövetséges Összhaderőnemi Felderítő, Felderítés elleni védelem, és Biztonsági Doktrína, NATO HQ, Brüsszel, 2002, p. 45.
[128] AAP-6 NATO Glossary of Terms and Definition, NATO Standardization Agency, Brussels, 2006. p. 344.
[129] U.o. p. 178.
[130] U.o. p. 111.
[131] AAP-6 NATO Glossary of Terms and Definition, NATO Standardization Agency, Brussels, 2006. p. 234.

azon eleme, mely során a kiválasztott, már elemzett információt/felderítési adatot a további felderítési adatok előállítása érdekében rendszerré alakítják."[132] A gyakorlatban az elemzést követően, szünet beiktatása nélkül folytatódik az adatok összegzése. A két tevékenységet minden szempontból egyként kezelik.[133]

A következő lépés az összefoglalás. Az információ/felderítési adat szisztematikus feldolgozása a Csoportosítás, Értékelés, Elemzés, Összegzés és Értelmezés végrehajtása során valósul meg. Ez az információvétel és nyilvántartás szabályozott végrehajtásának, valamint a felderítési adatot létrehozó, logikus, metodikus formába öntött mentális folyamatnak a kombinációja. Ez a mentális folyamat az elemző részéről az ellenség harceljárásainak, felszerelésének és szervezetének széles körű ismeretét, valamint sokrétű harcászati tapasztalatot követel meg, amely a logikus következtetések megalkotására való készséggel kell, hogy párosuljon.[134]

Az adatfeldolgozás utolsó fázisa a következtetés. Az ember azon tulajdonsága, hogy képes megalapozott döntések és értékelések megalkotására, valamint a „megérzésre" való intuitív képesség döntő fontosságú a feldolgozási folyamat lényegét jelentő elemző tevékenység sikeres végrehajtása érdekében. Ezeket a képességek, melyek kiterjedt, professzionális ismereteken, valamint hosszú időn át végzett elemzői gyakorlaton és tapasztalatokon alapulnak, inkább megszerezhetők, mintsem tanulhatók. Ez az egyik kulcsfontosságú eleme a felderítési adat előrejelző voltának.[135]

3.1.6.4 Adatelosztás

A felderítési ciklus utolsó eleme az adatelosztás. A fő követelmény az elosztással szemben – csakúgy, mint a felderítés egészével kapcsolatban – a megfelelő időben, a megfelelő helyre, a megfelelő mennyiségű és minőségű információt, felderítési-, vagy cél adatot kell eljuttatni.

Mindezek alapján az adatelosztás legfontosabb tényezői a következőek:

– *Időszerűség*: bármely felderítési adat, amely a rendeltetési helyét a szükségesnél később éri el, értéktelenné válik. Az időszerűség másik fontos összetevője az, hogy a felderítési adatok többsége, elsősorban harcászati, hadműveleti szinten, időérzékeny. Ez azt jelenti, hogy a felderítési adat értéke az idő múlásával egyre csökken, illetve teljesen el is veszik. Mindkét összetevő azt a követelményt erősíti, hogy a felderítési adatot a lehető leggyorsabban kell eljuttatni a felhasználóhoz. Amikor a határidők teljesítése érdekében szükségessé válik a feldolgozás lerövidítése, az így előállított felderítési adatot figyelmeztető jelzéssel kell ellátni, annak érdekében, hogy a felhasználó azt a szükséges mértékű körültekintéssel alkalmazza.

[132] U.o. p. 154.
[133] AJP-2.0 Szövetséges Összhaderőnemi Felderítő, Felderítés elleni védelem, és Biztonsági Doktrína, NATO HQ, Brüsszel, 2002, p. 23.
[134] U.o. p. 24.
[135] U.o. p. 25.

– *Megfelelőség*: az olyan felderítési adat terjesztésének, mely nem ad választ a felhasználó által megfogalmazott kérdésekre, nem érthető, vagy a terjesztés olyan rendszeren keresztül történik, amelyhez a felhasználó nem fér hozzá nem megfelelő. A felderítési adatot a felhasználónak megfelelő formátumban kell továbbítani. A felderítési adat meg kell, hogy feleljen a felhasználó által támasztott követelményeknek, a megfelelő nyelven kell azt továbbítani, valamint a továbbításra olyan rendszert kell alkalmazni, mely mind a küldő, mind a fogadó fél számára elfogadható. Amennyiben a felderítési adat nem felel meg a fenti követelmények valamelyikének, a későn érkező adathoz hasonlóan, értéktelenné válik.[136]

Mindezen követelmények magukban hordozzák annak a szükségességét, hogy legyen egy olyan egységes felderítő és adatelosztó rendszer, amely lehetővé teszi a fent említett követelmények kielégítését. Ilyen egységes felderítő rendszer elképzelés például a NATO Egységes Felderítő Információgyűjtő Rendszer *(ISTAR – Intelligence, Surveillance, Target Acquisition and Reconnaissance*), amely központi koordinációval integrálja a felderítő, megfigyelő és célfelderítő eszközöket a felderítés folyamatába.

C4ISR *(Command, Control, Communication, Computer, and Intelligence, Surveillance, Reconnaissance)* rendszereknek, azaz a felderítés által támogatott számítógépes vezetési és információs rendszereknek nevezzük,[137] azokat a rendszereket, ahol a vezetés közvetlenül – egy rendszerbe integráltan – irányítja és használja fel a tervezés és végrehajtás során azokat a felderítési adatokat, amelyeket az egységes számítógépes hálózaton keresztül a felderítés ad. A C4ISR rendszerek feladatait a következő definíciószerű meghatározás fejezi ki nagyon tömören és lényegre törően: *„Automatikus és folyamatos információ feldolgozással és továbbítással támogatják a parancsnokot és az alárendelteket."*[138]

3.2 A rádióelektronikai felderítés

Ahogy korábban megállapítottuk az *elektronikai felderítés fogalma alatt az elektronikai eszközökkel különböző hullámtartományokban végzett adatszerzést és ezen adatok feldolgozását értjük*, amely megjelenhet több adatforrás típus esetében is.

Ennek egyik megvalósítási formája a SIGINT.

[136] AJP-2.0 Szövetséges Összhaderőnemi Felderítő, Felderítés elleni védelem, és Biztonsági Doktrína, NATO HQ, Brüsszel, 2002, p. 34.

[137] A NATO által használt terminológia szerint a vezetési rendszereket Communication and Information System – CIS-nek nevezik.

[138] JP 6-02: A Hadműveleti/Harcászati Vezetési, Irányítási, Kommunikációs és Számítógépes Rendszerek Alkalmazásának Alapelvei, NATO HQ, Brüsszel, KIADÁS ÉVE????, p. 15.

A SIGINT két[139] részre osztható:
- COMINT;
- ELINT.

A COMINT a szemben álló fél kommunikációs kisugárzó eszközeinek észleléséből, lehallgatásából szerez információkat, illetve e kisugárzó eszközök települési helyét határozza meg. A COMINT adatforrásai lehetnek: rádiók, rádiórelék, vezeték nélküli telefonok, illetve egyéb kommunikációs céllal elektromágneses kisugárzást végző eszközök, rendszerek.

Az ELINT a szemben álló fél nem kommunikációs kisugárzó eszközeinek észleléséből, technikai paramétereinek meghatározásából és települési helyük meghatározásából állít elő információkat (például radarok, tűzvezető, vagy akár fegyverirányítási rendszerek).

A SIGINT adatszerzési részének tartalma és módszerei a következők:
- felfedés;
- iránymérés;
- helymeghatározás;
- figyelés;
- lehallgatás.

3.2.1. Felfedés

A *felfedés* olyan szervezett tevékenység, amely arra irányul, hogy az ellenség rádiólokációs, rádiónavigációs, rádió-távvezérlő és rádió-távközlő rendszereiben alkalmazott rádióelektronikai eszközöket érzékelve feltárja, és a felderítő ismérvek alapján meghatározza felderítési értéküket. A felfedés célja az új objektumok, adatforrások feltárása és ezen keresztül az ellenség teljes rádiólokációs, rádiónavigációs, rádió-távvezérlő és rádió-távközlő rendszere felépítésének és működésének megismerése.

A felfedés a kereséssel kezdődik. A keresést a lehető leggyorsabban és a lehető legjobb felderítési valószínűség mellett kell végezni. A keresés lehet:
- irány szerinti keresés;
- frekvencia szerinti keresés.

A rádiófelderítés esetében az *irány szerinti keresés* csak ritkán értelmezett, amikor irányított antennákkal, adott szektorokban végeznek csak felfedést. A *frekvencia szerinti keresés* a felfedő tevékenység alapvető módszere, amikor az egyes munkahelyek a teljes vételi sávban, vagy csak kijelölt alsávokban végeznek felfedést.

[139] Gyakran megjelenik egy harmadik fogalom is, mint SIGINT összetevő: FISINT (Foreign Instrumentation Signals Intelligence – külföldi kisugárzó eszközök felderítése).

A rádiótechnikai felderítés során az *irány szerinti keresés* az antennarendszerek mechanikus, vagy elektronikus forgatásával, a vételi frekvenciasávban végrehajtott mechanikus, vagy elektronikus hangolással végzett jelfelderítő tevékenység, melynek célja az elektronikai objektumok felfedése. Objektum észlelése esetén a keresés automatikus leállása, vagy leállítása után meghatározható a technikai paraméterek és a tartalmi jegyek alapján a felderítési érték. Az adatokat rögzítik a későbbi megfigyelés, összehasonlítás érdekében.

Az irány szerinti keresés garantált lassú módszere azt jelenti, hogy a felderítő állomás antennájának egy körülfordulása alatt a cél sugárforrás (forgó antennájú radarállomás) antennája legalább egyszer a felderítő állomás felé sugároz. Hátránya a hosszú észlelési idő. Az irány szerinti keresés garantált gyors módszer alkalmazásával a felderítő állomás antennájának olyan nagy sebességgel kell forognia, hogy a cél sugárforrás felderítő állomás felé sugárzásának ideje alatt legalább egyszer a sugárforrás felé nézzen. Hátránya a szükséges nagy (kereső)antenna sebesség, amely nehezen biztosítható. Az elektronikus átkapcsolásokkal működő, körkörösen, vagy a felderítendő szektorban elhelyezett szükséges számú antennákból felépített rendszerek, illetve a „fázis-rács" antennák iránykarakterisztikáinak elektronikus vezérlése (álló antenna esetén is) lehetővé teszi a garantált gyors keresést.

A *frekvencia szerinti keresést* lehet garantált lassú módszerrel végezni, amikor a kereső vevő frekvencia-áthangolásának ideje alatt a vevő sávszélességébe minden esetben legalább egyszer beérkezik a cél sugárforrás (radarállomás) legalább egy kisugárzott impulzusa. Hátránya a (viszonylag) hosszú felderítési idő. A garantált gyors frekvenciakeresés olyan nagy sebességgel történik, hogy minden kisugárzott impulzus ideje alatt legalább egyszer találkozik a vételi sáv a céladó jelével. Hátránya a (viszonylag) rövid analizálási idő.

A garantált lassútól gyorsabb, de a garantált gyorstól lassabb irány, illetve frekvencia szerinti keresések esetén a felfedés valószínűsége függ a felderítő és a felderítendő állomás közötti antennaforgatási, illetve frekvencia-áthangolás és impulzusidő viszonyoktól, az antennák kezdeti helyzetétől, a forgási irányoktól, illetve a vevő áthangoló rendszer hangolási irányától, fázishelyzetétől. Amennyiben ismert a felderítendő kisugárzó eszköz hozzávetőleges iránya illetve frekvenciája, akkor a keresés szektorosan, illetve rész-frekvenciatartományban nagyobb valószínűséggel elvégezhető.

A keresés nélküli irány illetve frekvencia felfedési eljárások azon alapulnak, hogy az irány illetve frekvencia szerinti felbontáshoz (pontossághoz) szükséges számú, párhuzamosan működő antenna illetve vevőberendezés üzemel. Így késedelem nélkül meghatározható, hogy milyen irányból, milyen frekvencián érkezett besugárzás.

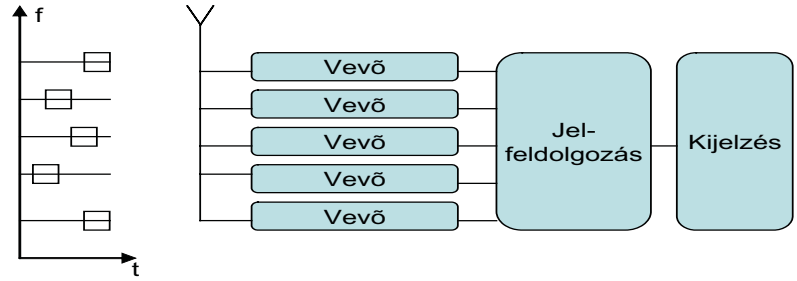
Ugyanakkor a korábban említett technikai és eljárásbeli kihívások komoly feladat elé állítják a SIGINT rendszereket is. Az új típusú, digitális, vezeték nélküli kommunikációs rendszerek megjelenése nyilvánvalóvá tette a hagyományos, analóg rádiófelderítő eszközök használhatatlanságát. Jelenleg a legnagyobb kihívást a már előzőekben ismertetett kiterjesztett spektrumú rádiórendszerek felderítése jelenti.[140]

[140] Haig, Zs. – Kovács, L. – Vass, S. – Ványa, L.: *Felderítési és zavarási technikák vizsgálata. Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett integrált elektronikai felderítő és zavaró rendszerhez*, ZMNE, Budapest, 2008. p. 123.

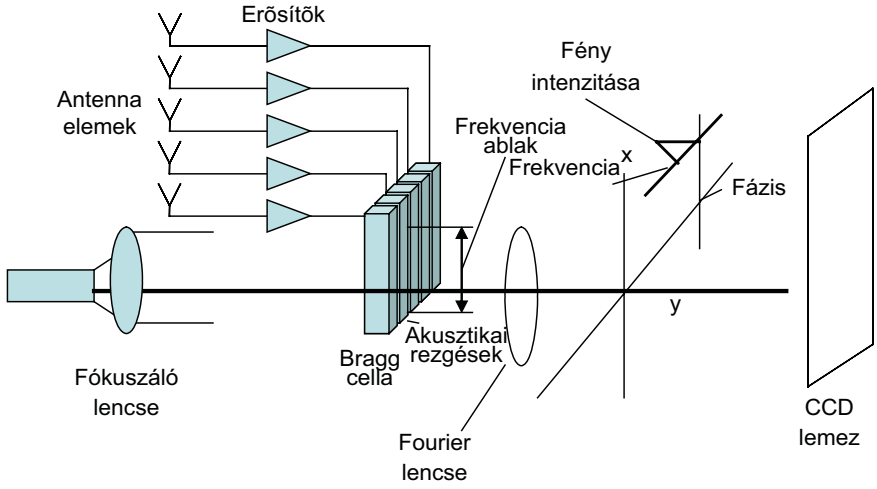
E kihívásra válaszul, az utóbbi években, például a frekvenciaugratásos kisugárzások vételére kidolgozták az úgynevezett keresés nélküli vevőket, amelyek egy időben dolgozzák fel a teljes sávot. Ilyenek a mátrixvevők elvén felépített, digitális szűrőbank–vevők és a Bragg–cellás vevők.

A *szűrőbankos felderítés* (3.3. ábra) olyan egymás mellé hangolt vevők sorozatát jelenti, amelyek összességében átfogják a kívánt frekvenciaspektrum egészét. A vevők egymással párhuzamosan veszik a saját frekvencia-tartományuknak megfelelően a kisugárzott jeleket és azokat egy jelfeldolgozó egységre juttatják. A jelfeldolgozó egység gyors Fourier transzformációt *(Fast Fourier Transformation – FFT)* használ, és a jelanalízis végeredménye folyamatos jel lesz.

A *Bragg* cellákkal kialakított vevőben (3.4. ábra) a vett bemenő jelek előerősítés és alacsonyabb frekvenciára történő átalakítás után piezoelektromos átalakítóra kerülnek.



3.3. ábra. **Szűrőbankos vevő elvi felépítése**[141]



3.4. ábra. **Bragg cellás vevő elvi felépítése**[142]

[141] Szerkesztették a szerzők.
[142] Szerkesztették a szerzők.

A piezoelektromos átalakítás után keletkezett ultrahang egy lézerfényforrás által megvilágított kristályban, a rezgéseknek megfelelő fénytörést idéz elő. A koherens fény elhajlási szöge ennek megfelelően összefüggésben van a beérkezett jel frekvenciájával. A fényt CCD chipre vezetve ábrázolható és megmérhető a beérkezett jel frekvenciája. Ezzel a módszerrel lehetőség van az adott jel frekvenciaugrásainak, illetve egy adott frekvencián eltöltött idejének megfigyelésére. Ez a megoldás sem alkalmas azonban az információtartalom visszafejtésére.[143]

Egy következő keresés nélküli módszer eszközt is jelent egyben, és az ELINT kategóriájába tartozik. Ez a *kompressziós* – vagy más néven microscan – vevő.[144] Ennek lényege a radartechnikából már ismert impulzuskompresszió elve. Lényege, hogy a vett jelet egy chirp jelet szolgáltató helyi oszcillátor jelével keverik, majd a chirp frekvenciamenetéhez illesztett karakterisztikájú diszperzív késleltető vonalra *(Dispersive Delay Line – DDL)* vezetik. A késleltető vonal kimenetén az eltérő frekvenciájú bemenő jelek eltérő időkéséssel jelennek meg, így az a bemenő jel frekvenciájának időméréssel történő meghatározásához szolgáltat alapokat.[145]

Ugyanakkor a digitális technika térnyerésével egyre gyakrabban a frekvenciaspektrum megfigyelésére, úgynevezett vízesés típusú megjelenítést alkalmaznak, melynek lényege, hogy amíg a korábbi ábrázolási eljárás a jeleket egy frekvencia-amplitúdó rendszerben ábrázolta, addig ez frekvencia-idő rendszerben mutatja a vett jeleket. Egy képernyősorban, mintegy felülről látjuk a frekvenciatengely egy adott söprési idő alatt mért értékeit. A következő sor a következő frekvenciasöprés mérési eredményeit szolgáltatja, és így tovább. Ahogy az idő telik, úgy szaporodnak a sorok, majd vízesésszerűen vonulnak a képen lefelé. Az adott frekvencián üzemelő adók térerősség információi sem vesznek el, mivel azt egy színskálán rendelik a képhez (3.1. kép). Ezt a mérési eljárást számítógép vezérli, ábrázolja, és például a letapogatási soronként keletkező soros digitális adatok rögzítésével tárolja.[146]

Természetesen a fent ismertetett rendszerekkel (eljárásokkal) az információtartalom megfejtésére nincs lehetőség, mivel e módszerekkel csak a kisugárzás tényét lehet detektálni, a vett jel paraméterei („rádiófrekvenciás ujjlenyomata") alapján az összetartozó

[143] Kovács, L.: *Az elektronikai felderítés korszerű eszközei, rendszerei és azok alkalmazhatósága a Magyar Honvédségben*. Doktori (PhD) értekezés, ZMNE, Budapest, 2003. p. 62.

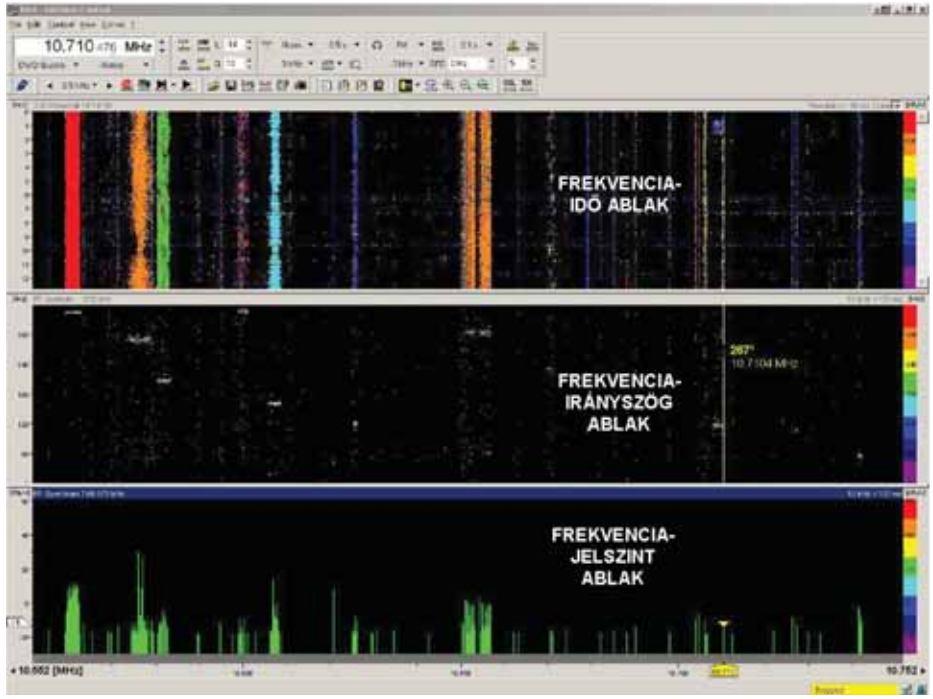
[144] Illés, A.: *Lehetőségek a radarok ESM eszközök elöli rejtettségének növelésére*. http://www.zmne.hu/tanszekek/ehc/konferencia/may/illes.htm (Letöltve: 2014.02.14.)

[145] Kovács, L.: *Az elektronikai felderítés korszerű eszközei, rendszerei és azok alkalmazhatósága a Magyar Honvédségben*. Doktori (PhD) értekezés, ZMNE, Budapest, 2003. p. 65.

[146] Ványa, L.: *Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre*. Doktori PhD értekezés. ZMNE, Budapest. 2002. p. 42.

kisugárzásokat össze lehet fűzni, és ezáltal a kisugárzó eszközt azonosítani, esetleges irányát és települési helyét lehet meghatározni.[147]

A felfedési tevékenység a vezetés, a kiértékelések, statisztikai elemzések, érdekében naplók, nyilvántartások formájában rögzítésre kerül. A korábbi papíralapú dokumentációk kitöltése, kiértékelése a megnövekedett felderítési adatmennyiség és a rövidülő reakcióidők következtében lehetetlenné vált. A számítógép vezérlésű elektronikai felderítő eszközök ezeket a statisztikákat akár alfanumerikus, akár grafikus formában később is képesek megjeleníteni (ha szükséges kinyomtatni). Az adatbázis kezelő programok – megfelelő algoritmusokkal – a papíralapú nyilvántartások kiértékelőitől több nagyságrenddel gyorsabban, pontosabban hoznak a parancsnoki döntésekhez felderítési támogató javaslatokat.



3.1. kép. **Vízesés típusú kijelző**[148]

147 Haig, Zs. – Kovács, L. – Vass, S. – Ványa, L.: *Felderítési és zavarási technikák vizsgálata. Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett integrált elektronikai felderítő és zavaró rendszerhez*, ZMNE, Budapest, 2008. p. 89.

148 Rohde-Schwarz. *Radiomonitoring and Radiolocation*. Products catalog 2003/2004.

3.2.2 Rádió iránymérés és helymeghatározás[149]

A rádió iránymérés célja egy tetszőleges forrású elektromágneses sugárzás irányvonalának *(Line of Bearing – LOB)* meghatározása a rádióhullámok terjedési sajátosságainak segítségével. A rádió iránymérés a föld felszínén elhelyezkedő rádióadók vagy rádiózavar források irányának meghatározásához használható fel.[150]

A rádió iránymérő egy, az elektromágneses hullámok beérkezési irányának (vagy azimutjának) egy referencia irányhoz vonatkoztatott meghatározására szolgáló elektronikai eszköz. Az elektromágneses jel irányának meghatározásához, az antennanyílásnál fellépő különbségi jelkésleltetést használják fel. Minden iránymérőben megtalálható egy antennarendszer, egy vevőberendezés és egy jelfeldolgozó processzor.

A korszerű iránymérő technikák a következő három csoportra oszthatóak:
- amplitúdó-érzékeny iránymérés;
- fázis-érzékeny iránymérés;
- kombinált fázis- és amplitúdó-érzékeny korrelatív vektor iránymérés és igen nagy felbontású iránymérés.

A leggyakrabban használt iránymérési technikák a következőek lehetnek:
- forgó antenna-karakterisztika;
- Wullenweber;
- Adcock/Watson-Watt;
- Doppler/pszeudo Doppler;
- interferométer;
- korrelációs.

3.2.2.1 Forgó antenna-karakterisztikájú iránymérő rendszerek

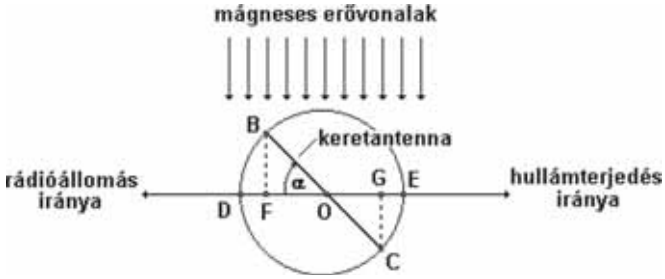
A legegyszerűbb iránymérésre használt eljárás, amikor a beesési irány érzékelésénél az antenna iránykarakterisztika jellegzetességeit alkalmazzák. A mechanikusan forgó irányantennára alapozó DF rendszereket már a XIX. század és XX. század fordulóján is használtak. Az ilyen, tipikusnak tekinthető rendszerek a csak egy, a vételi irányba eső null-hellyel rendelkező antennát használnak; a beesés iránya az antennának a minimális vételű helyzetbe történő beirányításával történik. Bellini és Tosi 1903-ban kezdték publikálni a szkennelt antenna eljárásokkal (rádió goniométer) kapcsolatos munkáikat.

[149] Haig, Zs. – Fürjes, J. – Kovács, L. – Vass, S. – Ványa, L.: *Felderítés hatékonyság minősítő eljárás kidolgozása. Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett integrált elektronikai felderítő és zavaró rendszerhez*, ZMNE, Budapest, 2008. p. 98.

[150] Rádiómérő módszerek és eljárások a Nemzeti Hírközlési Hatóság gyakorlatában (Letöltve: 2014.02.20.) http://meres.nhh.hu/u/document/200606/Korszeru_radiomeresek_az_NHH_gyakorlataban_6.pdf

Ezek a rendszerek – az antenna vételi karakterisztikájának elektromos úton történő „mozgatásával" – alternatívát kínálnak a mechanikusan forgatott antennákkal szemben.

A rádió iránymérés elve az indukció törvényén alapul, miszerint váltakozó mágneses térben elhelyezett vezetőben feszültség indukálódik. Ennek megfelelően egy rádióállomás jele által keltett váltakozó elektromágneses tér az ott elhelyezett vezetőkeretben (keretantennában) feszültséget hoz létre (3.5. ábra). Az adóállomás sugárzása vertikálisan polarizált, azaz a váltakozó mágneses hullámfront a vízszintes síkban terjed és halad át a vertikális keretantennán. A feszültség arányos a kereten áthaladó mágneses erővonalak számával, vagyis maximális akkor, ha a keret síkja merőleges az erővonalakra és zérus, ha párhuzamos azokkal.[151]



3.5. ábra. **Rádió iránymérés elve**[152]

Ha az ábra szerint (a felülnézetben látott) keretantennát a BC állásba forgatjuk, akkor az így áthaladó erővonalak száma cos α szerint aránylik a DE helyzetben áthaladó maximális erővonalszámhoz. Ebből következik, hogy a BC helyzetben mérhető feszültség is cos α-szorosa a DE helyzetben mérhető maximális feszültségnek. A keretantennán mérhető feszültség függ tehát az antennának az adóállomáshoz viszonyított irányától.

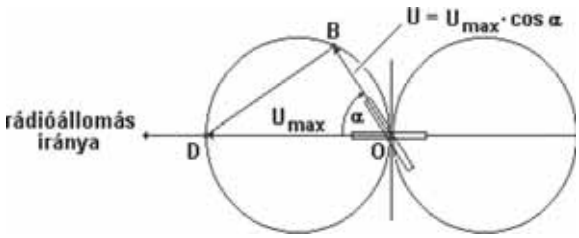
Ha a keretantennát körbeforgatjuk és az egyes irányokban mérhető feszültséget irány szerint ábrázoljuk, akkor a 3.6. ábrán bemutatott polárdiagramhoz (nyolcas diagram) jutunk. A polárdiagram szerint a kiindulási helyzethez képest a keret 90°-os elfordításakor zérus feszültséget, 180°-os elfordításakor ellenkező irányú maximális feszültséget, 270°-os elfordításakor ismét zérus feszültséget kapunk.

A rádió iránymérő berendezés a keretantennán mért feszültséget hangfrekvenciás jellé alakítja át. Ha a keretantennát a rádióállomás irányába fordítjuk, akkor maximális jelerősség hallható. A rádióállomás irányát meghatározhatjuk úgy is, hogy az antennát addig fordítjuk el, amíg a jel teljesen elhalkul. Ekkor az adóállomás a keret síkjára merőlegesen helyezkedik el. A gyakorlatban ez utóbbi módszert alkalmazzuk, mivel az emberi

[151] http://jegyzet.sth.sze.hu/ftp/!Muinfo/!Felsobb_eves/Szakiranyos/_Kozlekedesi_szakirany/Technika.III/ kt3.4.doc (Letöltve: 2014.02.18.)

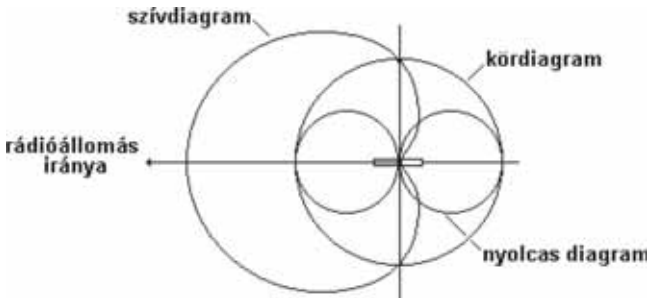
[152] Haig, Zs. – Fürjes, J. – Kovács, L. – Vass, S. – Ványa, L.: *Felderítés hatékonyság minősítő eljárás kidolgozása. Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett integrált elektronikai felderítő és zavaró rendszerhez*, ZMNE, Budapest, 2008. p. 123.

fül számára könnyebb egy jel elhalkulását (a hang megszűnését) érzékelni, mint annak maximális erősségét. Ez egyben pontosabb mérést is lehetővé tesz, mivel – mint ahogy az a polárdiagramon is látható – a jelerősség kisebb mértékben változik az antennának a maximum helyzet környezetében való elfordításakor, és nagyobb mértékben a minimum helyzet környékén.



3.6. ábra. **Nyolcas diagram**[153]

Az iránymérő skála 0° osztását a hajó hossztengelyének irányába állítják be. Ebben az esetben a mért irányok, mint egészkörös orrszögek olvashatók le. Az iránymérő skála lehet egy tájoló rózsája is (például kézi rádió iránymérőnél), ekkor valódi irányok határozhatók meg. A keretantenna elforgatásakor két minimum helyzet állítható elő, azaz a rádióállomás hozzánk viszonyított helyzetére két egymástól 180°-kal eltérő irányt kapunk. Ez a tulajdonság a rádió iránymérés kétértelműsége, amelynek megszüntetését oldalhelyzetmérésnek nevezzük. Ennek elvét a 3.7. ábra szemlélteti.



3.7. ábra. **Oldalhelyzet meghatározása**[154]

A keretantenna mellett (elvileg annak forgástengelyében) segédantennaként egy ostorantennát helyeznek el. Az ostorantenna jelerőssége független a rádióállomás irányától, azaz polárdiagramja egy kör. A segédantenna jelerősségét úgy állítják be, hogy

[153] Haig, Zs. – Fürjes, J. – Kovács, L. – Vass, S. – Ványa, L.: *Felderítés hatékonyság minősítő eljárás kidolgozása. Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett integrált elektronikai felderítő és zavaró rendszerhez*, ZMNE, Budapest, 2008. p. 134.

[154] U.o. p. 154.

az azonos legyen a keretantenna maximális jelerősségével (vagyis a kördiagram sugara, azonos a nyolcas diagram egy-egy körének az átmérőjével).

A segédantenna bekapcsolt állapotában a rádió iránymérő készülék a segédantenna és a keretantenna feszültségét összegzi. A keretantenna körbeforgatásakor az egyes irányokban mérhető eredő feszültség az ábra szerint alakul, azaz polárdiagramként egy úgynevezett szívgörbét (kardioid) kapunk. Az ábra alapján látható, hogy a rádióállomás irányában a két feszültség összeadódik és így maximális jelerősség lesz mérhető. A keretantennát 180°-kal elforgatva az abban indukálódó feszültség előjelet vált és így a segédantenna feszültségével összeadódva zérus eredő feszültséget kapunk.

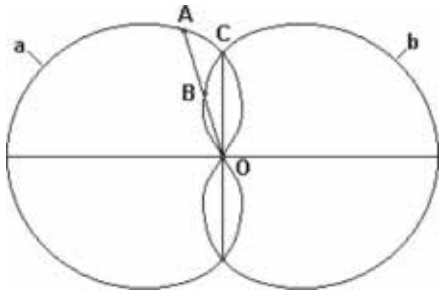
A korai rádió iránymérő készülék hátránya az volt, hogy az antennát a mérés helyén kellett felszerelni, és azt kézzel kellett forgatni. A mai rádió iránymérők kizárólag a Bellini-Tossi elven működnek, így kiküszöbölik ezeket a hátrányokat. A Bellini-Tossi rendszerben két egymásra merőlegesen rögzített keretantennát helyeznek el a hajón a vétel szempontjából a legkedvezőbb helyen. Az antennát úgy állítják be, hogy az egyik keret síkja a hajó hossztengelyével, a másik a kereszttengelyével legyen párhuzamos. A vevőkészüléket a mérés helyén helyezik el. A vevőkészülék két egymásra merőleges, úgynevezett mezőtekercset tartalmaz, amelyek közül az egyik a hossztengelyű, a másik a kereszttengelyű antennakerettel van összeköttetésben.

A két antennakeretben a rádióállomás jele által indukált feszültség a mezőtekercsekben váltakozó áramot indít. Ez a váltakozó áram ugyanolyan mágneses teret hoz létre a mezőtekercsek által közrezárt térben, mint amilyent az adóállomás az antennakeretekben. A mezőtekercseken belül egy úgynevezett keresőtekercset helyeznek el, amely egy kezelőgombbal forgatható. A mezőtekercsek mágneses terében elforgatott keresőtekercsben feszültség indukálódik és így az ugyanolyan irányban jelzi a maximális, illetve minimális jelerősséget, mint az adóállomás terében elforgatott keretantenna.

A rádió iránymérő mutatója a keresőtekerccsel szinkronban forog és a mutató mögötti iránymérő skálán, a már elmondottak szerint egészkörös orrirányok olvashatók le. Ha a hajó pörgettyűs tájolóval is rendelkezik, akkor olyan rádió iránymérő szerelhető fel, amely egy második – a pörgettyűs tájoló által vezérelt – iránymérő skálával (tájolórózsával) is rendelkezik. Ennek 0° beosztása a valódi északi irányt jelöli, és így a skálán valódi iránylatok olvashatók le.

A rádió iránymérő készülékek továbbfejlesztéseképpen először a vizuális, majd az automatikus rádió iránymérők jelentek meg. A vizuális rádió iránymérő egy katódsugárcsővel rendelkezik, amelynek kitérítő lemezeire csatlakoztatják a hossz- és kereszttengelyű antennakeretek végződéseit. A hossztengelyű antennakeretben indukálódó feszültség a katódsugarat le-fel, a kereszttengelyűt jobbra-balra mozgatja. A kitérülő fénypont egy vonalat ír le a képernyőn, amely a rádióállomás irányvonalát adja. A katódsugárcső körül elhelyezett iránymérő skálán a rádióállomás relatív iránylata leolvasható. A vizuális rádió iránymérők lehetővé teszik a hangerősség útján való iránymérést is. Az automatikus rádió iránymérőben a vétel egyidejűleg történik a keret- és a segédantennán. Ennek eredményeképp egy szívgörbét kapunk. A keresőtekercs kivezetéseit felcserélve a szívgörbe ellenkező irányúvá vált (3.8. ábra 'a' és 'b' jelű görbe).

A vevőkészülék így egy kiindulási helyzetben az ábra szerinti OA és OB jelerősséget méri váltakozva. Ebből a feszültségkülönbségből származó áramot egy, a keresőtekercset forgató motorba vezetik. Ennek hatására a keresőtekercs addig fordul el, amíg az áram zérussá nem válik, vagyis amíg a feszültség mindkét esetben fel nem veszi az ábra szerinti OC értéket. Ez a helyzet megfelel a nyolcas diagram szerinti minimumhelyzetnek.



3.8. ábra. **Automatikus rádió iránymérő elve**[155]

3.2.2.2 Elektronikus szkennelés Wullenweber rendszerek

Wullenweber az antenna-karakterisztika tulajdonságait antennakombináló technikák alkalmazásával tökéletesítette. Ezeknél a rendszereknél egy antenna helyett egy időben antenna csoportokat kapcsolnak. (3.2. kép)

3.2. kép. **Wullenweber iránymérő antennájának felépítése**[156]

[155] Haig, Zs. – Fürjes, J. – Kovács, L. – Vass, S. – Ványa, L.: Felderítés hatékonyság minősítő eljárás kidolgozása. Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett integrált elektronikai felderítő és zavaró rendszerhez, ZMNE, Budapest, 2008. p. 167.

[156] Gander: http://jproc.ca/rrp/gander.html (Letöltve: 2014.02.15.)

Az antennákat – az egy adott irányból érkező jelre fókuszolandó – kombináltan, jellegzetesen késleltető vonalakkal összekapcsolva alkalmazzák. Koncentrikus körök alakjában elhelyezkedő antennákat alkalmazó, vezérelhető antennakarakterisztikát előállító (keskeny sáv az összeg csatornában, nulla a különbségi csatornában) antennákkal működő, nagy látószögű iránymérő rendszereket alkalmaznak. A szkennelő módszernél alkalmazott irányhatás következtében ezek a rendszerek rendkívül érzékenyek. A komplex antennákból és a szükséges nagy infrastruktúrából adódóan – főleg a HF tartományú alkalmazásoknál – meglehetősen drágák.

3.2.2.3 Adcock/Watson-Watt iránymérők

Ezek a rendszerek az antennák és a jelfeldolgozás területén végbement fejlődést használják ki egy, csaknem azonnali leolvasást lehetővé tevő rendszer létrehozására. Az alkalmazott Adcock antennarendszer (1918-ban fejlesztették ki) dipól vagy monopol antenna párokból áll, amelyek az ismert „nyolcas" vételi karakterisztika kialakítása érdekében 180 fokos hibrid áramkörrel vannak összekapcsolva. (3.3. kép)

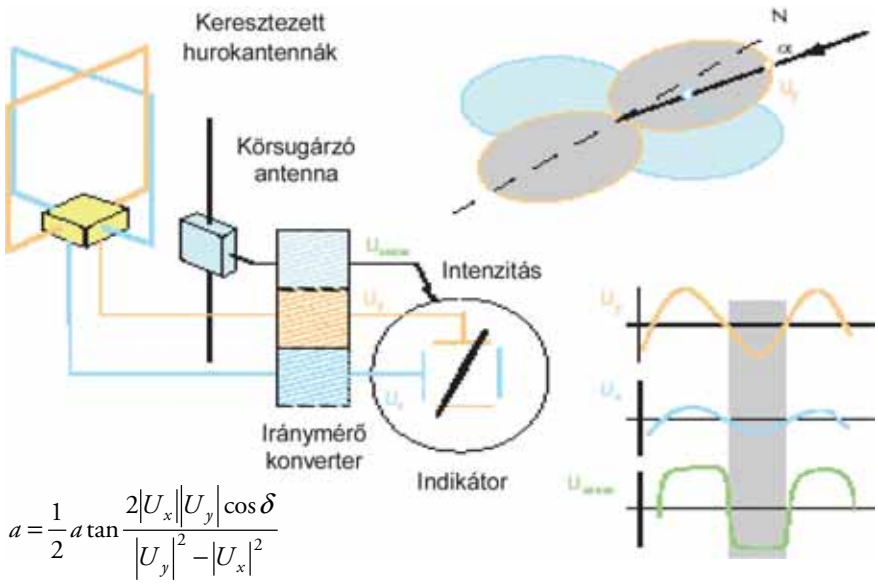
Ortogonális alapvonalakon elhelyezkedő két Adcock pár a jel beérkezési irányban olyan karakterisztikával rendelkezik, amely az egyik antenna beérkezési iránya szinuszával és a másik antenna beérkezési iránya koszinuszával arányos. Ez hasonlít a keresztezett hurokantennák karakterisztikájához.

3.3. kép. **Adcock antennarendszer**[157]

A Watson-Watt technika három fázisban illesztett vevővel dolgozik, szinusz és koszinusz függvényként megjeleníti a beérkezési szöget, valamint egy harmadik, a bizonytalansági problémák megoldására szolgáló omnidirekcionális (körsugárzó) csatornát. A klasszikus Watson-Watt technikánál a koordináta konverzió elvégzéséhez (erre azért

[157] http://jegyzet.sth.sze.hu/ftp/!Muinfo/!Felsobb_eves/Szakiranyos/_Kozlekedesi_szakirany/Technika.III/ kt3.4.doc (Letöltve: 2014.02.18.)

van szükség, hogy az operátor számára az irányvonal megjeleníthető legyen) a kijelző (katódsugárcső) X, Y és Z (intenzitás) bemeneteit használják fel. (3.9. ábra)



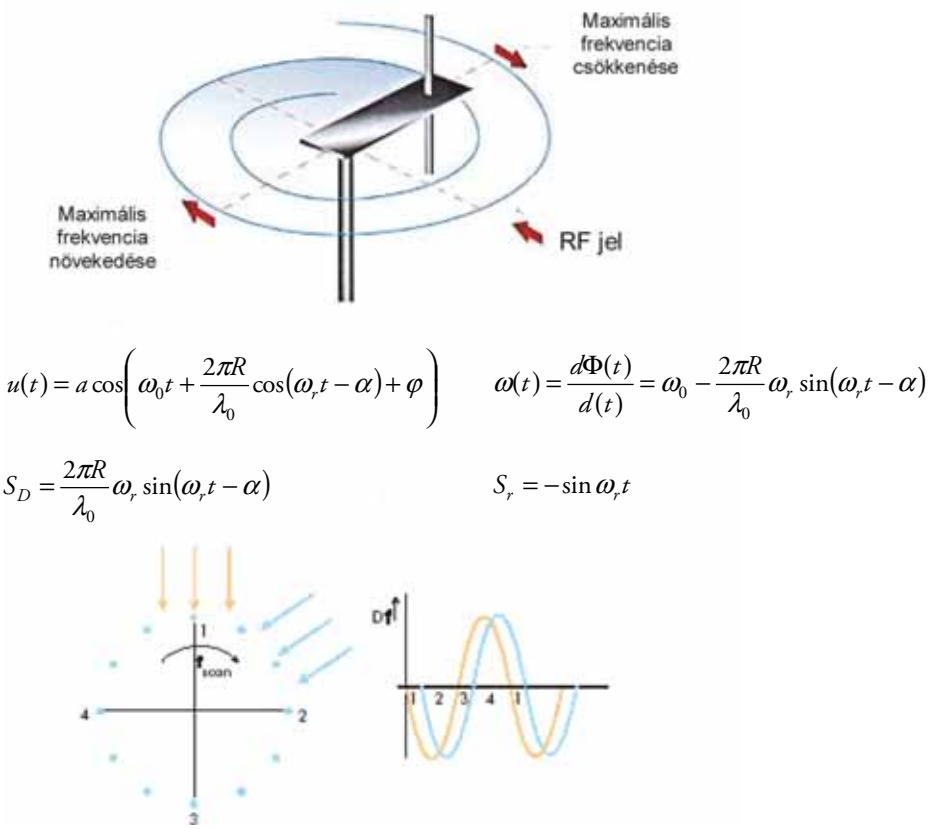
$$a = \frac{1}{2} a \tan \frac{2|U_x||U_y|\cos\delta}{|U_y|^2 - |U_x|^2}$$

3.9. ábra. **Watson-Watt iránymérő működési elve**[158]

3.2.2.4 Doppler/pszeudó-doppler iránymérők

A korszerű iránymérők az irány meghatározásához digitális jelfeldolgozó technikákat (DSP) alkalmaznak. A Doppler és a pszeudó-Doppler rendszereket az 1950-es években, a mozgó antenna és a vett jel között kialakuló Doppler eltolódás tanulmányozására alapozva fejlesztették ki. Kiderült, hogy egy r sugarú körív mentén mozgó monopol antenna a távoli állomás jelét a beérkezési szöggel és a vevőantenna forgásával arányos Doppler eltolódással veszi. A jel iránya a maximális Doppler eltolódás vételi helyénél érintőleges a forgási körre. (3.10. ábra)

[158] Makraduli, M.: *Direction Finding*. (Letöltve: 2014.01.28.) http://www.dtk.gov.mk/Portals/57ad7180-c5e7-49f5-b282-c6475cdb7ee7/INA_DF_makraduli.ppt



3.10. ábra. **A Doppler iránymérő működési elve**[159]

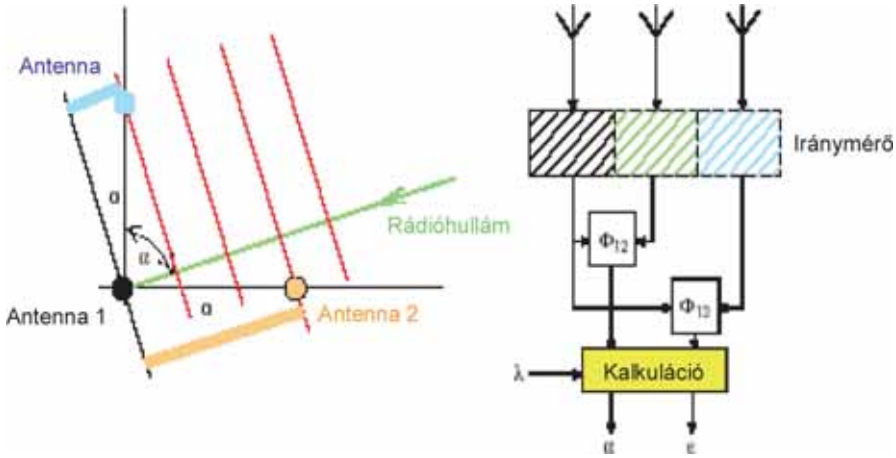
Az antenna mechanikus forgatása – különösen az UHF sáv alatti frekvenciákon – igen előnytelen, ezért kifejlesztettek egy elektronikus kapcsoló eljárást, amivel a fix, köralakban elhelyezkedő antennákból álló antennarendszer esetén is lehetőség van a forgatás elektronikus szimulálására. Ez a technika a pszeudó-Doppler módszer.

3.2.2.5 Interferometrikus eljárások

Az interferometrikus megoldás az irányvonal meghatározására szolgáló nagyon pontos módszer, melyet az 1950-es, 1960-as években fejlesztették ki. A rendszer különbségi fázist mér legalább két független antenna között. Kritikus eleme a fázisdetektor, amely a két vett jel közti fáziskésleltetést adja meg. A késleltetés segítségével megbecsülhető a beesési szög. Egy 3, 4, 5, vagy még több antenna kombinációjából álló rendszer segít-

[159] Makraduli, M.: *Direction Finding*. (Letöltve: 2014.01.28.) http://www.dtk.gov.mk/Portals/57ad7180-c5e7-49f5-b282-c6475cdb7ee7/INA_DF_makraduli.ppt

ségével – antennaforgatás nélkül – elérhető a 360°-os látószög. A különböző antennáktól érkező bemenőjelek kombinálására eredményesen használhatók fel a sokcsatornás vevőrendszerek és antenna-kapcsolók. (3.11. ábra)



3.11. ábra. **Az interferométeres iránymérő működési elve**[160]

3.2.2.6 Korrelatív interferometrikus (szuper-felbontású) rendszerek

A korrelatív interferometrikus rendszerek kettő vagy több szimultán társcsatornás jelfeldolgozására alkalmas rendszerek, amelyeknek korai kifejlesztését a rádiócsillagászatnak köszönhetjük. Ebben a megoldásban az antennák által vett jelek tartalmazta információkat bonyolult antennarendszerek és bonyolult statisztikai számítások segítségével állítják elő. Itt az antennarendszer elemeire vonatkozó autokorrelációs és keresztkorrelációs jelek kiértékelésére, és az áteresztő sávi többszörös jelek jelenlétének megállapításához kifinomult statisztikai eljárásokat (mint például a többszörös jelek osztályozása, *Multiple Signal Classification* – *MUSIC* algoritmus) alkalmaznak. Ezek a rendszerek tipikusan – a vett amplitúdó- és fázisértékeknek az antennarendszer kalibrált amplitúdó- és fázisadataival történő korrelációjával – a felbontott jelekre határozzák meg az irányvonalat. Ez a korrelatív interferometriának is nevezett eljárás képes a készülék és a helyfüggő hibák kiküszöbölésére és igen sokféle antennarendszerrel tud együttműködni.

Mindegyik iránymérő technikának megvannak a maga előnyei és hátrányai. A legegyszerűbb és legolcsóbb módszereknél lehetnek ugyan a pontossággal, érzékenységgel vagy polarizációval kapcsolatos problémák, azonban igen jól alkalmazhatók egyes mobil tájolási feladatokhoz. A legfejlettebb, számítógépeket igénylő technikák hordozhatósá-

[160] Makraduli, M.: *Direction Finding*. (Letöltve: 2014.01.28.) http://www.dtk.gov.mk/Portals/57ad7180-c5e7-49f5-b282-c6475cdb7ee7/INA_DF_makraduli.ppt

got és rendkívüli pontosságot biztosítanak. Ezen túlmenően ezek a modern rendszerek – mivel képesek a beeső jel elevációs szögének mérésére és a hagyományos azimut becslésre – a HF SSL tartományban is alkalmazhatók. A gyártók különböző változatokat kínálnak. Fontos azonban, hogy az iránymérő eszközök kiválasztásakor az üzemeltetési célok kellőképpen meg legyenek határozva. A műszaki és a gazdasági szempontok további összehasonlítását a célok pontos ismerete teszi lehetővé.

3.2.3 Figyelés

A figyelés a már felfedett, felderítési értéket képviselő elektronikai objektumok működésének, paraméterei változásának, forgalmi viszonyainak jellemzőire irányul. A figyelést folyamatosan, periodikusan, vagy véletlenszerű időközönként végzik. A figyelés eredményeit az objektumok adatbázisához csatolva rögzítik, és további vizsgálatok, statisztikák alapadataként használják fel.

A figyelés alapvető módszere az ellenőrzés. Az ellenőrzést az objektum fontossági fokának megfelelően, a korábban szerzett adatokkal összevetve, a változások regisztrálásával és azoknak a kiértékelőkhöz való továbbításával kell folytatni. A figyelés folyamán ellenőrzik a korábbi iránymérési adatokat, melyek alapján jelezhető az objektum mozgása. A figyelendő objektumra való „ráállást" megkönnyíti, (meggyorsítja) hogy már ismert tér- és frekvenciatartományban kell az objektum működésére utaló jeleket keresni.

A figyelés folyamán a felfedéskor rögzített adatok esetleges változásait értékelik, ezért az adatrögzítés, dokumentálás, (okmányolás) a felfedéssel megegyező eszközökkel és módszerekkel történik. A különbség, hogy míg a felfedés „üres lappal" indul, addig itt a nagymennyiségű, korábban szerzett –felfedési, figyelési – adathalmazt is kezelni kell. Az adatbázis tartalmazza az objektum típusa, észlelési idő, vivőfrekvencia, moduláció, üzemmód, antenna típus, sugárzási irány és egyéb paraméterek és korszerű berendezések alkalmazása esetén a jel analizátorok által szolgáltatott „elektronikus ujjlenyomatok" adatait. A klasszikus papíralapú „okmányolás" természetesen itt is visszaszorulóban van.

3.2.4 Lehallgatás

A lehallgatás a figyelés folyamán az átvivendő információ tartalmának, a telemetriai folyamat eredményének megszerzésére irányuló tevékenység. A lehallgatás az adatforrás folyamatos, megszakítás nélküli figyelését, ellenőrzését igényli.

A klasszikus lehallgatás célpontjai – a kommunikációs célú, nyílt, fónia adások – a digitális technika megjelenésével egyre ritkábban hallhatók az éterben. A moduláció a digitalizálással könnyen titkosítható, ami a lehallgató számára csak rendkívül nagy nehézségek árán, általában hosszú időt, erős számítástechnikai hátteret igényelve fejthető meg. A korszerű lehallgatás nem az információtartalmat, hanem az egyéb, felhasználóra

és működési szokásaira jellemző paramétereket keresi, melyek alapján az aktuális, vagy várható tevékenység jelezhető, illetve prognosztizálható.[161]

A korszerű lehallgató berendezés a vett jeleken végzett matematikai műveletek sokaságának eredményeként szolgáltatja az információtartalmat, ezért alapeleme a valós idejű (real time) tárolást biztosító memória (mágneses, optikai rögzítő eszköz). A tárolt jelsorozaton jelprocesszorok dolgoznak, melyek működése már csak közel valós idejű (near real time) eredményt szolgáltathat.

3.3 Az elektronikai támogatás

„Az elektronikai támogatás az elektronikai hadviselés azon területe, amely az ellenség helyzetére vonatkozó tájékozottság, és a fenyegetés késedelem nélküli felismerése céljából magában foglalja az elektromágneses kisugárzások kutatását, felfedését és azonosítását, valamint a kisugárzók helyének meghatározását."[162]

Az elektronikai támogatás információt szolgáltat az elektronikai ellentevékenységre, az elektronikai védelemre és más harcászati tevékenységekre vonatkozó azonnali döntések meghozatalához.

Az elektronikai támogatás általában harci információkat szolgáltat, melyek felhasználhatók a tüzérségi tűz kiváltásához, a csapatok manővereztetéséhez, illetve a közvetlen veszély elhárításához.

Az elektronikai támogató tevékenység hadműveleti-harcászati szintű információkkal hozzájárul a parancsnok felderítő adatgyűjtéséhez.[163]

Az elektronikai támogatás jellemzői:

- az elektronikai támogatás béke-, válság- és háborús helyzetben egyaránt folytatható. A tevékenység általános célja az adott műveleti területre vonatkozó elektronikai hadviselési adatbázis létrehozása, folyamatos aktualizálása;
- a tevékenység az időjárási körülményektől függetlenül, nappal és éjszaka, időben korlátlanul végezhető;
- nem észlelhető (passzív), a vezetési és irányítási rendszerét leszámítva rejtett tevékenység;
- képes feldolgozni az elektromágneses kisugárzások sokféleségét a rendelkezésre álló eszközök rendeltetésének és képességeinek függvényében;

[161] Haig, Zs. – Kovács, L. – Vass, S. – Ványa, L.: *Felderítési és zavarási technikák vizsgálata. Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett integrált elektronikai felderítő és zavaró rendszerhez*, ZMNE, Budapest, 2008. p. 178.

[162] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 67.

[163] AJP-2.0 Szövetséges Összhaderőnemi Felderítő, Felderítés elleni védelem, és Biztonsági Doktrína, NATO HQ, Brüsszel, 2002, p. 43.

– egyike a gyakran korlátozottan rendelkezésre álló harci információforrásoknak;
– információt biztosít az ellenség képességeiről és szándékairól.

3.3.1 Elektronikai támogatás a légierőben

Az elektronikai felderítés számára a légierő nyújtotta repülő eszközök – akár hagyományos, akár pilóta nélküli repülőgépekről van is szó – kiváló platformot jelentenek. Az energetikai viszonyok, az elektronikai láthatóság, az elektromágneses hullámok terjedési viszonyai, esetleg azok korlátai, illetve az új digitális modulációs módok mind-mind olyan hordozót követelnek a felderítő eszközök számára, amelyekkel rugalmasan, nagy mobilitással, és nem utolsósorban a felderítendő elektronikai és egyéb eszközök, vagy rendszerek közelébe lehet jutni, ráadásul úgy, hogy minél nagyobb területet tudjunk megfigyelni egyidejűleg.

Amennyiben az elektronikai hadviselést, mint tevékenységet mégis elválasztjuk az elektronikai felderítéstől, akkor napjainkban a légierő elektronikai hadviselése három – helyenként egymást átfedő – feladatra osztható:

– repülőgép önvédelmi elektronikai hadviselés és azok eszközei;
– kötelékoltalmazás elektronikai hadviselési eszközökkel és módszerekkel (ellenséges légvédelem lefogása – *Suppression on Enemy Air Defenses – SEAD*);
– elektronikai hadviselési támogatás a szárazföldi (például haditengerészet, különleges műveleti) erők számára.

A repülőgép önvédelmi elektronikai hadviselési rendszerének (3.12. ábra) egyik feladata az elektronikai támogatás. Ennek megfelelően napjainkban a repülőgépek egyik igen fontos fedélzeti rendszere az integrált elektronikai hadviselési rendszer, amely egyrészt biztosítja a feladat végrehajtást, másrészt hozzájárul a repülőgép túlélőképességének növeléséhez. Ehhez ma már a legkorszerűbb fedélzeti számítógépek, a különböző besugárzásjelzők és a passzív vagy aktív ellentevékenységi eszközök tartoznak.

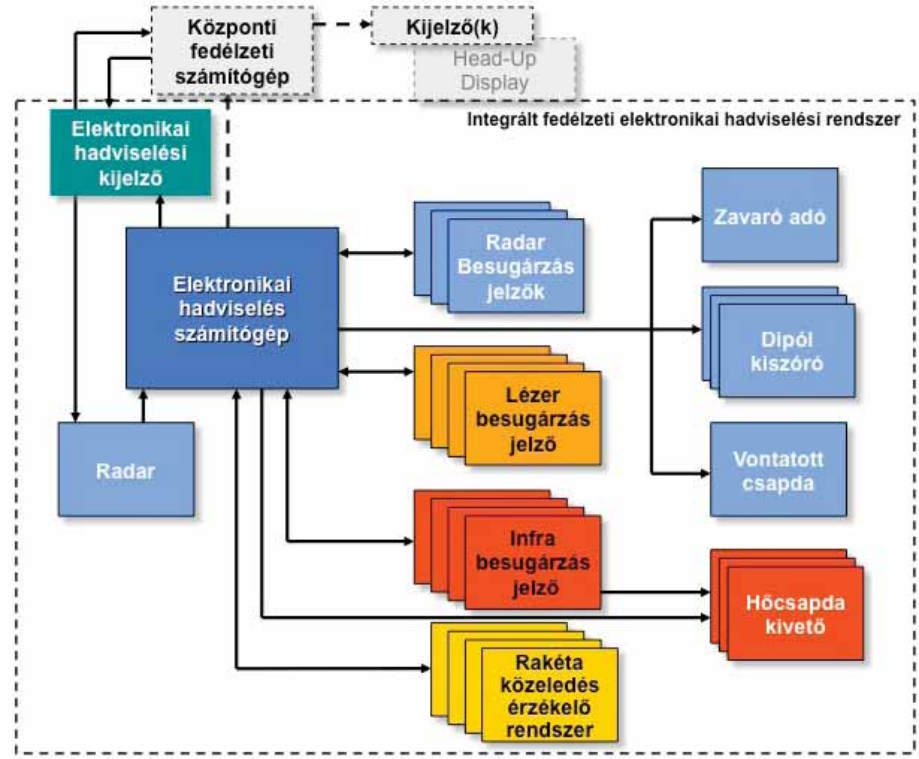
A repülőgép fedélzeti integrált elektronikai hadviselési rendszer funkciói a következők:

– a veszélyt jelentő elektromágneses (és/vagy egyéb – például infra, lézer – besugárzások vétele);
– a vett jelek paraméterei alapján a veszély azonosítása;
– automatikus ellentevékenység kiválasztása.

Mindezen feladatok csak egy jól működő elektronikai támogatási funkció mellett valósíthatóak meg.

A rendszer működése: a besugárzás jelzők veszik az elektromágneses (vagy más spektrum tartományú) besugárzást, e jel alapvető paramétereit megmérik – például frekvencia, jel teljesítménye, impulzus hossz, impulzus ismétlődési frekvencia, folyamatos jel –, majd ezt követően ez az előfeldolgozott jel az elektronikai hadviselési számítógépre kerül, ahol a pontos paraméterek meghatározása megtörténik. Ezután a számítógép e jelet összehasonlítja az adatbázisában (könyvtárában) lévő, előre definiált jelekkel. Ha

azonosat talál, akkor beazonosítható a jel, illetve a jelhez tartozó esetleges fegyverrendszer. Ezt követően a számítógép a szintén előre adatbázisban rögzített aktív vagy passzív ellentevékenységi módot fogja kiválasztani (működésbe hozni), illetve felajánlani a pilóta számára.



3.12. ábra. **Repülőgép fedélzeti integrált elektronikai hadviselési rendszer elvi vázlata**[164]

3.3.2 Az elektronikai felderítés és az elektronikai támogatás kapcsolata

Akkor, amikor a felderítés adatforrásairól beszélünk, meg kell határoznunk mi is a különbség az elektronikai felderítés és – az elektronikai hadviselés egyik területe – az elektronikai támogatás között, illetve ez a két terület – a különbségek ellenére – hogyan is függ össze egymással.

Az elektronikai felderítés és az elektronikai támogatás is ugyanazokat a rezgéstartományokat, illetve sugárzásokat „figyeli", és szerzi be belőlük, illetve ezek segítségével az

[164] Szerkesztették a szerzők.

információit. Mindkettő ugyanúgy használja a mechanikus rezgések tartományát, az elektromágneses hullámtartományt, illetve a részecske és kozmikus sugárzások tartományát. Azon kívül, hogy a hullámtartományokat közösen használják, nagyon sok esetben a felderítő eszközeik és berendezéseik is megegyeznek. Az egyetlen – de jelentős – eltérés a megszerzett információk mibenlétében és felhasználásában van. Addig, amíg az elektronikai felderítés *felderítési információkat* szerez és ad tovább, addig az elektronikai támogatás olyan gyorsan elévülő *harci információkat* szerez be, dolgoz fel és továbbít, amelyek azonnali veszélyjelzésre, vagy ellentevékenységi manőver megkezdésére, illetve ilyen rendszer (eszköz) indításához szolgáltatnak információkat.

3.4 Az összadatforrású felderítés

A kihívások és a megváltozott körülmények miatt olyan eljárásokat kell keresnünk az elektronikai felderítésben és az elektronikai támogatásban is, amelyek alkalmassá teszik az elektronikai felderítést, illetve az elektronikai támogatást arra, hogy a XXI. században is megfelelő mennyiségű, és nem utolsósorban, megfelelő minőségű, illetve valós idejű információkat tudjon szolgáltatni, amelyek reális alapját képezhetik a döntéshozatali mechanizmusnak.

A probléma összetett, de két olyan nagy kérdéskör köré csoportosíthatóak a megoldandó feladatok, amelyek vizsgálata és megoldása eredményre vezethet. Az egyik ilyen problémakör a túl sok információ. Az előbbiekből láthattuk, hogy a megváltozott technikai és tevékenységbeli körülmények új kihívások elé állították napjaink hadügyét, így az elektronikai felderítést is. Láthattuk azonban, hogy van megoldás a kihívásokra: vannak olyan szenzorok és elektronikai felderítő berendezések, amelyek alkalmasak a megváltozott technikai körülmények ellenére is információt szolgáltatni, és vannak olyan eljárások – például a pilóta nélküli repülőgépek alkalmazása – amelyek a megváltozott tevékenységi követelményekre adhatnak válaszokat. A probléma összetettsége azonban pont itt keresendő, ugyanis az új felderítő szenzorok és eszközök, kombinálva az olyan új hordozókkal, mint például az UAV, óriási mennyiségű adatot képesek szolgáltatni, de ez nem biztos, hogy teljes egészében kielégíti a felderítési igényeket. Egyrészt ezt a nagy mennyiségű adattömeget valamilyen módon tudni kell kezelni, másrészt – mint ahogy láthattuk a felderítő eszközök értékelésénél – olyan eljárásokra van szükség a valóban használható felderítési adat előállításához, amely nemcsak, hogy kezeli magát az adattömeget, de ezek között elemzéseket, összehasonlításokat végez, amelyekből következtetéssel állít elő új információt. Ehhez azonban nagyon sok esetben szükség van más forrásból származó – tehát nemcsak kizárólag az elektronikai felderítéssel megszerzett – adatok, információk összevetésére. Az eszközök elemzéséből kiderült, hogy például a modern kommunikációs adásmódokat használó rádióösszeköttetések esetében nincs ma mód az azonnali információtartalom reprodukálására. Tehát sok esetben a megszerzett információ csak részinformáció, hiszen csak azt tudjuk felderíteni, hogy hol, mikor, milyen technikai paraméterekkel rendelkező kommunikációs, vagy elektronikai rendszer üzemelt. A teljes kép kialakításához – a használható felderítési adat előállításához – tehát

szükség van más felderítési adatforrások által szolgáltatott, és az elektronikai felderítés különböző szenzorjai által szolgáltatott adatok összevetésére.[165]

Az *összadatforrású felderítés* különböző fajtájú, önálló felderítő rendszereket, valamint változást érzékelő adatgyűjtő szenzorrendszereket integrál magába. Feladata, hogy az ellenségről és a hadszíntéri környezet változásairól minden lényeges és fontos adatot, információt időben összegyűjtsön, és az illetékesek számára átadja. Az összadatforrású felderítő rendszer tehát fontos információ-átalakítási műveletet végez, vagyis a nyers adatokból és a nyers információkból felhasználható információkat hoz létre. Működése azon az elven alapszik, hogy a különböző felderítő és adatgyűjtő rendszerektől folyamatosan érkező részadatokat, paramétereket idő, hely és fontosság szerint rendezi, adott célobjektumokra összegyűjti. Ezt a folyamatot adat-, és információ összeolvasztásnak, idegen kifejezéssel adat- és információfúziónak nevezik.[166]

Az összadatforrású felderítés alapja a fúziós[167] adatfeldolgozás. Ez nem más, mint olyan *„új típusú információ-feldolgozási technológia, amely a különböző fajtájú adatforrásokból, különböző érzékelőkkel szerzett és különböző formátumú adatok, információk fúziós feldolgozása útján a megszerzett nyers elektronikai adatokból (meghatározott szempontok szerint csoportosított és kialakított, sűrített adathalmazokkal) összesített adatbázisokat hoz létre. Majd korábbi megbízható felderítő információkra alapozott új érték hozzáadásával, magasabb tartalmi értékkel bíró felderítési információkat szintetizál a meghatározott döntési szintű vezető számára az optimális döntések meghozatala érdekében.”*[168]

Ennek megfelelően a fúziós adatfeldolgozás a beérkezett adatokat összegyűjti, egymással a valamilyen rendező elv alapján összetartozó adatokat összehasonlítja, azokat korreláltatja, ezek eredményeit összegzi, majd a beérkező adatoknál magasabb szintű, értékesebb adatot, adatok sorozatát, azaz információt állít elő. A fúziós adatfeldolgozás célja tehát: a különböző forrásokból származó, különböző formátumban rendelkezésre álló adatokból – a döntés előkészítésben meghatározó jelentőségű – megbízható információt állítson elő.

Az adatfúziót végző szervezetnek, vagy technikai elemnek olyan feladatokat kell ellátnia, mint:

- az adatok fogadása;
- az adatok feldolgozható formába történő konvertálása;
- az adatok rendszerezett rögzítése;

[165] Kovács, L.: *Az elektronikai felderítés korszerű eszközei, rendszerei és azok alkalmazhatósága a Magyar Honvédségben*. Doktori (PhD) értekezés, ZMNE, Budapest, 2003. p. 87.

[166] Haig, Zs. – Kovács, L. – Vass, S. – Ványa, L.: *Felderítési és zavarási technikák vizsgálata. Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett integrált elektronikai felderítő és zavaró rendszerhez*, ZMNE, Budapest, 2008. p. 35.

[167] A fúzió szó *„társulás, egyesülés, összeolvadás”* jelentéssel bír eredetileg (Magyar Értelmező Kéziszótár, szerk.: Juhász József, Akadémiai Kiadó, Budapest, p. 445, 1972.)

[168] Fenyves, P.: *A rádióelektronikai felderítés és az elektronikus célobjektum tervezés hatékonyságának növelését biztosító fúziós elven alapuló adatfeldolgozási technológia vizsgálata*. Kandidátusi értekezés, Budapest, 1994. p.45.

– az adatok feldolgozása;
– az adatszolgáltatás a saját erők, ellenség, környezet vonatkozásában;
– a helyzetértékelés;
– az azonnali veszélyjelzés;
– a céltervezés;
– a felderítő erők elosztása.

A fúziós adatfeldolgozás területén számos technikai megoldás létezik. Az eddig használt és elterjedt módszerek, mint a becsléselmélet, a mintafelismerő taxonómia, vagy a Kálmán-szűrők mellett a mesterséges intelligencia fejlődésével, vagy a Fuzzy logika egyre szélesebb körű alkalmazásával új távlatok nyílnak a fúziós adatfeldolgozás területén is. Olyan adatok és adatsorok, amelyekről idáig nem volt eldönthető egyértelműségük – mert azok nem jellemeztek egy adott tényt határozott igennel vagy nemmel – is felhasználhatóak, így számottevően kibővült azoknak az adatoknak a halmaza, amelyek hozzájárulnak az információ előállításához.

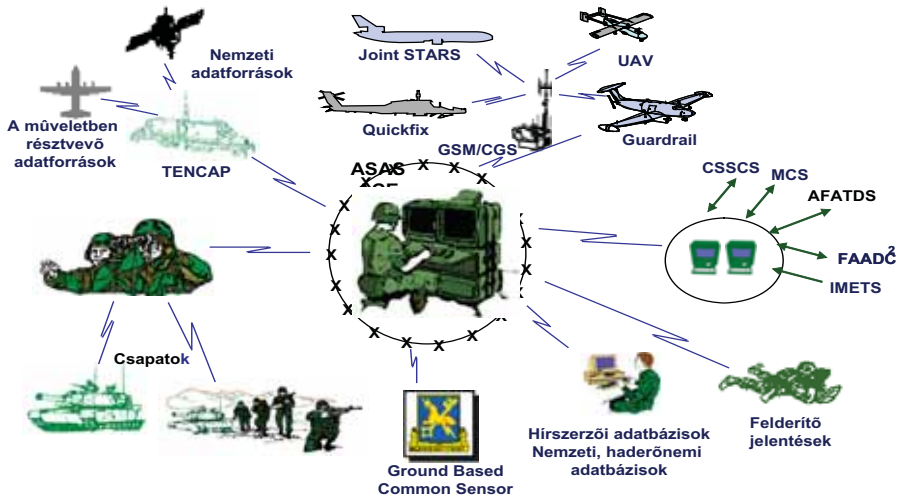
Azt az adatbázist, amelybe a fuzionált adatok és információk bekerülnek összesített fúziós felderítő adat-, és információbázisnak nevezzük. Ebből az adatbázisból kapják az illetékesek a feladatukhoz szükséges információkat. Az összadatforrású felderítő rendszer különböző méretű, képességű és funkciójú adatfúziós központokat működtet. Az adatfúziós központok alkalmazásával minden területen elérhető, hogy az illetékes parancsnok olyan információkat kapjon, amely számára fontos, és olyan rövid időn belül, amely lehetővé teszi számára, hogy időben döntsön, illetve döntési folyamatában időt nyerjen az ellenséggel szemben.

Az összadatforrású felderítő rendszer strukturális felépítése többszintű:
– első szint: adatgyűjtő szenzorok, melyek a különböző forrásból származó adatokat megszerzik;
– második szint: előfeldolgozást végző, előretolt fúziós központok, amelyek a megszerzett adatokat feldolgozható formába öntik, előfeldolgozást végeznek;
– harmadik szint: összadatforrású felderítő főközpont, amely az adatfúziós technológiát felhasználva összesített adatbázist hoz létre, és információszolgáltatást nyújt;
– negyedik szint: digitális híradó rendszer, amelyben az információkat szétosztják.

Az összadatforrású felderítő rendszer biztosítja a rendszerhez való hozzáférést a jogosultak számára, de szakjelentéseket nem készít. Ezért az információs műveletekben működő szaktiszteknek el kell sajátítani a rendszerhez való hozzáférés szakismereteit és fogásait, mivel mindenkinek magának kell az információkat összegyűjteni a közös összadatforrású felderítő adatbázisból. Példának megemlíthető az elektronikai hadviselés – mint az információs műveletek egyik összetevő elemének – felderítő támogatása, amely ugyancsak az összadatforrású fúziós központok szolgáltatásaira támaszkodik.

3.4.1 Összadatforrású felderítő rendszer (példa)

A gyakorlatban már az 1990-es évek elejétől kezdődően működnek olyan összadatforrású felderítő rendszerek, amelyek a fúziós adatfeldolgozás elvére építik fel tevékenységüket. Egy ilyen rendszer az amerikai Összadatforrást Elemző Rendszer *(All-Source Analysis System – ASAS)*, amely fúziós adatfeldolgozást használ alapul az elérhető adatforrásoktól származó nagytömegű adat feldolgozására. (A 3.13. ábra mutatja be az ASAS rendszer információs architektúráját).



3.13. ábra. **Az ASAS információs architektúrája**[169]

Az 1990-es évek elején került rendszeresítésre az Amerikai Egyesült Államok hadseregében az ASAS rendszer első, akkor még csak a kísérleti szakaszon alig továbbjutott verziója. Az ASAS rendszer rendszerfilozófiájának köszönhetően ma már a fejlődési szakasz harmadik szakaszában van.

Az ASAS egy folyamatosan fejleszthető, automatizált, számítógép-vezérelt, adatgyűjtő, adatfeldolgozó és adatmegjelenítő információs rendszer. A rendszer támogatja, segíti a parancsnokot a harc megtervezésében, megszervezésében, az információs hadviselés keretén belül gyorsan feldolgozott, nagy értékű információkat biztosít a harcról. A harctéren elhelyezett szenzoroktól kapott információkból szűrt és összegzett adatokat állít elő, így képes ábrázolni, megjeleníteni a harcmezőt. Ezen kívül pontos és időbeni célkoordinátákat biztosít, felderítési adatokat jelent, különböző támadás (fenyegetettség) előrejelző információkat szolgáltat. Az ASAS támogatja a felderítő főnök *(Military Intelligence Commander – MIC)* és a felderítő törzstisztek Felderítés- és Elektronikai

[169] Chopin, Ted – *Tradoc System Manager, Information Briefing* (Letöltve: 2014.01.15.) http://www.fas.org/irp/program/process/ASASBRF/sld009.htm (a forrás alapján szerkesztették a szerzők)

Hadviselésben (IEW) végzendő tevékenységét is. Az ASAS automatizált felderítést és információtovábbítást biztosít, amely magába foglalja az adatkezelést, a felderítő szenzorok összekapcsolását, illetve az előzetes adatfeldolgozást.

A rendszer kapcsolatban áll a Szárazföldi Erők Hadműveleti Vezetési Rendszerrel *(Army Battlefield Command System – ABCS)* az információáramlás időbeni és pontos végrehajtása érdekében. A felderítő (harctéri felderítő) szenzorokon túl a rendszer kapcsolatban áll más felderítő rendszerekkel, és ezen kívül felhasznál ügynöki felderítésből származó információkat is, illetve képes ezek továbbítására. Mindezek mellet az ASAS kapcsolatot biztosít a szárazföldi erők automatizált vezetése és irányítása, és az egyesített haderők felderítő processzorai, illetve ezek különböző elemei között. Ez teszi lehetővé a különböző felderítő egységek *(Military Intelligence – MI)* részére, hogy megfelelő prioritás mellett kielégítsék a több parancsnoki szintről érkező információigényt. Az ASAS felderítési információit gyakorlatilag a harcászati szinttől egészen az egyesített vezérkar szintig felhasználják a parancsnokok.

Az ASAS rendszer rendkívül gyors összehasonlítást végez a különböző forrásokból származó adatok között. A relációs adatbázisok közötti kapcsolata révén más felderítő szervezetek adatait is fel tudja használni az értékelés során. A rendszer „kimenetén" megjelenő adatok alkalmasak arra, hogy a parancsnok számára valós időben lehessen a harcteret megjeleníteni.

Az összadatforrású felderítő rendszerek funkcionálisan különválasztható részrendszerekből állnak. Ezek a részrendszerek egyenként és önállóan is képesek a feladatukat ellátni, de abban az esetben, ha a már elemzett technikai és eljárásbeli kihívásokra adandó válaszokat keressük, akkor ezen rendszerek összekapcsolásában rejlő potenciális erősokszorozó képességeket kell kihasználnunk. Ilyen erősokszorozó képesség lehet például az információáramlás sebességének maximális szintig történő növelése, ami nem más, mint annak az időintervallumnak a lehető legkisebb értékre történő lecsökkentése, amely az adatok megszerzéséhez, összegyűjtéséhez, feldolgozásához és felhasználóhoz való eljuttatásához szükséges. Ez a felfogás már nagyban hasonlít a hálózatközpontú hadviselés elvéhez, hiszen ott is a legfontosabb elem az idő, amely a döntéshozatali mechanizmus – a döntéshozó és a végrehajtó közötti – információáramlás sebességét növeli meg, ezáltal használva ki annak minden előnyét. A részrendszerek bár önállóan hajtják végre feladataikat, mégis tevékenységükkel más részrendszerek tevékenységét befolyásolják, így alkotva egy egész rendszert.

A következő részrendszereket találjuk a rendszer elemeiként:

- felderítő szenzorok;
- felderítő szervek, szervezetek;
- külső adatbázisok;
- fúziós adatfeldolgozó központ;
- adatelosztó rendszer.

A felderítő szenzorok és felderítő szervek szerzik és adják a bemenő információk zömét a fúziós adatfeldolgozó központ részére. Az elektronikus rendszerek elterjedésével az adatok jelentős része elektronikus formában áll a rendelkezésre. Ez digitális adatok

tömegét jelenti, de ezek a digitális adatok általában nem egy formátumban kerülnek a rendszerbe. Abban az esetben, ha egyfajta forrástípus által megszerzett adatról beszélünk – egy típusú forrásból származó adat – a probléma viszonylag egyszerű, mert ezeknek az adatoknak az összevonása, fuzionálása már szenzor szinten megtörténhet. Az adatszerző szenzorok általában saját felderítő rendszereikben előfeldolgozáson esnek át (a szenzorfúziónál említett módon és okok miatt), itt megtörténhet az első adatfúzió, és így már az egységes adat – információtartalommal – kerülhet bemenő adatként a fúziós adatfeldolgozó központba. Abban az esetben azonban, ha több típusú forrásból származó adatot kell feldolgozni, a probléma összetetté válik. Először egységes adatbázisban rögzíthető formára kell azokat alakítani.

Néhány adatformátum és a levonható következtetések:

Hang: digitalizálható, rögzíthető, archiválható. Az információtartalom kinyerése azonban egyelőre nem hatékony a hangfelismerő szoftverekkel, ahhoz továbbra is emberi elemző munka szükséges;

Írásos szöveg: az írásos szöveg szkenneléssel és karakterfelismeréssel hatékonyan digitalizálható. Ez azonban csak a digitális szöveg eléréséhez elegendő. Az írásos digitális szöveg feldolgozására szolgáló szoftverek fejlesztései kezdeti szakaszban vannak. A szövegekben való keresés a kereső szoftverekkel hatékonynak mondható. A keresést az első időkben a HTML *(Hyper Text Markup Language)* nyelv adta lehetőségek kihasználásával oldották meg, úgynevezett kulcsszavakat – az adott szövegre, vagy HTML oldalra legjellemzőbb szavakat – jelöltek ki, amelyeket a kereső szoftverek regisztráltak. Ma már a kereső robotok (szoftver robotok) nemcsak a HTML kódban megjelölt, vagy a szövegben meglévő kulcsszavakat, hanem összefüggéseket, fogalmakat is képesek kezelni.

Az írott, digitális formában rendelkezésre álló dokumentumok feldolgozásának egy másik – nagy újdonságot jelentő – módszere, hogy egy szoftver a dokumentumban előforduló földrajzi helyekre vonatkozó adatokat keres. (Ezek meglehetősen gyakoriak például az írásos felderítő jelentésekben.) Amennyiben a földrajzi helyre, koordinátarendszerre, illetve ezekhez logikailag kapcsolódó adatra bukkan, azt egy digitális térképen megjeleníti.[170] Így megteremti annak a módszerét, hogy nemcsak összekapcsolja a különböző formátumban rendelkezésre álló felderítési adatokat, de valamilyen szinten transzformálja is azokat.

Kép: A kép formátumban rendelkezésre álló adatok óriási jelentőségű információhordozónak számítanak. Az elmúlt 20 év háborúit és fegyveres konfliktusait figyelembe véve kijelenthető, hogy a képi információk elengedhetetlenek a siker eléréséhez. Az elektrooptikai felderítő eszközök széles körű térhódításával a képi információk nagy része elektronikus, digitális formában áll rendelkezésre. Egy nagyfelbontású kép azonban óriási mennyiségű adatot takar, amely továbbítása megfelelő adatátviteli kapacitást igényel. A műholdak megjelenésével, illetve az azokon elhelyezett multispektrális kamerák fejlő-

[170] John, F.: *Honing in Trouble. New Geosearch software accelerates comprehensive intelligence analysis*. ISR, 2003 september-october, p. 32.

désével kialakult a technikai és technológiai háttere a képi információ adathalmazként való továbbításának és feldolgozásának. A multispektrális felvételek általában úgynevezett BIL *(Band Interleaved by Line)*, azaz vonalanként beszúrt sávok formátumban kerülnek továbbításra. A feldolgozás első lépése az importálás és a feldolgozáshoz szükséges formátumba való konvertálás. Ehhez a képi információt hordozó adatsorokon kívül szükség van egy – általában a földrajzi koordinátákat leíró – kiegészítő fájl megküldésére is. E két adatsorból egy importáló és transzformáló szoftver előállítja a feldolgozás alapjául szolgáló földrajzilag elhelyezett képet, vagy például a multispektrális érzékelő esetében több – az érzékelt tartományok számával megegyező – képeket, amelyek alapján az értékeléshez szükséges RGB (*Red, Green, Blue* – vörös, zöld, kék, amely a három alapszín) kép nyerhető. Az értékelés – a redundanciák megszüntetése, a szűrőkkel történő leválogatás – után következhet. Napjainkban már meglehetősen sok képfeldolgozó szoftver áll a rendelkezésre, amelyek vektoros, raszteres, és attribútum értékek alapján dolgozzák fel a képi információt. Az ilyen fájlkezelés lehetővé teszi a kép adatainak adatbázisban történő rögzítését, illetve ezek összekapcsolását más adatokkal. A GIS alapra helyezett képfeldolgozás – például az ortofotóból előállított háromdimenziós terepmodell – hatalmas jövő előtt áll, és az ilyen módszerek alkalmazása a felderítő munka, különösen az elemzés és értékelés, valamint a megjelenítés területein jelenthet jelentős előrelépést.

Videokép (Mozgókép): Óriási előnye az állóképhez képest, hogy ezzel folyamatosan, dinamikájában lehet követni az eseményeket, és lehet így valós idejű információhoz jutni. Mindenképpen hátrány azonban, hogy a jó minőségű mozgókép átviteléhez szükséges a szélessávú kommunikációs,[171] vagy adatátviteli csatorna megléte.[172]

Külső adatbázisok: az összadatforrású felderítés minden olyan külső adatbázist is fel tud használni bemenő információforrásként, amely bár nem az adott katonai szervezet fenntartásában van, mégis tartalmazhat olyan adatokat, információkat, amelyek a végrehajtandó felderítési feladatban alapadatként jelentkezhetnek. Általában és jellemző módon a relációs adatbázis típust találhatjuk a legtöbb helyen.

Ilyen adatbázisok lehetnek:

- nemzeti adatbázisok;
- nemzetközi adatbázisok;
- szövetséges adatbázisok;
- NATO adatbázisok;
- polgári titkosszolgálatok adatbázisai;
- elektronikus könyvtárak.

[171] A jó minőségű átviteli mód például az ATM *(Asyncronous Transfer Mode)*, azaz az aszinkron, csomagkapcsolt átviteli mód, amely 25 Mbit/s-től egészen az elméletileg elérhető 2,5 Gbit/s adatátviteli sebességig képes adatokat továbbítani.

[172] Ez annak ellenére igaz, hogy a digitalizált mozgókép tömöríthető, ugyanis az 1/25 másodpercenként egymást követő képek az esetek többségében csak nagyon kismértékben térnek el egymástól, ezért felesleges minden kép minden információját átvinni, elegendő a változások követése, amelyekből a dekódolás során korrekcióval elő lehet állítani az eredeti mozgóképpel majdnem azonos minőségű képet.

Az adatbázisok közötti információcserének egyik elengedhetetlen feltétele az interoperabilitás, az azonos gépi nyelv, vagy a struktúrák eltérősége esetén azok konvertálhatósága. Mindezeket a rendszer tervezésénél figyelembe kell venni.

Fúziós adatfeldolgozó központ felépítése a következő:

Hardver: modul rendszerűen felépített, szállítható, alapvetően katonai kivitelre épülő elemek összessége. A folyamatos fejleszthetőség itt is igen fontos tényező, amely azonban nemcsak a hardver oldali technikai fejleszthetőség kérdését jelenti, hanem annak a problémának a legmesszebbmenőkig való figyelembevételét, hogy az új hardverelemek, illetve a már futó szoftverelemek képesek-e az együttműködésre. Ez különösen fontos abban az esetben, ha folyamatos, vagy kvázi folyamatos működés az elvárás a rendszerrel szemben.

Szoftver: szintén követelmény a folyamatos fejleszthetőség, amely a kompatibilitási kérdéseket hasonlóan tartalmazza, mint a hardver.

Az ASAS elemzéséből levonható egyik igen fontos következtetés, hogy kezdetben a központi munkaállomások, illetve a felderítő és adatgyűjtő rendszerekben meglévő eszközök, vagy rendszerek eltérő operációs rendszereket használtak.[173] Ennek következtében kompatibilitási problémák keletkeztek, amelyek például az elküldött jelentések feldolgozásában jelentkeztek, azaz a Unix alatt futó alkalmazások nem tudták a Windows applikációkat kezelni.

Fontos kérdés a GIS platform egységessége, illetve eltérő volta esetén az adatok, vagy információk konvertálhatósága. Ez azt is feltételezi, hogy van olyan szerv, vagy szervezet, amely biztosítja, és folyamatosan frissíti mindazon digitális térképeket, domborzati modelleket, amelyeket a központ működése során felhasznál.

Ma már elengedhetetlen kérdés a szoftverek esetében is a biztonság. Azon kívül, hogy megbízható működést kell, hogy jelentsenek a felhasznált szoftverek, biztosítaniuk kell a külső, illetve a belső illetéktelen hozzáférés, az illetéktelen adatbevitel elleni védelmet. Erre többféle elterjedt – katonai szabványokban és szabályzókban megjelent – megoldás létezik Ezek kialakításakor azonban nem szabad figyelmen kívül hagyni, a külső – szövetséges vagy nemzeti – rendszerek hasonló megoldásait, a kompatibilitás és az együttműködés biztosítása érdekében.

Megjelenítés: A számítógép információinak hagyományos megjelenítő eszköze az ember számára teszi érthetővé mindazokat az információkat, amelyeket ki akarunk nyerni a feldolgozás után. Ezek a hagyományos eszközök:

- monitorok;
- kivetítők;
- projektorok;
- nyomtatók;
- plotterek.

[173] A központi munkaállomások Unix, más csatlakozó felderítő rendszerek, pedig például Windows alapú operációs rendszereket üzemeltettek.

Ezek különféle konfigurációban összeállíthatók, a feladatnak megfelelően a kívánt méretben és felszerelésben. A feldolgozó munkahelyeken, a hagyományos monitorokon kívül általában helyet kapnak – hasonlóan a hagyományos vezetési pontokhoz – azok a nagyméretű kivetítők, vagy projektorok, amelyeken a munkavégzés áttekintéséhez szükséges információk jeleníthetők meg. Ilyenek például a térképek, helyzetvázlatok, videoképek.

Ezek azonban csak két dimenzióban képesek az információkat megjeleníteni. A jövő igen perspektivikus megoldásai lehetnek ezen a téren azok a rendszerek, amelyek a virtuális valóság eszközeit használják fel nemcsak az információk megjelenítéséhez, hanem a katonai vezetés feladatai közül egyre többet egy időben felvállalva. Ilyen – a virtuális valóság elemeire épülő – rendszer például a virtuális vezetési pont.[174] Ez nem csak az adatok megjelenítésére képes, hanem a vezetés egészének virtuális térbe helyezésével számol. A virtuális vezetési pontok több, egymástól fizikailag távol lévő vezetési pontok összességéből alakulnak ki. „*A virtuális vezetési pont több funkcionális helyiségből épül fel, amelyek önmagukban is egy-egy önálló – akár a többiektől teljesen független – virtuális környezetet képeznek*."[175]

A parancsnok és a más-más helyen lévő csapatok audio- és videokonferencia vonalakon tartják a kapcsolatot. Az audio-, a valós idejű videokapcsolat, a háromdimenziós terepmodell, a digitális térképi alap összességében megjeleníti a virtuális teret, illetve a virtuális valóságot, minden egyes résztvevő saját számítógépén egységes formában. A résztvevők egymás 3D-s virtuális mását is látják ebben a térben. A parancsnok így „személyesen" láthatja a munkatársakat, illetve lehetősége van a közös munkavégzésre anélkül, hogy fizikailag egy helyen lennének.

[174] A virtuális vezetési pont egyik kidolgozója és kutatója a Lionhearth Ltd. volt, amely e fejlesztése mellett számos a virtuális valósággal kapcsolatos projektben részt vesz.

[175] Munk, S.: *A közös munkavégzés új lehetőségei a virtuális vezetési pontokon*. Új Honvédségi Szemle, 2000/2. p. 40.

4. FEJEZET

Elektronikai ellentevékenység

A korszerű hadseregek hadrafoghatósága, a fegyverzet alkalmazhatósága, a vezetés szilárdsága alapvetően függ a vezetési és fegyverirányítási rendszerekben üzemelő elektronikai eszközök megbízható, rendeltetésszerű működésétől. Mivel sem a csapatok vezetése, sem a fegyverzet alkalmazása nem képzelhető el a megfelelő elektronikai berendezések nélkül, ezért napjainkra a hadviselő felek elgondolásaiban elsőrendű fontosságot kapott az ellenség elektronikai rendszerei ellen folytatott harc, illetve a saját rendszereink megóvásának kérdése.

Ezen fejezet azt foglalja össze, hogy az elektronikai hadviselésnek milyen ellentevékenységi módszerei, eljárásai, technikái és alkalmazási elvei állnak rendelkezésre az ellenséggel folytatott küzdelemben.

Definíció szerint*: „Az elektronikai ellentevékenység az elektronikai hadviselés azon területe, amely magába foglalja az elektromágneses és egyéb irányított energiák kisugárzását abból a célból, hogy megakadályozza vagy csökkentse az elektromágneses spektrum ellenség által való hatékony használatát.*"[176]

Az elektronikai ellentevékenység más szóval a frekvenciaspektrum feletti uralom megszerzésére irányuló erőfeszítések, rendszabályok és technikai eszközök összessége.

Az elektronikai ellentevékenységnek három fő területe van:

- az elektronikai zavarás;
- az elektronikai megtévesztés;
- és az elektronikai pusztítás.

4.1 Az elektronikai zavarás

„Az elektronikai zavarás az elektromágneses energiának szándékos kisugárzása, visszasugárzása vagy visszatükrözése azzal a céllal, hogy korlátozza vagy megakadályozza az ellenség által használt elektronikai eszközök, berendezések és rendszerek rendeltetésszerű működését."[177]

Az elektronikai és más zavarok olyan fizikai sugárzások, melyek megnehezítik, vagy kizárják az elektronikai eszközök útján továbbított hasznos jelek vételét és az információk kiválasztását. A berendezések vevőegységére hatva az elektronikai zavarok torzítják a megfigyelt és a végberendezés által rögzített jeleket, információkat, megnehezítik, illetve

[176] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína. MH HVK, 2005. p. 8.
[177] U.o.

kizárják a rádióforgalmazás lehetőségét, az adatátvitelt, a cél felderítését, csökkentik a felderítő eszközök megkívánt hatótávolságát és az automatizált vezetési rendszerek pontosságát, megtévesztik a kezelőket.

4.1.1 Az elektronikai zavarok osztályozása

Az elektronikai zavarok eredetük, keletkezési módjuk, kifejtett hatásuk, jellegük, frekvencia-, és időtartománybeli paramétereik, valamint még sok más műszaki jellemzőjük szerint osztályozhatóak. Keletkezésük szerint megkülönböztethetünk természetes és mesterséges elektronikai zavarokat.

4.1.1.1 Természetes elektronikai zavarok

A természetes elektronikai zavarok a természeti folyamatok által létrehozott elektromágneses és akusztikus zavarok. Lehetnek atmoszférikus, kozmikus, illetve a Föld körüli térség elektromágneses sugárzásából eredőek.

Atmoszférikus elektronikai zavarokat az atmoszférában lejátszódó elektromos folyamatok, főleg a légköri kisülések, villámlások keltenek. Az előfordulás helyén igen nagy teljesítményűek, nagy távolságra is észlelhetők. Hatásuk a 20 MHz alatti frekvencia tartományban jelentős. Előfordulási gyakoriságuk a földrajzi és éghajlati viszonyoktól, valamint az évszaktól függ. Az elektronikai eszközök villámvédelme rendszerint kellő védelmet nyújt a túl nagy teljesítményű hatás ellen. Az információközlésre gyakorolt hatásuk felismerhető, kiküszöbölhető, így zavaró hatásuk nem jelentős.

A kozmikus elektronikai zavarokat a nap, a csillagközi tér, az egész galaktika rádiósugárzása hozza létre. Időszakonként (nap, év) jelentősen változó erősségű. Rövid időszakokban és egyes frekvenciákon, vagy frekvenciasávokban egyenletesek, de lehetnek változó erősségűek is. Viszonylag tartós hatásúak. Főleg a 30-300 MHz frekvencia tartományban észlelhetők és kellő gyakorlattal a legtöbb esetben felismerhetők. Az antennával és a teljesítménnyel manőverezve hatásuk csökkenthető.

A Föld körüli térség szporodikus elektromágneses sugárzásából eredő elektronikai zavarokat az ionoszférában, magnetoszférában lévő töltött részecskék áramlása, továbbá a sarki fény rádiósugárzása, a Föld sugárzó övezetei, a meteor képződmények, valamint a Föld és a víz felszíneinek elektromágneses tükrözése kelti. Hatásuk a 30-500 MHz közötti frekvencia tartományban észlelhető. Az adott települési helyre jellemző tulajdonságaik felismerhetők. A települési hellyel, teljesítménnyel, antennával történő helyes manőverezés útján hatásuk csökkenthető.

4.1.1.2 Mesterséges elektronikai zavarok

Mesterséges elektronikai zavarok az elektromágneses hullámok energiáját tükröző visszaverők, illetve az elektromágneses rezgéseket kisugárzó berendezések által keltett zavarok, melyek akadályozzák egy meghatározott műszaki jellemzőkkel rendeltetésszerűen mű-

ködő elektronikai eszköz normális üzemét. A meghatározásból következően az előállítás módjától függően megkülönböztethetünk passzív és aktív zavarokat.

Passzív elektronikai zavarokat reflexió útján, valamely elektromágneses energiát visszaverő objektum, tárgy hozhat létre. Bármely frekvencián előfordulhat. Jellege, hatása változó lehet mind térben, mind időben és frekvenciánként. Az ilyen elektronikai zavarok ellen – többféle lehetőséget kihasználva (például teljesítmény, antenna, üzemmód, üzemi frekvencia változtatása, aktív zavarszűrő áramkörök) – védekezni lehet.

Aktív elektronikai zavarokról beszélünk, ha azokat elektromágneses rezgéseket előállító berendezés (adó) sugározza ki.

A kisugárzás célja és szándéka szerint megkülönböztetünk:

– nem szándékos; és
– szándékos zavarokat.

A nem szándékos elektronikai zavarok tekinthetők a működésből adódóan természetes eredetűnek, vagyis ha olyan elektromágneses sugárzásokról van szó, amelyeket a berendezések rendeltetés szerinti normális, illetve technikai hiba következtében hoznak létre. Ilyenek például:

– az ipari eredetű elektronikai zavarok;
– a konstrukciós eredetű elektronikai zavarok;
– az elektronikai eszközök kölcsönös zavarai (rádiófrekvenciás interferencia).

Ipari eredetű elektronikai zavarok a különböző elektromos berendezésekben, elektromos hálózatokban termelődő elektromágneses és akusztikus kisugárzások, amelyeket a gyors áramváltozások, a szikrázás, a rossz szigetelések, továbbá a gázok ionizációs, nagyfeszültségű és nagyfrekvenciás rezgéseket előállító berendezések keltenek. Igen széles frekvenciasávban hatnak (0-1 GHz). A térerősségük főleg nagyvárosi környezetben jelentős. Hatásukat a zavarforrásnál alkalmazott rendszabályokkal és elektromos zavarszűrőkkel csökkentik. A védekezés leghatásosabb módja az ilyen zavarforrástól távol település.

Konstrukciós eredetű elektronikai zavarok az adott elektronikai berendezés belső zajai, a felhasznált csövek, félvezetők és más elektronikus elemek, kapcsolások, működési sajátosságaiból eredően keletkeznek. Ezek lehetnek berendezés eredetű termikus zajok, csőzajok, hálózati zajok, modulációs, rendszer eredetű, intermodulációs és távíró torzítások.

A berendezés eredetű zavarok hatása főleg 15 MHz felett, az adott vevőkészülék alapérzékenységének meghatározója. A kívánt alacsony szinten tartása csak a gondos tervezéssel, alacsonyzajú alkatrészek beépítésével, a szűrt táplálással, esetleg mesterséges hűtéssel, az előírt üzemeltetési paraméterek betartásával biztosíthatók.

Elektronikai berendezések közötti kölcsönös elektronikai zavarokról vagy rádiófrekvenciás interferenciáról beszélünk, amikor egy időben azonos frekvencián, vagy különböző, de egymásra ható frekvenciákon kisugárzó eszközök hatást gyakorolnak egy adott helyen és üzemi frekvencián működő berendezésre. Hatása már két üzemelő eszköz esetén is felléphet, de általában ott kell vele számolni, ahol kis területen, nagy számban üzemeltetnek elektronikai eszközöket. Az ellene való védekezés az elektromágneses kompati-

bilitási (EMC) rendszabályok betartásával lehetséges, ami igen széles területet ölel fel és alapvetően az elektronikai védelem kérdéskörébe tartozik.

A szándékos, vagyis mesterségesen, adott hatásmechanizmusú elektronikai zavarás céljából létrehozott jelstruktúrák a megcélzott elektronikai berendezések normális működésének akadályozására, megbontására vagy befolyásolására létrehozott elektromágneses kisugárzások.

A szándékos elektronikai zavarok is tovább osztályozhatók a hatásjellemzők, a hatékonyságuk, a spektrum viszonyok és rávezetés szerint, valamint a sugárzási és egyéb műszaki jellemzők alapján. A hatásjellemzők szerint megkülönböztethetők álcázó és imitáló elektronikai zavarok.

Az álcázó elektronikai zavar torzítja a vett jel struktúráját és megnehezíti, vagy teljesen kizárja a vevőkészülékek számára az információ kiválasztásának, a jel szükséges paramétereinek mérési lehetőségét. A zavar teljesítményének növelésével az álcázó hatás is növekszik. Általában az álcázó zavar a vevő bemenetén lineárisan összegződik a hasznos jellel, azért összegző, azaz additív zavarnak is nevezik.

Az imitáló elektronikai zavarok megtévesztő, dezinformáló céllal kialakított jelek, amelyeket a hasznos jelhez hasonló sugárzásként érzékelnek a zavart elektronikai eszközök. A vevőben olyan hamis detektált jelet, illetve célkijelzést hoznak lére, amely a tényleges hasznos jelre hasonlít, vagy vele azonos. Az ilyen zavar csökkenti a csatorna áteresztő képességét, elvész a hasznos információ egy része, megnő a vaklárma, a hamis riasztások valószínűsége; a fegyverirányító rendszerekben – megszakítva, illetve átvéve a távolság, a sebesség, vagy az irány szerinti automatikus követést –, a rendszert a rádiózavar által okozott hamis célra vezeti át.

Az aktív, szándékos elektronikai zavarokat a vett hasznos jelekre gyakorolt hatásuk hatékonysága szerint három csoportba sorolják: gyenge, közepes és erős. A hatékonyság e három csoportját a vevő bemenetén a hasznos információkban keletkezett veszteség mértéke és a katonai eszközök harcfeladatának teljesítésére gyakorolt hatása alapján állapítják meg.

Gyenge elektronikai zavarok energiaszintje a vétel pontjában nem nagyobb a hasznos jelnél, az információ mintegy 15%-a vész el. Ez katonai szempontból a berendezés harcfeladatának teljesítését lényegesen nem befolyásolja.

A közepes elektronikai zavarok energiaszintje egyenlő, vagy nagyobb a hasznos jelek energia szintjénél a vétel pontjában. Az ilyen erősségű zavarok hatására a hasznos információnak legalább 50 %-a elvész. A harcfeladat teljesítésének lehetőségét lényegesen csökkenti.

Az erős elektronikai zavarok energiaszintje jelentősen túlhaladja a hasznos jelek energia szintjét a vétel pontjában. Hatásukra a hasznos információ több mint 75 %-a vész el. Az eszköz a harcfeladatát teljesíteni nem tudja.

Lényeges megjegyezni azonban azt, hogy a zavartatás mértékére és tényleges hatására a vett hasznos jel és a zavaró jel térerősségének aránya nem ad egyértelmű összefüggést, mivel a korszerű üzemmódok, jelfeldolgozási eljárások éppen ezt a zavarállóságot hivatottak nagymértékben javítani. Minden esetben meg kell vizsgálni az adott üzemmódra jellemző zavartűrési értékeket és az optimális zavarjel struktúráját.

Az elektronikai zavarok különböző amplitúdójú frekvencia összetevői a hasznos jelekhez hasonlóan a frekvencia tartományban különböző sávot foglalhatnak el. Rávezetésük a hasznos jelre, illetve a hasznos jel frekvenciasávjához való viszonyuk különböző lehet. A zavarok és a zavarandó hasznos jelek spektrumainak egymáshoz való viszonyától, és a zavar rávezetés módjától függően az aktív álcázó elektronikai zavarok lehetnek célzottak, szélessávúak, vagy csúszók.

A célzott, vagy keskenysávú elektronikai zavarok spektruma összemérhető (egyenlő, vagy 1,5-2-ször nagyobb) a zavart elektronikai eszköz hasznos jelének spektrumával. Mivel a zavarás hatékonysága függ a frekvenciasávok pontos egybeesésétől, a spektrális teljesítmény sűrűségtől és a vevőben alkalmazott jelfeldolgozás módjától, ezért célravezető a nagy spektrális teljesítmény sűrűség létrehozása.

A célzott zavarást éppen a nagy spektrális teljesítmény sűrűség jellemzi. Mivel a zavaró jelet keskeny frekvenciasávban sugározza ki a zavaró adó, ezért az lehet viszonylag kis teljesítményű is, ugyanakkor igen pontos frekvencia szerinti egyeztetésre van szükség, ami adott esetekben csak bonyolult módon valósítható meg.

A szélessávú elektronikai zavarok spektruma jelentősen nagyobb, mint a zavart eszköz hasznos jeleinek spektruma. A zavaró adó így egyszerre több, közeli frekvencián üzemelő berendezés zavarására alkalmas pontos frekvenciakövető, áthangoló berendezés nélkül. Az ilyen zavaráshoz általában nem kell pontosan ismerni a zavart berendezések adásjellemzőit, azért a szélessávú zavaró adók felépítése lényegesen egyszerűbb lehet. Ugyanakkor a szélessávú zavarás sajátossága, hogy egy adott zavarteljesítménynél a spektrális teljesítménysűrűség G_{ZAV} (W/MHz) a zavaró jel sávszélesség növekedésének arányában csökken.

$$G_{zav} = \frac{P_{zav}}{\Delta f_{zav}} \tag{4.1.}$$

ahol: P_{zav} – a zavaró adó teljesítménye [W];
Δf_{zav} – a zavaró jel sávszélessége [MHz].

Mivel a szélessávú zavarásnál a zavarjel energiája eloszlik az adott frekvenciasávban, ezért a keskenysávban dolgozó egy-egy zavart állomás vevőjére az összes energia csak egy kis része jut. A hatékony zavaráshoz szükséges nagy teljesítménysűrűség tehát csak nagy adó teljesítmény előállítása árán biztosítható.

Csúszó elektronikai zavarok a keskenysávú zavaró adó jelének széles frekvenciasávban történő gyors áthangolgatásával hozhatók létre. A rendszerint automatikus gyors áthangolás eredményeként a széles frekvencia sávban minden csatornán (több csatornás berendezések esetében), illetve minden, a zavarás frekvenciasávjába eső berendezés bemenetén egymás után gyorsan ismétlődve kellő nagyságú teljesítménysűrűség képződik. A gyors áthangolással átfogott frekvenciasáv lényegesen nagyobb a zavart vevő által vett hasznos jel sávszélességénél. Az áthangolási gyorsaság helyes megválasztásával elérhető, hogy a zavart berendezés vevője nem tudja a hasznos jelet feldolgozni az egymás után ismétlődő csúszó zavarástól.

Az aktív, szándékos elektronikai zavarok osztályozhatóak sugárzási és műszaki paramétereik alapján. Sugárzási jellemzőik szerint ezek lehetnek folytonos vagy impulzus üzeműek. Műszaki jellemzőik szerint mindkettő lehet modulálatlan, vagy modulált.

A modulálatlan aktív elektronikai zavaroknak két fő csoportja különböztethető meg. Az egyik a nagyfrekvenciás vivőjel közvetlen kisugárzása zavarás céljából, a másik a zajzavar rádióadó által történő kisugárzása. Az első esetben az adóberendezés által kisugárzott nagyfrekvenciás vivőhullám amplitúdója, frekvenciája, fázisa gyakorlatilag változatlan, mivel szándékosan nem változtatja meg semmilyen moduláló jel, a zajzavarok kisugárzásakor pedig az amplitúdó, a frekvencia és fázis bizonyos fizikai határok között véletlenszerűen fluktuál.

A zajzavarok az elektronikus elemek által előállított – azokon gerjesztett – természetes zajok teljesítményének felerősítése és kisugárzása révén hozhatók létre. A gyakorlatban sávkorlátozott fehér-zaj előállítására törekszünk, amely olyan sztochasztikus villamos jel, amelynek teljesítmény sűrűség spektruma bizonyos frekvenciatartományban (f_1-től f_2-ig) állandó, azon kívül pedig zérus.

Lényegesen jobb eredményt lehet elérni a nem normál eloszlású zajokból kialakított zajzavarral, mivel ezek sokkal univerzálisabbak. Eredményesen alkalmazhatók bármely adásmód, illetve bármilyen rendeltetésű rádiólokátor, navigációs rendszer, zavarással történő lefogására. Az ilyen zajzavarok képezik az álcázó zavarási eljárások alapját.

A folytonos üzemű, modulált rádiózavarok a zavaró adó által előállított vivőhullám egy, vagy több paraméterének megváltoztatásával állíthatók elő. A modulációs paramétertől függően megkülönböztethetők:

– amplitúdó modulált;
– frekvencia modulált;
– fázis modulált;
– és kombinált modulációjú jelek.

Valamennyi modulációs mód tovább csoportosítható attól függően, hogy a moduláló jel harmonikus rezgés, vagy zaj.

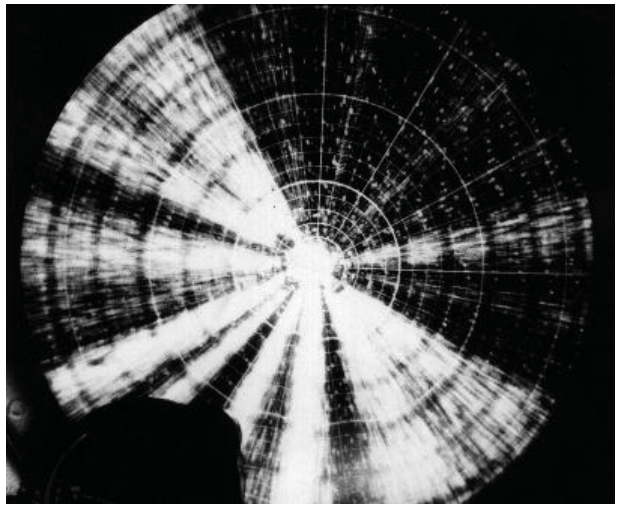
Az amplitúdó modulált folytonos elektronikai zavaroknál a zavaró adó által előállított vivőjel amplitúdója változik a moduláló jel-zaj függvényében. Ha a moduláló zaj spektrális sűrűsége állandó, akkor az előállított modulált nagyfrekvenciás rezgés spektrális teljesítménysűrűsége is állandó lesz, spektrumszélessége pedig kétszerese a moduláló jel frekvenciatartományának. A kimenő jel spektruma magába foglalja a vivőfrekvenciát és a két oldalsávot.

A rádiólokátorok indikátorán az ilyen zavarok hullám alakkal telített világos sávot hoznak létre, melynek mérete a moduláló frekvencia értékétől függ. A térképező típusú indikátorokon az amplitúdó modulált elektronikai zavarok radiális irányban elhajló világos szektorokat hoznak létre. Ha a zavarjel energiája elégséges a rádiólokátor antennájának oldalnyalábjain való vételhez, akkor az indikátoron több zavart szektor is kialakulhat. (4.1. kép)

A frekvencia modulált folytonos elektronikai zavarok olyan csillapítatlan harmonikus vivőrezgések, melyeknek frekvenciája változik meg egy moduláló harmonikus alacsonyfrekvenciás rezgés vagy zaj függvényében. A kialakított zavaró jel teljesítménye a moduláló jel frekvencialöketének kétszeres értékével azonos sávszélességben oszlik el. Igen hatékony zavaró jel struktúra érhető el, ha a moduláló jel változó amplitúdójú zaj és

a maximális löket megfelel a zavarandó csatorna sávszélességének. Nehézséget ez esetben ismét csak a frekvenciahangolás pontossága és stabilitása jelenthet.

A fázismodulált folytonos elektronikai zavarok olyan csillapítatlan harmonikus nagyfrekvenciás rezgések, amelyek pillanatnyi fázisa változik a moduláló jel függvényében. Az ilyen típusú modulációval előállított elektronikai zavarok közül elsősorban, a zajjal fázisban moduláltaknak van gyakorlati jelentősége.



4.1. kép. **Aktív zavar a rádiólokátor indikátorán**[178]

A korszerű, több adásmódban működő elektronikai berendezések működését eredményesen lefogni egyetlen modulációs módban üzemelő zavaró adóval általában már nem lehet. Ezért a gyakorlatban a rádió hírközlő, rádiólokátor, és rádió-navigációs rendszerek lefogására tervezett speciális zavaró adókban több, különböző modulációs módot alkalmaznak. Ilyenek a kombinált amplitúdó-frekvencia, illetve az amplitúdó-fázis modulációk. Ezeknél a kombinált modulációknál a kívánt sávszélesség és hatékonyság (viszonylag nagy teljesítménysűrűség előállítása közel egyenletes amplitúdó eloszlással) biztosítása érdekében az egyes modulációs módok előnyeit igyekeznek kihasználni.

Impulzus modulációt alkalmazó zavaró berendezések adói nagyfrekvenciás impulzusok formájában sugározzák ki a zavaró jeleket. Az impulzus moduláció során az időnek csak egy kis részében van kisugárzás. Az adás-szünet időbeni arányát kitöltési tényezőnek nevezzük, és úgy számolhatjuk ki, hogy az impulzus szélességét elosztjuk az impulzus ismétlődési idővel.

Adott átlagteljesítménnyel üzemelő adóberendezés impulzus üzemben jóval nagyobb csúcsteljesítmény előállítására alkalmas, ami az energiaviszonyok szempontjából lesz kedvező. A csúcsteljesítmény értékét megkapjuk, ha az átlagteljesítményt elosztjuk a ki-

[178] Forrás: a szerzők archívuma.

töltési tényezővel. Természetesen nem minden adóberendezés alkalmas impulzusüzemű működésre.

A zavaró impulzusok a folytonos elektronikai zavarokhoz hasonlóan lehetnek modulálatlanok és moduláltak. Az impulzus amplitúdójának, ismétlődési frekvenciájának, az impulzus időtartamának, illetve ezek közül néhány paraméternek egyidejű modulálásával elérhető, hogy a hasznos jel impulzusa és a zavaró jel a vevő számára nehezen, vagy egyáltalán nem különböztethető meg.

A hasznos és a zavaró impulzusok egymáshoz képest lehetnek szinkronban, vagy lehetnek aszinkronok.

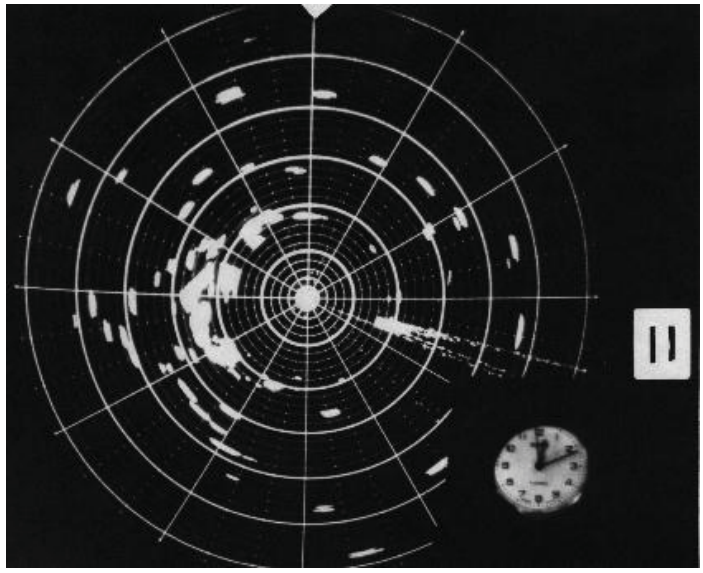
Szinkron impulzus zavarokról akkor beszélünk, ha a zavaró jel a hasznos jel ismétlődési frekvenciájával, vagy annak többszörösével (törtrészével) megegyező ismétlődési frekvenciával rendelkezik. Ekkor a hasznos jelek között a zavarjelek „állni látszanak".

Aszinkron zavarjelek esetén a két ismétlődési frekvencia között nincs többszörösségi kapcsolat, például a zavarjel ismétlődési frekvenciája szabálytalanul változik. Ekkor a zavarjelek fluktuálnak, „vándorolnak" a hasznos jelek között. A két változat között akkor kell dönteni, amikor az elérendő zavarási hatást kívánjuk megtervezni. Az indikátor képet kipöttyöző álcázó zavar létrehozására az aszinkron, míg célok imitálására pedig szigorúan szinkron zavarokat lehet használni.

Mindkettő lehet szabadon gerjesztett, vagy visszasugárzott válaszimpulzus. A válaszimpulzus is lehet egyszeres, vagy többszörös. A válaszimpulzus zavarok előállítása igen bonyolult feladat, mivel a mindenkori impulzus paraméterekhez hasonló impulzust kell előállítani. Ezért meg kell határozni a zavarni kívánt berendezés impulzusparamétereit, elemezni kell őket és a mért paramétereknek megfelelően kell a zavaró jel paramétereit beállítani. Az ilyen rendszerű zavaró berendezések fontos paramétere a jelfeldolgozási idő, hiszen a válaszjelet reális időkapuba kell bejuttatni, mintha az valós célról érkezett volna. A szabadon gerjesztett impulzus zavarok előállítása a zavaró adó bekapcsolása után a zavarandó berendezés jeleitől függetlenül megindul és a tervezett (beállított) paraméterekkel a kikapcsolásig kisugárzásra kerül. Ez a konstrukció önmagában csak ritkán hatékony.

Egyszeres válaszimpulzus zavar esetén a zavaró adó minden egyes hasznos impulzus vétele után, – arra válaszolva – bizonyos időeltolódással kisugároz egy zavaró, hamis impulzust. Arra kell törekedni, hogy a válaszimpulzus minden paramétere (például moduláció, időtartam, teljesítmény) a legjobban megközelítse az adott paraméterekkel rendelkező célobjektumról egyébként ilyenkor visszaverődő impulzus paramétereit. Rendeltetésétől függően, a visszasugárzott jel álló vagy mozgó célt is imitálhat.

Többszörös válaszimpulzus zavaroknál a zavaró adó minden egyes hasznos impulzus vétele után, válaszként bizonyos időeltolódással egymás után több zavaró impulzust, impulzussorozatot állít elő és sugároz ki. Az ilyen többszörös válaszimpulzus zavarok is a vett impulzus paraméterei szerint automatikusan változnak a mérés eredményeként, és így hasonlóak a zavart állomás hasznos jeleihez. A rádiólokátor rendszerekben az ilyen többszörös válaszzavarok az indikátoron több hamis célt hoznak létre. A célok imitálásán túl, elsősorban a fegyverirányító eszközök követő rendszereiben lehet impulzus zavarokkal helytelen működést előidézni. (4.2. kép)



4.2. kép. **A válaszimpulzus zavar megjelenése a rádiólokátor indikátorán**[179]

Az úgynevezett *elhúzó válaszimpulzus zavarok,* átvéve a célról visszavert valódi jel szerepét, magukra vonják a távolsági, vagy oldalszög követő rendszert, és a valódi céltól különböző csúszó időparaméterek bevitelével elvezetik a követő rendszert egy valóságban nem létező célra, más irányba.

Az irány szerinti automatikus követő rendszerek zavarásának fontos kritériuma, hogy a zavaró teljesítmény sokkal nagyobb legyen a jel teljesítményénél. Ezen zavarórendszerek előnyösen alkalmazhatóak úgy fedélzeten, mint földi állomásokon. A fedélzeti eszközök a rakéta-rávezető rendszerek hatékonyságát csökkenthetik, a földi zavaró állomások pedig a passzív önrávezető rendszerekkel rendelkező rakéták elleni oltalmazásban vesznek részt. A fegyverirányító rendszerek automatikus célkövető csatornái közül bármely csatorna, távolság, cél, irány szerinti elhúzása a legtöbb esetben nem csupán az adott lokátor állomás funkciójának, hanem az egész fegyverirányító rendszer működésének megbontásához vezet.

A sebesség szerinti elhúzó zavarokat a folyamatos kisugárzással üzemelő *(Continuous Wave – CW)* rádiólokátor-állomások ellen alkalmazzák, amelyek sebesség szerinti keresési csatornával és automatikus célkövetővel rendelkeznek. A mérés a Doppler frekvencia eltolódás jelenségén alapul. A követőrendszer normális működését az bontja meg, hogy a zavarjel hatására a mért Doppler frekvencia kicsúszik a mérés lehetséges tartományából, és így a követőrendszer elveszíti a céljelet.

[179] Forrás: a szerzők archívuma.

4.1.2 Az elektronikai zavarás fizikai elvei, módszerei

Az elektronikai zavarás említésekor sokszor csak a rádiók, vagy a lokátorok zavarásra gondolunk, de mint a korábban leírtakból már kiderülhetett, az elektronikai ellentevékenység a teljes spektrumot átfogja, az akusztikustól a fénytartományokig. Ebben az alfejezetben egy rendeltetés szerinti felosztást alkalmazva röviden áttekintjük a legfontosabb zavarási módszereket, azok elveit, megvalósításuk lehetséges eszközeit. Az elektronikai zavarás célpontjai természetesen nemcsak az ellenség hírközlési- és rádiólokációs célú elektronikai berendezései lesznek, hanem a felderítő berendezései, távérzékelő rendszerei, szenzorai is. A zavarási technikákat, mint látni fogjuk, az alkalmazott frekvenciatartomány fogja elsősorban befolyásolni. A zavarás mind támadó, mind védelmi célokat szolgálhat.

Az aktív zavarjeleket a rádiófrekvenciás tartományban az esetek nagy többségében, speciálisan erre a célra kifejlesztett zavaró berendezésekkel állítják elő, de alkalmazhatnak zavaró adapterrel kiegészített híradó berendezéseket is erre a célra.

A zavaró berendezések készletébe általában az alábbi alrendszerek találhatók:

- antennarendszer;
- vevő-analizáló alrendszer;
- iránymérő alrendszer;
- zavarmodulátor;
- adóberendezés;
- állomásvezérlő, távkezelő rendszer;
- kommunikációs alrendszer;
- energiaellátó rendszer.

Az egyes rendszertechnikai megoldásoknál némelyik hiányozhat, némelyik pedig kiemelt jelentőséggel bír. Ahol ez szükséges, ott részletesebben ismertetjük a zavaró állomás sajátosságait.

Az antennarendszerben vevő-, és adóantennák találhatók, amelyek feladata vételkor a sugárzott elektromágneses energia szabad térből való kicsatolása, a sugárzott energia vezetett energiává alakítása, illetve adáskor ennek reciproka, vagyis az előállított adójel szabad térbe való kisugárzása.

A vevő és analizáló rendszer feladata az elektromágneses spektrum egy adott tartományának letapogatása, az ellenséges elektronikai eszköz jeleinek felfedése, vizuálisan láthatóvá tétele, paramétereinek kézi, vagy automatikus mérése. Ha szükséges, illetve lehetséges, a jel detektálásával az információtartalom lehallgatható, rögzíthető. Az analízis legfőbb célja a célazonosításon kívül, az optimális zavarjel struktúrájának kiválasztása manuálisan, vagy automatizáltan. A vevő-analizáló rendszer a korszerű berendezésekben digitális jelek útján beállítási alapadatokat szolgáltat a zavaróadó számára.

Az iránymérő alrendszer feladata a célobjektum működési irányának meghatározása. Erre több okból is szükség lehet. Ezen információ segítségével irányított zavaróadó antennák irányba állítása, mozgó célobjektumok esetén a célok követése, a saját csapatok felé történő zavarkisugárzás megakadályozása és egyéb jól automatizálható feladatok

oldhatók meg. Az iránymérési adatok továbbítása és több állomás adatainak feldolgozása nyomán az elektronikai kisugárzó eszköz települési hely is behatárolható, bizonyos hibával. A korszerű fázisméréses elvű iránymérő berendezések kezelői beavatkozás nélküli, automatizált rendszerbe integrálhatóak.

A zavarmodulátor egység feladata az adóberendezés számára szükséges modulációs jel kialakítása. A jelanalízis során megállapított modulációs módokhoz hozzárendelhetők az optimális zavarjel-paraméterek, amelyek manuálisan, vagy automatizáltan kerülnek beállításra. A zavarmodulátor rádiózavaró állomásoknál lehet viszonylag egyszerű felépítésű is. Rádiólokációs zavaró berendezéseknél azonban igen bonyolult is lehet, mivel ott nemcsak a válaszjel időparaméterei szerinti struktúrát kell optimálisan előállítani, hanem a járulékos, impulzusokon belüli frekvencia-, zaj és egyéb modulációs jellemzőket is.

Az adóberendezés feladata a zavaráshoz szükséges rádiófrekvenciás jel előállítása, a moduláció és a teljesítményerősítés végrehajtása. A kijelölt frekvenciára való lehangolás a berendezés korszerűségétől függően történhet kézi hangolással, analóg, vagy digitális frekvencia szintetizációval. A legkorszerűbb nagy sebességű szintézerek és hangolt végerősítők lehetővé teszik a gyors frekvenciaváltást. Ma már az adók szempontjából nincs akadálya a frekvenciaugratásos rendszerek zavarásának, azonban a következő ugrási frekvencia meghatározása jelenleg még nem megoldott, így más zavarási metódust kell erre alkalmazni.

Az állomásvezérlő-, távkezelő rendszerek feladata, hogy számítástechnikai módszerekkel támogassák a kezelők munkavégzését, a kiadott emberi parancsok, vagy automatizált algoritmusok szerint vezéreljék a rendszer egyes berendezéseit. Az egyszerű, rádiócsatornán megvalósítható adás indítás-leállítástól, a mindent automatizáltan végrehajtó, felügyelet nélküli felderítő-zavaró rendszerig minden megvalósítható.

A zavaró állomások kommunikációs alrendszere a kezelőállomány híradóeszközök útján való irányítására, a távvezérlő csatorna létesítésére, az állomások adatátviteli kapcsolatainak biztosítására szolgálnak. Ma még az ultrarövid hullámú rádióktól kezdve, a rádióreléken át, a műholdas, teljesen digitális hang-, és adatátviteli berendezésekig minden megoldás létezik a hadseregek fegyverzetében.

Az energiaellátó rendszer feladata a zavaróállomás működtetéséhez szükséges villamos energia előállítása, szabályozása és tárolása. Az energiaszükséglet az állomások rendeltetésétől, méretétől, teljesítményétől függően például az egyszeri felhasználású zavaróadók esetén szükséges néhány Wattól, a rádiólokációs zavaróállomások több tíz kW-os teljesítményfelvételéig terjedhet. Ennek megfelelően az akkumulátoros, vagy vegyi aktivizálású telepektől, a külön gépjárműbe épített áramfejlesztő állomásig igen széles skála áll rendelkezésre.

A továbbiakban az egyes eszközcsoportokra jellemző vonásokat tekintjük át.

4.1.2.1 A kommunikációs rendszerek lefogásának elvei, módszerei, eszközei

A kommunikációs rendszerek lefogásának tárgyalásakor célszerű a rendeltetés, illetve az alkalmazott frekvenciatartomány szerinti felosztást követni, mivel a berendezés csa-

ládok és az ellenük vívott elektronikai hadviselés eszközei is ezt a felosztást követik az esetek nagy részében. Fizikai szempontból – vagyis az átviteli közeg milyensége alapján – első lépésben a kommunikációs rendszerek feloszthatók vezetékes és vezeték nélküli eszközökre.

A vezetékes eszközök lehetnek:

– polgári vezetékes távközlési rendszerek légkábeles, földalatti fémvezetékes és optikai kábeles átviteli szakaszai;
– katonai állandóhelyű és tábori híradást biztosító ugyancsak légkábeles, földre fektetett, vagy földalatti fémvezetős, illetve optikai szálas eszközök; valamint
– az eredeti rendeltetését tekintve például energiaellátást biztosító kábelrendszerekre ültetett, úgynevezett vivőzött átviteli hálózatok.

Az ellenséges vezetékes hírközlést biztosító polgári rendszerek elleni harc kiemelkedő jelentőséggel bír az ellenség területén vívott küzdelem során. A központokért, hírközlési csomópontok megszerzéséért folyó harc egyik célja az ellenőrzés és az infrastruktúra megszerzése, másrészt a birtokba vett területen maradt erők izolálása. A vezetékes eszközök hiányában kénytelenek rádió berendezéseket alkalmazni, amelyek felderítése, helyének bemérése és a közlemények tartalmának megfejtése jóval egyszerűbb feladat, mint a fémvezetékes, vagy optikai összeköttetések felderítése, lehallgatása. A helyi háborúk tapasztalatai azt mutatják, hogy a hadműveletek hírközlési feladatainak mintegy 70-80%-át polgári rendszereken keresztül bonyolították le. Ez úgy az amerikai hadsereg által az Öböl-háború idején bérelt polgári hírközlési csatornákra is igaz, mint a délszláv háborúban használt híradó berendezésekre. Ne feledjük el, hogy minden vezeték nélküli – műholdas, cellarádió rendszerű vagy akár polgári műsorszóró rádió és televíziós rendszereknek komoly vezetékes szakaszai vannak.

A birtokbavételért folyó harc hagyományos tűzfegyverekkel, diverziós csoportokkal, speciálisan kiképzett erőkkel, vagy összfegyvernemi alegységekkel folyik. A birtokbavétel sikertelensége vagy más, felsőbb szempontok esetén kerülhet sor a vezetékes összeköttetések rombolására. A cél, az összeköttetés megszakításán túl lehet az is, hogy minél kevesebb rombolással, hamar helyreállítható módon bontsuk meg a rendszer működését, mivel saját csapataink céljára alkalmazásba kerülhetnek ezek az eszközök.

A fent leírt módszerekkel az információs műveletek keretein belül folytatjuk a kommunikációs rendszerek elleni harcot, de nem közvetlenül az elektronikai hadviselés eszköztárának segítségével.

A másik módszer az elektronikai csapás kiváltása e hírközlő rendszerekre. A lényege az, hogy olyan, villámcsapáshoz, vagy a magas légköri atomrobbantás elektromágneses impulzusához hasonló, nagy energiájú elektromágneses besugárzást hozunk létre, amely a vezetékes eszközökben a megengedhető mértéknél nagyobb feszültséget indukál és a vezetékek, illetve a hozzájuk csatlakozó berendezések meghibásodását, tönkremenetelét okozza. Ezzel a területtel részletesebben a *4.3. Elektronikai pusztítás* fejezetben foglalkozunk.

Az optikai kábeles összeköttetések kábelszakaszain e fizikai hatás nem okoz zavart, azonban a hozzájuk csatlakozó erősítő-ismétlő állomások, végberendezések, ha más-

képp nem, de a villamos energiaellátó rendszeren keresztül csapást szenvedhetnek, és ugyanúgy tönkremehetnek.

A berendezések telepítésekor tehát messzemenően figyelembe kell venni az elektromágneses impulzusfegyverek által jelentett fenyegetést, és nemcsak az összeköttetés, de az energiaellátást biztosító rendszerekben is meg kell tenni a szükséges óvintézkedéseket. Ez védett, nagy vezetési pontok esetén a beruházás szerves része kell, hogy legyen, de ahogy haladunk az egyre védtelenebb tábori eszközök felé, annál nehezebb a szükséges mértékű óvintézkedéseket megtenni. A készülékek esetén ez már tervezési, konstrukciós kérdés és nem az alkalmazó feladata. Ezzel a problémával részletesen a jegyzet *Elektronikai védelem* című 5. fejezete foglalkozik.

A vezeték nélküli kommunikációs berendezéseket célszerű a frekvenciatartományuk szerinti csoportosításban tárgyalni, mivel ez lényegében be is határolja a rendszertechnikai felépítésüket, és az ellenük vívott harc eszközeinek jellemzőit is.

Ebben az aspektusban a vezeték nélküli kommunikációs berendezések besorolhatók az:

- igen hosszú hullámú;
- a hosszúhullámú;
- a középhullámú;
- a rövidhullámú;
- az ultrarövid hullámú; és
- a mikrohullámú eszközök csoportjaiba.

A frekvenciatartománybeli felosztáson kívül kulcsfontosságú a rendeltetés szerinti csoportosítás, vagyis, hogy milyen hordozó eszközön, milyen hírközlési feladatra rendszeresítették azt az adott berendezést.

Az igen hosszú hullámú (néhány kHz – néhányszor tíz kHz frekvenciájú) elektromágneses rezgéseket a tengeralattjárókkal folytatott kommunikáció céljára alkalmazzák. Sajátossága, hogy a tengervízben jól terjed, de az alacsony használható sávszélesség miatt a megvalósítható jelátviteli sebesség is alacsony. Hátránya, hogy a partvonalnál óriási hosszúságú antennát igényel és a tengeralattjáró sem képes tetszőleges nagy szálantennát hordozni, illetve vontatni.

A hosszúhullámú (70 kHz – 500 kHz) frekvenciatartományt katonai és polgári felhasználású globális navigációs rendszerek, valamint polgári rádió műsorszóró eszközök használják. A navigációs rendszerekről és az ellenük folytatható elektronikai hadviselésről a 4.1.2.8. alfejezetben lesz szó.

Álljunk meg egy pillanatra a műsorszóró rendszereknél! A rádió (televízió) műsorszóró eszközök, amelyek később, a magasabb frekvenciatartományokban is tömegesen elő fognak fordulni, rendeltetésük alapján a mindenkori hatalom birtokosainak a tömegtájékoztatásra, propagandára szolgáló eszközei. Nincs ez másként a háborús időszakokban sem, hiszen a leggyorsabb tájékoztató eszközök ezek, amelyek ma már minden háztartásban megtalálhatók, különösebb műszaki szervezést, pótlólagos beruházást nem igényel a hírek eljuttatása egyszerre több millió emberhez.

A tömegtájékoztatás eszközeivel folyó propaganda háború az információs műveletek csoportosításán belül a pszichológiai hadviselés szférájába tartozik. Amikor az adóháló-

zatok birtokbavételéről, a sugárzási kapacitások lehetőség szerint való megőrzéséről van szó, akkor ugyanazt lehet elmondani, mint amit a vezetékes rendszereknél elmondtunk a birtokbavételről. Ha lehet ez még kényesebb kérdés, mivel egy kiesett vezeték szakaszt viszonylag kevesebb szakértelemmel és egyszerű eszközökkel ki lehet pótolni, de egy esetleg már békében rombolásra előkészített televíziótorony megsemmisülése szinte helyreállíthatatlan kárt okoz, ami csak teljesen új telepítésével pótolható.

A tömegtájékoztatás eszközei ellen az elektronikai hadviselés berendezéseivel is fel lehet venni a harcot. Amennyiben nem lehet az adóhálózatot, vagy annak egyes elemeit birtokba venni, úgy elektronikai zavarással akadályozhatjuk, hogy a vevőkészülékek venni tudják a sugárzott műsort. Ez történhet földről stabil, vagy mobil eszközökkel, illetve repülőgépen elhelyezett zavaró berendezések segítségével. Békeidőben, a szocialista országokban politikai okokból zavarták például a Szabad Európa rádió adásait, de az utóbbi évek regionális konfliktusaiban, Panamában, a Perzsa Öbölben, Haitin, és a jugoszláviai háború során is fontos szerephez jutottak a speciálisan erre a célra kifejlesztett berendezések. Az USA Nemzeti Gárda légierejének állományába tartozik a Harrisbergben állomásozó 193. Különleges Rendeltetésű Légi Század. Repülő eszközei között találhatók azok az EC-130E típusú *(Rivet Rider)* repülőgépek (4.3. kép), amelyek rádió és televíziós adóberendezések sokaságával vannak felszerelve és képesek a műholdas műsortovábbító rendszeren át vett, vagy saját stúdiórendszerükben előállított műsorok, közlemények sugárzására az ellenséges adók zavarására, műsoraik kiváltására.

A hosszúhullámú frekvenciatartományt egyre kevesebb országban használják, egyre kevesebb vevőkészülék alkalmas a vételére, inkább csak a régebbi berendezések, illetve a szélessávú rövidhullámú vevők. Összességében katonai jelentősége alacsony, de a teljesség kedvéért számolni kell vele.

4.3. kép. **Az EC-130E Rivet Rider repülőgép**[180]

[180] http://www.fas.org/programs/ssp/man/uswpns/air/special/ec130.html (Letöltve: 2014.02.12.) – Oops! That page can't be found.A hivatkozott forrás oldal nem elérhető!!!

A középhullámú (500 kHz – 1500 kHz) frekvenciasáv már jóval fontosabb. A középhullámú, országos lefedettséget biztosító polgári rádiórendszerek dolgoznak itt, valamint a katonai repülés irányadó berendezéseinek egy része. A polgári műsorszóró hálózatba stúdiók, műsorszétosztó vezetékes áramkörök, adóállomások és infrastrukturális berendezések tartoznak. A nagy ellátási körzethez nagyteljesítményű, több száz kW-os adóberendezések szükségesek, amelyek ebben a frekvenciatartományban igen nagyméretűek, nehezen mobilizálhatóak, nem is beszélve az óriási antennatornyokról.

Az információs műveletek keretében az elfoglaláson kívül lehetséges a zavarás is. A fentebb említett EC-130E típusú repülőgép az alacsonyabb frekvenciatartományokban való hatékony sugárzás céljából úgynevezett haladóhullámú antennát használ, ami egy felszállás után kibocsátható 2400 m hosszú, vontatott huzalantenna.

Középhullámon csapathíradásban alkalmazott rádióberendezések nem üzemelnek, így ennek a sávnak inkább a pszichológiai műveletekben van kiemelt jelentősége.

A rövidhullámú frekvenciasávot a nyugati katonai rádiók az 1,5 MHz – 30 MHz között, a volt VSZ országokban rendszeresített eszközök pedig az 1,5 MHz – 20 MHz között fogták át. A katonai híradásban fontos helyet kapott ez a frekvenciatartomány. A hullámterjedési sajátosságai globális méretű hírrendszerek létrehozását tették lehetővé, amely a mai napig megmaradt. Az USA kontinensek közötti repüléseket kiszolgáló értesítő rádiórendszerei, valamint többek között az atomeszközök ellenőrző-riasztó rendszerei is ebben a tartományban üzemelnek.

Az atomeszközök széles körű alkalmazásával számoló hadműveleti tervezésben kulcsfontosságúvá lépett elő a rövidhullámú híradás, mivel az ultrarövid hullámú hírközlés az atomrobbanás ionizációs sugárzása és a légkörfizikai változások miatt jó ideig használhatatlan lett volna. Napjainkra a műholdas hírközlés elterjedésével a nagytávolságú rövidhullámú híradás jelentősége csökken, ugyanakkor a digitális adásmódok megjelenése és az atomeszközök alkalmazási viszonyai közötti jó tulajdonságai miatt ez a sáv a reneszánszát éli.

A korszerű számítástechnikai eszközök alkalmazásával lehetővé vált a légkörfizikai tulajdonságok automatizált mérése és adatgyűjtése, valamint ezek alapján még precízebb hullámterjedési előrejelzések elkészítése. A korábban már bemutatott felületi és térhullámú terjedési tulajdonságok, az éjszakai és nappali terjedés közötti különbségek, a csatornainterferenciák és fadingek új berendezés-konstrukció kifejlesztését tették szükségessé. Az úgynevezett adaptív rádió széles körűen támaszkodik a számítástechnikai eszközökre és egyéb digitális rádióáramkörökre. Működésének lényege, hogy a rádióháló tagjai előre leprogramozott, vagy menet közben digitális úton letöltött program szerinti frekvenciákon üzemelnek mindaddig, amíg a csatorna minőségi tulajdonságai megfelelőnek minősülnek. Ez idő alatt, a kezelőtől függetlenül, a berendezések vizsgálják a többi csatorna paramétereit is, és amennyiben szükséges, a következő, arra legmegfelelőbb csatornára vezénylik át a rendszert. Mindez a kezelő, vagy a beszélgetést folytató személy beavatkozása, sőt tudomása nélkül folyik, a közlemények megszakadása nélkül. Ez hasonló a mai, korszerű GSM rendszerű cellarádiók optimális bázisállomás kiválasztási algoritmusához.

A rövidhullámú híradás eszközei a hullámhosszhoz való illeszkedési követelmények miatt még mindig elég nagyméretűek. Ezek közül is az adóberendezések igényelnek több száz, vagy ezer W-os teljesítményt, illetve az antennarendszerek is igen robosztusak. A stabil telepítésű, polgári, vagy katonai adók haladóhullámú antennát, V-antennát, G-antennát, dipólt, paplanantennát, függőleges botantennát (tornyot), vagy logaritmikus-periodikus antennát használnak. A huzalantennákat magas (50-100 m) tornyok között feszítik ki, a logperiodikus antennát pedig forgathatóan, toronyra emelik. Ez a módszer lehetővé teszi a kisugárzás irányának változtatását, a kilövés szögének kívánt értékre való beállítását.

A mobileszközök a régi típusoknál napjainkra jóval kisebbek lettek, az antenna konstrukciók azonban nem túl sokat változtak. Némi könnyebbséget jelent a pneumatikus, vagy hidraulikus árbocok széles körű elterjedése. Az állomások telepítési-bontási idejének igen nagy részét az antennarendszer teszi ki.

Az elektronikai ellentevékenység szempontjából a birtokbavételre korábban leírtakhoz képest nincs változás. A zavarás szempontjából azonban nagy különbségek vannak. Ez az a frekvenciasáv, ahol a rádiózavarás, *a rádióháború* megszületett. Itt jelentek meg először a híradás céljára épített, de lehallgatásra, majd kiegészítőkkel, vagy azok nélkül, de már elektronikai zavarásra, megtévesztésre alkalmazott eszközök. Abban az időben a híradó csapatok hajtották végre az ilyen feladatokat, erre külön speciális alegységet csak később szerveztek.

A rövidhullámú rádiózavarásnak igen sok eszközét dolgozták ki a fejlesztők. Abban mindegyik megegyezik, hogy a nem megtévesztési célú zavaró állomások erővel, vagyis az adóból kisugárzott nagy elektromágneses energiával fogták le az ellenséges vevőkészülékeket.

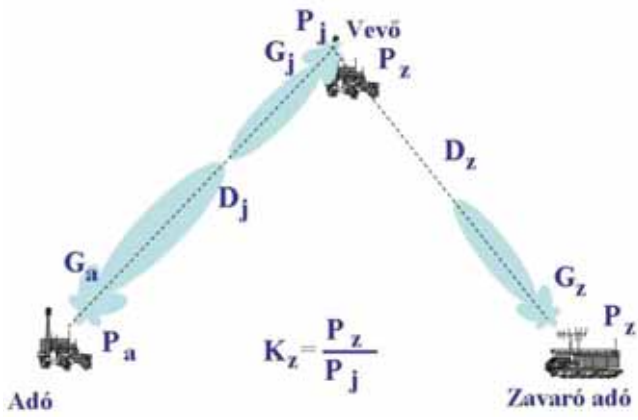
A fizikai lényege ennek az, hogy a kommunikációs rendszer adóállomása által kisugárzott energia a vevő bemenetén bizonyos nagyságú feszültséget hoz létre. Amennyiben ez a feszültség a környezetből és a készülékből, önmagából származó zajokat egy adott mértékben (ezt nevezzük határérzékenységnek) meghaladja, akkor a vevőkészülék képes detektálni, feldolgozni a jelet, a kívánt információ megjelenik a kimenetén. A zavaró állomás feladata az, hogy frekvenciában egyeztetett, lehetőleg a vevő irányába kisugárzott elektromágneses energiájával a vevő bemenetén olyan nagyságú zavaró jelet hozzon létre, amely a hasznos információt hordozó jellel együtt bejutva a vevőkészülékbe, megakadályozza a hasznos információ feldolgozását, illetve a kimenetre jutva, a hasznos információ tartalma ne legyen felismerhető. A frekvenciában való egyeztetésre azért van szükség, mert egy vevőkészülék, elvileg csak a vételi sávszélességébe eső jeleket engedi tovább, az azon kívül eső jeleket kizárja. A gyakorlatban minden berendezésbe bejutnak a vételi sávon kívül eső frekvenciájú jelek is, igaz, hogy nagy csillapítással. Az ilyen hamis vételt okozó jelek egy része előre prognosztizálható, vagy a későbbiekben laboratóriumi körülmények között kimérhető.

A berendezések jóságára nézve adnak adatokat a vevő szelektivitási, intermodulációs elnyomási paraméterei. Az intermodulációs termékek több hullám kikeveredéséből származó eredő hullámok, amelyek akár nem szándékosan, de mégis zavart okoznak a berendezésekben. Ezek száma nagyteljesítményű berendezések közelében megnőhet.

Ezzel a problémával az elektronikai védelem témakörén belül, az elektromágneses kompatibilitással foglalkozó alfejezetben részletesebben találkozhatunk.

A vevőkészülék bemenetén egy időben megjelenő zavaró jel és a hasznos jel energiaviszonya sok tényezőtől függ. Ezek közül a leglényegesebbek az alábbiak:

- az adóberendezés teljesítménye;
- az adó antennarendszerének nyeresége (a vevőkészülék irányában);
- az adó és a vevőkészülék között fellépő valós szakaszcsillapítás;
- a vevőantenna nyeresége (az adókészülék irányában);
- a vevőkészülék érzékenysége;
- a zavaró adó teljesítménye;
- a zavaró adó antennarendszerének nyeresége (a vevőkészülék irányában);
- a zavaró adó és a vevőkészülék között fellépő valós szakaszcsillapítás;
- a vevőantenna nyeresége (a zavaró adó irányában). (4.1. ábra)



4.1. ábra. **A rádiózavarás elvi vázlata**[181]

Ehhez járul az úgynevezett modulációs illeszkedés, amit optimális zavartípus kiválasztásnak is nevezhetünk. A rádiózavarás tervezése során a cél annak az eldöntése, hogy a zavarás adott paraméterek mellett hatékony lesz-e vagy sem, mivel a feleslegesen folytatott, energetikailag hatástalan zavarási feladat csak a kezelőállományt és az állomás biztonságát veszélyezteti.

A számításokban szereplő adatok egy része csak bizonyos közelítéssel, becsléssel, adott valószínűséggel adható meg. Az ellenséges adókészülék típusát, ezen keresztül az adóteljesítményét, alkalmazott antennáját csak a legritkább esetben lehet megmondani, például csak akkor, ha egy mélységi felderítő azt pontosan jelenteni tudta. Általában a hadműveleti elhelyezkedésből, a peremvonaltól való távolságból, az esetleg más úton felderített hadrendi hovatartozásból, a forgalmazás jellegéből, tartalmából, az adott ve-

[181] Szerkesztették a szerzők.

zetési szinten működő eszköztípusok jellegzetességeiből valószínűsíthetőek ezek a paraméterek.

Ha adó-vevő párok forgalmaznak, akkor a helyzet egyszerűbb, mert az adási periódusok alatt végzett iránymméréses helymeghatározással a terepen elfoglalt pozíciójuk nagy valószínűséggel meghatározható. Lehetnek persze olyan speciálisan kedvezőtlen helyzetek, például nagyreflexiójú erdős-hegyes terep, vagy nagyvárosi beépítettség, ahol az iránymérés rossz, vagy nem egyértelmű, tehát használhatatlan eredményeket szolgáltathat. A működés helyének ismeretében közöttük terepmetszet készítéssel, hullámterjedési modellek alkalmazásával a szakaszcsillapítás nagy megbízhatósággal meghatározható.

Korábban a zavarási feladatok meghatározásánál egy átlagos (gyakorlatban esetleg megfigyelt, kipróbált) zavarási mélységbe eső célok közül a fontosnak ítélteket jelölték ki zavarásra. Az objektív kontroll abban nyilvánult meg, ahogy a forgalmi rendszerben dolgozó kezelők a zavarás tényére reagáltak. Ha a titkosított összeköttetésből nyíltra váltottak, majd újra zárni próbáltak, a közlemények ismétlését kérték, frekvenciamanővert kezdtek, vagy nyíltan beszéltek a zavarás tényéről, akkor a zavar hatékonynak bizonyult. Ellenkező esetben, tehát ha nem reagáltak, folytatták az addigi rend szerint a közlemények váltását, nagy valószínűséggel hatástalan volt a zavarás, illetve alájátszó, hamis, imitációs célból üzemeltetett rádióforgalmi rendszerről volt szó. Az automatizált zavaró állomások az ilyen célokra való tevékenységet egy beállított, úgynevezett „ledobási" idő után otthagyják, mivel értelmetlen tovább zavarni.

Összességében igen bonyolult megfontolások, műszaki és harcászati kritériumok sorozatából épül fel a hatékony zavarás, illetve zavarbeszüntetés algoritmusa. Mivel a kezelők kiképzésében is megjelentek ezek az elvek, a zavarokra nem volt szabad nyíltan reagálni, az adott rendben kellett a közlemények adását folytatni, és befejezni. Egy kétoldalú, nagy türelmet igénylő küzdelem folyt, mivel a zavaró állomás várhatóan egy idő után úgyis beszüntette az adott frekvencián a zavarást. Különösen igaz volt ez a kézi hangolású, lassú frekvenciaváltású berendezéseknél. Ma, az automatikusan, és gyorsan hangoló zavaró adók felismerik a kijelölt frekvencián újra forgalmazni kezdő rádióhálót és visszatérnek rá.

Az adaptív rádiók megjelenése után a kézi hangolású zavaró állomások számára a rádiózavarás összetettebb feladat lett, mivel ezek a berendezések zavar észlelése esetén automatikusan frekvenciát váltottak, amit a felderítő rendszernek újra meg kellett találnia. A felderítés és az adott frekvencián való zavarkiváltás jóval hosszabb ideig tart, mint egy áthangolás.

A zavarás teljesítményviszonyai még nem adnak választ a zavarás hatékonyságára. A hatékonyság igen nagymértékben függ a végberendezés típusától. Ha az információt egy kezelő veszi, akkor az ő képességeitől, felkészültségétől, gyakorlottságától, tehát egy sor szubjektív tényezőtől függ az, hogy a zavarjelek közül ki tudja-e szűrni a neki szóló közleményt. Műszeres mérésekkel meg lehet határozni, hogy mekkora a zavarjel és a hasznos jel feszültségének (teljesítményének) aránya akkor, amikor a zavart hatékonynak ítéljük meg. A hatékonyságot egy sor szubjektív tényező befolyásolja. Egy automatikus Morse jeleket vevő készülék sokkal előbb fogja téveszteni a vett jeleket, mint egy tapasztalt kezelő. Az emberi szem is sokkal nagyobb valószínűséggel ismer fel

egy zajos képet, mint egy alakfelismerő optikai rendszer. Statisztikusan megadható az a szám, amely adott körülmények között az információnak olyan jelentős torzulásához vezet, amely nem alkalmas további feldolgozásra.

Az optimális zavartípus kiválasztásának is az a célja, hogy egy adott üzemmódban (modulációs móddal) dolgozó berendezéshez olyan zavarjelet sugározzunk ki, amelynél a teljesítményviszonyokban a legkisebb zavarási teljesítményt követelik meg.

Tehát azt a számot, amely a zavaró teljesítmény és a hasznos jel teljesítményét adja meg adott üzemmódban, *lefogási tényezőnek* nevezzük:

$$K = \frac{P_Z}{P_J} > K_Z \qquad (4.2.)$$

ahol: K – a lefogási tényező számított értéke;
P_z – a zavaró jel teljesítménye a vevő bemenetén;
P_j – a hasznos jel teljesítménye a vevő bemenetén;
K_z – az adott üzemmódhoz tartozó előírt arány.

A zavarás akkor hatékony, ha a mérések, vagy gyakorlati kísérletek eredményeképpen megállapított K_z tényezőnél nagyobb arányú zavar/jel viszonyt sikerül előállítani a vevőkészülék bemenetén.

Ha adott paraméterekkel rendelkező rádióösszeköttetés zavarásának energiaviszonyait megvizsgáljuk, azt tapasztaljuk, hogy az adó körül mindig kialakul egy olyan térrész, ahol a vevőkészülék bemenetén mindig kisebb lesz a zavar/hasznos jel arány, mint a hatékony lefogáshoz szükséges lenne. Ezt le nem fogható zónának nevezzük. Ezzel magyarázható, hogy a zavarhatékonyság sohasem lehet 100%-os, mivel energetikailag lehetetlen ezt elérni. A lefogás matematikai levezetése a 2. fejezetben részletesen megtalálható.

A fentebb leírt általános zavarási megfontolások egyaránt érvényesek a rövidhullámú, az ultrarövid-, és mikrohullámú zavarásra, amennyiben a hasznos jel elnyomására törekszünk.

A rövidhullámú frekvenciasávban üzemelő berendezések zavarása során meg kell különböztetnünk a térhullámú és a felületi hullámú terjedéssel működő lefogást. A térhullámú zavarás eszközeit a lefogandó, általában hadászati, hadműveleti rendeltetésű nagytávolságú összeköttetésektől távol, 100-200 km-re kell telepíteni, hogy a terjedési holtzónát a saját területünkön tartsuk. A térhullámú zavarás hatékonysága nagymértékben függ az ionoszféra egyes visszaverődési rétegeinek állapotától, a napszaktól, a napfolttevékenységtől, az ionizáció pillanatnyi fokától. A térhullámú zavarás lefogási számításai ennyi időben és térben változó paraméter mellett meglehetősen bizonytalanok. A zavaráshoz több kW teljesítményű, robosztus, nagy antennarendszerű zavaró állomásokat fejlesztettek ki, amelyek mobilitása elég alacsony volt. Ezek a hátrányok, a védelmi stratégiára való áttérés, valamint a berendezések fizikai elöregedése vezethetett oda, hogy a térhullámú zavarásra szolgáló állomásokat több országban kivonták a rendszerből.

Napjainkban az 1-1,5 kW kimenő teljesítményű állomások a legelterjedtebbek. Az automatizáltság fokát illetően ma még megtalálhatók úgy a kézi hangolású, csöves

berendezések, mint a számítógép vezérelte, távkezelhető, integrált áramkörös, tranzisztoros zavaró állomások. Ebben a frekvenciatartományban egyszeri felhasználású zavaró adókat általában nem alkalmaznak.

Az ultrarövid és az alsó mikrohullámú frekvenciatartomány 20 (30) MHz-től 1 GHz-ig terjed. A frekvencia-felosztási táblázatok több tartományt is kijelölnek ebben a sávban, de a gyakorlatban azért ezt nevezik az ultrarövid-hullámú sávnak, mert a technológia és az alkatrészek konstrukciója e fölött tér át a koncentrált paraméterűről, az elosztott paraméterűre. Az alsó 20-52 MHz-es, (a nyugati berendezések esetében 30-83 MHz-es) tartományban üzemelnek a harcászati-hadműveleti URH rádiókészülékek. Ezek képezik a csapatok híradó berendezéseinek zömét és a rádiózavarás objektumait a harcászati-hadműveleti zónában.

Az ilyen eszközök nyílt és titkosított hang- és adatátvitelre alkalmasak. A régebbi konstrukciójú eszközök általában hagyományosnak nevezhető frekvenciamodulációt alkalmaznak. Az adástechnikai fejlesztések eredményeképpen egyre nagyobb számban találhatók meg a csapatoknál a korszerű, digitális beszédkódolású, és a frekvenciaugratásos rádió berendezések. Az ilyen rádiók felderítése, iránymérése, lehallgatása és zavarása az analóg eszközökkel már nem lehetséges, ezek teljesen más működési elvű, számítógép támogatású rendszereket igényelnek.

A magasabb tartományokban általában rádiórelék, sokcsatornás kép-, hang- és adatátvitelt biztosító analóg, majd egyre nagyobb számban digitális átviteli rendszerek dolgoznak.

A *műholdas kommunikációs rendszerek* az ötvenes évektől indultak rendkívül dinamikus fejlődésnek. A műholdas rendszerek rendeltetésüket tekintve két nagy csoportra oszthatók. Az első csoportba a valamilyen szolgáltatást nyújtó, navigációs-, meteorológiai-, hírközlési, tudományos kutató holdak tartoznak, a másodikba a felderítő rendeltetésűek. A felderítő műholdakkal az elektronikai támogatás fejezetben (3.3) foglalkoztunk.

A kommunikációs célú műholdas rendszerek a rádiótávközlés olyan rendszerei, amelyben a földi berendezéseken kívül egy vagy több műholdat használnak fel. A műholdas állandóhelyű szolgálatok stabil telepítésű földi végpontok között létesítenek távbeszélő, adatátviteli, televíziós, vagy rádióösszeköttetést. (4.4. kép) Az összeköttetés lehet pont-pont közötti, vagy műsorszóró felépítésű, vagyis egy ponttól a kiválasztott többi pont felé irányuló. A műholdas mozgószolgálatok hírközlési rendszerében üzemelő földi berendezések javarészt mozgó, vagy kézi hordozható készülékek. A földi kommunikációs rendszerekhez való csatlakozás stabil központokon keresztül történik. A felhasználók között kétoldalú, vagy konferenciakapcsolás is létesíthető. Ilyen mozgó műholdas rendszer például az IRIDIUM. A korszerű rendszerek már kivétel nélkül digitálisak, míg a korábbiak sokcsatornás, többszörös hozzáféréses rendszerben épültek fel.

A kommunikációs célú műholdak harmadik nagy családja a közvetlen műholdas műsorszórás *(Direct Broadcasting Satellite – DBS)*, amelyre példaként szolgálhatnak a legnagyobb tömegben elterjedt televíziós műsorszóró holdak (például ASTRA, EUTELSAT, GORIZONT).

4.4. kép. **Egy műholdas kommunikációs rendszer földi antennái**[182]

A műholdas kommunikációs rendszerek előnye, hogy az alkalmazott frekvenciatartomány és az eszközök műszaki paraméterei lehetővé tették az igen kis apertúrájú antennák alkalmazását. A mérsékelt atmoszférikus és interferencia zavarok miatt – ha egyébként a vétel optikai láthatósági feltételei adottak – egyenletes minőségű szolgáltatás biztosítható. Katonai alkalmazásra különösen alkalmas, mivel nagy régiók egyenletes lefedése biztosítható, tehát a földi végpontok igen rugalmasan telepíthetők át, új felhasználók egyszerűen léptethetők be, a rendszer számítógépes módszerekkel gyorsan átkonfigurálható.

A földi felderítés és zavarás ellen viszonylag jól védett, de speciálisan erre a hírközlési fajtára szakosodott kisszámú felderítő berendezés számára nem jelent nagy gondot a felderítésük. A zavarásuk fizikailag a Föld-műhold irányon fellőtt frekvenciában célzott, nagyteljesítményű zajzavarral minden további nélkül elképzelhető, ugyanakkor nemzetközi egyezmény tiltja a műholdak zavarását.

4.1.2.2 A rádiólokációs eszközök zavarásának módszerei, eszközei

A rádiólokációs eszközök olyan berendezések, amelyek rendeltetése a tárgyak, vagy más objektumok felderítése, koordinátáinak, mozgás és más paramétereinek meghatározása. Alkalmazási viszonyait tekintve alapvetően megkülönböztethetünk:

- földi telepítésű, földi objektumokat felderítő rádiólokátorokat, például a harctéri, mozgó célokat felderítő eszközök;
- földi telepítésű, légi objektumokat felderítő rádiólokátorokat, amelyek lehetnek:
  - távolfelderítő rádiólokátorok;
  - közepes hatótávolságú felderítő rádiólokátorok;

[182] AN/TSC-93A and AN/TSC-93B Satellite Communications Terminals (Letöltve: 2014.02.12.) https://www.fas.org/spp/military/program/com/an-tsc-93.htm

  - kismagasságú légi célok megfigyelésére alkalmas rádiólokátorok;
  - magasságmérő rádiólokátorok;
  - bemérő és tűzvezető rádiólokátorok;
  - légvédelmi rakéta egységek célmegjelölő rádiólokátorai;
  - tüzérségi lövedék röppályáját bemérő rádiólokátorok;
  - egyéb speciális rendeltetésű rádiólokátorok (például sebességmérő radarok);
- földi telepítésű, meteorológiai rádiólokátorokat;
- légi járműre telepített, földi objektumokat felderítő rádiólokátorokat, amelyek lehetnek:
  - áttekintő típusú terepkövető rádiólokátorok;
  - követő típusú terepkövető rádiólokátorok;
  - oldalt felderítő rádiólokátorok;
  - kismagasságú repülést biztosító rádiólokátorok;
- légi járműre telepített, légi objektumokat felderítő rádiólokátorokat, amelyek lehetnek:
  - repülőgép-fedélzeti korai előjelző és riasztó rendszer rádiólokátora (*Airborne Early Warning – AEW);*
  - vadászrepülők légi célfelderítő, rakéta rávezető rádiólokátora;
  - repülőgép-fedélzeti légi helyzet felderítő és harcvezető rádiólokátorok (*Airborne Warning and Control System – AWACS*);
- űreszközre telepített, földi objektumokat felderítő rádiólokátorokat;
- víz alatti hangfelderítő lokátorokat.

A rádiólokátorok lehetnek állandó telepítésűek, szállíthatóak, vagy a hordozó eszközükkel együtt mozgók.

Igen fontos rendszertechnikai ismérv a rádiólokáció módja, amely valamelyikébe minden eszköz besorolható.

Az aktív rádiólokáció esetén a rádiólokátor adója által előállított letapogató energianyaláb kisugárzásra kerül a kutatott térbe. Ha a nyaláb útjába olyan fizikai közeg, anyag kerül, amely a kisugárzott energiát nem nyeli el, és nem ereszti át változatlanul, akkor a közeget ért energia szóródni fog, többek között a rádiólokátor irányába is. A szóródás más irányban is jelentkezik, ezért az adó és a vevő nem törvényszerűen kell, hogy egy helyen legyen, bár az esetek többségében azonos antennarendszert használnak. A vevő- és indikátor egységek a visszavert jelet erősítik, feldolgozzák és a mérendő paraméterek kényelmes leolvasását elősegítő formában megjelenítik.

Az aktív válaszos aktív rádiólokáció esetén a céltárgyat ért besugárzást – ami általában kódolt jelsorozat – a fedélzeti vevőberendezés veszi, kialakítja a szükséges válaszjelet és visszasugározza. Az ilyen megoldást szekunder lokációnak is hívják. Ilyen üzemet használnak a polgári repülőgépek, amelyek a légtérirányító rádiólokátorok kérdező impulzusaira a fedélzeti transzponder által kialakított válaszjelet sugározzák vissza. A válaszjelben a magasságon, járatszámon kívül egyéb, például segélykérő információk is lekódolhatók. Hasonló elven működnek a saját-ellenség felismerő, azonosító rendszerek is.

4.5. kép. **P-35 felderítő rádiólokátor állomás**[183]

Ennek a rendszernek az az előnye, hogy a lokátor vevője nem a céltárgyról szóródott, kisteljesítményű jelet veszi, amely a céltárgyig és onnan vissza is megteszi az utat, hanem egy adóberendezés által kisugárzott, egyszeres utat megtett jelet kell feldolgozni.

4.6. kép. **Földi telepítésű földi mozgócél felderítő radar**[184]

A félaktív rádiólokáció esetén csak vevőrendszerünk van, amely a céltárgyról, más aktív rádiólokátor besugárzó jeléből származó visszavert jelet veszi. Több vevő esetén nemcsak a céltárgy iránya, de az összes koordinátája is meghatározható. Ezt a lokációs típust alkalmazzák a légvédelmi rakéták egy részében. A célmegvilágítását egy lokátor végzi, a rakéták pedig a visszavert jel nyomán vezetik ki magukat a célig.

[183] http://www.honvedelem.hu/cikk/35068_3d-s_radar_kisebb_energia_nagyobb_teljesitmeny (Letöltve: 2014.02.12.)
[184] http://www.npostrela.com/ru/products/75/567/ (Letöltve: 2014.02.12.)

Passzív rádiólokáció esetén a vevőberendezés a céltárgy által kibocsátott elektromágneses-, vagy infrasugárzást veszi, és a sugárforrás irányát határozza meg. Ezt rádióteleszkópokban, passzív önirányítású rakétákban alkalmazzák leggyakrabban.

A moduláció módja szerint a lokátorok lehetnek:

- folytonos kisugárzású rádiólokátorok (CW);
- frekvenciamodulált folytonos kisugárzású rádiólokátorok;
- monopulse rádiólokátorok;
- impulzusüzemű rádiólokátorok:
  - modulálatlan impulzus üzemű rádiólokátorok;
  - segédmodulációval ellátott impulzus üzemű rádiólokátorok;
  - impulzuskompressziós rádiólokátorok;
- infralokátorok;
- lézerlokátorok.

A fent leírt rendszertechnikai csoportosításokból jól látható, hogy nagyon sok működési elvű, alkalmazási módszerű rádiólokátor létezik. Az alábbiakban röviden ismertetésre kerül néhány olyan rádiólokációs zavarási eljárás, amely a legáltalánosabban elterjedt, napjainkban harci körülmények között alkalmazott.

Az aktív rádiólokációs zavarásról célszerű, ha a zavarandó lokátor rendeltetése, hordozója szerinti besorolásban beszélünk.

Ily módon a számunkra leginkább érdekesek lehetnek az alábbiak:

- a földi telepítésű, földi objektumokat felderítő rádiólokátorok zavarása;
- a földi telepítésű, légi objektumokat felderítő, célmegjelölő rádiólokátorok zavarása;
- a repülőeszközök fedélzetén üzemelő térképező, célfelderítő, fegyverirányító, terepkövető, oldalfelderítő, magasságmérő, kismagasságú repülést biztosító rádiólokátorok zavarása.

A földi telepítésű, földi objektumokat felderítő rádiólokátorok zavarása fizikailag folyamatos zajzavaró, vagy impulzusüzemű zavaróadókkal egyaránt megvalósítható. Az első lépcsős csapatok peremvonalhoz közeli területeken alkalmazott rádiólokátorainak megtévesztésére a passzív álcázó, imitáló eszközök, valamint a több hullámtartományban reális céljeleket szolgáltató makettek széles alkalmazást nyertek úgy a 70-es évek helyi háborúiban, mint az Öböl-háborúban.

A legnagyobb berendezéscsoportot a *földi telepítésű, légi objektumokat felderítő rádiólokátorokat zavaró berendezések* képezik. Ezek lehetnek a repülő köteléket kísérő elektronikai zavaró repülőgépek fedélzeti berendezései, konténerben, függesztő ponton elhelyezett önvédelmi zavaró berendezések, vagy a korszerű repülőgépek saját önvédelmi besugárzásjelző-zavaró rendszerének elemei. A kísérő zavaró repülőgépek feladatukat végrehajthatják a kötelékben repülve, vagy pedig úgynevezett stand-off – tűzhatáson kívüli – őrjáratozási zónából. Az Egyesült Államok légiereje és a haditengerészet repülőgépei egyre nagyobb számban rendelkeznek saját fedélzeti zavaróállomásokkal.

A B-1B hadászati bombázó az AN/ALQ-161A[185] típusú zavaró berendezéssel van ellátva, amely méreteire jól jellemző, hogy a tömege több mint 2300 kg, az ára eléri a tízmillió dollárt. A 0,2-20 GHz-es tartományban képes felderíteni, azonosítani és prioritási sorrendbe állítani a felfedett földi felderítő, célmegjelölő lokátorokat, valamint a légi vadászirányító és harcvezetési pontokat. Imitáló impulzus-, és álcázó zajzavarokat állít elő egy időben több lefogandó lokátornak. Automatizált vezérlőrendszer biztosítja az optimális célelosztást és a zavarási feladatok leghatékonyabb végrehajtását.

A B-52G, a C-130, az EC-130H és E típusokra szerelt AN/ALQ-172(V)1 és (V)2[186] beépített, vagy konténerben függeszthető zavaró berendezés a 3 és 10 cm-es hullámtartományban üzemel. Automatikus üzemben képes egy időben több célfelderítő, légvédelmi rakéta, sőt monopulse lokátor lefogására.

Az Egyesült Államok és a Szovjetunió lokátor zavaró technikai fejlesztési koncepciói két külön úton jártak. Az Egyesült Államokban a fő hangsúlyt a légierő és a haditengerészeti repülők fedélzetére szerelt elektronikai hadviselési eszközök fejlesztése kapta, ami az elektronikai hadviselési eszközök fejlesztésére fordított összegből mintegy 70%-os részesedést jelentett. Nézeteik szerint úgy a földi telepítésű, mint a légi hordozókon elhelyezett radarokat a levegőből célszerű zavarni. Ez a szemlélet megfelel a haderők mozgékonyságával, bevethetőségével szemben támasztott követelményeknek, hiszen a feladatok végrehajtásakor igen fontos szempont a kijelölt kötelék rugalmas kialakítása és a szükséges speciális eszközökkel való ellátása.

A szovjet/orosz zavarási koncepció szerint repülőgép fedélzetén elhelyezett berendezésekkel fogják le a légvédelemben üzemelő felderítő, célmegjelölő lokátorokat, a támadó repülőgépek fedélzeti felderítő, bombacélzó, oldalfelderítő, kismagasságú repülést biztosító lokátorainak lefogására pedig olyan földi, mobil zavaró állomásokat dolgoztak ki, amelyeknek nincsen nyugati megfelelője.

Ezek a zavaró állomások válaszimpulzus-zavarok és zajzavarok előállítására szolgáltak a 2-3 cm-es hullámtartományban. A válaszimpulzus-zavaró állomások egy, vagy több beállítható paraméterű objektum jelét dolgozták ki, amelyek jellemzői hasonlítottak az oltalmazott objektum által létrehozott céljelhez. A zavarjel kidolgozásához bizonyos időre van szükség, ezért a zavaró állomásokat a támadó repülőgépek várható repülési irányába, az objektum elé kell telepíteni. Van olyan típus, amely az impulzusonként át nem hangoló lokátorok számára megelőző impulzuszavart is képes kidolgozni, ezért ez az objektum mögé is telepíthető. A korszerűbb típusok rendelkeznek automatikus célkövető és veszélyes cél kiválasztó rendszerrel is. A zavaró jel vivőfrekvenciájának reprodukcióját mátrixvevő elven valósították meg analóg szűrőkkel és keverő rendszerrel.

A rádiólokátorok zavarásának megvalósítása a bonyolult adásmódok, jelfeldolgozási eljárások és zavarvédelmi fejlesztések eredményeképpen egyre nehezebb. Széles körben

[185] AN/ALQ-161A Defensive Avionics System http://www.fas.org/man/dod-101/sys/ac/equip/an-alq-161.htm (Letöltve: 2014.02.12.)

[186] AN/ALQ-172 Countermeasures System (CMS) http://www.fas.org/man/dod-101/sys/ac/equip/an-alq-172.htm (Letöltve: 2014.02.12.)

terjednek a speciális adásmódokat, impulzus kompressziót, impulzuson belüli frekvencia-, és fázismodulációt alkalmazó rádiólokátorok, ami oda vezetett, hogy a 80-as évek végén az USA átértékelte az elektronikai hadviselés elveit. Ennek köszönhetően az elektronikai ellentevékenységen belül az elektronikai csapás kiváltása egyre nagyobb hangsúlyt kapott.

Ennek eszközei az impulzus- és nagy energiájú rádiófrekvenciás fegyverek, amelyekről, mint a rádiólokátorok elleni harc eszközeiről a *4.3. Elektronikai pusztítás* fejezetben lesz részletesen szó.

A passzív zavaró eszközök alapvető sajátossága, hogy saját belső energiaforrással nem rendelkeznek, a róluk lesugárzott energia egy másik, úgynevezett megvilágító eszköztől származik. Primer rádiólokációs eszköz esetén a légtérbe kisugárzott elektromágneses energia a passzív zavaró eszközbe ütközve – megfelelő fizikai feltételek teljesülése esetén – arról szétszóródik, visszaverődik, többek között a rádiólokátor antennarendszere felé is. Fizikai hatásában ugyanaz a jelenség lép fel, mintha passzív céltárgyról visszaverődött jelet vennénk.

A passzív szándékos zavarok előállításának egyik eszköze a rezonáns, fél hullám hosszúságú fémfóliából, fémezett papírból, vagy fémezett üvegszálakból készülő úgynevezett dipól visszaverő. Ezeket elsősorban repülőeszközök passzív rádiólokációs álcázására, a felderítő, rávezető lokátorok elleni zavarfelhő előállítására használják. Az oltalmazni kívánt repülők beérkezése előtt fedélzeti dipólszóró konténerből, vagy rakétából kiszórják a dipólok sokaságát, amelyeket a légköri turbulencia szét is oszlat a légtérben. A dipólok alakját úgy határozzák meg, hogy adott frekvencián a hatásos visszaverő felületük minél nagyobb legyen, és a kiszóródás után a süllyedési sebességük a lehető legkisebb legyen, vagyis a dipólfelhő minél tovább „lebegjen". Nyugodt légköri viszonyok esetén az átlagos süllyedési sebesség 20.000 m felett 60-180 m/min, 20.000 m alatt pedig 25-70 m/min.

A dipólokat konténerben tárolják kiszórás előtt, és elektromechanikus, pneumatikus, vagy pirotechnikai elven működő automatikus kidobó berendezéssel juttatják ki a megfelelő mennyiségben. A szükséges rezonáns hossz megállapítása érdekében előzetesen rádiótechnikai felderítő repülést hajthatnak végre. Ha ez nem lehetséges, vagy eddig nem működtetett új eszközök bekapcsolása várható, akkor célszerű az automatizált dipólvágóval felszerelt szóró konténerek alkalmazása. Ezek a repülés során megmérik az éppen üzemelő rádiólokátorok frekvenciáit, és azonnal a szükséges hosszra vágva szórják ki a dipólokat.

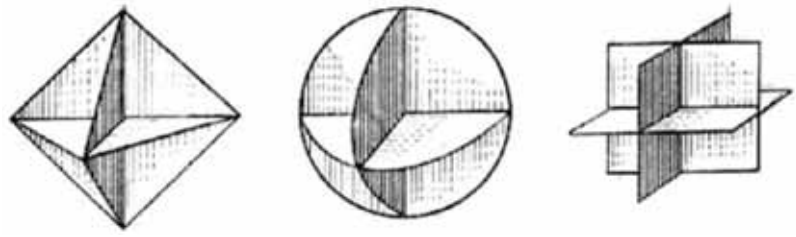
A szétszóródott dipólfelhő a rádiólokátor indikátorán fénylő pontok sokaságaként jelentkezik, a keskeny sávú zajzavarok hatásával mutat hasonlóságot. Eredményeképpen a mögöttes légtérben mozgó repülőgép az indikátoron nem lesz látható.

Ez a felhő a légtérben csak lassan mozog, ami lehetővé teszi, hogy a rádiólokátor passzív zavarszűrő berendezése, az állócélokhoz hasonló módon kiszűrje. A problémát csak az jelenti, hogy a dipólfelhőben található önálló elemek véletlenszerűen, időben sztochasztikus módon verik vissza a lokátor impulzusait, ennek köszönhető a zajszerű fizikai viselkedés.

Ez a módszer tehát földi telepítésű, vagy légi hordozón üzemelő rádiólokátorok passzív, álcázó jellegű zavarására szolgált.

A szögvisszaverők fizikai kivitelüket tekintve egymásra merőlegesen elhelyezett fémlemezekből állnak, amelyekről a beeső rádióhullámok az optikai tükrözési törvényekkel analóg módon a besugárzás irányában visszaverődnek. A gyakorlatban ez azt jelenti, hogy egy rádiólokációs eszköz által besugárzott szögvisszaverő nem szórja a beeső energiát, hanem jó hatásfokkal visszaveri, tehát egy viszonylag nagy rádiólokációs hatásos visszaverő felületű céltárgy jelét produkálja.

A legegyszerűbb konstrukció két, egymásra merőleges vezető felületből, például fémlemezből áll. A visszaverődött hullám polarizációja a kétszeres visszaverődés után azonos lesz a beeső hullám polarizációjával. A kétlemezes sarokvisszaverő hátránya, hogy viszonylag szűk a hullámtükrözés lehetséges szögtartománya. Ezen úgy lehet javítani, hogy egy harmadik lemezzel egészítjük ki, amely mind a két eddigi lemezre nézve merőlegesen áll, vagyis egy sarkot képezünk. A gyakorlatban megépített szögvisszaverők egymást metsző síkokból állnak, így összesen nyolc sarokreflektor képződik.



4.2. ábra. **A leggyakoribb szögvisszaverő formák**[187]

Ha a fémfelületek lineáris méretei jóval meghaladják a beeső hullám hullámhosszát, akkor olyan tükörként működik a rendszer, amelynek vannak fő nyalábjai és vannak oldalszirmai. A háromoldalú saroknak mind horizontális, mind vertikális síkban három maximuma van. A középső maximum a háromszoros visszaverődés miatt alakul ki, és a szögvisszaverő szimmetriatengelyével párhuzamos. A másik két, kisebb maximum a kétszeres visszaverődések miatt alakul ki.

A különböző alakú és méretű szögvisszaverők effektív hatásos visszaverő felülete a fizikai méret és a hullámhossz ismeretében számítással is meghatározható. A háromszög oldalú szögvisszaverő esetében például:

$$\sigma_{max} = \frac{4\Pi a^4}{3\lambda^2} \quad \text{és} \quad \Theta_{0,5} \cong 60° \tag{4.3}$$

ahol: σ_{max} – a szögvisszaverő hatásos rádiólokációs visszaverő felületének elméleti maximális értéke [m^2];
$\Theta_{0,5}$ – a félteljesítményű pontok között szög nagysága;
a – az oldalhosszúság [m];
λ – a hullámhossz [m].[167]

[187] Palij, A. I.: *Radioelektronnaja Borba*. Voennoje Izdatyelsztvo, Moszkva, 1989. p. 79.

A szögvisszaverőket gyakran csoportokban telepítik, mivel az irányhatásuk meglehetősen lyukas, tehát nem biztosítanak bármely irányból megfelelő rádiólokációs álcázást. A zavaró hatás tovább fokozható, ha például négy háromszög oldalú szögvisszaverőt egy forgó keretre erősítenek. A forgás következtében a hatásos visszaverő felület pillanatról-pillanatra változik, ami a visszavert jelben amplitúdó modulációt okoz. A reflektáló felületek közeledése és távolodása miatt egy fázis, következésképpen frekvenciamoduláció lép fel a visszavert jelben.

A körpolarizált hullámokat a háromszori visszaverődés a beeső hullám ellenkezőjére fordítja, ezért a polarizációs veszteség csökkentése céljából fázistoló bevonattal lehet ellátni valamelyik felületet, és így a visszavert jel fázishelyes lesz.

A szögvisszaverőket álcázási, vagy imitálási célból telepítik. Ha a célunk az, hogy például a földi, vagy az oldalfelderítő lokátorral végrehajtott felderítés ellen elfedjünk, álcázzunk egy adott nyílt útvonalat, amelyen technikai eszközök fognak elhaladni, akkor oda oszlopokra kettesével, négyesével felfüggesztett szögvisszaverőket telepítenek az út mentén. Ez természetesen egy alacsony környezeti rádiólokációs kontrasztosságú háttéren „világító" vonalként fog megjelenni, amivel várhatóan nem az álcázást, hanem az ellenkezőjét fogjuk elérni.

Ha adott ismertető jegyekkel rendelkező objektumokat akarunk imitálni, akkor arra kell törekedni, hogy a lehető legtöbb hullámtartományban, és térben létrehozzuk az arra az objektumra jellemző fizikai effektust. Tehát egy harckocsi legyen például elég nagy, elég zöld, elég nagy mágneses tömeg, legyen adott végén megfelelő intenzitású hőkibocsátása, legyen rádióforgalma. A rádiólokációs hatásos visszaverő felületétét szögvisszaverőkből lehet egyszerűen létrehozni. Ügyelni kell ugyanakkor arra is, hogy az objektumunk ne egy kis fényes pont legyen a felderítő lokátor ernyőjén, hanem egy megfelelő nagyságú fénylő folt. A fénylő foltot több, kisebb szögvisszaverő területen való elhelyezésével lehet elérni, azonban ennek pedig olyannak kell lenni, hogy az önálló fénypontok összefüggőnek látsszanak, nehogy „szétessenek". Fizikailag ez azt jelenti, hogy közelebb kell lenniük egymáshoz, mint a lokátor felbontóképessége.

Ma már a korszerű multispektrális (több hullámtartományban egyszerre dolgozó) felderítő eszközök az egyes tartományokban szerzett adataikat korreláltatják, és többszintű megerősítési folyamattal szűrik ki a hamis célokat a valódiak közül. Az Öbölháború jó példával szolgált arra is, hogy ha nem elégséges számú és szintű információ áll rendelkezésre, akkor a célok azonosításának hibái következtében mennyi felesleges csapásra került sor makettekre.

4.1.2.3 Az infratechnikai eszközök és zavarásuk

Az infravörös sugarak a látható fény és a milliméteres hullámok között helyezkednek el a mikrométeres hullámtartományban. A -273,16 °C hőmérséklet felett minden test infravörös, szemmel nem látható sugárzást bocsát ki. Az infravörös tartományt a katonai alkalmazások széles körben alkalmazzák úgy mérési, érzékelési, mint hírközlési célokra. A méréstechnikai felhasználás során a testek által kibocsátott hőt a háttér hősugárzásával, vagy referencia hőmérsékletet biztosító anyag hőmérsékletével (például folyékony

nitrogénnel) hasonlítják össze. Az érzékelő fejek, pelengátorok és képalkotó eszközök által szolgáltatott jeleket erősítés, jelfeldolgozás után egy vezérlőrendszerbe juttatják, vagy valamilyen monitoron teszik láthatóvá.

A hírközlési alkalmazásokban infravörös sugarakat kibocsátó sugárzók és érzékelők veszik át az adó-, és vevőantennák szerepét. Széles körben alkalmazzák távirányítókban is, mert zárt helyen meglehetősen zavarvédett, optikai álcázás után nincs nemkívánatos melléksugárzása.

Az infravörös sugárzást alkalmazó berendezéseket két nagy csoportba sorolhatjuk: az aktív és passzív eszközök csoportjába.

Az aktív infravörös berendezések működtetéséhez infravörös megvilágító eszközök, reflektorok és megfelelő vevőberendezések szükségesek. A reflektor által megvilágított testekről visszaverődött hősugárzást veszi a vevő, és azt használja fel a rendeltetésének megfelelően.

Előnye, hogy érzéketlenebb vevőeszközökkel is jó eredmény érhető el, járulékos modulációkkal pedig a szándékos zavarok elleni védettségi jellemzők javíthatók. Hátránya, hogy a megvilágító sugárforrások intenzív áruló tényezők. Aktív infra reflektorok találhatók a harcjárművek éjjellátó rendszereiben, amely a kezelők éjszakai tevékenységét, a jármű vezetését, és a tájékozódást biztosítják a terepen.

A passzív infravörös berendezésekben nem alkalmaznak külön megvilágítást, hanem azt használják ki, hogy a testek a háttér környezetüktől eltérő intenzitású – következésképpen eltérő hullámhosszúságú – hősugarakat bocsátanak ki. A passzív infravörös berendezésekhez tartoznak a hőpelengátorok, az éjjellátó eszközök, foton sokszorozós éjszakai távcsövek, infra fényképező-, és video rendszerek.

Az infravörös sugárzás mértékét a sugárzási intenzitás jellemzi.

$$I = \varepsilon \sigma T^4 S / \Pi \tag{4.4}$$

ahol: ε – a sugárzási együttható, amely például repülőgép hajtóművek esetén = 0,8-0,9; A gázturbinák kiáramló gázsugarára e = 0,2;

σ – a Stephan-Boltzmann állandó;

T – a hajtómű, a gázsugár, vagy adott test hőmérséklete [K];

S – a hatásos sugárzó felület nagysága a megfigyelés irányában.

Az összefüggésből látható, hogy az infravörös sugárzás intenzitását a hőmérséklet befolyásolja a legjobban, mivel annak negyedik hatványa szerint változik az intenzitás.

Egy repülőgép hajtómű alkatrészeinek hőmérséklete 500-1200 K között van, a kiáramló gázsugár mintegy 900 K, utánégető üzemmódban elérheti az 1700 K hőmérsékletet. A Holizin-Wien-féle eltolódási törvénynek megfelelően a repülőgépek infravörös kisugárzásának hullámtartománya a 2,4-6,4 mm közé esik, utánégető alkalmazása esetén pedig 1,7-6,4 mm közé.

A korszerű levegő-levegő osztályú rakéták infravörös kereső fejének érzékelési tartománya a 2-6 mm hullámtartományban van. Ahhoz, hogy megértsük az infravörös tartományú önirányító rendszerek zavarásának elvét, röviden tekintsük át egy önirányító fej felépítését és működését. Az infravörös önirányító fej a rakéta fejrészében helyezkedik el. Az orrészben található objektív mögötti optikai szűrő kiszűri a 2 mm-nél nagyobb

hullámhosszúságú hullámokat. A beérkező sugárzást egy modulátorra vezetik, majd a célról kapott, modulált sugárzást elektromos jelekké alakítja át egy fényelem. Ez alapján a rakéta giroszkópikus követő berendezése dolgozza ki a kormányszervek részére szükséges parancsjeleket.

Az infravörös zavarás egyik fő alkalmazási területe a repülőgépek önvédelmi rendszere, amely az infravörös önrávezérlésű rakéták eltérítésére, vezérlésének megbontására szolgál, de széles körben alkalmazhatják a földi infra önrávezetős páncéltörő rakéták zavarására is. Nem közvetlenül, de a zavaráshoz sorolhatjuk azokat a passzív, konstrukciós megoldásokat, amelyek csökkentik a hajtóművek, motorok, súrlódó felületek hőkisugárzását. Ezek lehetnek az alacsonyabb hőmérsékleten való működésre irányulók, vagy a létrejött hőt szétszóró, árnyékoló, vagy hűtő megoldások. A repülőgépek közül például az A-10A csatarepülő tűnik ki a rendkívül kis intenzitású infravörös sugárzásával, amit a speciálisan kiképzett hajtómű kimenettel, hőterelő és szétszóró burkolattal értek el.

Az infravörös sugarak igen fontos tulajdonsága, hogy az emberi szem számára nem láthatóak, de az emberi látást korlátozó ködön, füstön keresztül kis csillapítással áthaladnak. Ez teszi igen alkalmassá a harctéri körülmények között végzett felderítésre.

Az infravörös önrávezető páncéltörő eszközök ellen speciális aerosolokat fejlesztettek ki, amelyek összetétele olyan, hogy a látható és az infravörös hullámokat is erősen csillapítják. Ezzel lehetővé válik az aerosolos hőálcázás, amely mögött a technikai eszközök felderítési zónahatára igen lecsökken.

A megtévesztő hőcélok rendeltetése, hogy a védendő objektumok létezéséről, koordinátáiról megtévesztő információkat szolgáltasson az infrafejes önirányító rendszerek számára. A megtévesztő hőcélok lehetnek:

- speciális repülőeszközök, amelyek az oltalmazandó objektummal azonos spektrumú hőképet állítanak elő, és magukra vonják a légvédelmi, vagy légiharc rakétákat;
- hőimitáló lövedékek, amelyeket a támadás észlelésekor a fedélzeti önvédelmi rendszer automatikusan kilő, vagy kazettából sorozatban kidob;
- ejtőernyős, sikló és kábelen vontatott hőimitátorok.

Az infravörös vezérlő fejek ellen hatásos eszköz lehet az érzékelő elem túlterhelése, amely a rakéta előtt intenzív fényfelvillanást okozó pirotechnikai eszközzel érhető el. (4.7. kép) Elméletileg a fénydetektor például lézerfény segítségével megrongálható, azonban repülés közben gondot okoz a pontos célzás.

A pirotechnikai hőimitátorok, hőcsapdák kifejlesztésükkor – a 70-es években – először igen hatásosnak bizonyultak. Az infra önrávezető fejes rakéták a legintenzívebb hősugárzásra, a legrövidebb hullámhosszúságú, 1-2 mm-es kisugárzásokra voltak optimalizálva. Az ilyen rakéták ellen megfelelő hatékonyságú védelmet nyújtottak a veszély esetén kilőtt pirotechnikai csapdák, mint például az MJU-7 és 10-es típus, amelyből például egy A-10A csatarepülő fedélzetén 240 db-ot helyeztek el. Az önrávezető fejek korszerűsítése során a fejlesztők rájöttek, hogy a repülőgép hőspektruma és a hőcsapda spektruma meglehetősen eltér egymástól, vagyis szelektálni lehet, azaz vannak jellegzetes vonások bennük, ami alapján meg lehet különböztetni őket. Fizikailag ez azon

alapszik, hogy az intenzitás növelésével a spektrum megváltozik, ami nem kívánatos. A 80-as években megalkotott infra önrávezető fejek két különböző hullámtartományban dolgozták fel a céljeleket. Kiterjesztették a működési tartományt a spektrum 4-4,8 mm-es részére is, és jelfeldolgozó processzort alkalmazva hatékonyan különválasztották a valós és hamis célokat.

A korszerűsített – például Sidewinder – rakétákat a hőcsapdák kiszűrésére új optikai szűrővel szerelték fel, amelyek már csak a 4-5 mm-es hullámtartományba eső infravörös sugarakat engedik át, amelyek a repülőeszközökre jellemzőek, de a hőimitátorokra nem.

4.7. kép. **Infracsapdák kidobása egy szállító repülőgépről**[188]

Ennek következtében a repülőeszközök sérülékenyebbé váltak, a hőcsapdák hatékonysága nagymértékben visszaesett. Az utóbbi évek kutatásainak egyik területévé vált a fentebb leírt probléma leküzdése. A megoldás alapvetően két irányban bontakozott ki. Az egyik a repülőgépet ért rakétatámadás jelzésére szolgáló berendezéseknek *(Missile Approach Warning System – MAWS)* a kifejlesztése, amelyeknek alapvetően két fajtája létezik: az impulzus-doppler rádiólokációs és az optoelektronikai. A magas fokú automatizáltság eredményeképpen a rendszer a riasztáson kívül kiválasztja az optimális ellenrendszabály fajtáját, meghatározza a támadó rakéta mozgásparamétereit, és a saját manőver figyelembevételével az infracsapdák, dipólok, aerosolok kibocsátásának, vagy a zavaró berendezés bekapcsolásának optimális idejét, üzemmódját. A másik, a vontatott, vagy önálló hajtóművel repülő hamis célok, decoy-ok alkalmazása, amelyekről még részletesen szólunk.

Az infravörös hullámtartományban kifejlesztettek lokátorokat is, amelyek hatótávolsága eléri a 10 km-t, a szög szerinti felbontó képessége pedig a 4 fokpercet. A működési

[188] http://htka.hu/2010/04/28/sajat-infracsapdaja-rongalt-meg-egy-ausztral-oriont/ (Letöltve: 2014.02.14.)

elve azonos az impulzus lokátorokéval, csak elektromágneses impulzus helyett infravörös impulzust sugároznak ki. Az ellenük való tevékenység úgy a hőálcázási, hőimitációs módszerekkel, mint az aktív vakítási módszerekkel eredményesen folytatható.

4.1.2.4 Az optikai hullámtartományú eszközök és zavarásuk módszerei

Az optikai eszközöket egyrészt az ellenséges csapatok felderítésére, másrészt a saját csapatok álcázási rendszabályainak ellenőrzésére használjuk.

A látható fény hullámtartományában, a 0,4-0,7 mm között működik az emberi látás és az azt segítő optikai berendezések, mint például a távcsövek, foto- és video eszközök, a képfelvevő, képrögzítő berendezések. A vizuális megfigyelésen kívül a harctérfelderítés sok optikai tartományú elektronikai berendezéssel folyik. A felderítő rendeltetésű pilóta vezette és pilóta nélküli repülő eszközök, programozott cirkáló rakéták, kamerákkal, fényképezőgépekkel, valós idejű video képet szolgáltató kamerákkal lehetnek felszerelve.

Az optikai rendszerek elleni tevékenység egy része a rejtés és álcázás, az elektronikai védelem és a hadműveleti biztonság kérdéskörébe tartoznak, ezért ezekre más fejezetekben térünk ki részletesebben.

Az aktív ellentevékenységi rendszabályok közé tartoznak a ködösítés, a füstök, aerosolok alkalmazása. A ködöt, füstöt ködgránátokkal, ködgyertyákkal, vagy a harcjárművek saját ködfejlesztő berendezéseivel lehet előállítani. A legegyszerűbb például a harckocsik kipufogó rendszerébe juttatott gázolaj, amely nem lánggal ég el, hanem sűrű, jó állékonyságú füstöt generál.

Aktív optikai megtévesztési módszer a makettek, imitációs eszközök alkalmazása is. A makettek mesteri megtervezése és kivitelezése egyáltalán nem egyszerű feladat, mivel a vizuális megtévesztésen kívül a makettnek úgy az infravörös tartományban, mint a rádiólokációs eszközökkel szemben is a valóságos harceszközt mindenben hűen kell ábrázolnia.

A makettek a korszerű háborúban is fontos szerepet játszanak. Az Öböl-háború tapasztalatai alapján kijelenthető, hogy a több hullámtartományban végzett felderítés, a számítógépes feldolgozás ellenére igen nagy számban ért rakéta és egyéb csapás iraki rakétaindító állásokat imitáló maketteket. Ez komoly meglepetést is okozott, hiszen a számítások szerint már több indítóállást is sikerült megsemmisíteni, mint amennyiről egyáltalán tudomása volt a szövetséges csapatoknak. És ezután kezdődött az izraeli városok Scud rakétákkal való terrorizálása. A vezetésben és felderítő rendszerben keletkezett meglepetésnek köszönhetően komoly előrelépések történtek a felderítő rendszerben áramló célinformációk korreláltatására, megbízhatóságuk növelésére. A műszeres, műholdas és repülőfedélzeti optikai felderítés a multispektrális felderítés tökéletesítése felé halad, amit nagymértékben támogatnak az utóbbi években egyre tökéletesedő képdigitalizálási, képtömörítési és feldolgozási eljárások.

4.1.2.5 A lézerfényt alkalmazó eszközök zavarásának módszerei, elvei

A lézersugarak legfontosabb jellemzői, hogy monokromatikusak és koherensek. A monokromatizmus azt jelenti, hogy egy lézer sugárforrás által előállított sugárzásban csak egy hullámhosszúságú rezgés található meg, ellentétben például a fényhullámokkal, amelyek széles spektrumot foglalnak el. A koherens sugárzás azt jelenti, hogy a sugárzást a tér bármely pontjában egyetlen, a fázis- és amplitúdó viszonyokat összefoglaló összefüggéssel lehet leírni, ahol tehát a hullámok a tér adott pontjában bármikor szinkron és egybevágó jellegűek. A rádióantennák által kisugárzott rádióhullámok is koherens hullámok, tehát az antennától bármely távolságban a fázis és amplitúdó viszonyok egyértelműen meghatározottak. A jegyzet terjedelme nem teszi lehetővé, hogy a lézerfény előállításával és a fizikai folyamatokkal bővebben foglalkozzunk. Annyit kell róla itt elmondani, hogy a különböző energiájú lézereket katonai célokra széles körben alkalmazzák. A kisteljesítményű lézerfényt távmérőkben, célzókészülékekben, sebességmérőkben, fegyverirányító eszközökben, a hírközlésben, a közepes teljesítményűeket a lézerrávezetésű rakétarendszerekben alkalmazzák, míg a nagyteljesítményű változatokat, az úgynevezett átégető típusú lézereket a technikai eszközök pusztítására, rongálására használhatják.

A nagyteljesítményű lézereszközök kulcsszerepet játszanak a Hadászati Védelmi Kezdeményezés néven ismertté vált csillagháborús tervekben. A teljesítményszükséglet mértékét jól szemlélteti, hogy a gerjesztő energiát nukleáris láncreakcióval tervezik előállítani. A program még kísérleti fázisban leállításra került ugyan, de egyes részeredményeit az irányított energiájú fegyverek *(Directed Energy Weapon – DEW)* fejlesztése során felhasználják.

A lézersugárral működő berendezések ellen olyan speciális aerosolok alkalmazhatók, amelyek az optikai ködösítéssel analóg módon elnyelik, vagy nagymértékben csillapítják a lézerfényt, és ezzel akadályozzák a visszavert jel bejutását a vevődetektorba. A közvetlen zavarás másik módja vakító lézerforrások üzemeltetése, amelyek energiája jóval nagyobb, mint a tárgyakról visszavert hullámok, így telítésbe viszik a vevőberendezést és kiértékelhetetlenné válnak a reális objektumokról kapott jelek. A hatékonyság alapvető feltétele a hullámhossz pontos ismerete, mivel a nemkívánatos zavaró jelek viszonylag egyszerűen kiszűrhetők, ha nem pontosan az üzemi hullám áteresztési tartományába esnek.

A lézersugarak elleni védekezés céljából olyan speciális szemüvegeket dolgoztak ki, amelyek megvédik a kezelő állományt a részleges, vagy végleges vakítástól. A lézerfénynyel való vakítást nemzetközi szerződés is tiltja.

4.1.2.6 Az akusztikai tartományú zavarás módszerei, eszközei

Az akusztikai hullámtartománynak három fő katonai felhasználási területét különböztethetjük meg:

- az akusztikai felderítő eszközökkel végzett harctéri felderítő tevékenységet;
- a vízfelszíni és víz alatti hajók – például tengeralattjárók, torpedók – felderítését, amelyet hidroakusztikai felderítésnek nevezünk; és
- az élőerő ellen irányuló akusztikai besugárzást.

A harctéri akusztikai felderítést előbb az emberi fül irányérzékenységére, majd később a műszeres, elektronikus eszközökkel való regisztrálásra építették. A repülőgépek megjelenésekor az első légvédelmi figyelőposztok – úgynevezett fülelők, tölcsérek – között helyet foglaló kezelők segítségével mérték be a repülőgépek pillanatnyi helyét. A vietnami háborúban, a dzsungelben mozgó harcosok és technikai eszközök jelzésére az amerikai csapatok ballonokra függesztett mikrofonokat és rádióadókat helyeztek el, hogy idejében riaszthassák a csapatokat a várható veszélyről. A harctéri szenzorok egy része az akusztikai tartományban üzemel, ami lehetővé teszi, hogy a felderítési zónahatáron belül megállapíthassák az arra mozgó járművek jellegét, darabszámát, emberek jelenlétét, több szenzor adatainak kiértékelésével pedig mozgásuk irányát, sebességét. Vannak olyan tüzérfelderítő eszközök, amelyek a lövedék hangja alapján képes a tüzelést folytató eszköz pozíciójának bemérésére.

A harctéri akusztikai felderítés elleni tevékenység állhat a felfedett berendezések megsemmisítéséből, passzív, álcázó rendszabályok bevezetéséből, és aktív akusztikai zavarok – hangeffektusok – mesterséges előállításából.

A hidroakusztikai felderítő tevékenység kiemelkedő fontosságú a haditengerészet számára. Mivel a vízben az alacsonyfrekvenciás mechanikai rezgések a rádióhullámoktól eltérően kiválóan terjednek, ezért a vízfelszíni, vagy víz alatti objektumok által kibocsátott zajok megfelelő eszközök segítségével igen nagy távolságból felfedhetők. Minden hajónak, tengeralattjárónak saját hangspektruma van, amely csak rá jellemző és azonosítja is. A világtengereken folyó szüntelen tengeralattjáró bújócska legfontosabb eszközeit a szonárok és hanglokátorok képezik. (4.8. kép)

A megtévesztésükre, lefogásukra irányuló hidroakusztikai zavarás passzív és aktív rendszabályokra osztható.

4.8. kép. **Helikopterre függesztett hangfelderítő szonár**[189]

[189] AN/AQS-22 ALFS Sonar System https://www.defenseindustrydaily.com/154m-for-3-aqs-22-alfs-sonars-et-al-03643/ (Letöltve: 2014.02.14.)

A passzív hidroakusztikai ellentevékenység eszközei közé sorolhatók mindenekelőtt azok a tervezési, konstrukciós megoldások, amelyek egyrészt csökkentik a hajótestek hangátvezető képességét, a hajtóművek mechanikai zúgását, a hajócsavarok forgása által keltett gőzbuborékok (kavitáció) hangját, másrészt csökkentik a hajótest akusztikus visszaverődési képességeit. A hajótestek több rétegből állnak, amelyek között hangszigetelő anyagok helyezkednek el. A hajtóművekből száműzték például a legnagyobb mechanikai zajforrást, a fogaskerekes áttételi műveket.

A hajócsavarokat ma már számítógéppel tervezik, modellezik és optimalizálják, hogy a nyomatékátadás és a lapátok által keltett hangok a lehető legoptimálisabb arányt adják. A külső burkolatokat lágy műanyag, polipropilén, természetes kaucsuk, vagy más korszerű, nagy hangelnyelő tulajdonságú anyaggal vonják be. Fontos szerepet játszik az akusztikai védelmi rendszabályok ellenőrzése, amely az esetleges meghibásodásokra is fényt deríthet. Mérések sorozatával felveszik a tengeralattjárók különböző üzemmódjaiban jellemző zajossági értékeket, és a harcfeladatok idején ezek ismeretében választható ki az optimális tevékenységi mód. Mivel az atomhordozó tengeralattjárókat a világtengereken szigorúan nyilvántartják, mozgásukat követik, így diplomáciai „rendkívüli eseménynek" számít egy ismeretlen hangspektrumú egység megjelenése, vagy eltűnése, elvesztése.

Az aktív hidroakusztikai ellentevékenység magába foglalja:

– a hidroakusztikai zavaró berendezések;
– imitációs zajforrások;
– hamis céltárgyak – vontatott, sodródó, vagy saját meghajtással rendelkező decoy-ok – alkalmazását.

A hidroakusztikai zavaró berendezések feladata a szonárt kezelők túlterhelése. A zavaró berendezés veszi a környezetéből érkezett zajokat és rögzíti, majd visszasugározza. Ezzel olyan a valós helyzettől teljesen eltérő zajállapotot teremt, amelyben a valós helyzet kiderítése igen nehéz.

Az imitációs zajforrások is a figyelem elterelésére, megosztására szolgálnak. Ezek olyan vegyi anyagokkal teli tartályok, amelyek a tengervízzel való érintkezéskor intenzív pezsgést, gázképződést indítanak el, amely hangja a vízben jól terjed. Hátrányuk, hogy a vízben nem mozognak, így nem áll elő a mozgó testekre jellemző Doppler frekvencia eltolódás jelensége.

Olyan előre rögzített zajt sugároznak, amely valamely valós hajóegység egy adott tevékenysége mellett a valóságban fennáll. A célokat persze nemcsak az általuk keltett hangtartományban mérik, hanem például az általuk okozott mágneses tér változást is indikálják. Ahhoz, hogy egy imitátor mágneses szempontból is hitelesen működjön, árammal átjárt hosszú kábelt alkalmaznak, amely mágneses mezőt hoz létre maga körül. A cél befogásakor derül csak ki, hogy egy imitációs adóról van szó.

A hamis céltárgyak feladata nemcsak a figyelem elvonása, hanem a hajók oltalmazása is. Ezeket a vízfelszíni hajók, vagy tengeralattjárók azért vontatják maguk után, hogy a decoy-ok magukra vonják a passzív, vagy aktív akusztikus önrávezető rendszerrel ellátott torpedókat.

A hajóegységet ért támadáskor a tengeralattjáró előbb bekapcsolja a fedélzeti hidroakusztikai zavaró berendezését, amely telítésbe viszi a támadó fél hangfelderítő berendezését. Ezután elindítanak egy, vagy több hamis céltárgyat, amely magára vonja a figyelmet, miközben a valódi hajóegység minden zajforrását kikapcsolva vár, hogy üldözője eltávolodjon a hamis célt követve.

4.1.2.7 Az egyszeri felhasználású zavaró berendezések

Az egyszeri felhasználású zavaró berendezések az elektronikai zavaró eszközök azon fajtái, melyeket egy bevetésre terveztek. A szemben álló fél területére repülőeszközzel, tüzérséggel, vagy ember által kijuttatva, önműködően kezdik meg működésüket és emberi beavatkozás, illetve felügyelet nélkül hajtják végre a célobjektumként kijelölt elektronikai eszközök folyamatos vagy szakaszos üzemű lefogását.

Rendeltetésük tehát, a szembenálló fél harcászati – hadműveleti mélységében üzemelő ultrarövid hullámú hírközlő rendszerek, rádiólokációs eszközök aktív zavarással történő lefogása, saját eszközeink üzemelésének álcázása.

Az egyszeri felhasználású zavaró berendezések a harcászati-műszaki paramétereik alapján feloszthatók teljesítmény, modulációs mód, frekvencia tartomány, zavarjel sávszélesség, üzemidő, működési mód, kijuttatási mód és automatizálási fok szerint.

A kisugárzott jel *teljesítménye* szerint lehetnek:
- kis, 0,1-0,5 W;
- közepes, 0,5-5 W; vagy
- nagy teljesítményű eszközök 5 W felett.

A kisugárzott zavarjel *modulációs módja* szerint megkülönböztethetünk:
- amplitúdó modulációs;
- frekvencia modulációs;
- impulzus modulációs üzemmódban dolgozó zavaróadókat.

Az üzemi *frekvencia tartomány* alapján szolgálhatnak:
- ultrarövid hullámú híradó berendezések zavarására;
- rádiórelé eszközök zavarására;
- rádiótechnikai célfelderítő-, és tűzvezető eszközök zavarására;
- lokátor-vezérlésű rakéták zavarására.

A *zavarjel sávszélessége* szerint lehetnek szélessávú (elfojtó), vagy keskenysávú (célzott) zavaróadók.

Az *üzemidő* szerint megkülönböztetünk rövid, 5-30 perc, és hosszú üzemidejű, 30 perc fölötti eszközöket.

A lehetséges üzemidő szempontjából döntő fontosságú az akkumulátorok kapacitása, a zavarjel üzemmódja és az eszköz általános működési módja.

*Működési mód*juk szerint lehetnek folyamatos üzemelésűek, vagy szakaszos működtetésűek.

A meghatározott zavarási célkörzetbe való *kijuttatás módja* szerint megkülönböztetünk:

- tüzérségi eszköz által kijuttatott;
- repülőgép, helikopter által ledobott;
- ügynökök, mélységi felderítők által telepített;
- a harc megkezdése előtt a saját területen elhelyezett, és később aktivizált eszközöket.

Az *automatizáltság fejlettségi foka* szerint lehetnek:

- mechanikus aktivizálásúak;
- késleltetett bekapcsolásúak;
- elektronikusan programozottak;
- távműködtetésre is alkalmasak.

Előnyös tulajdonságuk, hogy zavaró hatásukat a célobjektum közvetlen közelében fejtik ki, így az energiaviszonyok a hagyományos rádiózavarási pozíciókhoz képest jóval kedvezőbben alakulnak. A saját csapatok elektronikai védelme szempontjából is igen kedvező a tőlünk viszonylag távol és kisebb teljesítménnyel létrehozott zavarás, mint a saját harcrendben üzemelő nagy teljesítményű zavaró adók. Az egyszeri felhasználású zavaró berendezések segítségével olyan területeken települt harcrendi elemek rádióösszeköttetései is zavarhatók, amelyek a terep domborzati, vagy fedettségi viszonyai miatt saját harcrendben elhelyezett zavaró berendezés számára hatékonyan nem sugározhatóak be.

További előnyként értékelhető, hogy működés közben a zavaró állomások karbantartást nem igényelnek.

Amennyiben a kijuttatásuk a tervekben meghatározott időben megtörténik, a harccselekmények döntő momentumaira koncentrálható a zavarás.

4.1.2.8 A navigációs eszközök zavarása

A navigációs eszközök helymeghatározásra, útvonal regisztrálásra, beprogramozott útvonal követésére szolgálnak. A hajók, tengeralattjárók, repülőgépek helyzetének meghatározására az esetek többségében nem áll rendelkezésre stabil viszonyítási pont, ezért egy egész műszercsoport szükséges a pozíció beméréséhez. A navigációs rendszerek felosztathatók:

- autonóm navigációs rendszerekre; és
- nem autonóm navigációs rendszerekre.

Az autonóm navigációs rendszerekhez tartoznak azok a berendezések, amelyeknél az adott hordozó fedélzetén elhelyezett egységekhez más külső eszköz nem szükséges. Ilyen autonóm navigációs rendszer például:

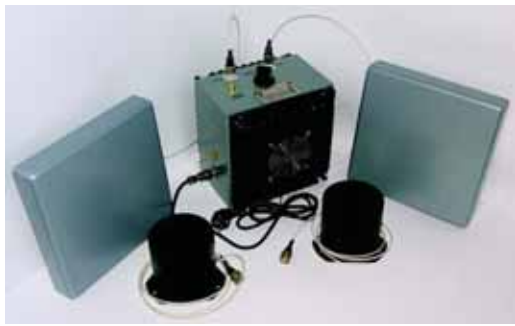
- a csillagászati;
- az inerciális;
- a doppler rádiólokátoros.

A nem autonóm rendszereknek a fedélzeti egységeiken kívül földi, vagy műholdas segédberendezései vannak, amelyek nélkül a működtetésük nem lehetséges. Ilyen nem autonóm navigációs rendszerek például:

- a rádió iránytűs rendszerek (VOR, DME);
- a földi, kódolt jeleket sugárzó vezetőállomásos rendszer (TACAN);
- a műszeres leszállító rendszerek (RSZBN);
- a globális hiperbolikus navigációs rendszerek (LORAN, DECCA, OMEGA);
- a műholdas globális helymeghatározó rendszerek (NAVSTAR GPS, GLONASS).

Összességében elmondható, hogy az elektronikai zavarás szempontjából az autonóm rendszerek közül a doppler rádiólokátoros az egyedül hozzáférhető. A nem autonóm rendszerek közül kimondottan a TACAN zavarására fejlesztettek ki zavaróállomást, amely mind az oldalszögmérő csatornát, mind a távolsági és kódcsatornát zavarta. A globális hiperbolikus rendszerekre és a rádióirányítűkre nincs kidolgozott zavaró rendszer. Szükség esetén ezek elemeit diverziós csoportokkal, rombolással lehet működésképtelenné tenni. A műszeres leszállító rendszerek elemeit a repülőterekre alkalmazott szélessávú, és több sávot érintő zavaró bilincs létrehozásával szükség szerint, időlegesen meg lehet bénítani.

Napjainkban a műholdas, globális helymeghatározó rendszerek közül az amerikai NAVSTAR GPS és az orosz GLONASS rendszer terjedt el világméretekben. A NAVSTAR GPS *(NAVigation System using Time And Ranging – Idő-, és távolságmérő navigációs rendszer)* kifejlesztését az amerikai védelmi minisztérium követelményei szerint 1973-ban kezdték el a TRANZIT/ DOPPLER navigációs rendszer leváltására. A cél az volt, hogy kifejlesszenek egy pontos, háromdimenziós hely és sebesség-meghatározó rendszert, amely a világ bármely pontján, bármely időjárási körülmények között, korlátlan számú felhasználó számára biztosít illetéktelen hozzáféréstől védett hely és időadatokat a nap 24 órájában. A fejlesztési program elérte a kitűzött célokat. A NAVSTAR GPS a Föld bármely térségében hasonló pontossággal üzemel a korábbi hasonló berendezéseknél gyorsabban, pontosabban és gazdaságosabban.



4.9. kép. **Navigációs rendszereket zavaró berendezés**[190]

[190] Carlo Kopp *Air Defence System Defensive Aids*: http://www.ausairpower.net/APA-SAM-DefAids.html (Letöltve: 2014. 02.14.)

Az orosz fejlesztésű globális műholdas navigációs rendszer *(GLObal'naya NAvigatsionnaya Sputnikovaya Sistema – GLONASS)* oly sok más fejlesztéshez hasonlóan több elvi azonosságot mutat, ugyanakkor a megvalósításában jelentős rendszertani eltérések találhatók. Ezen rendszer is műholdakra épülő, mindenidős, 3D helymeghatározó, sebességmérő, időjel szolgáltató, korlátlan számú felhasználó számára hozzáférhető rádió-helymeghatározó rendszer.

4.1.2.9 A vontatott, vagy önálló hajtóművel rendelkező hamis célok, decoy-ok

A 80-as években intenzív fejlesztések indultak az amerikai hadseregben abból a célból, hogy egyedi vagy csoportos védelmet biztosítsanak a repülőgépek számára a légvédelmi rakéta eszközök ellen. Ennek egyik iránya a vontatott, vagy önálló hajtóművel rendelkező aktív hamis célok, az úgynevezett decoy-ok kifejlesztése volt. Rendeltetésük, tömeges repülő kötelék, vagy egyedi légi cél elektronikai eszközökkel való imitációja az ellenséges légvédelmi rendszer megtévesztése, túlterhelése céljából, valós repülő kötelékben repülve pedig a légvédelmi rakéták magukra vonása, és ezáltal a valódi feladatot végrehajtó repülőgépek oltalmazása. A különösen fontos vezetőket körülvevő hasonmások példájához hasonlóan, az önfeláldozó alteregó szerepét töltik be.

Az Öböl-háborúban az amerikai légierő a Bagdad elleni légitámadás előtt indított BQM-74 típusú pilótanélküli decoy-okat, a haditengerészet A-6-os repülőgépeiről pedig harcászati, légi indítású hamis célokat *(Tactical Air-Launched Decoy – TALD)*. Az elgondolás lényege, hogy tömeges légicsapás imitálásával provokálni kell a légvédelmi rendszert, vagyis az előrejelző eszközöktől a légvédelmi komplexumokig minden eszközt bekapcsoltatni. A felderítő rendszer ekkor fel tudja térképezni a rendszer felépítését és működési rendjét. Ha ezután nincs idő a valódi csapás kiváltásáig újraszervezni a rendszert, akkor nagy valószínűséggel ugyanazon eszközök és ugyanott fognak működni, tehát a zavarásuk, pusztításuk egyszerűen megvalósítható. Igen fontos szerepet játszik ebben a rendszerben az időhadviselés, tehát aki hamarabb tud felkészülni a csapás kiváltására, mint a másik fél a rendszer átszervezésére, az fog sikert elérni. Ez a taktika korábban az arab-izraeli háborúkban már bevált.

Az amerikai légierő csoportos céljainak oltalmazására alapeszközként tartják számon a 2000 utáni években a Korszerű Védelmi Kutatásokat Tervező Intézet *(Defense Advances Researches Programme Agency – DARPA)* által kifejlesztett miniatűr légi indítású imitátort, amely a MALD *(Miniature Air-Launched Decoy)* nevet viseli. Ezt fejlesztette tovább a Raytheon az amerikai haditengerészet Super Hornet repülőgépei számára. (4.10. kép)

A MALD olyan légi célokat (többek között csoportos célokat is) imitál, mint az F-16, F-15, B-52, valamint az F-117, B-2A és más repülőgépek. Képes átfogni valamennyi, a légvédelmi eszközök által használt hullámsávot, a méteres, deciméteres és centiméteres tartományt is. Kivitelét tekintve lehet az F-16-os külső függesztéke, vagy a lopakodó technológiájú perspektivikus F-22 és JSF belső elhelyezésű berendezése. A célimitátorok repülési sebessége eléri a 0,9 Mach-ot, a repülési magasságuk a 10000 m-t, a harcászati rádiuszuk pedig a 450 km-t.

A MALD hossza 225 cm, átmérője 15 cm, a tömege pedig 50 kg. Egy Super Hornet repülőgépre egyszerre három készlet függeszthető fel. A programozott útvonalrepülés biztosítására a NAVSTAR GPS műholdas globális helymeghatározó rendszert használják. Egy készlet ára – a jóval hatékonyabb alkalmazhatóság ellenére is – csak mintegy negyede a TALD-nak, és csak mintegy harmincezer dollárt tesz ki.

4.10. kép. **A MALD légi hamis cél imitátor**[191]

A MALD hasznos terhelését képező 15 kg tömegű fedélzeti elektronikai rendszert a Northrop-Grumann cég fejlesztette ki. A méteres hullámtartományú adó-, és vevőantennákat a szárnyakban, míg a magasabb frekvencián üzemelőket az orr- és farok részben helyezték el. Az antennák tömege mintegy 5 kg.

A működés alapelve az, hogy a fedélzeti vevőrendszer veszi a különböző hullámtartományokban üzemelő rádiólokációs eszközök jeleit. Ezek közül képes a rendeltetésüket, üzemmódjukat meghatározni és a megfelelő prioritást felállítani közöttük. A letapogató jelek erősítésével és jelparamétereik megváltoztatásával elérhető, hogy a kisugárzásra kerülő válaszjel arra a repülő eszközre legyen jellemző, amelynek az imitációjára beprogramozták. Beállíthatóak a különböző hatásos visszaverő felületű repülő típusok, cirkáló rakéták, pilóta nélküli repülő eszközök (UAV), sőt a lopakodó típusok jellemző paraméterei is. A lopakodó repülőkre jellemző, hogy amíg a deciméteres és centiméteres lokátorokon nem, vagy alig okoznak értékelhető céljeleket, addig a méteres lokátorok képesek bizonyos távolságon belül felfedni őket. Ezt a felsőbb frekvencia tartományokban elhaló, a méteresben fel-felbukkanó visszavert jelet a MALD is elő tudja állítani.

[191] Raytheon and US Navy begin MALD-J Super Hornet integration (Letöltve: 2014.02.14.) http://rpdefense.over-blog.com/article-raytheon-and-us-navy-begin-mald-j-super-hornet-integration-107847534.html

Ennél az eszköznél már jól megfigyelhető a fejlesztők multispektrális, komplex imitációra való törekvése, ami az imitátoroknál a korszerű viszonyok között elengedhetetlen követelmény lesz.

4.2 Elektronikai megtévesztés

4.2.1 Fogalma, célja

„Az elektronikai megtévesztés az elektromágneses energiának a szándékos kisugárzása, átalakítása, visszasugárzása, elnyelése vagy visszatükrözése azzal a céllal, hogy megtévessze, félrevezesse, összezavarja és eredeti szándékától eltérítse az ellenséget, vagy annak elektronikai rendszereit."[192]

Rendszerint részét képezi az átfogó hadműveleti álcázásnak és szinte sosem alkalmazzák önállóan. Az elektronikai megtévesztés a saját eszközeink által történő kisugárzással történik, amely lehet:

- manipulációs;
- szimulációs (demonstrációs);
- és imitációs elektronikai megtévesztés.

A manipulációs és szimulációs megtévesztést nem a felderítő és elektronikai hadviselési csapatok hajtják végre. A manipulációs és szimulációs elektronikai megtévesztés megtervezéséért és végrehajtásáért a híradó tiszt felelős.

Ugyanakkor az imitációs megtévesztés a szakmai-technikai feltételek miatt alapvetően a felderítő és elektronikai hadviselési alakulatokhoz tartozik. Az elektronikai megtévesztés a zavaráshoz hasonlóan elektronikai védelmi célokat is szolgál azáltal, hogy az ellenséges felderítést téveszti meg.

4.2.2 A manipulációs elektronikai megtévesztés

A manipulációs elektronikai megtévesztés rendeltetése a saját rádióelektronikai rendszereink jellemzőinek megváltoztatása. A saját elektromágneses kisugárzásunk manipulálásánál az ellenséges elektronikai hadviselési, rádió-felderítő erőket fokozott tevékenységre késztetjük. A manipuláció megvalósítható úgy, hogy a technikai jellemzők és rendszer profilja alapján az ellenség az általunk kívánt szándékot, tevékenységet állapítja meg a saját csapatainkról, míg a másik megoldás, hogy félrevezető információkat sugárzunk ki az ellenség megtévesztésére.

[192] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína. MH HVK, 2005. p. 8.

A manipulációs elektronikai megtévesztés célja, hogy az ellenség elektronikai felderítési értékelőit olyan, valósnak tűnő adatokhoz juttassuk, melyek alapján téves következtetésre jutnak csapataink tevékenységét és szándékát illetően.

A manipulációs elektronikai megtévesztésnek két fajtája van: a manipulációs rádiómegtévesztés és a manipulációs egyéb elektronikai eszközzel történő megtévesztés.

A manipulációs megtévesztés végrehajtásához tökéletesen kell ismerni a saját erőink híradó rendszerei működését a különböző időszakokban és harchelyzetekben.

Az ellenséges elektronikai analizálók, értékelők már békében és minden helyzetben szüntelenül kutatják a híradási szokásokban a különbözőségeket. Ezek az eltérések nagy valószínűséggel jelezhetik egy-egy ország és szövetségesei tervezett tevékenységét.

A manipulatív megtévesztés lehet:

- megtévesztő vezetési szintre jellemző forgalmazás;
- megtévesztő gyakoriságú forgalmazás;
- hosszú, terjengős táviratok adása;
- irányítás manipulálás;
- elektronikai fedések;
- a híradó-biztonsági rendszabályok irányítottan történő megszegése.

Az egyéb elektronikai eszközzel történő manipulációs megtévesztés elvei megegyeznek a manipulációs rádió-megtévesztéssel. A technikája természetesen különbözik, mivel másfajta technikai eszközöket alkalmaznak. A kisugárzó eszközök aktivitását növeljük vagy csökkentjük attól függően, hogy milyen látszatot akarunk kelteni az egységről. Mind a híradó, mind az egyéb elektronikai megtévesztés alapvetően függ a saját híradó és rádió-felderítő, valamint az ellenséges rádiófelderítésről rendelkezésre álló adatbázistól, melynek létrehozása az elektronikai védelemmel foglalkozó értékelő és analizáló személyek feladata.

4.2.3 A szimulációs (demonstrációs) elektronikai megtévesztés

A szimulációs elektronikai megtévesztés rendeltetése az ellenség tudatos félrevezetése a saját csapatok valóságos összetételét, elhelyezkedését és képességeit illetően. A szimulációs elektronikai megtévesztő tevékenységek célja az ellenség figyelmének felkeltése bizonyos tevékenységre, illetve figyelmének elvonása más tevékenységről.

Az elektronikai demonstráció a csapatok demonstrációs tevékenységének része, önállóan általában nem alkalmazzák, viszont demonstráció nem képzelhető el az elektronikai eszközök széles körű, aktív alkalmazása nélkül. A hadműveletek során az ellenség nagymértékben számít az elektronikai hadviselési és rádió-felderítő csapataira, amelyek észlelik a valóságban nem létező, szimulált egységeket, azok ténykedését. Más esetekben a valóságban létező csapatokat hamis diszlokációban imitáljuk.

Szimulációs megtévesztésre alkalmazhatók mind a híradó, mind egyéb elektronikai kisugárzó eszközök attól függően, hogy az ellenség milyen felderítő eszközét akarjuk megtéveszteni.

Szimulációs megtévesztő eljárások lehetnek:

Alakulat szimulálása. Olyan hírhálózatot és egyéb elektronikai kisugárzó eszközöket telepítenek és üzemeltetnek, melyek kisugárzása és tevékenységi rendje megfelel az általunk imitálni kívánt alakulat hiteles jellemzőinek. A csapatmozgásokat például adott mennyiségű sugárzó elektronikai eszköz és a kötelék nagyságának megfelelő méretű rádiólokációs visszaverő felületet biztosító szögvisszaverő együttes mozgatásával hajtják végre.

Új vagy más típusú eszköz szimulálása. Az elektronikai jellemzők megváltozása új vagy eltérő eszközzel valós vagy imitált alakulatról félrevezetheti az ellenséget, mivel azt feltételezi, hogy új technikai eszközök és lehetőségek vannak csapataink birtokában.

A valótlan diszlokációt szimuláló elektromos jellemzőket felerősítjük, ugyanakkor a valósnál a kisugárzást erősen korlátozzuk.

4.2.4 Az imitációs elektronikai megtévesztés

Az imitációs elektronikai megtévesztés (elektronikai dezinformáció) irányulhat mind a híradó, mind az egyéb elektronikai kisugárzó eszközök ellen. Az imitációs híradó megtévesztéssel hamis parancsokat vagy félrevezető információkat juttatunk be közvetlenül a rádióforgalmi rendszerekbe. Az imitáló távírász belép az ellenséges rádióforgalmi rendszerbe, mint saját távírász és addig dolgozik ott, amíg a kívánt félrevezető információt le nem adta az ellenségnek. A belépést különös gondossággal kell végrehajtani az ellenséges híradó rendszerekbe, mivel minden egyes adónak meg van a saját jellemzője. A megtévesztő adónak gyakorlatilag azonos paraméterekkel kell rendelkeznie, mint az ellenségnek. Az imitációs megtévesztés lehetőségei az ellenséges felderítés minőségétől és az alkalmazott technikai eszközök megtéveszthetőségétől függnek.

Ilyen lehetőségek:

- a rádióforgalmazásba történő belépéssel, annak megzavarása;
- távirat adása belépéssel;
- rejtjelezett szöveggel (eszközzel) való belépés;
- megtévesztő zavarás.

A forgalmazás megzavarása kivételével mindegyik módszer széles körű technikai felkészültséget és speciálisan képzett kezelőket igényel. A forgalmazás megzavarása csak kompatibilis rádióeszközt és idegen nyelvtudást igényel. Mindegyik eljárás speciális szervezést és felkészültséget igényel.

Az egyéb elektronikai eszközök elleni imitációs megtévesztést hasonló célok vezérlik, mint a híradó eszközök elleni megtévesztést. Magába foglalja azt az eljárást, amikor az elektromágneses kisugárzást bejuttatjuk az ellenséges elektronikai rendszerekbe imitálva a saját jeleiket, és ezáltal megzavarjuk vagy megtévesztjük azt. A harcterületen elhelyezkedő különféle felderítő, célmegjelölő és elektronikai felderítő rendszerek mindegyikének megvannak a saját technikai jellemzőik, így az egyéb elektronikai eszközök elleni megtévesztés komoly technikai hátteret igényel.

Számos ellenséges lokátor megtéveszthető ismétlő-berendezéssel, szögvisszaverőkkel és válaszadóval, melyek utánozzák az eredetit, vagy válaszjelet imitálva a lokátor normál üzemét. A sikeres megtévesztéshez alaposan kell ismerni az ellenséges lokátorok jellemzőit, mintha zavarni akarnánk azokat. Ugyanakkor, ha ez sikerül a megtévesztés eredményesebb, mint a zavarás. Amikor az ismétlőket és a válaszzavarókat zavaróként alkalmazzuk, azt az ellenség hamarosan felismeri, mint a problémák okát, és bekapcsolják a zavarvédő berendezéseket, vagy más ellenrendszabályokat léptetnek életbe.

Amikor ugyanezen eszközöket imitációs megtévesztésre használjuk, akkor az ellenség nehezen ismeri fel a megtévesztést, mivel a berendezéseik ugyanúgy üzemelnek, mint normál esetben. Másrészről viszont, a megtévesztés finomsága miatt, ellentétben a zavarással, sokkal nehezebb megállapítanunk a megtévesztő tevékenység konkrét eredményét a harctevékenységre.

Az egyéb elektronikai eszközök elleni imitációs megtévesztési technikák:

- hamis célok létrehozása vagy imitálása;
- távolságjelző, közelségi gyújtó megtévesztése;
- felderítő sugárnyaláb modulálása;
- fordított nyereségű jel visszasugárzása.

4.3 Az elektronikai pusztítás

„Az elektronikai pusztítás az elektromágneses és egyéb irányított energiák, valamint önrávezetésű fegyverek alkalmazása az ellenség elektromágneses spektrumhasználaton alapuló rendszereinek időleges vagy tartós rombolása céljából."[193]

A jövőben számolni kell olyan irányított energiájú fegyverek megjelenésével, amelyek elegendő energiát képesek sugározni a célobjektumok felé, hogy azok kezelő állományát harcképtelenné, eszközeit pedig használhatatlanná tegyék. Az elektronikai pusztítás irányított energiájú eszközei közé tartoznak:

- a nukleáris robbanás elektromágneses impulzusa és ionizációs hatása;
- a nagy energiájú rádiófrekvenciás sugárforrások;
- az impulzusbombák;
- az akusztikus zaklatás eszközei.

A nukleáris robbanás elektromágneses impulzusa elsősorban a korszerű félvezetős eszközök megjelenése óta okozhat számottevő pusztítást a katonai és polgári elektronikai berendezésekben. Az elektroncsöves berendezések alkalmazásának korában végrehajtott kísérleti robbantások során megvizsgálták a rádiólokációs és hírközlési berendezésekre gyakorolt hatásokat is. Azt tapasztalták, hogy az atomrobbanás keltette részecskeáramlás nagy villamos feszültséget indukált a kábelekben, vezetékekben, amelyek a csatlakozások

[193] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína 1. kiadás, 2004, MH kiadvány, p. 9.

átütéséhez, a forrasztások leolvadásához vezettek. A berendezésekben okozott kárt az epicentrum közvetlen környezetét kivéve közepesnek és viszonylag hamar kijavíthatónak értékelték. A magaslégköri atomrobbantás elektromágneses impulzusa a többi pusztító tényezőhöz képest kiemelkedően nagy, ezért ezt a fajta robbantási módot tervezték az elektronikai berendezések pusztítására. A félvezetők megjelenése nyomán azonnal felmerült a probléma, hogy ezek a vákuumcsöveknél jóval érzékenyebbek a túlfeszültségre, különösen a CMOS integrált áramköri elemek. A félvezetőgyárak és főleg a katonai elektronikai berendezésekhez alkatrészeket szállító vállalatok különleges tokozású, ólomburkolattal ellátott integrált áramköröket konstruáltak, amelyek ára is nagyságrendekkel meghaladta a kommersz eszközök árát.

A mai katonai elektronikai rendszerek igen sok, a polgári követelmények szerint épített, a kereskedelemből beszerezhető eszközt alkalmaznak. Ezek messze nem felelnek meg azoknak a szigorú követelményeknek, amelyek az atomfegyver alkalmazásának viszonyai között biztosítanák az életképességüket. Egy rendszer tervezése során ezt feltétlenül számításba kell venni, még akkor is, ha ma az atomfegyverek alkalmazásának valószínűségét kisebbnek tartjuk, mint a hidegháború éveiben.

A nukleáris robbanás ionizációs hatása az elektronikai eszközök normális működését ugyanúgy gátolhatja, mint a berendezéseket ért hatások, tehát ezeket is figyelembe kell venni. A Föld légkörének természetes, folyamatos év- és napszaktól függő ionizációját a Nap ionizációs sugárzása idézi elő. Az ionizáló sugárzást képező protonok, alfa-részecskék és nehéz atommagok hozzák létre a Föld légkörében a megnövelt sűrűségű – szabad elektronokat és pozitív ionokat tartalmazó – ionoszférát. Az ionoszféra fizikai tulajdonságait, idő és magasság szerinti változásait évek során mérésekkel feltérképezték és a rövidhullámú rádió hullámterjedési előrejelzések alapján ma már nagy biztonsággal tervezhetővé váltak az összeköttetések.

A nukleáris robbanás során a nagy sebességű elemi részecskék korpuszkuláris ionizáló kisugárzása, továbbá a gamma és röntgensugárzás, valamint a robbanás hő- és ultraibolya sugárzásának hatására végbemegy a légkör ionizációja. A megnövekedett ionizáció az igen hosszú hullámok hatótávolságát csökkenti, a hosszú- és középhullámok terjedési viszonyait nem befolyásolja nagymértékben, mert azok az ionoszféra sűrűségétől függetlenek. A rövidhullámok az ionoszférán többszörös visszaverődést szenvednek el, ami fokozott energiaveszteséggel és végeredményben az összeköttetések megszakadásával járhat. Az ultrarövid hullámok tartományában távolterjedési jelenség lép fel, ami nagymértékben megnöveli a csatorna interferenciák valószínűségét, vagyis nagytávolságú kölcsönös zavartatások jönnek létre.

*A nagy energiájú rádiófrekvenciás sugárforrások***,** mint az elektronikai eszközök támadásának lehetséges eszközei már régóta ismertek, azonban sokáig a konstrukciós nehézségek miatt a kísérleteknél nemigen jutottak tovább még az iparilag fejlett katonai hatalmak sem. Ronald Reagen amerikai elnök 1983-ban meghirdetett csillagháborús tervei azonban újabb lökést adtak a kutatásoknak. A nagyteljesítményű adástechnika területén folyó eszközfejlesztések során olyan speciális vákuumcsöveket, magnetronokat, klisztronokat fejlesztettek ki, amelyek mérete lehetővé tette, hogy koncentrált energianyalábot lőjenek ki vele harctéri körülmények között. Az így kisugárzott rádiófrekvenciás

energia a vevőantennán átjutva a bemeneti áramkörre kerül, amely a nagy túlterheléstől tönkremegy. Előnye a többszöri felhasználhatóság. A fejlesztések jelenleg a méretcsökkentés irányában folynak, így azokat pilóta nélküli repülők fedélzetére helyezve ki lehet juttatni az ellenséges légvédelmi eszközök, hírközlő pontok közvetlen közelébe. A közeli térből már jóval kisebb energiaszükséglettel is hatékony elektronikai csapást lehet mérni anélkül, hogy emberi, vagy fizikai pusztítást okoznánk.

Az impulzusbombák szintén az elektronikai berendezések megrongálására, működésképtelenné tételére szolgálnak. A fizikai működési mechanizmusukban abban különböznek a nagy energiájú rádiófrekvenciás sugárforrásoktól, hogy csak egy hatalmas teljesítményű elektromágneses impulzust állítanak elő, miközben fizikailag megsemmisülnek, illetve véglegesen megrongálódnak. A rezgéskeltéshez szükséges energia előállításának egy módja lehet, hogy vegyi robbanóanyag robbanási energiáját alakítják elektromos energiává, majd ezt egy üregrezonátorra sütik rá, amely a sajátfrekvenciáján létrehozott rezgést egy tölcsérsugárzón, vagy helixes kicsatoláson egy parabolatükörre sugározza. A hatás annál nagyobb, minél rövidebb impulzust sikerül előállítani ugyanakkora átlagteljesítmény esetén.

4.3. ábra. **Az impulzusbomba alkalmazási elve**[194]

Az impulzusbombák alkalmazása a gravitációs bombavetéshez hasonló módon történhet. A célobjektum (például harcálláspont, hírközpont) fölött kioldva, a bomba közel függőleges helyzetben közeledik a föld felé. Amikor eléri a meghatározott pusztítási sugár nagyságához tartozó magasságot, létrehozza az elektromágneses impulzust, ami közel kör alakú területen pusztítja, rongálja az elektronikai eszközöket. Ez a bevetés meglehetősen nagy pontosságú, szelektív csapás kiváltását teszi lehetővé, és a saját csapatok elektronikai eszközeinek védelmét is biztosítja a nemkívánatos rongálástól.

Az akusztikus zaklatás eszközei eredményüket tekintve a pszichológiai hadviseléshez tartoznak, azonban a fizikai hatást elektronikai eszközökkel állítják elő, ezért itt, az elektronikai ellentevékenység fejezetben kell róluk szót ejteni.

[194] http://www.ausairpower.net/XIMG/empfootprint.gif (Letöltve: 2014.02.14.)

Már régen ismert, hogy az emberi szervezet bizonyos akusztikai hullámtartományban kisugárzott rezgésekre érzékenyen reagál. A 10 Hz alatti rezgések pánikérzetet, menekülési kényszerképzetet okoznak, a mintegy 7,5 Hz-es rezgés pedig a szívvel lép interferenciába, ami kritikus esetben halált is okozhat. Egyes kutatók szerint a természetes körülmények között például a Bermuda-szigetek térségében előforduló hasonló rezgések okozzák a vízi és légi járművek nagyszámú katasztrófáját.

Harctéri körülmények között már a II. világháború alatt is végeztek hasonló kísérleteket, de egyrészt az infrahangsugárzók nagy mérete, másrészt a saját csapatok megóvásának problémái miatt nem jártak eredménnyel a kísérletek. Napjainkban újra előkerült ez az elgondolás, de most sikerült megoldani mindkét korábbi gondot. A permvonalban egymástól jelentős távolságra két nagyteljesítményű piezo sugárzórendszert helyeztek el úgy, hogy az ellenség felé sugározzanak. Egy közös központból vezérelve az egyik sugárzóra például 200 kHz, a másikra pedig 200,01 kHz frekvenciájú jelet kapcsolnak, amelyeket a piezo sugárzók akusztikus hullámok formájában sugároznak le. Abban a zónában, ahol mind a két sugárzó jele észlelhető, ott egy nemlineáris elemen, mint például az emberi fül, kikeveredik az összeg és a különbségi jel is. A 400,01 kHz-es összegjelet nem érzékeli az ember, ellenben a 0,01 kHz-es azaz 10 Hz-es különbségi infrahangra már a fent leírt módon reagál. A rendszer hangolható, a saját csapatokra nézve teljesen veszélytelen, mivel a sugárzás jól irányítható és hátrafelé keverésre alkalmas zóna a leírások szerint nem alakul ki. A sugárzókat telepítő személyzetre ható közeli, körülbelül 200 kHz-es rezgés érzékelhető hatást nem gyakorol.

A harc humán tényezőjét támadó másik eljárás az akusztikus zaklatás *(Acoustic Harassment)*, amely lényege, hogy speciális jellel modulált rádiófrekvenciás jeleket sugároznak az emberi tartózkodásra meghatározott helyre, például törzsek munkaterületére. A bekapcsolás után az embereken idegesség lesz úrrá, képtelenek uralkodni magukon és a harci körülmények okozta, amúgy is felfokozott stresszhelyzetben a törzs belső munkarendje felborul, a törzs normális munkára alkalmatlanná, harcképtelenné válik.

Az ilyen eszközök diverziós csoportokkal, pilóta nélküli repülőeszközökkel és még sok más módon kijuttathatók, a működtetésük lehet programozott, vagy távvezérelt.

4.11. kép. **AGM-88E rádiólokátorok elleni rakéta**[195]

[195] http://indolinkenglish.wordpress.com/2012/04/30/india-developing-anti-radiation-missile/ (Letöltve: 2014.02.14.)

Az elektronikai pusztító eszközök csoportjába soroljuk azokat az önrávezérlésű rakétafegyvereket, amelyek valamely elektromágneses kisugárzás bemérése és követése útján, aktív, félaktív vagy passzív önirányítással találnak célba. A legelterjedtebb változat a rádiólokátorok ellen alkalmazott légi indítású rakéta, amely a rádiólokátorok antennarendszeréből származó kisugárzásokra vezették rá magukat. A nevüket is innen kapták: *Anti-radiation Missile – ARM*. (4.11. kép)

Annak, hogy elsősorban a rádiólokátorokat támadják, a célok értékén kívül az az oka, hogy a magasabb frekvenciatartományokban sokkal egyszerűbb a pontos iránymérés. Elvileg rádióeszközökre is lehet ilyet konstruálni, de az önrávezetéshez szükséges iránymérés technikai megvalósítása a nagyobb hullámhossz miatt nehezen megoldható.

5. FEJEZET

Elektronikai védelem

A fejezet a szerző 2000-ben társszerzőként megjelentetett „Elektronikai védelem”[196] című jegyzetének alapján, annak átdolgozásával, aktualizálásával készült a szövegrészek, ábrák és képek felhasználásával.

5.1 Az elektronikai védelem fogalma, tartalma

Az elektronikai és főleg rádiófrekvenciás eszközök rohamos terjedése jelentősen befolyásolja az új harcmódok és harceljárások kialakítását. Az elektronikai védelem a korszerű fegyveres küzdelemben meghatározó fontos tényezővé, a fegyverek és csapatok hatékonyságát jelentősen befolyásoló erővé vált.

A vezetést és fegyverirányítást biztosító rendszerek minőségéből és hierarchiájából adódóan az elektronikai védelem céljait megvalósító sokrétű tevékenység kihat a harcolók teljes szervezetére, csoportosítására, valamennyi haderőnem és fegyvernem tevékenységére, a fegyverek és a csapatok alkalmazási elveire, módszereire.

Az elektronikai védelem az elektronikai hadviselésnek egyik fontos eleme, melynek vizsgálatát az elektronikai hadviselés minden összetevőjével együtt, egymásra gyakorolt kölcsönhatásukban kell végezni.

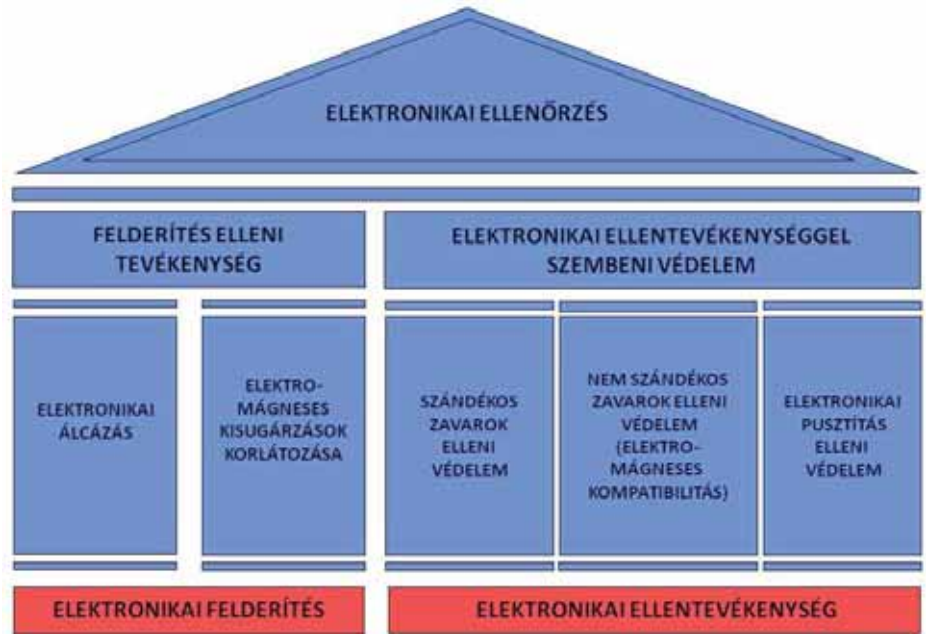
Az elektronikai védelem (Electronic Protective Measures – EPM) az elektronikai hadviselés azon területe, amely biztosítja az elektromágneses spektrum saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok által okozott nem szándékos (kölcsönös) rádiózavarok előfordulása ellenére.[197]

Az elektronikai védelem alapvetően három fő területre osztható fel, úgymint az elektronikai támogatás (elektronikai felderítés) elleni tevékenység, az elektronikai ellentevékenységgel szembeni védelem és az elektronikai ellenőrzés. A felderítés elleni tevékenység magába foglalja az elektromágneses kisugárzások korlátozását és a felderítés előli kitérés különböző módozatait. Az elektronikai ellentevékenységgel szembeni védelemhez a szándékos és a nem szándékos elektromágneses zavarok elleni tevékenységek és az elektronikai pusztítás elleni védelem tartozik. Az elektronikai ellenőrzés, amely, mint a két fő terület rendszabályai betartásának ellenőrzését magába foglalja. Ugyanakkor,

[196] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000.

[197] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína. MH HVK, 2005. p. 10.

mint az előző fejezetekben látható volt, az elektronikai védelem sikeres megvalósítása megköveteli a szoros együttműködést az elektronikai hadviselés más összetevőivel is. Az 5.1. ábra az elektronikai védelem területeit mutatja.



5.1. ábra. **Az elektronikai védelem területei**[198]

Az elektronikai védelem területei szorosan összefüggnek egymással, a kapcsolódó szaktevékenységek kihatással vannak az azokra épülő más szaktevékenységek eredményességére.

Az elektronikai védelem célja vezetési és fegyverirányító rendszereink folyamatos, megbízható működésének biztosítása olyan módon, hogy az ezeket kiszolgáló elektronikai eszközöket megvédjék az ellenség felderítése, elektronikai zavarása ellen, valamint a saját nem szándékos zavarokkal szemben.

Az elektronikai védelem szorosan kapcsolódik a híradó biztonsági előírásokhoz. Az alapvető eltérés az információ milyenségében van, melyet védeni kell az ellenséges felderítés ellen. Az elektronikai védelem feladata a kisugárzó eszközök védelme az ellenséges észlelés, helymeghatározás és azonosítás ellen.

Az elektronikai védelem úgymond elrejti az elektromágneses jeleket és eszközöket az ellenséges felderítés, helymeghatározás és azonosítás elől. A híradó biztonsági előírások magát az információt védik az ellenséges felderítés ellen, melyet a különböző híradó- és

[198] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 9.

elektronikai rendszereken keresztül továbbítanak. Számos kezelői megoldás szolgálja egyidejűleg az elektronikai védelmet és a híradó biztonsági előírásokat.

Az elektronikai eszközök felhasználási területének kiszélesedésével együtt jelentősen megnőtt az elektronikai védelem szerepe is, mivel a fejlett elektronika birtokában ennek egyes elemeit, mint például a technikai felderítés elleni tevékenységet a szemben álló felek már békében is aktívan és széles körűen folytatják.

Harchelyzetben az ellenség a mi elektronikai rendszereink és eszközeink rendeltetésszerű üzemének zavarására és megbontására törekszik, azzal a céllal, hogy a csapatok vezetését, fegyverirányítását megnehezítse, megbontsa, megakadályozza. Ezzel szemben csapatainknak az elektronikai védelem módszereit kell komplex módon alkalmazniuk.

Egy konfliktus kezdeti szakaszában (a határátlépést megelőzően) az ellenség számára az egyik legfontosabb információforrás az elektronikai felderítés, amely lehetővé teszi saját elektronikai rendszereink felépítésének és működésének megismerését. Ezen ismeretek birtokában a leghatékonyabban tudja időben, térben és a harchelyzetnek megfelelően a tűz- és az elektronikai csapásokat megtervezni. Ennek megakadályozása érdekében szigorúan be kell tartani az elektronikai védelem rendszabályait. A rendszabályokat az ellenség vezetési- és fegyverirányítási rendszerének elektronikai felderítésével, elektronikai zavarásával és az elektronikai objektumaira mért tűz- és elektronikai csapásokkal összhangban kell megtervezni, megszervezni, végrehajtani.

Az elektronikai védelem megvalósítása és célja szerint lehet csoportos vagy egyéni védelem. Az egyéni védelembe tartozik minden olyan tevékenység, amelyet az egyes harceszköz a saját védelme érdekében hajt végre (például infracsapdák, dipólok, zavaró konténerek alkalmazása). Egyéni védelmi eszközökkel minden korszerű harceszköz fel van szerelve, amelyek alkalmazása általában számítógéppel vezérelve automatikusan történik.

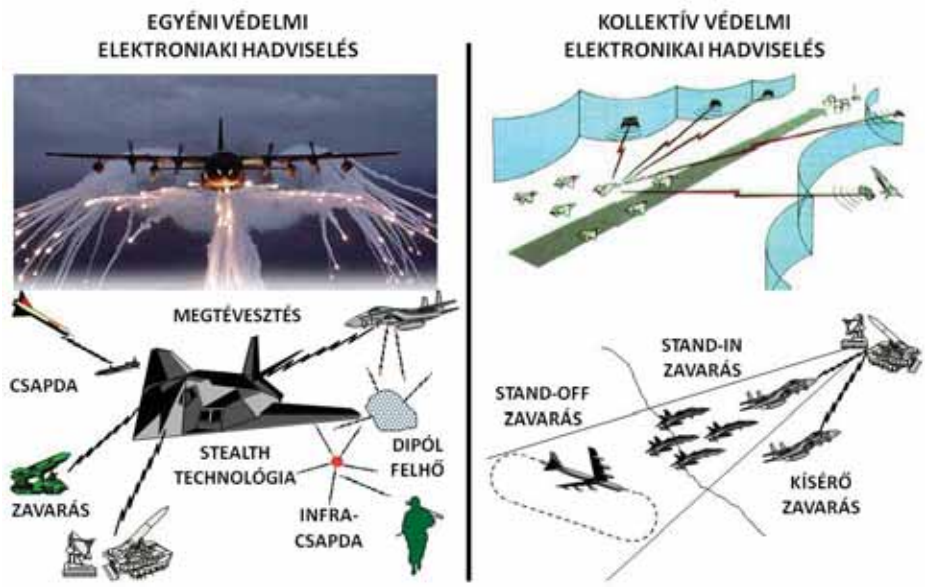
A csoportos védelmet olyan speciális eszközök hajtják végre, amelyek fő feladata az egyes csoportok elektronikai védelmének biztosítása. Ilyen tevékenység lehet például a repülő kötelékekben – vagy azokon kívül – speciális zavaró repülőgépek alkalmazása, amelyek az ellenség felderítő rendszerében üzemelő rádiólokátorok lefogásával – felderítési hatótávolságuk csökkentésével – biztosítják a repülő kötelékek korai felderítés elleni védelmét. Az 5.2. ábrán az egyéni és csoportos védelem főbb területei és módszerei láthatóak.

A helyi háborúk tapasztalatai bebizonyították, hogy az elektronikai védelem jelentősége és szerepe nő a korszerű fegyveres harcban. Tanulmányozni kell az ellenség új eszközeit és módszereit, amelyekkel a saját erők elektronikai rendszereinkre hatni tudnak (vagyis felderíthetik, lefoghatják, tűz- vagy elektronikai csapást mérhetnek azokra). Mind technikailag, mind a módszerek vonatkozásában fel kell készülni ezek hatékony kivédésére.

A vezetési- és fegyverirányítási rendszerek elektronikai védelme érdekében elsősorban az ellenség felderítése elleni tevékenységet kell előtérbe helyezni, hiszen ez az elektronikai zavarás, illetve az elektronikai információk alapján irányított fegyverekkel való megsemmisítés előfeltétele.

Az elektronikai védelem passzív és aktív védelmi rendszabályok alkalmazása, valamint a saját kisugárzások ellenőrzése útján valósul meg. A *passzív elektronikai védelem*

az elektromágneses spektrum hatékony felhasználását biztosító, az elektronikai eszközök alkalmazási módjával és technikai jellemzőivel összefüggő, nem észlelhető rendszabályokon alapul. Az *aktív elektronikai védelem* az elektromágneses spektrum hatékony felhasználását biztosító, az adóberendezések paramétereinek megváltoztatásán nyugvó, észlelhető rendszabályokon alapul.



5.2. ábra. **Egyéni és csoportos védelem főbb területei és módszerei**[199]

A nem szándékos elektromágneses interferenciák megelőzése a frekvencia felhasználás szakmai szabályokon alapuló tervezésén, valamint az elektronikai eszközök harcászati, harcászat-technikai üzemeltetési előírásainak betartásán alapul. A saját eszközök között kialakuló elektromágneses interferenciák – rádiózavarok – megszüntetésére adminisztratív és mérőszolgálati módszerek szolgálnak.

Az elektronikai védelem tervezése összhangban kell, hogy legyen a feladattal és a harcra vonatkozó elgondolással.

A tervezés azzal kezdődik, hogy megállapítjuk, hogy melyek azok a fontos elektronikai eszközök és összeköttetések, amelyeket védeni kell. A saját elektronikai eszközeink sebezhetőségét úgy kell értékelni, hogy figyelembe kell venni az ellenséges felderítő és elektronikai hadviselés csapatok képességeit. Az elektronikai védelmet ezek után úgy kell megtervezni, hogy kizárjuk az ellenség ez irányú lehetőségeit.

[199] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 11.

Az elektronikai védelem összetett feladatok soraiból áll, amelynek tervezése és vezetése széles körű adatgyűjtést, megbízható információáramlást, gyors kiértékelést és reagálást igényel.

Az elektronikai védelem tervezése és vezetése csak akkor lehet eredményes, ha biztosított a valós idejű adatok folyamatos információáramlása. Mindent azonnal közölni kell, ami változást jelenthet csapataink védettségében. Csak annyi elektromágneses kisugárzás engedhető meg, amennyi elegendő a harcfeladat sikeres végrehajtásához, ami pedig úgy érhető el, ha minden pillanatban a tér minden pontjáról megfelelő elektronikai információ áll rendelkezésünkre.

Saját csapataink és elektronikai eszközeink védelme, áruló kisugárzásaik felderítése és csökkentése, továbbá az ellenség felderítő és fegyverirányító rendszereinek az elektronikai védelem érdekében történő zavarása az elektronikai hadviselés csapatok szoros együttműködését, térben, időben és tevékenységek szerint történő egyeztetését igényli minden fegyvernemmel és szakcsapattal.

Az elektronikai védelem megtervezéséért, irányításáért és az összhaderőnemi törzsön belüli koordinálásáért az Elektronikai Hadviselési Koordinációs Részleg tartozik elsődleges felelősséggel. Az elektronikai védelem végrehajtásáért a katonai műveletekbe bevont harci és harci támogató erők törzsei a felelősek.[200]

A katonai műveletekben az elektronikai védelem minden parancsnoki szinten jelen lévő feladat és felelősség. Ennek keretében a parancsnok:

- meghatározza az elektronikai rendszerekre vonatkozó passzív és aktív védelmi rendszabályokat, valamint iránymutatást szab az alkalmazásukra;
- a felkészítés és kiképzés rendszerében tökéletesíti a szakmai jártasságot, a hangsúlyt az alkalmazandó rendszabályokra, az érvényben lévő szabályzókra helyezve;
- az elektronikai védelem középpontjában az ellenség rádióelektronikai felderítő (elektronikai támogató) és elektronikai ellentevékenysége eredményességének minimális szintre csökkentése áll. E cél érdekében az alábbiak szükségesek:
  - a személyi állomány rendszeres tájékoztatása az elektronikai fenyegetettségről;
  - a rádióelektronikai felderítő (elektronikai támogató) tevékenység elleni rendszabályok alkalmazásának kiterjesztése valamennyi biztonsági időszakra;
  - az állomány jártasságának elmélyítése a zavarviszonyok közötti harci munkában.[201]

A parancsnokot és a törzset az elektronikai védelemmel kapcsolatos feladataikban az elektronikai hadviselési szakemberek, az Elektronikai Hadviselési Koordinációs Részleg állománya támogatja. A részleg javaslataival – egyebek mellett – hozzájárul a híradó és informatikai törzs kisugárzási korlátozások tervének kidolgozásához is.

[200] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína. MH HVK, 2005. p. 11.

[201] U.o. p. 31.

5.2 A felderítés elleni tevékenység tartalma, módszerei és eszközei

Ahhoz, hogy az ellenség ismerje elektronikai eszközeinket és objektumainkat, „hatni tudjon" (felderítse, elektronikai eszközökkel lefogja, tűz és elektronikai csapást mérjen) rájuk, felderítést kell végrehajtania. A felderítés különböző technikai eszközeit komplexen alkalmazzák a földi, a tengeri, a légi és kozmikus objektumokon. A felderítő eszközök és rendszerek lehetőségeit a 3. fejezet részletesen tárgyalta. A felderítés elleni tevékenységet úgy kell végrehajtani, hogy az ellenség számára minél kevesebb áruló jellel szolgáljanak elektronikai eszközeink és rendszereink.

Az áruló jelek pontos ismeretében ki lehet dolgozni, és be kell tartani az adott objektumokra vonatkozó felderítés elleni tevékenység rendszabályait.

A felderítés elleni tevékenység lehetőségeinek és módszereinek elemzése előtt tekintsük át azokat az áruló jeleket, amelyek alapján elektronikai eszközeink és rendszereink felderíthetők.

5.2.1 Az elektronikai eszközök és rendszerek áruló jelei

Az áruló jelek a felderítendő csapatok tevékenységére, objektumaira, technikai eszközeinek működésére jellemző egyedi vagy csoportos sajátosságok, jellegzetességek, amelyek lehetővé teszik (ismétlődő tevékenységek során), hogy alapos elemzéssel az adott csapatok, objektumok, technikai eszközök (kezelők) felderíthetők és felismerhetők legyenek.

Az elektronikai vezetési- és fegyverirányítási rendszerek áruló jelei két nagy csoportba sorolhatók úgy, mint hadműveleti-harcászati jellegű, valamint technikai jellegű áruló jelek csoportjába. A hadműveleti-harcászati jellegű áruló jelek alapján elsősorban a csapatok csoportosítására lehet következtetni, míg a technikai jellegű áruló jelek alapján például az elektronikai rendszerek színvonalára, védettségére, zavarállóságára, rendeltetésére, típusára, hovatartozására.

A hadműveleti-harcászati áruló jelek közé az alábbiak tartoznak:

- a felderített objektumoknál és eszközöknél:
  - = azok mennyisége;
  - = a terepen való elhelyezkedésük rendje;
  - = egymástól és az államhatártól való távolságuk;
- a felderített csapatoknál például:
  - = az egyidejű előremozgási útvonalak száma;
  - = a menetoszlopok hossza;
  - = a menetoszlopok tagozódása;
  - = a menetoszlopokon belül a technikai eszközök elhelyezkedése;
  - = a körletek méretei és a terepen való elhelyezkedésük;
- a harci- technika csoportosításánál például:
  - = a csoportosítás rendje;

= egymáshoz viszonyított távolságuk;
= mennyiségük;
– a vezetési pontoknál például:
= méretük;
= országhatártól és egymástól való távolságuk;
= elhelyezkedési rendjük a terepen;
= településük rendje;
– az aktív sugárzó eszközöknél például:
= mennyiségük;
= települési helyük;
= csoportosításuk;
= távolságuk egymástól;
= elhelyezkedésük rendje a terepen;
= típusuk.[202]

A felsoroltak azért válhatnak áruló jelekké, mivel azok a harcrendből és a szervezeti szintekből következően ismétlődő, közel azonos adatok és tevékenységi formák.

A technikai jellegű áruló jelek rejtése az ellenség korszerű technikai felderítő eszközei esetén különösen nagy jelentőségű, mivel azok minden eddiginél pontosabb és részletesebb adatok megszerzését teszik lehetővé. Az elektronikai eszközökre vonatkozó technikai jellegű áruló jelek csoportosíthatók:

– a kibocsátott és visszavert jelek:
= térbeli alakja (például irányítottságuk, méreteik);
= belső struktúrája (például vivőfrekvenciájuk, modulációs módjuk, modulációs tartalmuk, a modulációjuk minősége) szerint;
– a sugárzó eszközök (például):
= üzemi frekvenciája;
= frekvencia stabilitása;
= frekvencia váltogatása (zavarás hatására);
= harmonikus sugárzása;
= sávon kívüli sugárzása;
= vivőelnyomása alapján;
– az antenna berendezések (például):
= külső geometriai méretei (alakjuk, felépítésük);
= iránykarakterisztikái;
= a tér figyelési módja (forgatás, lengetés) szerint; valamint
– az információ továbbítása alapján például úgymint:
= továbbítás módja (például adásmód, üzemmód);
= a szükséges vagy az elfoglalt sávszélesség jellemzői;

[202] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 16.

= az egyidejű csatornák száma;
= az időosztásos csatornák képzése.[203]

5.2.2 A felderítés elleni tevékenység tartalma, módszerei

A felderítés elleni tevékenység célja észlelni, megbecsülni és megakadályozni az ellenséges felderítési adatok gyűjtését.

A felderítés elleni tevékenység tartalmazza az ellenség teljes felderítő adatgyűjtő rendszerének feltárását, a saját sebezhető pontok megállapítását, valamint a biztonsági rendszabályokat és azok értékelését.

A felderítő eszközök elleni védelem feladatait mind békében, mind háborúban folyamatosan és maradéktalanul végre kell hajtani.

Az elektronikai eszközökről és rendszerekről azok üzem közbeni kisugárzása során, valamint funkcionális feladataikból adódó – az előzőekben ismertetett – áruló jelek alapján szerezhetők be információk. A felderítéssel szembeni tevékenység közben alapvető követelmény az eredeti harcképesség, illetve védettség megőrzése. A felderítés elleni tevékenység nem csökkentheti a védelem alatt álló csapatok, objektumok, harci lehetőségét.

A felderítéssel szembeni tevékenység alapvető módszerei a következők:

– a felderítő eszközök és azok hordozói, valamint az információgyűjtő és felderítő központok megsemmisítése, elfoglalása, megrongálása;
– a felderítő berendezések és az adatokat továbbító híradó eszközök elektronikai zavarása;
– a saját elektronikai eszközök sugárzásainak korlátozása;
– a felderítés ellen védendő csapatok, objektumok, eszközök és tevékenységekre utaló áruló jelek megszüntetése, elektronikai álcázása.

5.2.2.1 A felderítő eszközök és azok hordozói, valamint az információgyűjtő és felderítő központok megsemmisítése

A felderítő eszközök és azok hordozóinak helymeghatározása – mivel ezek elsősorban passzív eszközöket (vevőberendezéseket) tartalmaznak – csak komplex felderítési tevékenység eredményeképpen lehetséges. A felderítő központokban üzemelhetnek aktív kisugárzással működő eszközök is, amelyek speciális felderítő eszközökkel érzékelhetők és ezek alapján a helymeghatározás végrehajtható. Ennek ismeretében lehetővé válik az objektumok tüzérségi vagy repülő csapásokkal való megsemmisítése, illetve elfoglalása.

[203] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 17.

5.2.2.2 A felderítő berendezések és az adatokat továbbító híradó eszközök elektronikai zavarása

A felderítő rádiólokátorokkal, rádió- és rádiótechnikai felderítő vevőkkel, felderítést irányító, adattovábbító rendszerek, infravörös- és hidroakusztikai felderítő berendezések vevőivel szemben az elektronikai zavarás hatékonyan alkalmazható.

Az aktív rádiólokációs, elektro-optikai felderítő rendszerek folyamatos vagy válaszimpulzus zavarokkal, a passzív felderítő eszközök általában célzott, vagy szélessávú zavarokkal foghatók le. Ezekről részletesen a 4.1. fejezetben szóltunk.

5.2.2.3 Az elektromágneses kisugárzások korlátozása

Az elektromágneses kisugárzás korlátozása a siker kulcsa lehet az ellenséges hatásokkal szemben, amelyek megakadályozzák, zavarják a saját híradó rendszereink üzemét. Az adóberendezéseket csak a feladat végrehajtásához szükséges időtartamig szabad bekapcsolni, mivel az ellenség felderíti, analizálja rendszereinket és megkeresi azokat a kisugárzásokat, amelyekkel használható információt nyerhet.

Amikor kisugárzási tilalom van – vagyis a rádióadóink nincsenek bekapcsolva – az ellenség felderítése nem tudja felderíteni híradó rendszereinket. Ebben az esetben a kisugárzás korlátozása teljes. Akkor is érvényesül a kisugárzás korlátozása, amikor a parancsnok elhatározása alapján rádió tilalmat vagy rádiócsendet vezetnek be.

Az adóberendezéseket csak minimális ideig szabad bekapcsolni, amely idő alatt az információt is továbbítani kell.

Ez a módszer azonban egyedül nem képes kiküszöbölni a saját adóink felfedését és iránymérését, ezért kombinálni kell más felderítés elleni módszerekkel is, amelyek tovább nehezítik adóink települési helyének meghatározását. Könnyen belátható, hogy az elektronikai eszközeink kisugárzásának csökkentésével megakadályozhatjuk, hogy a szemben álló fél felfedje, analizálja és hatást gyakoroljon saját elektronikai rendszereinkre.

5.2.2.4 Elektronikai álcázás

A szemben álló felek folyamatosan végzik egymás elektronikai rendszereinek technikai felderítését. Az egyre fejlődő technikai színvonalú felderítő eszközökkel szemben csak korszerű technikai eszközökkel és módszerekkel lehet eredményesen tevékenykedni, amelyekben nagy szerepe van az elektronikai álcázásnak.

Az elektronikai álcázás a hadműveleti álcázás kategóriájába tartozik. Az elektronikai álcázás az elektronikai objektumok (eszközök), és a csapatok tevékenységének lényeges, csak rájuk jellemző „áruló” tulajdonságaik kiküszöbölésével, meghamisításával, illetve az ellenség számára hozzáférhetetlenné tételével érhető el.

Az elektronikai álcázást mind békében, mind háborúban, minden év- és napszakban, az egész ország területén folyamatosan meg kell valósítani.

Az elektronikai álcázás magába foglalja az elektronikai rejtést és az elektronikai megtévesztést. Az elektronikai megtévesztés az elektronikai ellentevékenység egyik fajtája

a felderítő rendszerek félrevezetésével, hamis információk továbbításával az elektronikai védelem érdekében kerül végrehajtásra. Az elektronikai megtévesztésről a 4.2. fejezetben részletesen írtunk, így a továbbiakban csak az elektronikai rejtéssel foglalkozunk.

Az elektronikai rejtés aktív és passzív tevékenységek és rendszabályok összességét jelenti.

Az aktív elektronikai rejtő tevékenységek közé a következők tartoznak:

- rádiózavarás;
- rádiólokációs zavarás;
- infra zavarás.[204]

A felsorolt aktív rejtő tevékenységek álcázó zavarokkal elfedik a védendő elektronikai kisugárzásainkat, így azokat az ellenséges felderítő rendszerek a zavarok miatt nem képesek felfedni.

A passzív elektronikai rejtő tevékenységek közé az alábbiak sorolhatók:

- az elektronikai eszközök áruló jeleinek megszüntetése;
- az ellenség rádiólokátorainak passzív zavarása (szögvisszaverőkkel, tükrökkel, dipólusokkal, lencsékkel);
- elektro-optikai felderítés elleni álcázás (füstökkel, ködökkel, festékkel és egyéb anyagokkal);
- akusztikai álcázás (zajcsökkentő megoldásokkal);
- elektromágneses kisugárzások árnyékolása (árnyékoló eszközök alkalmazásával).

Az ellenség már ismertetett különböző felderítő eszközei ellen az alábbi tevékenységeket, eszközöket és módszereket célszerű és kell alkalmazni saját csapataink tevékenységének, eszközeinek rejtésére.

Optikai felderítés elleni rejtés

Az optikai felderítés elleni rejtés megvalósítható:

- a terepdomborzat, növényzet, terep- és műtárgyak védő tulajdonságainak kihasználásával;
- az időjárás, év- és napszak sajátosságainak figyelembevételével, továbbá különböző fényforrások használatának korlátozásával;
- az objektumok jellegzetes formáinak és optikai kontrasztosságának megváltoztatása különböző típusú alakmásítást biztosító álcahálókkal (5.1. kép);
- különböző aerosolok (füstök, ködök) széles körű alkalmazásával.[205]

[204] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 21.

[205] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 21.

A földi célok megfigyelése 6-8 km-es távolságból, a 300-2400 méter magasságban tartózkodó repülő eszközökből a légi figyelés 16 km-es sávba lehetséges. Ilyen nagy terület láthatósága feltétlenül indokolttá teszi a különböző aerosolok alkalmazását.

Az eddigi háborúk igazolták, hogy a megfigyelők elvakítása, vagy objektumok aerosolokkal történő álcázása, megakadályozza a szabad szemmel történő megfigyelést. Ha például a megfigyelő és a tárgy között füstfelhő van, akkor a füst optikai inhomogenitása miatt, valamint a füst és levegőrészecskék határán végbemenő optikai jelenségek (fényszórás és elnyelés) miatt csökken a szemmel történő megfigyelés lehetősége.

5.1. kép. **Álcaháló alkalmazása optikai felderítés ellen**[206]

A füstben lévő tárgy láthatatlanná válik, ha az őt körülvevő háttérrel összehasonlítva a kontraszt a szem kontraszt érzékelési küszöbénél kisebb. A kontraszt értéke függ a füstréteg vastagságától, tehát törekedni kell megfelelő vastagságú füstfüggöny kialakítására. A füstök alkalmazása 10-15-szörös mértékben csökkentheti a felderítés és célzás hatékonyságát. A füst és ködfüggönyöket a vegyi csapatok erői és eszközei állítják elő. A többi fegyvernem és szakcsapat gránátok, ködgyertyák, termikus ködképző berendezések, ködlövedékek, valamint ködbombák alkalmazásával végezhet ködösítést.

Lézer felderítő eszközök elleni rejtés

Lézer felderítő eszközök elleni rejtés megvalósítható:

- a terep és tereptárgyak tulajdonságainak kihasználásával;
- aerosolok (ködfüggönyök és füstfelhők) alkalmazásával.

[206] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 22.

A ködök alkalmazásával például 3-5-szörös mértékben lehet mérsékelni a látható, az ultraibolya és a közeli infravörös tartományban dolgozó lézerek alkalmazásával működő lézeres irányító és felderítő berendezések hatékonyságát.

A köd úgy lecsökkenti a lézersugárzás energiáját a megvilágító berendezés és a cél közötti úton, valamint a célról történő visszaverődés után, hogy a kereső rendszer már nem tudja azt felderíteni.

Infravörös felderítés elleni rejtés

Az infravörös felderítés elleni rejtés megvalósítható:

- a domborzat és a tereptárgyak tulajdonságainak kihasználásával;
- az objektumok (eszközök) hőkibocsátó eszközökkel (infracsapdákkal) való színlelésével;
- füst és ködfüggönyök alkalmazásával;
- különböző bevonatok (álcahálók) alkalmazásával.

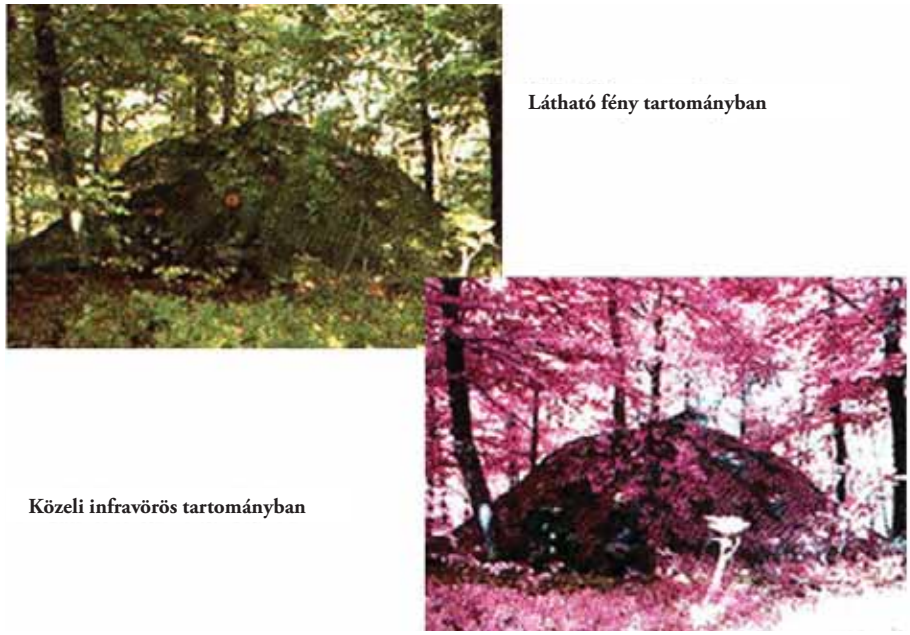
A füstfüggöny a hősugárzás forrása és a megfigyelő között csökkenti a láthatóságot, sőt nagy vastagságú füstfelhő esetén megakadályozhatja az infra felderítő berendezés általi megfigyelést. (5.2-5.3. kép)

Látható fény tartományban **Infravörös hő tartományban**

5.2. kép. **Katonai gépjármű látható és infravörös hő tartományban**[207]

Ha megfelelő koncentrációjú a köd, amelyet antrocén keverékkel állítanak elő, akkor az éjszakai megfigyelő berendezés képének fényerejét 2,5-szeresével csökkenti, míg ködképző keverékkel előállított köd 11-szeresen csökkenti ezt. A ködgránátok felrobbantása következtében egy magas hőmérsékletű zóna keletkezik, amely egy percen keresztül infravörös tartományban is biztosítja a védelmet.

[207] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 23.



5.3. kép. **Álcahálóval letakart objektum**[208]

Hidroakusztikai, akusztikai felderítés elleni rejtés
A hidroakusztikai, akusztikai felderítés elleni rejtés megvalósítható:
- a vízben vagy vízpart közelében üzemelő hajók, gépek zajszintjének csökkentésével;
- mesterséges zajfüggönyök létrehozásával;
- természetes és szándékos hidroakusztikai, akusztikai zavarok kombinált alkalmazásával;
- színlelt akusztikai célok, hangelnyelők alkalmazásával.

Mágneses mérésen alapuló felderítés elleni rejtés
A mágneses mérésen alapuló felderítés elleni rejtés megvalósítható:
- a technika és fegyverzet mágneses terének csökkentésével, megváltoztatásával;
- „valós" objektumokkal, fegyverzettel és haditechnikai eszközök alkalmazásával.

Rádiólokációs felderítés elleni rejtés
A rádiólokációs felderítés hatékonysága attól függ, hogy az objektumoknak vagy technikai eszközöknek milyen az elektromágneses hullámokat visszaverő képessége a környezethez viszonyítva. Ez függ az objektum anyagától, formájától, méretétől.

[208] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 24.

A tárgyak terepen való rádiólokációs felderítésének elve azon alapul, hogy a háttér és az objektum közötti kontraszt pontosan kirajzolódik a lokátor vevőkészülékének indikátorán.

Az objektum rejtése érdekében ezt a kontrasztot kell csökkenteni úgy, hogy az ne emelkedjen ki a környezetéből. Speciális eszközökkel hamis célok is megjeleníthetők, vagy elektronikai zavarokkal lefoghatók az ellenség felderítő rádiólokátor berendezései.

Rádiólokációs felderítés elleni rejtés megvalósítható:

- a terep és tereptárgyak árnyékoló tulajdonságának kihasználásával;
- alakmásító rádióhullámokat elnyelő bevonatok alkalmazásával;
- aktív rádiózavarokkal;
- színlelt objektumok, rádiólokációs felderítési pontok szögvisszaverőkkel való létesítésével.

Az álcázáskor figyelembe kell venni a környezet álcázó sajátosságait is. A természetes álcákat a következőképpen lehet osztályozni:

- a terep domborzatának egyenetlensége;
- a terep fedettsége (erdők, cserjék, fasorok műtárgyak, építmények, széna, szalma és más helyi tárgyak).

Az álcázó anyagok hatékonysága nagymértékben függ azok nedvességtartalmától.

Alakmásító rádióhullámokat elnyelő bevonatok alkalmazása esetén a harceszközökről visszavert jel energia szintjét 10-20%-kal csökkenthetjük, mert a felderítési távolság a felére csökken, mivel a visszavert teljesítmény arányos az effektív visszaverő felület negyedik gyökével.

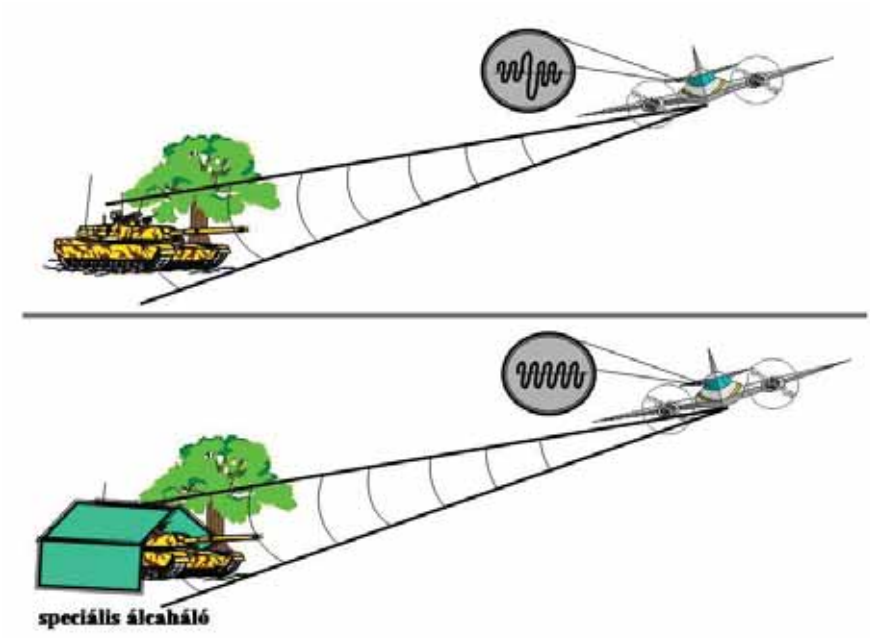
Az 5.3. ábrán harckocsi álcázása látható rádiólokációs felderítés ellen speciális álcaháló felhasználásával.

Jelenleg a rádiólokációs hullámok visszaverésének csökkentésére elnyelő anyagokat alkalmaznak. Az elnyelő réteg csökkenti a hullámok visszaverődését, és a beérkező elektromágneses energiát hővé alakítja át. Sokrétegű elnyelő anyag felhasználásával nő az elnyelés frekvenciasávja.

Természetesen épületeket is lehet rejteni a rádiólokációs felderítés ellen. A falakat több rétegben beton és grafit keverékével vonják be. Az ilyen bevonat elnyeli (abszorbeálja) a hullámokat az üregeiben.

Valamennyi eddig ismertetett visszaverődést csökkentő eljárás eredményes kiegészítője az acélporos védőfesték-bevonat. A festéket a bekevert mikroszkopikus acélrészecskék vezetővé teszik, ennek következtében a visszatükrözés a besugárzott eszköz minden részén megvalósul, csökkentve ezáltal az alakfelismerés lehetőségét.

Színlelt objektumok, rádiólokációs felderítési pontok létesíthetők szögvisszaverőkkel, vagy aktív válaszzavaró adókkal is. A szögvisszaverők segítségével imitálható például híd, vagy komp, vasúti csomópont, sziget. Aktív válaszzavaró adókkal imitálhatók egyedül álló objektumok, objektumcsoportok.



5.3. ábra. **Harckocsi álcázása rádiólokációs felderítés ellen speciális álcaháló felhasználásával**[209]

Ha az objektum körül hamis objektumokat telepítünk, csökken a valós objektum megsemmisülésének valószínűsége. A hamis és valós objektumok közötti távolságnak olyanak, kell lennie, hogy a valós objektum ne semmisüljön meg a hamis objektumra mért csapás esetén.

Rádió- és rádiótechnikai felderítés elleni tevékenység

A rádió- és rádiótechnikai felderítés ellen aktív és passzív módszerek szigorú betartásával védekezhetünk.

Az aktív módszerek a következők:

- az ellenség felderítő eszközeinek megsemmisítése;
- az ellenség felderítő eszközeinek elektronikai zavarása;
- az ellenség megtévesztésével kapcsolatos tevékenységek.

A passzív módszerek az alábbiak:

- kis felderítési valószínűséggel rendelkező eszközök tervezése és alkalmazása (frekvenciaugratásos, kiterjesztett spektrumú eszközök);
- eszközök, rendszerek előírás szerinti telepítése és üzemelése.

[209] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 26.

A felderítés elleni tevékenység főbb módszerei a következők:

– minimális kisugárzás, amely elérhető:
  = csak a szükséges kisugárzás biztosításával (teljesítmény, idő);
  = a kisugárzás előtt az üzenet megtervezésével (felesleges kisugárzási idő csökkentése érdekében);
  = kisugárzás gyors és pontos végrehajtásával (érthető beszéd, megfelelő modulációs mód, helyes rádióforgalom);
  = olyan eszköz alkalmazásával, amely képes az adatok szétdarabolt továbbítására (a harcászati műholdas távközlési rendszerekben így lehet nagymértékben csökkenteni a kisugárzási időt);
  = a lehetőségek függvényében alternatív eszközök alkalmazásával (kábel, huzal, futár);
– az ellenség felderítésétől védett adások alkalmazása, amely elérhető:
  = alacsony teljesítmény alkalmazásával;
  = helyes antenna kiválasztásával (a kimenő teljesítménynek megfelelő nagyságú és iránykarakterisztikájú antenna kiválasztásával);
  = irányított antennák alkalmazásával;
  = a lehetséges legrövidebb antennák alkalmazásával;
  = az ellenség felderítésétől védett hely kiválasztásával, amely árnyékolja az adó jelét;
  = mobil antennák alkalmazásával (gyors áttelepíthetőségi lehetőség);
  = megtévesztő antennák alkalmazásával (a vizuális felderítés megtévesztése érdekében);
  = változtatható nulla helyzetet érzékelő antennák alkalmazásával;
– a helyes kezelői fogások begyakorlása, amelyekbe beletartozik:
  = a kezelői sajátosságok csökkentésének begyakorlása (frekvencia, hívónév változtatásával);
  = a rendszertelen rádióforgalom alkalmazása (rendszertelen jelentési idők bevezetése, rendszeres jelentések más kommunikációs eszközön történő továbbítása);
  = azonosítás (hitelesítés) nem titkosított eszköz alkalmazásakor (azonosítás kérése, azonosító jellemzők rendszertelen megváltoztatása);
  = az összes saját nélkülözhetetlen információt tartalmazó adat titkosítása;
  = híradó biztonsági eszközök alkalmazása;
  = rövidítések, kulcsszavak alkalmazása.[210]

[210] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 28.

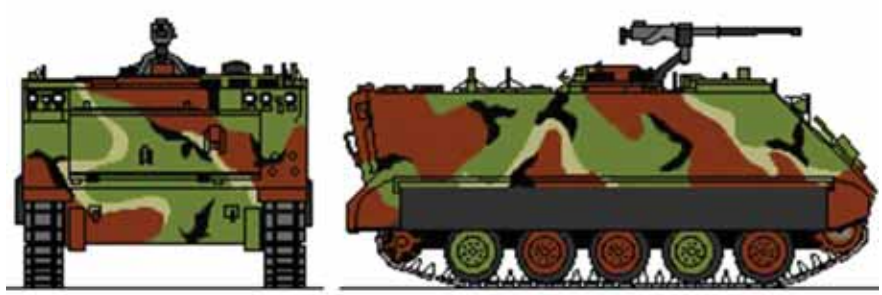
5.2.3 A felderítés elleni tevékenység eszközei

A felderítés elleni tevékenység egyes részterületeinek végrehajtását különböző szakalegységekkel, illetve technikai eszközökkel biztosíthatjuk.

A technikai eszközök a következők lehetnek:

- festékek, bevonatok;
- különböző mesterséges álcák;
- álcázó ködök;
- vakító eszközök;
- infraálcázó eszközök;
- kis valószínűséggel felderíthető eszközök.[211]

Festékeket, bevonatokat az ellenség optikai és rádiólokációs felderítése ellen alkalmazzuk. A festékek elsősorban a harci technika védőfestését (egyszínű festék) és alakmásító (többszínű foltos) festését teszik lehetővé. (5.4-5.5. kép)



Harcjármű

Gépjármű

A MH-ség álcázó mintái

5.4. kép. **Álcázó festékek alkalmazása**[212]

[211] U.o. p. 30.

[212] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 30.

5.5. kép. **Helikopterek álcázó festése**[213]

A technikai eszközökön alkalmazott rádiófrekvenciás elnyelő-, csillapító anyagot tartalmazó védőbevonatok az elektromágneses hullám visszaverődésének csökkentésére szolgálnak, ezáltal lehet csökkenteni felderítési valószínűségét.

A mesterséges álcák alkalmazása akkor jelentős, amikor a természetes viszonyok nem biztosítják a megfelelő álcázást. Egyik csoportjukat az optikai felderítés ellen alkalmazzák. Ezek lehetnek a rendszeresített álcahálók, takarók. (5.6. kép)

A másik csoportjukba tartoznak a rádiólokációs álcák, melyek képesek az objektumok rádiólokációs képét eltorzítani, illetve színlelt rádiólokációs képek létrehozásával a szemben álló fél rádiólokációs felderítését félrevezetni.

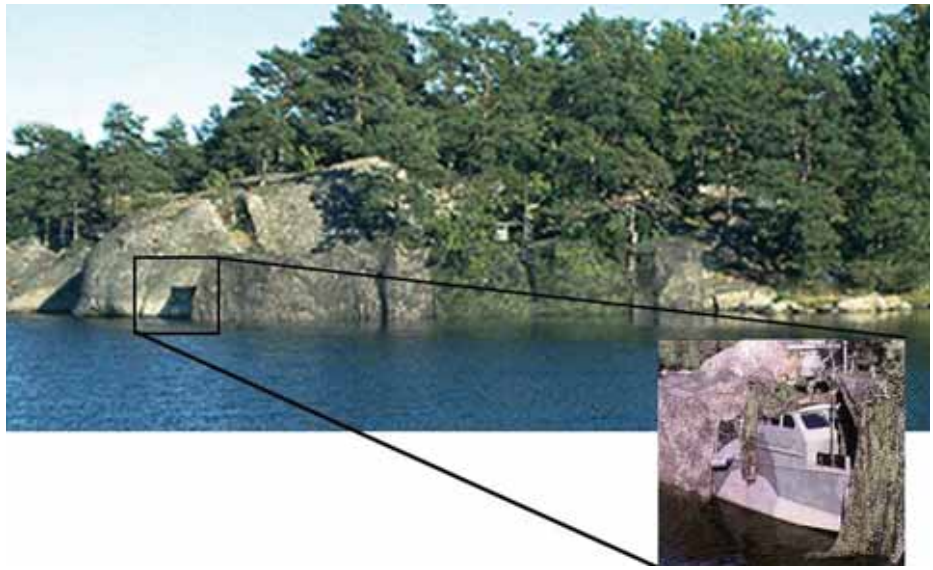
A rádiólokációs álcákat feloszthatjuk zavaróálcákra, melyeket szögvisszaverőkből (lásd a 4.1. fejezetet) készítenek, illetve ernyőálcákra, amelyeket különféle elektromágneses energiát elnyelő anyagok felhasználásával készítenek.

Az ernyőálcák közül figyelemre méltó tulajdonságokkal rendelkezik az LCSS *(Lightweight Comouflage Screen System)*[214] álcaháló, melynek fontosabb adatai a következők:

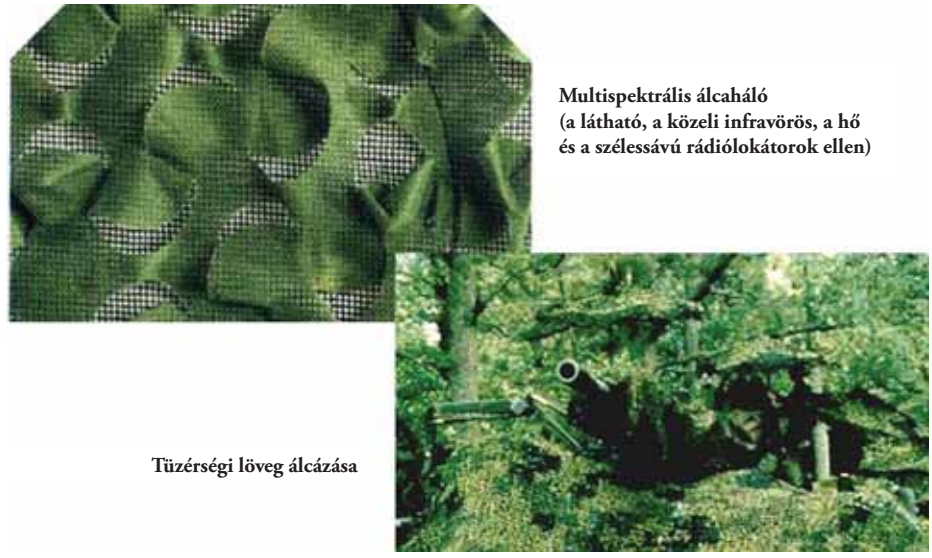
- súlya 50 kg;
- felülete 82-83 m^2;
- színezése erdős, sivatagi, sarkvidéki lehet.

Az álcaháló biztosítja a vizuális, optikai, rádiólokációs (fémszálak beépítésével) felderítés elleni álcázást. (5.7. kép)

[213] U.o. 31.
[214] http://www.fas.org/man/dod-101/sys/land/lccs.htm (Letöltve: 2014.01.23.)



5.6. kép. **Álcaháló alkalmazása**[215]



5.7. kép. **Multispektrális álcaháló alkalmazása**[216]

[215] QuickCam – Camouflage System (Letöltve: 2014.01.23.) http://www.saabgroup.com/en/Land/Force_Protection/Signature_management/Static_Camouflage/Camouflage_Systems/Quick_Cam_camouflage_system/Features/

[216] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 33.

Egy másik típusú ernyőálca a rádiólokációs hullámokat elnyelő borító, melynek jellemzői az alábbiak:

– a borító olyan szőr és gyékény, amely gumival van telítve, emellett a gyékény minden szála félvezető vékony gumiréteggel van bevonva;
– a borító a fém felületéről a 10 cm-es hullámok visszaverődését 100-szorosan, a 3,2 cm-es hullámhossznál 300-szorosan, míg a 1,2 cm-eseknél 1000-szeresen gyengíti;
– a borító vastagsága 3-9 cm-t tesz ki, amely korlátozza a felhasználását.

Az álcázó ködök általában olaj alapúak, vagy cink alapú fémködök, melyek hatékonyan biztosítják a rádiólokációs felderítés elleni álcázást.

A ködfüggönyöket általában más álcázástechnikai eszközök alkalmazásával, színlelt csoportosítások és objektumok, illetve tevékenységek imitálásával egyidejűleg komplex tevékenység részeként célszerű alkalmazni.

A ködösítés megvalósítása nagy körültekintést igényel, mivel számos előnyével és kedvező hatásával szemben jelentős mértékben zavarhatja és gátolhatja a saját csapatok tevékenységét.

A ködösítést minden fegyvernemi alegység a rendszeresített eszközeivel hajtja végre saját tevékenységének rejtése érdekében.

Például: egy PSZH-ra 12 db 66 mm-es ködgránátot a két oldalára hatosával lehet felszerelni. A járműtől 20-25 m távolságra 13 m magas 38 m széles ködfüggönyt, 2-3 másodperc alatt lehet létrehozni, amely 1-3 percig marad meg. Az 5.1. táblázaton köd- és imitáló lövedékek alapvető harcászat-technikai adatai láthatók.

5.1. táblázat. **A köd- és imitáló lövedékek alapvető harcászat-technikai adatai**[217]

Ködanyag megnevezése	Súly [kg]	Ködképzés időtartama [perc]	Az át nem látszó ködfüggöny		
			Hossza [m]	Szélessége [m]	Magassága [m]
84 M ködgyertya	2.5	4–8	100-120	10-15	10-15
BDS–5 harckocsi ködgyertya	40	7-10	500	100	30-40
82 mm av. ködgránát	3.41			25-30	2-3
120 mm av. ködgránát	16.6		25-30	25-35	7-9
122 mm á.tar. ködgránát	22.55		25-35	25-35	7-9

[217] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 34.

A vakítás az ellenség harctevékenységének akadályozásában jelentős szerepet tölt be. Az ellenség vakítása alatt az ellenség figyelésének, felderítésének, éjjellátó eszközei alkalmazásának, hatékony tűzvezetésének és a terepen való tájékozódásának teljes vagy részleges korlátozását értjük.

Az éjszakai harctevékenység folyamán a különböző fényforrások lényeges változást idéznek elő az optikai, illetve elektro-optikai műszerek, berendezések használatában, és így a látás feltételeinek biztosításában. A fény bizonyos esetekben jelentősen növeli ezen eszközök hatékonyságát, bizonyos esetekben viszont részlegesen, vagy teljesen, esetleg időlegesen korlátozhatja alkalmazásukat.

Egy vakító lövedékkel biztosítandó 22 lux megvilágítási erősséget figyelembe véve az 5.2. táblázatból leolvasható a vakítás terepszakaszának az optikai műszerek (figyelők) terepszakaszától való távolságot, valamint a világítólövedék robbanópontjai közötti tűzlegyező térköz távolsága.

5.2. táblázat. **A vakítás terepszakaszának az optikai műszerek terepszakaszától való távolsága és a tűzlegyező térköz nagysága optikai műszerek vakításakor**[218]

Vakítólövedék (akna) típusa	Terepszakasz távolsága [m]	Tűzlegyező térköz [m]
122 mm-es SZ-463	100	150
120 mm-es SZ-9	100-150 200	300 200
82 mm-es SZ-832 SZ	50	100

A vakítás, több világítólövedék (akna) – a vakítás terepszakaszára, a meghatározott tűzlegyező térközzel – módszeres tűzben történő kilövésével a szükséges időtartamig fenntartható. A módszeres tűz üteme – mivel a szem a fáklya égését követően még huzamosabb ideig káprázik – meghaladja a fáklya égésének idejét.

A korszerű passzív rendszerű elektro-optikai műszerek képcsöveinek védelmét egy túlterhelés elleni védőszerkezet beépítésével oldották meg, amely szerkezet erős fényhatás esetén automatikusan lezár. Azonban a műszer a fényvédő retesz lezárásának időtartalma alatt használhatatlan.

A passzív rendszerű elektro-optikai műszereket tehát éppen legfőbb előnyük, a fényérzékenységük teszi könnyen vakíthatóvá. Az elektro-optikai műszerek elhelyezési körletének, terepszakaszának mintegy 8-10 lux erősséggel történő megvakítása már biztosítja ezen eszközök vakítását, alkalmazásuk korlátozását.

Mivel az ellenség részéről a figyelők terepszakaszain, a tűzszakaszokon az optikai és elektro-optikai felderítő műszerek, irányzékok általában vegyesen helyezkednek el, ezért a vakításukat az optikai műszerek, és így valamennyi műszer vakítását biztosító eszközök és a terepszakasz távolsága, tűzlegyező térköz alapján célszerű végrehajtani.

[218] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 35.

Az ellenség optikai, elektro-optikai felderítő műszereinek, irányzékainak, páncéltörő rakétáinak és más, közvetlen irányzású tűzeszközeinek vakítása, tájékozódásának akadályozása megvalósítható ködlövedékek (aknák) alkalmazásával is.

A ködlövedékeket a robbanásukkor keletkező ködfelhő méretei jellemzik, amely az 5.3. táblázatban látható.

5.3. táblázat. **A tüzérségi ködlövedékek és aknák robbanásakor keletkező ködfelhő méretei**[219]

A lövedék (akna) űrmérete [mm]	A ködfelhő szélirányra merőleges kiterjedése [m]	A ködfelhő magassága [m]
122	30-40	7-9
120	30-40	7-9
82	10-15	2-3

Az infrafelderítő eszközök elleni álcázást, illetve az infrafejjel ellátott önirányítású rakéták elleni tevékenységet az álcázott objektum hőkisugárzásának csökkentésével és színlelt hőkisugárzó berendezések alkalmazásával hajthatjuk végre.

A meleg felületek árnyékolásához fémlemezeket és egyéb éghetetlen anyagokat, hőszigetelőket (üvegszálat, azbesztet) célszerű használni. A motorok kipufogógázai hőmérséklete csökkentésének alapfeltétele, hogy a kipufogógázok füst nélküliek legyenek.

A hőfelderítés elleni álcaháló jellemzői:

– két részből áll, egy belső hőtakaróból, amely hőtükröt képez a hőkibocsátó jármű részére és egy külső hőtakaró rétegből, amely elrejti a járművet a háttérben;
– a hőtakarónak van egy műanyag bevonatú fémrétege, valamint egy szellőzőnyílásokkal rendelkező szövetrétege, amely lehetővé teszi a meleg levegő ellenőrzött elvesztését.

Az álcaháló alkalmazható:

– vizuális felderítés ellen;
– infravörös közeli tartományban történő felderítés ellen és;
– rádiólokációs felderítéssel (1-1.5 cm és 10 cm hullámhossznál) szembeni álcázásnál.

Az álcaháló főbb adatai:

– súlya 12,5-45 kg-ig;
– terület 50 m^2;
– mintázata erdei és havas;
– telepítéséhez két fő szükséges.

[219] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 36.

A kis valószínűséggel felderíthető (kiterjesztett spektrumú) eszközök alkalmazása a SIGINT elleni védelem egyik leghatékonyabb megoldása. A korszerű háborúkban a csapatvezetés szilárdságának fokozásával kapcsolatos törekvések előtérbe kerültek, ami azt jelenti, hogy törekedni kell olyan eszközök használatára, amelyek elektronikai zavarás esetén is megbízhatóan üzemelnek. A felderítés eszközei is korszerűsödtek, és egyre nagyobb mértékben tudják a hagyományos rádióforgalmi rendszereket felkutatni, lehallgatni, települési körzetüket behatárolni.

Ezen problémák megoldására kiterjesztett spektrumú hírközlő eszközöket (rádió adó-vevőket) kezdtek fejleszteni, amelyek alkalmazásával nagyobb megbízhatósággal tarthatók fenn az összeköttetések és felderítésük, lehallgatásuk, települési körzetük meghatározása hagyományos elven működő rádiófelderítő, iránymérő berendezésekkel nem lehetséges. Így napjainkban egyre jobban elterjednek, és nélkülözhetetlenné válnak a kiterjesztett spektrumú modulációs elven működő átviteli eszközök.

A nyugati katonai terminológia kis valószínűséggel felderíthető rádióadásoknak nevezi *(Low Probability of Interception – LPI)* a felderítés és zavarás ellen nagy védelmet nyújtó eljárásokat.

A kiterjesztett spektrumú átviteli rendszerek alaptulajdonsága, hogy azonos alapsávi forgalom esetén a bennük alkalmazott speciális csatornakódolási (modulációs) eljárások következtében a csatornákban felhasznált teljes sávszélesség nagyobb, (esetleg nagyságrendekkel), mint a hagyományos modulációs rendszerekkel létrehozott jelek sávszélessége. A kiterjesztett spektrumú átviteli rendszerek másik fontos tulajdonsága az álvéletlen *(pseudo random)* jelleg, ami annyit jelent, hogy az átviteli csatornákon folyó kommunikáció egy rendszeren kívüli megfigyelő számára nagy sávszélességű, zaj jellegű véletlen jelnek tűnik, a rendszeren belüli partnerek viszont – ismerve a csatornakódolás szabályait – dekódolni tudják a jeleket és kinyerik az információt.

A kiterjesztett spektrumú jel:

- nagy sávszélességű;
- nehezen deríthető fel;
- nehezen fejthető meg;
- egyes esetekben automatikusan védelmet nyújt a fading hatások ellen.

A kiterjesztett spektrumú modulációnak elméletileg a következő változatai lehetnek:

- közvetlen zajmodulációs eljárás *(Direct Sequence – DS)*;
- frekvenciaugratásos eljárás *(Frequency Hopping – FH)*;
- impulzus frekvenciamoduláció vagy chirp eljárás *(Pulse Frequency Modulation – PFM)*;
- időugratásos eljárás *(Time Hopping – TH)*;
- hibrid rendszerek.[220]

[220] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 42.

A kiterjesztett spektrumú modulációhoz a megfelelő jelet úgy állíthatjuk elő, hogy az információt hordozó jelet megszorozzuk a spektrumot kiterjesztő álvéletlen jelsorozattal, amelyre két lehetőség van:

– az információs jelet ténylegesen megszorozzuk egy (gyors) álvéletlen jelsorozattal;
– a vivőfrekvenciát véletlenszerűen (álvéletlenszerűen) széles tartományban változtatjuk.

Az előbbit közvetlen zajmodulációs eljárásnak, az utóbbit frekvenciaugratásos rendszernek nevezik.

A közvetlen zajmodulációs jelet előállító adóberendezés kettős modulációval dolgozik:

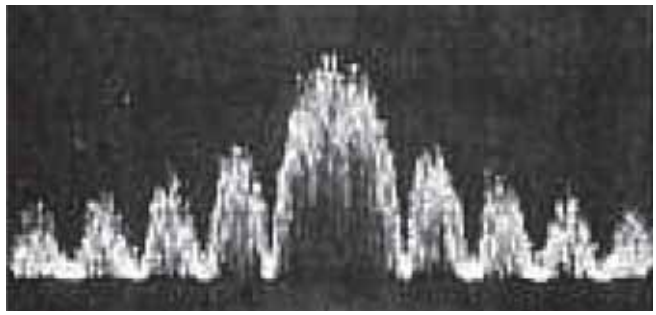
– az első a szokásos módon keskenysávú moduláció a vezéroszcillátorban, a moduláló jel lehet analóg vagy digitális jellegű;
– a második moduláció a teljesítményerősítő előtt történik, a vezéroszcillátor jelét (mint vivőt) a fázismodulátorban digitális zajjal billentyűzik, (*Binary Phases Shift Keying – BPSK* – bináris fázisbillentyűzés) majd erősítés után ez kerül kisugárzásra. (5.10. kép)

A vevőben a helyi oszcillátor jelét (melynek frekvenciája a középfrekvenciával tér el a vételi csatornáétól) billentyűzik digitális zajjal, így a keverő után már a szokásos középfrekvenciás jel áll rendelkezésre.

A legnehezebb feladatot a vevőoldali kódgenerátor szinkronizálása jelenti az adóéhoz képest.

A szinkronizálásra alapvetően három eljárást dolgoztak ki:

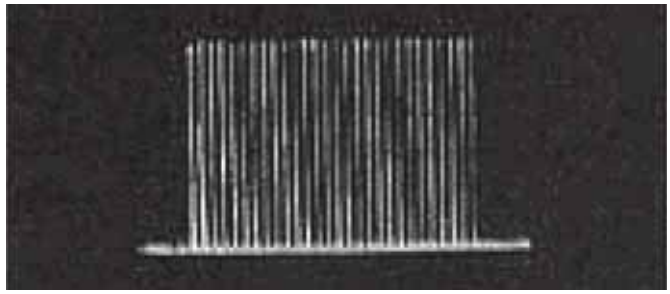
– az információval együtt a frekvenciakód kisugárzása;
– frekvencia- és fázisszinkronizáció egy harmadik jel, például etalon frekvenciájú állomások segítségével;
– a kiterjesztett spektrumú jel egyedi kiértékelésével történő szinkronizáció.



5.8. kép. **A közvetlen zajmodulációs rendszer spektrumképe**[221]

[221] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 42.

A frekvenciaugratásos adókban a vivőfrekvencia pillanatnyi értékét változtatjuk úgy, hogy egy frekvenciakészleten belül az egyes diszkrét frekvenciák felhasználási sorrendjét egy álvéletlen generátorral programozzuk. Maximális hosszúságú álvéletlen sorozatot alkalmazva 2n-l féle frekvenciát állíthatunk elő. (5.9. kép)



5.9. kép. **A frekvenciaugratásos adóberendezés spektrumképe**[222]

Az adott frekvencián tartózkodás ideje t(a) fontos paraméter, mely néhány ms-tól néhány száz ms-ig terjedhet és jellemzője a berendezésnek, valamint a használt frekvenciasávnak. A rövidhullámú, 5-30 MHz-es tartományban t(a)=100-200 ms, a 30-88 MHz-es URH tartományban t(a)=5-20 ms.

Már ismertek olyan rendszerek, amelyek a frekvencián tartózkodás idejét is folyamatosan változtatják, ezzel tovább növelve a felderíthetőség és zavarás elleni védettségüket. (5.10. kép)

5.10. kép. **Frekvenciaugratásos rádióberendezés**[223]

Az adó és vevőberendezés azonos időbeni áthangolását szinkronrendszer biztosítja. Mivel az összeköttetés frekvenciáját, és annak sorrendjét elvben csak az adó és vevőponton ismerik előre, így a felderítővevőnek az egész DF sávban kell keresnie, amíg megtalálja az adást.

[222] U.o. 45.

[223] http://punjab-pk.all.biz/prc-2505-vhf-frequency-hopping-transceiver-g35887#show0 (Letöltve: 2014.04.20.)

Ugyanilyen nehéz a válaszzavarás kiváltása is, hiszen először venni kell a zavarandó frekvencián az adó jelét, azt azonosítani (a zavarandó rádiókapcsolathoz tartozik-e), majd indítani a zavarást. Ez hosszadalmas, bonyolult, sok matematikai műveletet is kívánó folyamat, ami csökkenti annak lehetőségét, hogy a zavarjel még időben a vevő bemenetére kerül.

A frekvenciaugratásos rendszereknek három jellegzetes alaptípusa van:

– a lassú frekvenciaugratásos rendszer *(Slow Frequency Hopping – SFH)*, mp-ként néhányszor tíz frekvenciaváltás;
– közepes sebességű (mp-ként néhány száz) frekvenciaváltás;
– a gyors frekvenciaugratásos rendszer *(Fast Frequency Hopping – FFH)*, mp-ként ezer körüli frekvenciaváltás.

A kiterjesztett spektrumú eszközök jellemző tulajdonsága, hogy nagy zavarvédelemmel rendelkeznek a természetes, szándékos és véletlen zavarok ellen.

5.3 Az elektronikai ellentevékenységgel szembeni védelem

Az elektronikai ellentevékenységgel szembeni védelmen belül alapvetően a szándékos és nem szándékos zavarok, illetve az elektronikai pusztítás elleni tevékenységgel foglalkozunk részletesen.

Az elektronikai eszközök alkalmazása a harctevékenység valamennyi kulcsfontosságú területén szükségessé teszi ezen eszközök elektronikai ellentevékenység (zavarás) elleni védelmének fokozását.

Az elektronikai ellentevékenység (zavarás) elleni tevékenységet az elektronikai felderítéssel, elektronikai ellentevékenységgel, illetve az ellenség vezetési és fegyverirányítási eszközeinek a megbontására irányuló minden más tevékenységgel összhangban kell megvalósítani.

Az elektronikai eszközök ellenséges elektronikai ellentevékenységével (zavarásával) szembeni védelemnek, ha nem is elektronikai, de mindenképpen a leghatásosabb módszere a zavarforrások (zavaró állomások) megsemmisítése. Az elektronikai zavarás elleni tevékenységgel kapcsolatban használjuk a zavarstabilitás és zavarvédettség fogalmát.

A zavarstabilitás az elektronikai rendszerek azon tulajdonsága és képessége, amely kifejezi, hogy az adott rendszer az elektronikai zavarás viszonyai között képes-e funkcionális feladatainak végrehajtására.

A zavarvédettség az elektronikai eszközök azon tulajdonsága, hogy milyen mértékű, intenzitású, típusú zavaró jelekkel szemben védettek. Ez azt jelenti, hogy a rendszeren belül minél zavarvédettebb eszközök vannak, annál nagyobb a rendszer zavarállósága.

Az egyes eszközök zavarvédettségét alapvetően a fejlesztés-, tervezés-, kivitelezés során kell biztosítani, és lehetővé tenni, hogy a berendezések minél nagyobb mértékben legyenek képesek kiszűrni a zavarokat.

5.3.1 A szándékos zavarok elleni védelem módszerei

A szándékos zavarás hatékonyságát csökkentő általános módszerek a következők lehetnek:

- a zavarás és zavarok felismerése:
  - = a zavar eredetének meghatározása (a zavar külső, ha a zavar az antennán keresztül jut be a vevőbe, a zavar belső, ha a zavar nem az antennán keresztül jut be a vevőbe, akkor berendezéshiba);
  - = a zavar hovatartozásának meghatározása (például a zavar szándékos ellenséges zavarás esetén, a zavar nem szándékos saját eszköz zavarása, atmoszféra zavarok estén);
- a zavarás és a zavarok hatékonyságának csökkentése:
  - = az üzemelés folytatása (a zavar hatékonyság felmérésének akadályozása céljából);
  - = a hasznos jel és a zavaró jel arányának javítása;
  - = a vevőberendezés beszabályozása (például helyi oszcillátor, sávszélesség, hangerő beszabályozása);
  - = az adó kimenő teljesítményének növelése;
  - = az antenna beszabályozása vagy megváltoztatása (antenna polarizáció megváltoztatása minden állomáson, nagyobb terjedelmű antenna alkalmazása);
  - = átjátszó állomás létesítése;
  - = az antenna helyének a megváltoztatása;
  - = alternatív híradó útvonalak alkalmazása;
  - = frekvencia megváltoztatása;
  - = másik műholdra való átállás.

A szándékos zavarok elleni védelemnek – az elektronikai eszközök felhasználásának függvényében – alapvetően három módszere különböztethető meg:

- az elektronikai eszközök széttelepítése;
- az információt továbbító elektronikai eszközök manőverező képességének kihasználása;
- az ellenség által zavarással lefogott elektronikai eszközök, rendszerek helyettesítése.

Az *elektronikai eszközök széttelepítése* során is biztosítani kell a folyamatos információáramlást az alábbi szempontok mérlegelésével:

- az adott rendszer milyen mértékben biztosítja közbeeső csomópont kiesése esetén az információk kerülő úton történő eljuttatását;
- az adott rendszer milyen mértékben biztosítja az információ egy időben több, funkcionálisan ugyanazon rendeltetésű, azonos, vagy különböző forgalmi rendszerekben való továbbítását.

Az *információtovábbítás időszakában* az információ biztonsága érdekében az alábbi lehetőségeket kell mérlegelni:

– az adott forgalmi rendszerekben felhasználható üzemi és tartalék frekvenciák optimális lehetőségeit;
– azokat a lehetőségeket, amelyeket az adott rendszerben üzemelő elektronikai eszközök üzemi- technikai jellemzői, adottságai biztosítanak.

Az *elektronikai eszközök helyettesítésére* az alábbi lehetőségeket lehet felhasználni:

– tartalék – eddig nem aktivizált – rendszerek bekapcsolását;
– a vezetékes összeköttetéseket;
– Az információ egyéb úton, például futárok útján történő továbbítását;
– jelek- jelzések alkalmazását.

E módszerekkel csak akkor érhetjük el az információk kellő időben és megfelelő minőségen történő továbbítását, ha arra felkészülünk és az áttérést kellő szinten begyakoroljuk.

A szándékos zavarok elleni védelem általános módszereinek áttekintése után megállapítható, hogy azokat egyrészt szervezési (például alternatív híradó útvonalak), másrészt technikai (például az adó kimenő teljesítményének növelése) módszerekkel lehet biztosítani.

A továbbiakban különböző elektronikai eszközök közül a rádiólokációs-, rádió- és rádiórelé berendezések szándékos zavarok elleni védelemének módszereit tekintjük át részletesebben.

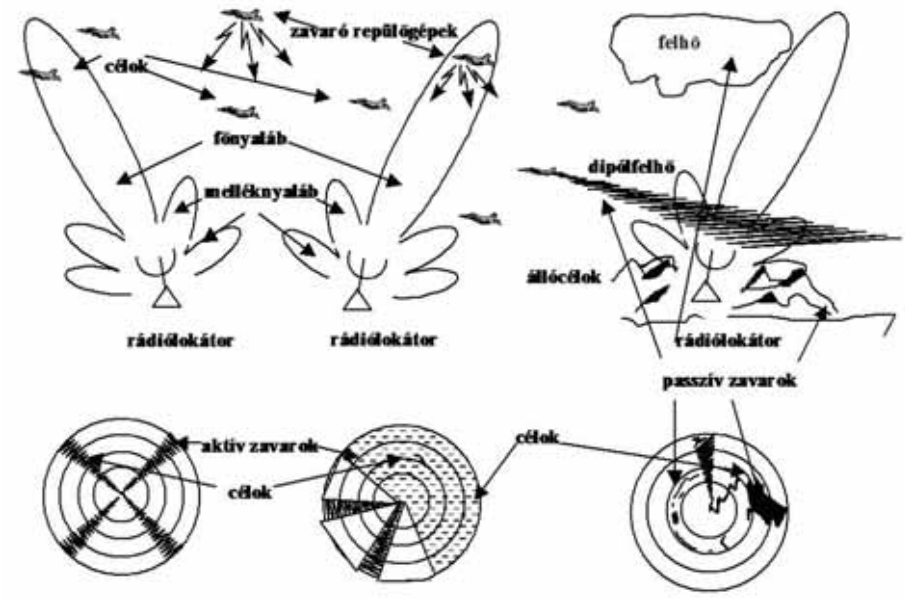
5.3.1.1 A szándékos zavarok elleni védelem módszerei a rádiólokációs berendezéseknél

Háborús konfliktus esetén az ellenfelek mindent elkövetnek saját repülőeszközeik rejtettségének fokozására, a szembenálló rádiólokátorok felderítési lehetőségeinek csökkentésére. Erre a célra a legkülönbözőbb aktív és passzív zavaróeszközöket alkalmazzák, melyek ”mint nap a szemet”, igyekeznek ”elvakítani” a radarokat. Az 5.4. ábrán néhány zavarfajta alkalmazása és radarokra kifejtett hatásuk látható a körkörös indikátoron.

A rádiólokátorokkal kapcsolatos elektronikai hadviselés a II. világháborúban fejlődött ki, amikor az első elektronikai ellentevékenységi eszközök alkalmazásával jelentős eredményeket értek el az egyutas hullámterjedés nyújtotta teljesítmény (négyzetgyök) kisebb volta miatt, a radaroknál szükségszerűen alkalmazott kétutas hullámterjedés esetén jelentkező csillapítás (negyedik gyök) csökkenéssel szemben. Ebben az időben kidolgozásra kerültek a ma is széles körűen alkalmazott passzív zavarás első eszközei (például a dipólfelhők – *chaff*, hamis célok – *decoys*), hogy rejtsék a valódi célokat, vagy hamis céljeleket állítsanak elő segítségükkel (lásd a 4.2. fejezetet).

A szándékos zavarok elleni védelemnek *szervezési és technikai módszerei* a következők lehetnek.

A szándékos zavarok elleni védelem *szervezési módszerei*:
- különböző frekvenciasávban üzemelő rádiólokátorok együttes alkalmazása;
- üzemi frekvenciamanőverek végrehajtása;
- az egységes rádiólokációs mező biztosítása mellett a rádiólokátorok területi manővereztetése;
- a rádiólokátor kezelők magas szintű kiképzése, amellyel elérhető, hogy a kezelők helyesen és időben alkalmazzák az általuk ismert zavarás elleni módszereket.



5.4. ábra. **Zavarok alkalmazása és hatása a körkörös indikátorra**[224]

A technikai módszerek alkalmazásának kulcskérdése a rádiólokátorok zavarvédettsége. A rádiólokációs berendezések zavarvédettsége például az energia, a jelstruktúra, a frekvencia áthangolás sebessége, az antenna karakterisztika, a letapogatás módja szempontjából értékelhető. Egy adott rádiólokációs berendezés zavarvédettsége annál nagyobb, minél nagyobb zavaróteljesítmény szükséges a zavaráshoz.

Általános elektronikai védelmi filozófia az, hogy legyőzzék a teljesítményveszteségekből fakadó hátrányokat, minimalizálják a megtévesztő zavarás hatását, vagy rákényszerítsék a szembenálló felet (különösen) szélessávú zavarójelek előállítására, melynek következtében a zavarás hatékonysága jelentősen csökkenhet. Mivel a szélessávú zavarójeleknek csak a vevő sávszélességébe eső (töredék) része jelenik meg, mint zavar, ezért hatékonysága is ennek arányában csökken. (Ebben az esetben ugyanis a rádiólokátor

[224] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 63.

vevője által vett zavarójel teljesítménye már kisebb lehet, mint a céltárgyról visszavert hasznos jelé.)

A rádiólokátor vevőrendszer zavarvédelmi képességeinek növelése (például szelektivitás, dinamika tartománynövelés, antenna oldalnyaláb szintcsökkentés) mind olyan lehetőségek, amelyekkel jelentősen csökkenthető az elektronikai ellentevékenység hatása. Napjainkra már a korszerű MTI/MTD *(Moving Target Indicator – MTI* – mozgó céltárgy indikátor, *Moving Target Detector – MTD* – mozgó céltárgy detektor) technikák és útvonalképző algoritmusok, eljárások hatására, ha nem is szüntethetők meg, de jelentősen kompenzálhatók a különböző passzív zavarást alkalmazó eljárások (például a dipólfelhők, hamis célok) céltárgy felderítést rontó képessége. A rádiólokátorokban alkalmazott technikai jellegű, fő elektronikai védelmi eljárások az 5.4. táblázatban kerültek összefoglalásra.

5.4. táblázat. **A rádiólokátor alrendszerekben alkalmazható technikai jellegű elektronikai védelmi eljárások**[225]

Rádiólokátor alrendszerek *(Radar Subsystems)*	**Elektronikai védelmi eljárások**
Antenna *(Antenna)*	Nagy irányítottságú antennák *(High Directive Antennas)* Több sugárnyaláb *(Multiple Beams)* Alacsony oldalnyalábszint *(Low Sidelobes)* Oldalnyaláb „blankolás" Oldalnyaláb elnyomás Adaptív fázisrács *(Adaptive Arrays)* Véletlenszerű letapogatás *(Random Scanning of Main Beam)*
Adó *(Transmitter)*	Nagy energia-kisugárzás *(Radar with Large ERP)* Teljesítmény vezérlés időben és térben *(Management of Power in Time and Space)* Frekvencia agilitás és diversiti *(Frequency Agility and Diversity)* Belső impulzus moduláció *(Intrapulse Coding)* Indítás változtatás, szaggatás, kódolás Automatikus frekvencia kiválasztás Milliméteres hullámtartomány használata *(Use of Milimeter Waves - MMW)*
Vevő *(Receiver)*	Kétszeres frekvencia konverzió *(Dual-Frequency Conversion)* Nagy dinamika tartomány *(Large Dynamic Range Receivers)*
Jelfeldolgozás *(Signal Processing)*	Digitális koherens és adaptív mozgócél kiválasztás *(Digital Coherent and Adaptive Moving Target Indicator - MTI)* Detektálás előtti vaklárma normalizálás *(CFAR Detectors)* Impulzus szélesség és ismétlődési frekvencia diszkriminátor *(Pulsewidth and Pulse Repetition Frequency - PRF Discriminator)*

[225] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 65.

Természetesen az elektronikai hadviselés is tovább fejlődik, sokkal kifinomultabb elektronikai ellentevékenységi eljárások és eszközök kerülnek kidolgozásra, alkalmazásra, kikényszerítve ezzel az eddig ismert elektronikai védelmi eszközök és eljárások továbbfejlesztését. Ez végső soron az ultra-szélessávú radarok és nagyon kis oldalnyaláb szintekkel rendelkező antennák (*Side Lobe Cancellation* – SLC technikák) kidolgozásához vezet, melyet sokoldalú, különösen fejlett jelfeldolgozás egészít ki. A radarokban egyre fejlettebb impulzus-kompressziós eljárások kerülnek alkalmazásra, melyek tovább javítják a zavarállóságot.

Az úgynevezett „csendes radar"-ok szintén a közeljövőben széles körűen elterjedő katonai radarok csoportját alkotják, jelentősen megnehezítve ezzel az elektronikai ellentevékenységi eszközök hatékony alkalmazhatóságát. Ez elsősorban azért lehetséges, mivel ezeket az ellenséges vevők kis valószínűséggel képesek „elfogni" *(Low Probability of Intercept Radar – LPIR)*, melynek következtében a direkt nagypontosságú zavarás lehetősége jelentősen csökken, illetve ennek megvalósíthatósága jelentősen megdrágul.

5.3.1.2 A szándékos zavarok elleni védelem módszerei a rádió és rádiórelé berendezéseknél

A rádió és rádiórelé állomásoknál – a rádiólokációs berendezésekhez hasonlóan – a szándékos zavarok elleni védelem (zavarvédettség fokozása) *szervezési és technikai módszerekkel* biztosítható.

A fontosabb *szervezési módszerek* a következők lehetnek:

- tartalék rádióhálók és irányok szervezése;
- rejtett rádióhálók és irányok szervezése;
- kerülő hírcsatornák, közbeeső állomások szervezése és az átjátszó módszer szerinti forgalmazás;
- tartalék üzemi frekvenciák meghatározása és a hívójelek nélküli összeköttetés felvétele;
- üzemmód váltása;
- közlemények különböző hírcsatornákon való egyidejű adása és vétele;
- rádiórelé vonalak és berendezések települési helyének helyes kiválasztása.

A fentiek közül mindig azon módszert célszerű alkalmazni, amelyik a legnagyobb zavarvédettséget biztosítja az ellenséges zavarás ellen.

A rádió- és rádiórelé állomások szándékos zavarok elleni védelemének fokozását biztosító *technikai módszerek* hasonlóak a rádiólokátor berendezéseknél már ismertetekhez.

A fontosabb technikai módszerek például a következők lehetnek:

- az adó teljesítményének növelése;
- különböző szelektivitást növelő módszerek alkalmazása;
- vételzavar elleni védett hibajavító kódok alkalmazása;
- gyors adók, frekvenciaugratásos rádió-berendezések alkalmazása.

Az *adók teljesítményének növelése* ugyan az ellenség szándékos zavarása elleni védelem legegyszerűbb módja, de ez a saját nem szándékos zavarok jelentős növekedéséhez vezethet. Egyben megkönnyíthetjük az ellenség rádiófelderítését, így fokozhatjuk berendezéseink megsemmisítésének valószínűségét. Ezért a teljesítménynövelést akkor célszerű alkalmazni, amikor már kimerítettük a szándékos zavarok elleni védelem összes többi lehetőségét.

A *térszelekció* az élesen irányított adó- és vevőantennák alkalmazásával biztosítható, amelynek megvalósítása az ultrarövid-hullámú sávban már nem ütközik nehézségbe. Az antenna sugárzási diagramjának forgatásával, fáziskompenzációs módszerrel a zavaró jelek elnyomhatók. Nézzük meg közelebbről e technikai módszer lényegét.

A vevőberendezésnél egymástól néhány üzemi hullámhossz távolságra két vevőantennát telepítünk merőleges iránnyal a hasznos jel sugárzási irányára. A kisugárzott hasznos jeleket két antennával egyidejűleg vesszük, azaz egyenlő fázissal. Ha a hasznos jel frekvenciáján zavarás van, és ha a zavaró jel kisugárzási iránya különbözik a hasznos jel kisugárzási iránytól, akkor a vevőantennák a zavaró jelet bizonyos fáziskülönbséggel veszik.

A zavaró jel elnyomásához meg kell változtatni a hasznos és zavarójel közötti fáziskülönbséget (mivel a két antenna között fellépő fáziskülönbség 180°), majd pedig amplitúdóit is egyenlővé kell tenni. A fáziskülönbség megváltoztatását fázisfordítóval, az amplitúdók kiegyenlítését pedig az antennákra épített variométerrel és szintautomatikával lehet végrehajtani.

A két ellentétes fázisú és különböző amplitúdójú jel összegzésének eredményeként a vevő bemenetén a hasznos jel a zavarójelhez képest kisebb gyengülést szenved. *Időszelekció* alkalmazása esetén a vevőberendezések csak a hasznos jel megjelenésének időszakában működnek.

Amplitúdó-szelekció a vevőfokozatban a különböző zajvágó áramkörökkel hozható létre. *Frekvenciaszelekció* a vevőberendezésben alkalmazott különböző rezgőköri elemekkel érhető el. (Viszonylagos egyszerűségénél fogva ez a legjobban elterjedt szelektivitást növelő módszer.)

A szándékos zavarok elleni védelem fokozásának egy további módszere a *védett kódok* alkalmazása.

Azokat a kódokat nevezzük vételzavar védetteknek, amelyekkel az üzem során a kódokat rejtjel- kombinációban felfedjük, bizonyos feltételek mellett pedig ki is javítjuk a hibákat.

Különböző hibajelző és hibajavító kódok például a következők lehetnek:

- a „ Hamming „ – redundancián alapuló hibajelző javító;
- a „ Ciklus „ – állandó arányú ellenőrzés (például 7=3+4);
- a „ Paritásos „ – páros vagy páratlan jelszámúra kiegészítő-ellenőrző (egyedi);
- a „ Fire „ – vertikális és longitudinális bitösszeg blokk (csoport) ellenőrző.

A fent megvizsgált szándékos zavarok elleni védelmet fokozó módszerek csak a zavarok egy bizonyos csoportjára hatásosak. Ugyanakkor napjainkban az elektronikai eszközök zavarvédettségét fokozó technikai módszerek egyetlen ismert eszköze sem biztosítja

az elektronikai zavarás elleni teljes védettséget. A zavarvédettség megoldását a szervezési és technikai módszerek komplex alkalmazásában kell keresni.

Korszerű viszonyok között az elektronikai hadviselésen belül a saját elektronikai rendszereink, eszközeink szándékos zavarok elleni védelmének új területei látnak napvilágot, ezek a területek még igen sok megoldatlan szervezési és technikai problémát vetnek fel.

5.3.2 A nem szándékos zavarok elleni védelem módszerei

Az elektromágneses kompatibilitás (nem szándékos zavarok elleni védelem) olyan szaktudomány általános elnevezése, amely az elektronikai (elektromos) készülékek működése során fellépő, más eszközökre ható elektromágneses tér által okozott nem szándékos elektromágneses zavarjelek (továbbiakban elektromágneses zavarok) elnyomásával, valamint hatásainak csökkentésével foglalkozik.

Elöljáróban célszerűnek látszik – az egyértelműség érdekében – néhány, az elektromágneses kompatibilitással kapcsolatos fogalmat definiálni.

Elektromágneses kompatibilitásnak (Electromagnetic Compatibility – EMC) nevezzük egy készülék, berendezés vagy rendszer azon képességét, hogy elektromágneses környezetben kielégítően tud működni, és ugyanakkor nem hoz létre elfogadhatatlan mértékű elektromágneses zavar jelet.[226]

Az előzőekben ismertetett elektromágneses kompatibilitás meghatározásából is látható, hogy az elektromágneses kompatibilitás átfogja az elektromos, illetve elektronikus és villamos berendezések alkalmazásának minden területét. Így könnyen belátható, hogy valamely eszköz elektromosan kompatibilisnek tekinthető egy adott környezetben, ha a környezete által keltett elektromágneses tér jelenlétében megfelelően tud működni, illetve működése közben az általa keltett elektromágneses tér a környezetét nem zavarja.

Egy bármely célú, részben vagy egészben elektromos vagy elektronikus berendezés tehát akkor számít kompatibilisnek, ha zavarforrásként az előírt érték alatt bocsát ki zavaró jeleket (nem hasznos jeleket), ugyanakkor, mint zavart elszenvedő vevőnek megfelelő nagyságú zavarállósága van a zavaró jelekkel szemben, vagyis megfelelő a zavarálló képessége.

Elektromágneses zavarnak (Electromagnetic Interference – EMI) nevezünk minden olyan elektromágneses jelenséget, amely valamely készülék, berendezés vagy rendszer hasznos jelfeldolgozását, üzemelését (működését) rontja. Az elektromágneses zavar lehet elektromágneses zaj, nemkívánatos jel vagy maga a médium változása.[227]

Az elektromágneses zavarok a különféle elektronikai eszközök, rendszerek működését befolyásolják. Az inkább csak a bosszantó „rádiórecsegésen" túl komoly veszélyeztetést jelenthetnek például az információ- és adatátviteli rendszerekben, irányító rendszerek-

[226] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 113.

[227] U.o.

ben, ezért megszüntetésük vagy legalábbis megfelelő mértékű csökkentésük nélkülözhetetlen a társadalmi, gazdasági életben is.

Zavarvédettségnek (elektromágneses érzékenységnek) (Electro-magnetic Susceptibility – EMS) nevezzük valamely elektronikus berendezés tűrőképességét a nemkívánatos elektromágneses energia hatásával szemben. Egy adott áramkör, egység vagy rendszer érzékenységi szintjét az a zavarkörnyezet határozza meg, amelyben az még megbízhatóan működni képes.[228]

Az elektronikai eszközök közötti elektromágneses kompatibilitást:

- a tervezés;
- a gyártás;
- az üzemeltetés előtti rendszertervezés;
- az üzemeltetés időszakaiban kell biztosítani.[229]

5.3.2.1 A katonai elektronikai eszközök közötti sugárzott elektromágneses zavarok keletkezésének főbb okai

A katonai eszközök és rendszerek közötti elektromágneses kompatibilitás biztosítása háborúban jóval nehezebb feladat, mint a polgári rendszereké, mert adott esetben a harcászati (hadműveleti) helyzetek gyors változása miatt, például az elektronikai eszközök egymás közötti távolsága véletlenszerűen változó. Ezért az elektronikai eszközökkel szemben támasztott elektromágneses kompatibilitás-követelmények is szigorúbbak, amelyeket külön katonai szabványokban fogalmaznak meg.

A katonai szakirodalom szerint a sugárzó elektronikai eszközök közötti elektromágneses zavarok keletkezésének főbb okai a következők:

- az elektronikai eszközök koncentrált alkalmazása;
- a frekvenciatartományok telítettsége, felhasználásának egyenlőtlensége;
- az adóberendezések teljesítményszintjének, valamint a vevők érzékenységének növekedése;
- az antennák sugárzási sajátosságai;
- az adóberendezések sávon kívüli sugárzásai és a vevőberendezések mellékvételi csatornái;
- egyéb okok.[230]

Az elektronikai eszközök koncentrált alkalmazása

Napjainkban minden fegyvernemnél, szakcsapatnál nagy számban vannak rendszeresítve különböző típusú elektronikai eszközök. Az elektronikai eszközök legnagyobb

[228] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 113.

[229] Vass, S.: *A Magyar Honvédségben az elektronikai harc – ezen belül az elektronikai védelem – számítógépekkel biztosított tervezése, különös tekintettel az elektromágneses kompatibilitás kérdéseire.* Kandidátusi értekezés. Budapest, Zrínyi Miklós Katonai Akadémia, 1995. p. 20.

[230] U.o. p. 36.

mennyiségben valószínűleg az első lépcsőben elhelyezkedő magasabb-egységeknél, egységeknél, alegységeknél lesznek aktivizálva.

A frekvenciatartomány telítettsége, felhasználásának egyenlőtlensége
Tény, hogy a rendelkezésre álló frekvenciatartomány, amelyben az elektronikai eszközök üzemelnek, korlátozott. Jellemző, hogy ezt a spektrumot nem egyenletesen használják fel. A katonai eszközök eddig leginkább a méteres és deciméteres hullámsávban működtek, napjainkban viszont erősödik a centiméteres és a milliméteres hullámtartomány igénybevétele.

Az adóberendezések teljesítményszintjének, valamint a vevők érzékenységének növekedése
Az adóberendezések teljesítményének és a vevőberendezések érzékenységének növelése azért szükséges, hogy a hatótávolság, valamint az információátvitel megbízhatósága nagyobb legyen. Ugyanakkor a nagy érzékenységű vevőkészülékek bemenetére jutó, viszonylag alacsony szintű zavarójelek is komoly problémát okozhatnak, mivel torzítják az eredetileg venni szándékozott hasznos jelet.

A zavarvédelem egyik módjaként gyakran alkalmazták azt, hogy növelték az adó hasznos teljesítményét, és így biztosították a megfelelő nagyságú hasznos jelet a zavaró jelhez képest a vevőberendezéseknél. Az ilyen fajta zavarvédelem nemcsak értékelhető áruló jelekhez juttatta a szemben álló felet, hanem számtalan egyéb elektromágneses kompatibilitási problémához is vezetett (például a sávon kívüli sugárzások szintjének növekedése). Ezért az ilyen módszer ma már nem alkalmazható zavarvédelmi eljárásként.

Az antennák sugárzási sajátosságai
Az elektronikai eszközök antennarendszerei iránykarakterisztikájának nem tökéletes volta, a nagyszintű oldal- és hátsó szirmok rontják a térbeli szelektálás lehetőségeit, és elősegítik az elektromágneses zavarok létrejöttét. Ugyanakkor bizonyos elektronikai eszközöknek (például a harcászati rendeltetésű mobil rádió adó-vevők) minden irányba sugározniuk kell elektromágneses jelet.

Az adóberendezések sávon kívüli sugárzásai és a vevőberendezések mellékvételi csatornái
Az elektronikai eszközök között kialakuló elektromágneses zavarok nemcsak az egybeeső frekvenciákon történő üzemeltetéskor léphetnek fel (fő kisugárzás esetén és alapvételi csatornán) – amelyeknek elkerülésével alapvetően a frekvenciagazdálkodás foglalkozik –, hanem elektromágneses zavarok léphetnek fel a zavarforrás sávon kívüli sugárzásának a zavart elszenvedő vevő alapvételi csatornáján, illetve a zavarforrás fősugárzásának a zavart elszenvedő vevő mellékvételi csatornájára gyakorolt hatása következtében is.

A sávon kívüli sugárzás teljesítménye, egyes típusú adóberendezésekben csak 30-40 dB értékkel kevesebb, mint a fősugárzás teljesítménye. A zavarforrások adóberendezéseinek sávon kívüli sugárzása nem szükséges a hasznos információközlésben.

Az elektronikai eszközök vevőberendezéseinek mellékvételi csatornáit nem használják a hasznos információ kiválasztására. Ezek a csatornák egyenesen károsak, mivel jelentősen rontják a vevőberendezés szelektivitását. A vevőberendezéseknél a mellékvételi

csatornák száma 30-50 is lehet, viszont ezek érzékenysége csak néhány dB-el kisebb, mint az alapvételi csatorna érzékenysége.

A frekvencia-egybeesések alapján az elektromágneses kompatibilitás biztosítása szempontjából a következő esetekben kell számolnunk zavarás kialakulásával:

– a zavarforrás adóberendezésének fő kisugárzása egybeesik a zavart elszenvedő vevőberendezés alapvételi csatornájának áteresztési sávjával;
– a zavarforrás adóberendezésének sávon kívüli sugárzásai egybeesnek a zavart elszenvedő vevőberendezés alapvételi csatornájának áteresztési sávjával;
– a zavarforrás adóberendezésének fősugárzása egybeesik a zavart elszenvedő vevőberendezés mellékvételi csatornájával.

Az elektromágneses zavarok keletkezésének egyéb okai

A zavarok további oka lehet az elektronikai eszközök frekvencia-instabilitása, valamint az egyes típusú elektronikai eszközök alacsony zavarvédettsége.

Ezenkívül a berendezések kisugározhatnak, a vevőberendezések pedig vehetnek jeleket az antennán kívül is a berendezések elégtelen árnyékolása-, valamint a táp- és kapcsoló áramkörökben fellépő elektromágneses zavarok következtében.

Egy adott területen települt elektronikai eszközök között zavarás alakulhat ki például:

– pontatlan behangolások;
– indokolatlan kisugárzások;
– helytelen antenna-kiválasztás és telepítés;
– egymástól eltérő üzemmód állítása;
– a végberendezések szakszerűtlen csatlakoztatása;
– szükségtelen emelt teljesítmény alkalmazása miatt is.[231]

5.3.2.2 Az elektromágneses kompatibilitás tervezésének és biztosításának módszerei

Az elektromágneses kompatibilitás biztosítása az elektronikai védelem egyik fő feladata, azoknak a szervezési és technikai rendszabályoknak az összessége, amelyeket az elektromágneses zavarások megelőzésére, illetve megszüntetése céljából foganatosítanak.

Valamennyi vezetési szinten az elektromágneses kompatibilitás biztosítása érdekében a törzsek általános feladatai között szerepel az elektronikai eszközök üzemeltetésének frekvencia szerinti, területi- és időbeni szétválasztása.

Az elektromágneses kompatibilitás biztosításának technikai rendszabályai

A technikai rendszabályokat alapvetően az elektronikai eszközök tervezésekor és kivitelezésénél alkalmazzák. Ezek a következők:

[231] Vass, S.: *A Magyar Honvédségben az elektronikai harc – ezen belül az elektronikai védelem – számítógépekkel biztosított tervezése, különös tekintettel az elektromágneses kompatibilitás kérdéseire.* Kandidátusi értekezés. Budapest, Zrínyi Miklós Katonai Akadémia, 1995. p. 39.

– a megválasztott frekvenciasávban olyan műszaki jellemzőkkel rendelkező eszközök fejlesztése, amelyek kielégítik az (ugyanezen frekvenciasávra kialakított) elektromágneses kompatibilitással kapcsolatos szabványelőírásokat;
– a szabványokban előírt követelményeken is túl olyan speciális zavarvédelmi eljárásokat, szelekciós és jelfeldolgozási módszereket, antennakarakterisztikákat és kombinált megoldásokat kell realizálni, amelyek biztosítják a fejlesztendő elektronikai eszközök zavarvédettségét különböző elektronikai helyzetben is.

Az elektromágneses kompatibilitás biztosításának szervezési rendszabályai
Az elektronikai eszközök telepítése és üzemeltetése során biztosítani kell az elektromágneses kompatibilitás főbb szervezési rendszabályainak realizálását, amelyek alapvetően a hagyományos, fixfrekvenciás eszközök esetén a következők:
– üzemi és tartalék frekvenciák területi elosztása, igények szerinti kijelölése;
– az elektronikai eszközök térbeli széttelepítése az alkalmazási körzetben;
– az elektronikai eszközök üzemi szektorainak kisugárzási és vételi viszonyok alapján történő elosztása;
– azonos körzetben telepített eszközök üzemeltetésének koordinálása a fegyvernemek, szakcsapatok, a polgári szervek feladatainak fontossága szerint, ha szükséges, akkor az elektronikai eszközök működési idejének szakaszolásával a potenciálisan össze nem férő (nem kompatibilis) eszközök működési idejének és körzetének elkülönítésével;
– az elektromágneses zavarok okainak időben történő feltárása, megszüntetése;
– az elektronikai eszközök üzemelési rendjének rendszeres ellenőrzése, a szükséges nyilvántartások, okmányok vezetése.

5.3.3 Elektronikai pusztítás elleni védelem

Az elektronikai pusztítás elleni védelmen belül
– a nagy energiájú lézerfegyverek;
– a kis energiájú lézerbesugárzók;
– infrahang fegyverek;
– elektromágneses impulzusbombák;
– nagy energiájú rádió frekvenciás sugárzások
elleni védelemmel foglalkozunk.

A nagy energiájú lézerfegyverek elleni védelem alapvető módszere, ha a fegyverrendszer felderítése után a lehetséges pusztító eszközökkel azonnal megsemmisítjük.

A kis energiájú lézerbesugárzók elleni védelem megoldása, lehet olyan speciális szemüveg alkalmazása, amely a besugárzás érzékelése után azonnal lezár, így védve meg a katonák szemét a lézersugár káros roncsolása ellen.

Infrahang fegyverek elleni védelem alapvető módszere lehet, ha az infrahang fegyver felderítése után a lehetséges pusztító eszközökkel azonnal megsemmisítjük.

Az *elektromágneses impulzusok* elleni védelem alapvető problémája, hogy nem ismert az elektromágneses impulzus nagysága a védett eszköznél. Így nehéz megállapítani, hogy milyen nagyságú elektromágneses impulzust kell lecsökkenteni olyan mértékre, amelyet még károsodás nélkül elviselnek az érzékeny elektronikai eszközök. A szükséges érték ismeretében lehetőség lenne meghatározni azt az optimálisan szükséges védelmi módszert és eszközt, így nem kellene minden esetben a maximális védelmi értéket biztosító eljárást vagy eszközt alkalmazni.

Az *elektromágneses impulzusbombák és nagy energiájú rádiófrekvenciás sugárforrások* elleni védelem eszközei a következők lehetnek:

- árnyékoló és elnyelő anyagok;
- szikraközös villámhárító eszközök;
- hálózati szűrők;
- fémoxid varistorok;
- elektro-optikai eszközök és fényvezetők;
- nagy sebességű zener diódák.

Az elektromágneses impulzusbombák és nagy energiájú rádiófrekvenciás sugárforrások elleni védelem lehetőségei a következők lehetnek:

- elektro-optikai eszközök alkalmazása (például fénykábelek);
- elektromágneses hullámok elleni árnyékolás.

Elektro-optikai eszközök (például fénykábelek) széles körűen alkalmazhatók a katonai:

- adat- és kommunikációs csatornáknál;
- energiafigyelő és -irányító rendszereknél;
- ellenőrző irányító rendszereknél;
- őrzésvédelmi rendszereknél;
- egyéb biztonsági rendszereknél.

Az árnyékoló és elnyelő anyagokkal az elektronikai eszközök teljes lefedésével ideális védelem biztosítható az elektromágneses impulzusok ellen, bár ilyen védelem megvalósítása az esetek többségében nem lehetséges, mivel más elektronikai berendezésekkel is biztosítani kell a kapcsolatot.

Elektromágneses hullámok elleni árnyékolás módszerei lehetnek:

- abszorbeáló;
- reflektáló.

Az abszorbeáló árnyékolási módszernél rádiófrekvenciás energiát elnyelő anyagokat alkalmaznak, ahol az energia elnyelés nagyságától és a frekvenciasávtól függően a vastagság a 60 cm-t is elérheti. Az árnyékolt területen átlátszó, üvegezett felületek nem megengedhetők. Ezt az árnyékolási módszert általában laboratóriumoknál alkalmazzák.

A reflektáló árnyékolási módszernél a védendő teret rádiófrekvenciásan reflektáló anyagokkal vonják be, oly módon, hogy a bevonat folyamatos legyen. Az árnyékolás

elválasztja a külső teret a védendő belső tértől, a jel a reflektáló rétegen csak erősen csillapítva (50-120 dB) juthat át.

Nagy előnye ennek az eljárásnak, hogy lényegesen olcsóbb, mint az abszorbeáló módszer, sokkal kevesebb a helyigénye, és fényáteresztő üveg felületek is megengedhetők. A reflektáló módszer előnyös tulajdonságai miatt szinte kivétel nélkül ezt a megoldást alkalmazzák a rádiófrekvenciás árnyékolásban.

A leghatékonyabb ilyen védekezés az úgynevezett „Faraday kalitka". Ez egy fémből, vagy fémhálóból készült doboz, amelybe belehelyezve az adott elektronikai eszközt, az védve van a külső elektromágneses tér elől.[232]

A számítógéptermek, műszerszobák védelme esetén a teljes védendő tér körül Faraday- kalitkát kell kialakítani. Ez azt jelenti, hogy a teret határoló teljes falfelületet vezetőanyaggal kell borítani, a vezetőképesség nem szakadhat meg a felületek találkozásánál, sőt a nyílászáróknál sem. A védett térbe belépő vezeték (például erősáram, telefon, beléptető rendszer, biztonságtechnikai és tűzvédelem, számítógépes hálózat) megfelelő szűréssel kell ellátni. Külön gondot kell fordítani a védett térbe vezető klíma- és szellőzőrendszer kialakítására, a megfelelő potenciálra hozására, ellenkező esetben ezek, mint szekunder antennák és csatolók továbbítják a sugárzott jelet. Az ekvipotenciális felületek minél ritkábban szakítandók meg ablakokkal és ajtókkal, mivel ezek árnyékolása lényegesen költségesebb, és potenciális hibaforrást is jelenthetnek.

Az elektromágneses hullámok a védett térbe bejuthatnak vezetéken haladva (induktív-, vagy kapacitív csatolással) vagy elektromágneses sugárzással, ezért az árnyékolásnak, mind a vezetett, mind a sugárzott zavarás ellen megfelelő védelmet kell biztosítania.

Az elektromágneses árnyékolás a megvalósítást tekintve lehet pontszerű vagy területi. Pontszerű árnyékolás esetén az árnyékolást egy szűk területre, például egy alkatrészre korlátozódik, területi árnyékolás pedig egy bizonyos területen elhelyezett összes elektronikai berendezés árnyékolását biztosítja.

Az elektromágneses árnyékolás kialakításának lehetséges módszerei a következők lehetnek:

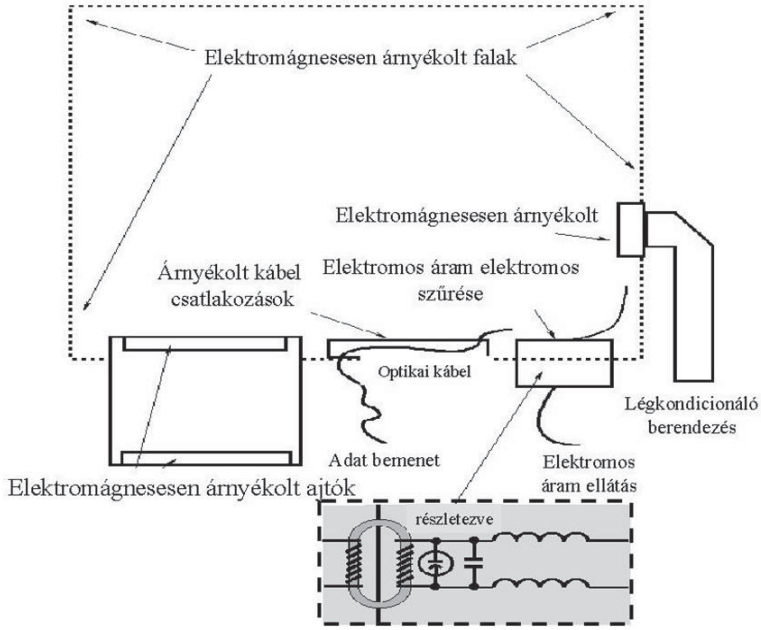
- rendszer árnyékolás;
- alrendszer árnyékolás;
- eszköz, alkatrész árnyékolás.[233]

Az elektromágneses árnyékolás megvalósításánál az oldalfalakon kívül nagy figyelmet kell fordítani a nyílászárók árnyékolására is, illetve biztosítani kell a védett térbe csatlakozó vezetékek (például áramellátás, számítógépes hálózat) elektromágneses szűrését.

[232] Self-standing modular Faraday cage (Letöltve: 2014.01.23.) http://www.shieldingsystems.eu/index.php?p=Nieuws&id=159&Lang=2&gclid=COGyscOF-7oCFUiN3godAA8AHg

[233] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 134.

Az árnyékolások kivitelezésére és azok tesztelésére számos szabvány létezik, amelyek betartásával megfelelő védelem biztosítható az elektromágneses impulzusbombák és nagy energiájú rádiófrekvenciás sugárforrások ellen. Az 5.5. ábrán egy számítógépes szoba elektromágneses árnyékolása látható.



5.5. ábra. **Számítógépes szoba elektromágneses árnyékolása**[234]

A szikraközök alaptípusának felépítése és működése egyszerű. Két elektróda között szigetelőrétegként vákuum, levegő, vagy valamilyen gáz helyezkedik el. Alaphelyzetben az elektródák között a szigetelőréteg miatt nem folyhat áram, ezért ez az állapot a kapcsoló nyitott helyzetének felel meg. Ha az elektródák közötti feszültséget emeljük, akkor elérjük azt a feszültséget, amelyen bekövetkezik az átütés, és elektromos ív alakul ki. Az ív nagyon kis ellenállású elektromos összekötésnek tekinthető, ezért ez az állapot a kapcsoló zárt helyzetének felel meg. Az átütési feszültséget az elektródák távolsága határozza meg: úgy állítják be, hogy az átütés hamarabb következzen be a szikraközben, mint a védett fogyasztóban.[235]

[234] U.o.

[235] EMC villámvédelem és túlfeszültség-védelem V. rész (Letöltve: 2014.01.23.) http://epa.oszk.hu/00000/00025/00001/feher.html

A hálózati szűrők alkalmazásával kiszűrhetők az elektromos és számítógépes adathálózaton terjedő zajok, zavarok és túlfeszültségek, amelyek a tápegységek, adatátviteli eszközök korai meghibásodásához vezethetnek.[236]

Az adatátviteli vonalakon a túlfeszültség tovaterjedése elleni védelemre sikeresen alkalmazható dióda, varistor, gázlevezető, melyeket érdemes kombinálni. A dióda az egyenfeszültséget nem engedi át a berendezés felé, míg a gázlevezető túlfeszültség esetén hirtelen leföldeli a rendszert.

Elektro-optikai eszközök alkalmazásával megoldható az adatátviteli kábelek védelme. Ezen eszközök széles körűen alkalmazhatók az adat- és kommunikációs csatornáknál, az energiafigyelő és -irányító rendszereknél, az ellenőrző irányító rendszereknél, az őrzésvédelmi rendszereknél és egyéb biztonsági rendszereknél.

A nagy sebességű zener diódák működése azon alapszik, hogy belső ellenállását igen gyorsan megváltoztatja (rövidre zár) ha a rákötött feszültség hirtelen megnövekszik, illetve átlépi a meghatározott küszöbszintet. A korszerű zener diódáknál a folyamat sebessége a 10^{-9} másodperc, az elméleti határ pedig 10^{-12} másodperc is elérheti. Eltérően a varistoroktól a zener dióda jellemzői többszöri túlterhelés hatására sem változnak.

5.4 Elektronikai ellenőrzés

Az elektronikai védelem komplex technikai és szervezési rendszabályok összessége, amelyek betartásának hatékonyságát speciális eszközökkel felszerelt elektronikai ellenőrző csapatok végzik.

Az elektronikai ellenőrzés olyan tervszerűen végrehajtott tevékenység, amely az elektronikai védelmet biztosító rendszabályok helyzetének ellenőrzésével adatokat szolgáltat azok értékeléséhez és tökéletesítéséhez.

Csak korszerű és hatékony elektronikai ellenőrzéssel biztosítható az elektronikai védelem hatékony megvalósítása, így növelve saját csapataink túlélőképességét, amely döntő fontosságú lehet a hadműveletek és harcok megvívása során. Az elektronikai ellenőrzést olyan elektronikai ellenőrző rendszernek kell végeznie, amely technikai eszközeit és felkészültségét tekintve az ellenség felderítő, zavaró és vezérelt fegyverei képességével összemérhető állandó helyű és mobil ellenőrző egységekből és alegységekből áll.

Az elektronikai ellenőrző rendszernek a szemben álló fél szerepében kell végrehajtania feladatait olyan áruló jeleket keresve, amelyek csapatvezetési és fegyverirányító rendszerünk felépítéséről, technikai és harcászati lehetőségeiről értékes információkat juttathatnak a szemben álló fél tudomására. Ezek az információk elősegíthetik a szemben álló felet, hogy hatékonyan alkalmazza technikai felderítő eszközeit, zavaró eszközeit vagy irányított fegyvereit.

[236] Hálózati szűrők. (Letöltve: 2014.01.23.) http://cmswebdav.weidmueller.de/cms/gu_hu/letoltesek/katalogusok/Tulfeszultseg/E_Halozati%20szurok.pdf

Az elektronikai ellenőrzés tehát figyelmeztet, méréseivel útmutatást, segítséget nyújt az elektronikai védelmi intézkedések, rendszabályok tökéletesítéséhez. Az elektronikai ellenőrzés hatékonyan szolgálja a saját csapatok elektronikai eszközei között kialakuló kölcsönös zavarok elleni védelmet is. Mérései alapján ajánlásokat lehet kidolgozni az eszközök elhelyezésére, technikai és szervezési rendszabályainak megtervezésére, modellezésére.

5.4.1 Az elektronikai ellenőrzés területei

Ahhoz, hogy az elektronikai ellenőrzés hatékony legyen, széles területet kell átfognia, amelyet három alapvető csoportra lehet bontani:

- védett katonai objektumok például:
  - = a speciális rendeltetésű katonai szervezetek, objektumok;
  - = a hadműveleti- harcászati csoportosítások;
  - = a haditechnikai kísérleti bázisok;
  - = a speciális rendezvényekre kijelölt helyiségek, objektumok;
  - = az elektronikai objektumok;
  - = a színlelt objektumok és létesítmények;
  - = az adatfeldolgozó, -titkosító, – távíró és távbeszélő központok;
- haditechnikai eszközök például:
  - = a fegyverirányítás elektronikai eszközei, rendszerei;
  - = a rádiónavigáció rádió- és rádiótechnikai eszközei;
  - = a vezetés, adatfeldolgozás, adatátvitel, rejtjelezés, titkosítás elektronikai eszközei;
  - = a felderítés elektronikai eszközei;
  - = az elektronikai hadviselés elektronikai eszközei;
  - = az elektronikai álcázó és rejtő eszközök;
- jelentősebb katonai tevékenységek:
- csapatok, intézetek diszlokációja;
- csapatmozgások, gyakorlatok;
- harckészültségi és mozgósítási feladatok végrehajtása;
- hadműveleti- harcászati tevékenységek álcázása;
- módszertani és technikai bemutatók;
- haditechnikai kísérletek.[237]

Az elektronikai ellenőrzéseket természetesen rendszeresen kell végrehajtani már a haditechnikai eszközök gyártása, csapatpróbája, rendszerbe állítása és alkalmazása során

[237] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 136.

is, mert csak így biztosítható, hogy az elektronikai védelem rendszabályait folyamatosan és nem csak „váratlan" ellenőrzések alkalmával tartják be csapataink.

Az elektronikai ellenőrzés széles területéből is látható, hogy az elektronikai ellenőrzés kiterjed a honvédség valamennyi tevékenységére, eszközére és objektumára.

5.4.2 Az elektronikai ellenőrzés fő feladatai

Ahhoz, hogy az elektronikai ellenőrzés komplex, tehát mindenre kiterjedő legyen, célirányos feladatmegoldások sorozatát kell alkalmazni. Az elektronikai ellenőrzés fő feladatait négy csoportra oszthatjuk fel, amelyek között szoros kapcsolat van. Ezek az ellenőrzési tevékenységek folyamán nem minden esetben választhatók szét ilyen élesen.

Az elektronikai ellenőrzés fő feladatai a következők:

- a technikai felderítés elleni tevékenység ellenőrzése;
- az elektromágneses kompatibilitás ellenőrzése;
- a saját elektronikai eszközök zavarvédettségének ellenőrzése;
- a vezetési és fegyverirányítási elektronikai eszközök elektronikai ellentevékenység elleni és önirányítású fegyverek elleni védelmének ellenőrzése.[238]

A technikai felderítés elleni tevékenység ellenőrzésének feladatai magukba foglalják például:

- az optikai (megfigyelő, fényképező, televíziós) felderítés elleni védettség ellenőrzését;
- az infravörös megfigyelő- és termovíziós felderítés elleni védettség ellenőrzését;
- a rádiólokációs felderítés elleni védettség ellenőrzését;
- a rádió és rádiótechnikai felderítés elleni védettség ellenőrzését;
- az akusztikai és hidroakusztikai, szeizmikus és egyéb fizikai rezgések által történő felderítés elleni védettség ellenőrzését;
- mágnesesség mérésén alapuló felderítés elleni védettség ellenőrzését;
- titkos információk védettségének ellenőrzését.[239]

Az elektromágneses kompatibilitás ellenőrzésének feladatai

Az elektromágneses kompatibilitást és ezen belül annak ellenőrzésének feladatait alapvetően két részterületre lehet felosztani úgy, mint új elektronikai eszközök tervezésének, kivitelezésének, valamint üzembe helyezésének (rendszerbe állításának) elektronikai ellenőrzési feladatai és a meglévő elektronikai eszközök, objektumok elektromágneses kompatibilitásának ellenőrzési feladatai.

[238] Balajti, I. – Vass, S.: *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 137.

[239] U.o. 136.

A létesítendő új elektronikai eszközök, objektumok elektromágneses kompatibilitásának ellenőrzési feladatai az alábbiak:

- az elektromágneses kompatibilitást növelő, új műszaki megoldások vizsgálata;
- a beépített alkatrészek üzembiztonsági ellenőrzése, majd az elkészült berendezések ellenőrzése;
- a létesítendő új elektronikai eszköz, objektum zavarvédettségének vizsgálata;
- az ellenőrzés eredményeinek elemzése és javaslat kialakítása az előírt műszaki normákkal;
- új berendezések elhelyezési lehetőségének felmérése az adott elektromágneses környezetben;
- a már üzembe helyezett új berendezések térbeli, időbeli és frekvenciatartománybeli elosztásával kapcsolatos előírások betartásának ellenőrzése.

A meglévő elektronikai eszközök, objektumok elektromágneses kompatibilitása ellenőrzésének főbb feladatai közé tartozik:

- az elektromágneses zavarforrások felkutatása, intézkedés a zavar megszüntetésére;
- az elektronikai eszközök antennáira, illetve műantennáira történő elektromágneses sugárzás jellemzőinek mérése és összehasonlítása az előírt műszaki normákkal;
- adatok gyűjtése, és azokra alapozva az alkalmazási tervek elkészítése, majd a visszaellenőrzés végrehajtása.

A saját elektronikai eszközök zavarvédettségének ellenőrzési feladatai:

- felmérni, hogy az elektronikai eszközök milyen szándékos zavarteljesítmény mellett képesek még funkcionális feladataikat ellátni;
- megállapítani, hogy milyen típusú zavarokat képes a kezelőszemélyzet hatékonyan kivédeni a különböző zavarvédő berendezések alkalmazásával;
- meghatározni, hogy adott képességű (például teljesítmény, jelstruktúra) zavaró berendezés milyen távolságról képes lefogni az elektronikai eszközt.

A vezetési és fegyverirányítási elektronikai eszközök elektronikai ellentevékenység elleni védelmének ellenőrzésével kapcsolatos főbb feladatok:

- a zavarvédettséget növelő műszaki megoldások és technikai eljárások alkalmazásának vizsgálata;
- az elektronikai ellentevékenység elleni védelmet növelő szervezési és technikai rendszabályok betartásának ellenőrzése;
- a kezelők tevékenységének értékelése a zavarás viszonyai között végzett üzemeltetésre vonatkozóan.

6. FEJEZET

Az elektronikai hadviselés vezetése

6.1 Integrált felderítés és elektronikai hadviselés a műveleti vezetési rendszerben

Az elektronikai hadviselés hatékony végrehajtásának egyik alapvető feltétele, a vezetés minősége, vagyis a minden területre kiterjedő részletes és hatékony tervezés, szervezés és irányítás. Az elektronikai hadviselés vezetési folyamata az általános hadműveleti és harcászati vezetési folyamathoz illeszkedik, annak részét képezi.

Az MH Törzsszolgálati Szakutasításának megfogalmazása szerint, az: *„irányítás a parancsnokra ruházott jogkör a meghatározott küldetés teljesítése érdekében, amely tartalmazza az alárendeltek bevetésére (alkalmazására), valamint irányításuk megtartására vagy átadására vonatkozó jogosultságot.*

A vezetés hatáskör és felelősség, amelyet az egyszemélyi parancsnokra ruháznak a célkitűzések meghatározása, a szervezetek struktúrájának és állományának kialakítása, hatékony működtetése, a tevékenységek szabályozása és vezetése céljából. Lényege a parancsnoki akarat és szándék megvalósítása. Magába foglalja az alárendelt erők alkalmazásának jogkörét és a felelősséget a feladat sikeres teljesítése érdekében."[240]

Az MH műveleti vezetési rendszere (MVR) egy egységes rendszerben felépített vezetési struktúra, mely egy egységes rendszert alkotva a katonai vezetés minden szintjén (katonai stratégiai, hadműveleti, harcászati) biztosítja a szövetségben alkalmazott eljárások alkalmazásával, a döntés előkészítéssel (műveletervezéssel), a műveletvezetéssel és az együttműködéssel, koordinációval kapcsolatos feladatok zökkenőmentes végrehajtását béke időszakban és különleges jogrend kihirdetése esetén végrehajtott műveletek során egyaránt.

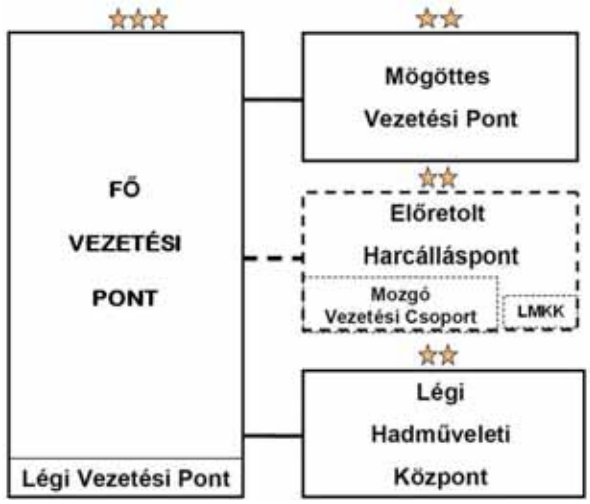
Az összhaderőnemi hadműveleti szintű vezetés feladata: a politikai iránymutatás és a katonai stratégiai célkitűzések elérése érdekében a hadműveleti célok meghatározása, a cselekvési változatok és parancsnoki döntést követően a műveleti terv kidolgozása, majd a műveleti siker érdekében szükséges tevékenység vezetése és szinkronizálása.

A hadműveleti szintű vezetés alapelemei az alábbiak:

– Fő Vezetési Pont (FVP);
  - Légi Vezetési Pont;

[240] Ált-4/457 A Magyar Honvédség Törzsszolgálati Szakutasítása. HVK Hadműveleti Csoportfőnökség kiadvány, p. 1-3.

– Előretolt Harcálláspont (EH);
  ❁ Mozgó Vezetési Csoport (MOVCS);
  ❁ Légi Műveletek Koordinációs Központ (LMKK);
– Mögöttes Vezetési Pont (MVP);
– Légi Hadműveleti Központ (LHK). (6.1. ábra)



6.1. ábra. **Az MH összhaderőnemi hadműveleti szintű vezetési elemei**[241]

Az összhaderőnemi hadműveleti vezetést a Fő Vezetési Pont végzi, annak kiesése, valamint a mögöttes műveletek tekintetében pedig az a Mögöttes Vezetési Pont feladata.

A szárazföldi haderőnem tekintetében a haderőnemi vezetés alapvető szervezete az Előretolt Harcálláspont, amely a Fő Vezetési Ponton belül, vagy abból kikülönítve működhet. A légierő haderőnem tekintetében a haderőnemi vezetést a Légi Hadműveleti Központ valósítja meg. A logisztikai erőket a Fő Vezetési Ponttal közösen, vagy attól elkülönülten települő Mögöttes Vezetési Pontról vezetik. (6.1. táblázat)

A harcászati szintű haderőnemi vezetést az MH Összhaderőnemi Parancsnokság (ÖHP) közvetlenül valósítja meg. A szárazföldi haderőnem harcászati szintű vezetési alapelemei a dandár (ezred), zászlóalj és század szintű vezetési pontok rendszere. A harcászati szintű vezetési elemek dandár (ezred) és zászlóalj esetében felépítésben és az egyes elemek rendeltetésében megegyeznek. A harcászati szintű vezetési pontok rendszerét (jellegét, funkcióját és települését) a 6.2. táblázat szemlélteti.

[241] Ált-4/457 A Magyar Honvédség Törzsszolgálati Szakutasítása. HVK Hadműveleti Csoportfőnökség kiadvány, p. 2-4.

6.1. táblázat. A hadműveleti szintű vezetési pontok rendszere[242]

Megnevezés	Jellege	Település	Funkció
Fő Vezetési Pont (FVP) EH Légi Vezetési Pont	Összhaderőnemi-, haderőnemi tervező	▪ Béke elhelyezési körletben ▪ Védett létesítményben ▪ Katonai/civil objektumban ▪ Tábori elhelyezésben	**Elsődleges vezetési pont** Műveletek tervezése, vezetése, irányítása
Légi Hadműveleti Központ (LHK/AOC)	Haderőnemi tervező, vezető-irányító	▪Védett létesítményben	Légierő műveletek tervezése, vezetése, irányítása
Mögöttes Vezetési Pont (MVP)	Összhaderőnemi támogató	▪ Béke elhelyezési körletben ▪ Védett létesítményben ▪ Katonai/civil objektumban ▪ Tábori elhelyezésben	**Másodlagos vezetési pont** ▪ Támogatás tervezése, vezetése ▪ Mögöttes műveletek ▪ FVP tartaléka
Előretolt Harcálláspont (EH)	Összhaderőnemi művelet vezető/ Szárazföld alapú	▪ Katonai/civil objektumban ▪ Tábori elhelyezésben	Operatív vezetési pont
Mozgó Vezetési Csoport (MOVCS)	Összhaderőnemi művelet vezető	▪ Páncélos csoport ▪ Helikopter	Operatív vezetési pont

6.2. táblázat. A harcászati szintű vezetési pontok rendszere[243]

Megnevezés	Jellege	Település	Funkció
Fő Harcálláspont (FH) Mozgó Vezetési Csoport (MOVCS)	Harcászati tervező, vezető	Katonai/civil objektumban, tábori elhelyezésben	Elsődleges operatív vezetési pont Harc tervezése, vezetése
Tartalék Harcálláspont (TH)	Harcászati támogató	Katonai/civil objektumban, tábori elhelyezésben	Másodlagos operatív vezetési pont Támogatás tervezése, vezetése FH tartaléka
Mozgó Vezetési Csoport (MOVCS)	Harcvezető	Páncélos csoport	Operatív vezetési pont

Az ismertetett hadműveleti és harcászati szintű vezetési rendszerekben a különböző szinteken és azokhoz illeszkedő vezetési pontokon belül különböző csoportokat, főnökségeket, illetve részlegeket hoznak létre.[244]

[242] Ált-4/457 A Magyar Honvédség Törzsszolgálati Szakutasítása. HVK Hadműveleti Csoportfőnökség kiadvány, p. 4-2.
[243] U.o. p. 2-4.
[244] Bővebben lásd a Magyar Honvédség Törzsszolgálati Szakutasítását.

Összhaderőnemi hadműveleti szinten a Fő Vezetési ponton lévő Összhaderőnemi Hadműveleti Csoport és azon belül az Összhaderőnemi Felderítő Főnökség a közvetlen felelős az elektronikai hadviselésért. A főnökségen belül kerül kialakításra az Elektronikai Hadviselés Koordinációs Részleg *(Electronic Warfare Coordination Cell – EWCC),* illetve a Rádióelektronikai Felderítő Részleg *(Signal Intelligence Section)*. Az elektronikai hadviselés és a rádióelektronikai felderítés összehangolása érdekében az összhaderőnemi parancsnok a két részleget összevonhatja, és megalakíthatja a Rádióelektronikai Felderítő és Elektronikai Hadviselés Műveleti Központot *(Signal Intelligence and Electronic Warfare Operations Centre – SEWOC)*. Rajtuk kívül az elektronikai hadviselés koordinációja érdekében a – csoporton belül létrehozott – Összhaderőnemi Hadműveleti Főnökséggel és az Összhaderőnemi Hatásértékelő Főnökséggel van szoros együttműködés.

Harcászati szinten a Fő Harcálláspont törzsében található Felderítő Főnökség/Részleg felel az elektronikai hadviselés vezetéséért, szoros együttműködésben a Hadműveleti Főnökséggel/Részleggel és a Tűztámogató és Koordináló Részleggel.

Az 1. fejezetben már érintettük az integrált felderítő és elektronikai hadviselési elvek alapján az egységes rendszer létrehozásának szükségességét. A felderítő és elektronikai hadviselési rendszeren belül minden vezetési szinten megtalálhatók a parancsnokok, koordinálók, kidolgozók és végrehajtók.

A parancsnok fontos szerepet játszik a felderítő és elektronikai hadviselési rendszer megtervezésében. Meghatározza mindazon követelményeket, melyek hatást gyakorolnak a rendszer működésére. A parancsnoknak ismernie kell az elektronikai hadviselés alapelveit, a szervezetszerű elektronikai hadviselési erők alkalmazási elveit, harcképességüket, valamint tevékenységi rendjüket.

A felderítésnek és elektronikai hadviselésnek az egységes harcászati-, hadműveleti koncepcióba való beillesztésében kulcsszerepe van a felderítő és a hadműveleti törzseknek. A rendszert a *felderítő és hadműveleti főnökök koordinálják*, akik felelősek a felderítés és elektronikai hadviselés összehangolásáért a különböző parancsnokságokon, beleértve a támogatókkal, elöljáró és alárendelt parancsnokságokkal, valamint a szomszédokkal való együttműködést is. Az MH hadműveleti és harcászati vezetési rendszerében az elektronikai hadviselési feladatok szorosan vett, és szervezetszerű koordinálása a felderítő törzshöz kapcsolódik.

Az elektronikai hadviselés sikere attól függ, hogy az milyen mértékben kapcsolódik a harc-, hadművelet tűz és manőver tervéhez. A teljes integráció a szisztematikus tervezéssel és a befolyásoló körülmények mindenoldalú figyelembevételével valósítható meg. A Hadműveleti Főnökség/Részleg felelős azért, hogy az elektronikai ellentevékenység illeszkedjen a tűz és manőver tervhez.

A Felderítő Főnökség/Részleg integráns része az *Elektronikai Hadviselés Koordinációs Részleg*, amely az adott szinten képes a csapatok valamennyi elektronikai hadviselési tevékenységének hatékony koordinálására. A részleg a parancsnok utasítása alapján végzi az elektronikai hadviselési eszközök irányítását. A részleg összetétele és létszáma a küldetéstől függően változhat, azonban mindenkor arányosnak kell lennie az elektronikai hadviselés katonai műveletben betöltött szerepével.

Az Elektronikai Hadviselés Koordinációs Részleg együttműködik:
- a Hadműveleti Főnökséggel/Részleggel, a hadművelet céljainak eléréséhez szükséges elektronikai hadviselési igények koordinálása érdekében;
- a Felderítő Főnökséggel/Részleggel a felderítési igények összehangolása-, a felderítő adatbázis karbantartása-, és a felügyelt frekvenciák *(Guarded frequency)* egyeztetése érdekében;
- az információs műveleteket tervező szerv minden elemével[245] a feladatok összehangolása érdekében;
- a Híradó és Informatikai Főnökséggel/Részleggel a Korlátozott Frekvenciák Jegyzékének *(Restricted Frequency List – RFL)* koordinálása, a kisugárzás korlátozások tervezése és jelentése, valamint a zavarások és interferencia események területén.

Ez az együttműködés biztosítja, hogy az elektronikai hadviselés pontosan illeszkedjen a harctevékenységhez, feleljen meg a parancsnok elvárásainak, a felderítési prioritásoknak, az információkkal kapcsolatos követelményeknek és segítse a parancsnokot elhatározása megvalósításában. Az Elektronikai Hadviselés Koordinációs Részlegnek biztosítania kell, hogy az elektronikai hadviselési tevékenység és az adott szintű törzs Tűztámogató- és Tűzkoordináló Részlegének tevékenysége összehangolt legyen. Az Elektronikai Hadviselés Koordinációs Részleg, vagy a részlegtől kijelölt személy integránsan részt vesz a Tűztámogató- és Tűzkoordináló Részleg munkájában a tűzcsapás és az elektronikai hadviselés szoros összehangolása érdekében.

Az Elektronikai Hadviselés Koordinációs Részleg felelősséggel tartozik az elektronikai hadviselési erők eredményes alkalmazásáért. Ezért az Elektronikai Hadviselés Koordinációs Részleg egyik elsődleges feladata irányítani a támadó jellegű elektronikai hadviselést. A tevékenységet pontosan egyeztetik a tűztámogatással, hogy biztosítsák a tűzcsapások és az elektronikai ellentevékenység összhangját. Az elektronikai ellentevékenység részére meghatározott feladatokat végrehajtásra átadják a végrehajtó erők harctevékenységet irányító központjának. Ennek megfelelően feladatai a következők:
- a katonai műveletek vezetése szempontjából fontos információk összegyűjtése, feldolgozása;
- aktív részvétel az információs műveletek megtervezésében;
- az alábbi adatbázisok karbantartása:
  - elektronikai harcrend;
  - Korlátozott Frekvenciák Jegyzéke;
  - katonai és polgári kisugárzó eszközök adatai;
  - elektronikai hadviselési eszközök képességei és sebezhetőségei;
- az elektronikai helyzetértékelés végrehajtása, azon belül:
  - az elektronikai hadviseléssel összefüggő információk elemzése és adatok értékelése;

[245] Összhaderőnemi vezetési szinten az Összhaderőnemi Hatásértékelő Főnökséggel, aki az információs műveletek koordinálásáért, vezetéséért felelős.

- ❁ az ellenséges elektronikai rendszerek elektronikai ellentevékenységgel sebezhető pontjainak feltárása;
- ❁ a folyamatban lévő és a tervezett tevékenységek támogatása érdekében az elektronikai hadviselés céllistájának kidolgozása, összehangolása a tűztámogatással;
- ❁ ajánlások kidolgozása az elektronikai hadviselés alkalmazási rendszabályaira;
- ❁ az ellenség elektronikai hadviselési képességének értékelése és javaslattétel a szükséges elektronikai védelmi rendszabályokra;

– jelentés az elektronikai helyzetben beállt változásokról a törzs, az alárendeltek és a közvetlen elöljáró parancsnoki szint felé;
– a zavarási hatékonyság ellenőrzésének koordinálása;
– az elektronikai hadviselési módszerek, eljárások pontosítása a szomszédos, a megerősítő-, és szövetséges erők felé.

Az összhaderőnemi hadműveleti szinten a parancsnok döntése szerint megalakítandó *Rádióelektronikai Felderítő és Elektronikai Hadviselési Műveleti Központot* működtetésének az elsődleges célja, hogy a rádióelektronikai felderítő és az elektronikai hadviselési erőforrásokat egyesítve, a tevékenységeket koordinálva, optimalizálja az összhaderőnemi műveletek döntéshozatali folyamatainak támogatását. A Rádióelektronikai Felderítő és Elektronikai Hadviselési Műveleti Központ a felelős az elkülönítetten alkalmazott Rádióelektronikai Felderítő részlegre és az Elektronikai Hadviselési Koordinációs Részlegre háruló valamennyi feladat ellátásáért. A központ a tervezési, vezetési, elemzési, információkezelési és elosztási feladatait a két integrált szakterület szakmai szabályainak maradéktalan betartásával végzi.[246]

6.2 Az elektronikai hadviselés tervezésének folyamata, általános elvei

6.2.1 A tervezés folyamata

A katonai döntéshozatali folyamat magában foglalja az információgyűjtést, a döntés előkészítését és meghozatalát, valamint a parancs kiadását, és eljuttatását az alárendeltekhez. A szükséges információkat a parancsnok az elöljáró dokumentumaiból, az őt körülvevő környezet elemzéséből, valamint az automatizált irányítási rendszerekből nyeri.[247] A döntés előkészítés alapvetően a vezetés folyamatán belüli *tervezés,* amelynek során az előre kitűzött cél(ok) eléréséhez vezető különböző lehetséges tevékenységi vál-

[246] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 23.
[247] Ált-4/457 A Magyar Honvédség Törzsszolgálati Szakutasítása. HVK Hadműveleti Csoportfőnökség kiadvány, p. 5-9.

tozatokat lehet felvázolni, amelyet a vezetési folyamat egy további fázisában (a döntés során) konkretizálni lehet. Vagyis a tervezés alapfeladata különböző megoldási változatok kidolgozása a probléma megoldására.

A vezetési folyamaton belül a tervezés is egy több mozzanatból álló folyamatnak fogható fel, amelynek kiinduló pontja a célkitűzések megfogalmazása. A tervezés első mozzanatában a megfelelő információkra támaszkodva leírható a *kialakult és a várható helyzet*, ami a következő mozzanatban teljes részletességgel, minden lehetséges körülményt figyelembe véve *elemezhető, értékelhető*. Az értékelés során figyelembe kell venni a cél(ok) elérését elősegítő és hátráltató összes tényezőt. Az értékelés eredményeként meghatározhatók azok a lehetséges megoldási változatok, amelyek alapján eredményes döntés születhet.

A tervezés során az adott harctevékenység (hadművelet) céljának elérése érdekében hajtják végre a *kialakult és a várható helyzet értékelését*, a tevékenység sikerét elősegítő és hátráltató körülmények figyelembevételével, majd ennek eredményeként *cselekvési változatokat* dolgoznak ki a parancsnoki döntés támogatására. A szervezés során egyrészt végrehajtják az adott törzs belső munkájának megszervezését, másrészt az alárendeltek részére meghatározzák a konkrét feladatokat, az erők-eszközök célszerű elrendezését, megszervezik az együttműködést. Ez a tevékenység az alárendeltek felé alapvetően harcintézkedések, és harcparancsok formájában realizálódik, amelyek alapján az alárendeltek megkezdik saját tevékenységük előkészítését.

A harcfeladat megtervezését harcérintkezésen kívül a parancsnok az alábbi lépésekben hajtja végre:

- feladat vétele;
- feladat tisztázása;
- elgondolás kialakítása:
  - cselekvési változatok kidolgozása;
  - cselekvési változatok elemzése;
  - cselekvési változatok összehasonlítása;
  - cselekvési változat kiválasztása (döntés);
- harcparancs összeállítása.[248]

Az elektronikai hadviselés tervezése követi a törzsekben általában alkalmazott tervezési eljárást. Ez az elöljáró intézkedésével, a parancsnok utasításával és követelményeinek meghatározásával kezdődik, melynek eredményeképpen elkészül az:

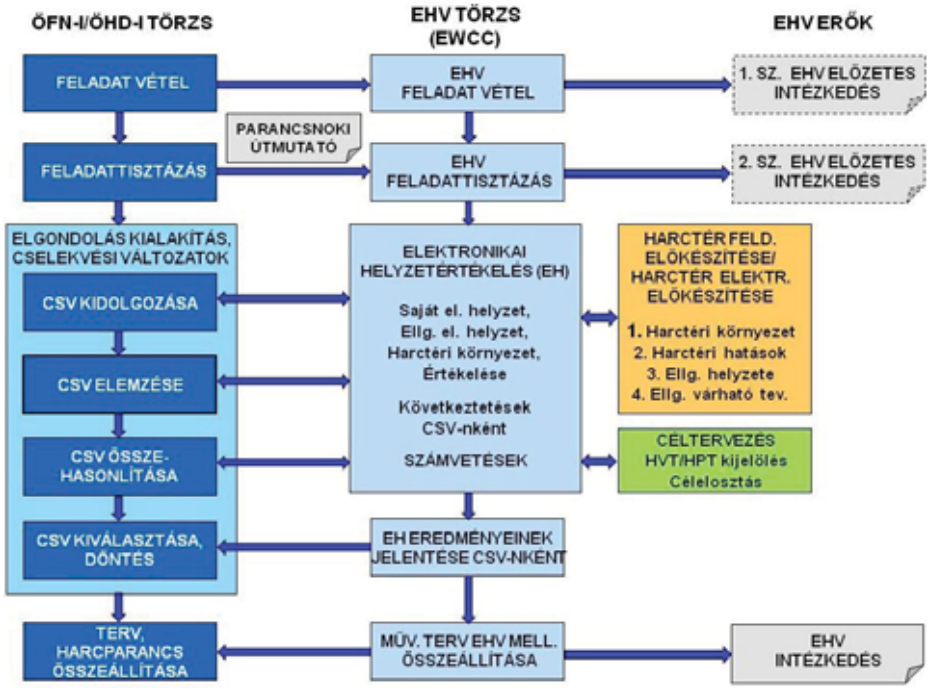
- elektronikai feladattisztázás és helyzetértékelés;
- a műveleti terv elektronikai hadviselési melléklete; valamint
- az elektronikai hadviselési céllisták (zavarási tervek).

[248] Ált-4/457 A Magyar Honvédség Törzsszolgálati Szakutasítása. HVK Hadműveleti Csoportfőnökség kiadvány, p. 5-9.

A törzs az elektronikai feladattisztázás és helyzetértékelés során, azzal párhuzamosan az alárendeltek részére előzetes intézkedést adhat ki, hogy időben felkészüljenek a várható feladatra és tevékenységre. (6.2. ábra)

Az elektronikai hadviselés megtervezésekor mindig figyelembe kell venni a *harcterület általános felderítési tervét* és a *harctér felderítő előkészítését (Intelligence Preparation of the Battlefield – IPB).*[249]

Az *elektronikai helyzetértékelés* a tervezési folyamat legfontosabb része. Az elektronikai helyzetértékelés végrehajtásakor az Elektronikai Hadviselés Koordinációs Részleg felhasználja a harctér felderítő előkészítésének produktumait, amelyből megismerik az ellenség elhelyezkedését, nagyságát, típusát, elektronikai harcrendjét és tevékenységét. A részleg az elektronikai helyzetértékelést a törzs munkarendjén belül, a cselekvési változatok kidolgozásának, elemzésének és összehasonlításának részeként hajtja végre.



6.2. ábra. **Az elektronikai hadviselés tervezésének folyamata**[250]

Az elektronikai helyzetértékeléssel párhuzamosan zajlik a *céltervezési folyamat,* amelynek eredményeként meghatározásra kerülnek az elektronikai hadviselés azon célob-

[249] Elsworth, Adam T. ed.: *Electronic Warfare*. Nova Science Publishers, Inc. New York, 2010. p. 193.

[250] Szerkesztették a szerzők.

jektumai, amelyek ellen a harc különböző fázisaiban elektronikai támogató, és/vagy ellentevékenységet kell folytatni. A hatékony célmeghatározás a helyes helyzetértékelésen alapszik, és azt az adott parancsnokság teljes hadműveleti és érdekeltségi területén végre kell hajtani.

Az elvégzett elektronikai helyzetértékelés eredményeit, következtetéseit a cselekvési változatok kiválasztása során jelenteni kell a parancsnoknak. A jelentés elfogadását követően az Elektronikai Hadviselés Koordinációs Részleg együttműködésben a többi törzzsel és tervező részleggel elkészíti a műveleti terv elektronikai hadviselési mellékletét, mely részletesen tartalmazza a harctevékenység (hadművelet) elektronikai hadviselési támogató tevékenységét, az elektronikai hadviselési csapatok alkalmazásának rendjét.

6.2.2 A tervezés általános elvei

6.2.2.1 A célobjektumok kategorizálása, osztályozása

Az elektronikai hadviselés tervezése során a célokat különböző kategóriák alapján különböztetik meg. Tervezés szempontjából az elektronikai hadviselési feladatok célpontjai azonosak a tüzérségi feladatokéval és osztályozásuk is megegyezik. Így a célok meghatározásánál meg kell különböztetni az úgynevezett *nagy értékű célokat (High Value Targets – HVT)* és a *nagy fontosságú célokat (High Payoff Targets – HPT).*

A nagy értékű célok alatt az ellenség számára a feladata teljesítéséhez legjobban szükséges erőket, eszközöket kell érteni. Ez elektronikai hadviselés szempontjából azon különböző vezetési és fegyverirányítási rendszerekben működő elektronikai eszközöket és objektumokat jelenti, amelyek az ellenség adott szintű feladat végrehajtásának sikeréhez elengedhetetlenek.

A nagy fontosságú célok alatt azokat a nagy értékű célokat kell érteni, amelyek sikeres támadása jelentős mértékben hozzájárul a saját harcászati (hadműveleti) célkitűzések eredményes teljesítéséhez. Ez tehát azt jelenti, hogy a nagy fontosságú célok a nagy értékű célok közül kerülnek kijelölésre, vagyis minden nagy fontosságú cél egyben nagy értékű cél is, de nem minden nagy értékű cél lesz nagy fontosságú cél. Az ellenség helyzetének és várható szándékának elemzése alapján jelölik ki a nagy értékű célpontokat. Az így azonosított céloknak a parancsnok elgondolásával és a harc megvívására vonatkozó elképzeléseivel történő összevetése alapján jelölik ki közülük a nagy fontosságú célpontokat.[251,252]

A tervezés során az elektronikai hadviselés szempontjából a célokat, az ellenük való tevékenység szerint az alábbiak alapján osztályozhatjuk:

- pusztítandó célok;
- elektronikai zavarással lefogandó célok;

[251] FM 3-36, Electronic Warfare, Department of the Army, 2012. p. 4-12.

[252] Joint Publication 3-60, Joint Targeting, 31 January 2013 , by United States Government US Army p. I-5.

– információszerzés céljából felderítendő ellenséges kisugárzó eszközök; és
– megtévesztendő ellenséges elektronikai rendszerek, eszközök.

Az osztályozás további kritériumát képezi – hasonlóan a tüzérségi célokhoz – a tervezés során a célok kijelölése és céllistában való megjelenítése. Ez alapján a célokat a következők szerint csoportosíthatjuk:
– tervezett célok *(Planned Targets)*;
– előre tervezett elektronikai hadviselés célpontok *(Pre-planned Targets)*;
– igénylés alapján kijelölt elektronikai hadviselés célpontok *(On-call Targets)*;
– alkalomszerű (új) célpontok *(Targets of Opportunity)*;
– nem tervezett célok *(Unplanned Targets)*; és
– nem várt célok (Unanticipated Targets).[253]

Elektronikai hadviselés szempontjából *az előre tervezett célpontok* olyan tervezett kommunikációs és nem-kommunikációs eszközök, melyeket a tervezési időszakban jelölnek ki, és amelyekre előre tervezetten kell tűz- vagy más, például elektronikai csapásokat mérni a katonai műveletek meghatározott időszakaiban. Ezek a célpontok a tervezési fázisban megjelölhetők, mint a harc során nagy fontosságú zavarandó, vagy lehallgatandó objektumok. Az egyes célpontok települési helyeit a harctér felderítő előkészítése során, vagy a meglévő adatbázis alapján lehet előre jelezni. Ezen objektumok elleni elektronikai hadviselési tevékenység fontossági sorrendjét és időrendjét az elektronikai helyzetértékeléssel párhuzamos zajló céltervezés során határozzák meg.

Az igénylés alapján kijelölt célpontok olyan tervezett célok, amelyeket a harctevékenység során, felfedésük és helymeghatározásuk után jelölnek ki zavarásra, vagy lehallgatásra. Ezek olyan objektumok, melyek jelenlétét a harc megindulása előtt nem lehetett előre látni, és amelyek fontosságára a harc során derül fény.

Az alkalomszerű célpontok olyan célok, melyek ismertek, de konkrét tervezett célként nem határoztak meg *(nem tervezett célok)*, vagy nem ismertek és megjelenésük sem várt az adott művelet során *(nem várt célok)*. Az alkalomszerű célokat az elektronikai támogatás, vagy elektronikai ellentevékenység során az operátor fed fel és azonosít. Felfedésüket követően azonban ezek a zavarás, vagy lehallgatás célobjektumait képezik, bár rendszerint alacsonyabb fontossági besorolást kapnak, mint az előre tervezett, vagy igényelt célok.[254]

Az ellenséges célpontok kategóriába sorolását a hadműveleti törzs – azon belül a Tűztámogató és Koordinációs Részleg – végzi az Elektronikai Hadviselés Koordinációs Részleg és más szakterületek felelősei segítségével. E tevékenység eredményekét készül el a fenti kategóriáknak megfelelően, és azokat fontossági sorrendbe állítva a Nagyfontos-

[253] Joint Publication 3-60, Joint Targeting, 31 January 2013 , by United States Government US Army p. I-7.
[254] Joint Publication 3-60, Joint Targeting, 31 January 2013 , by United States Government US Army p. I-8.

ságú Célok Listája *(High Payoff Target List – HPTL)*. Ez az eljárás megkönnyíti a további tervezést, és lehetővé teszi, hogy minden nagy fontosságú célobjektum ellen a legoptimálisabb eszköz és módszer kerüljön alkalmazásra. Mindez a Csapásmérési Útmutató Mátrixban (*Attack Guidance Matrix* – AGM) kerül meghatározásra, amely tartalmazza, hogy melyik célt hogyan, mikor, mely csapásmérő eszközzel (például tüzérség, légierő, elektronikai zavaró eszköz) tervezik lefogni.[255]

A harctevékenység megindulása előtt lefolytatott tervezési folyamat során határozzák meg az előre tervezett célpontok kategóriáit. A folyamat a katonai művelet során is folytatódik az igénylés alapján kijelölt célpontok, illetve az alkalomszerű célpontok feladatszabásával. A céltervezési folyamatban az elektronikai hadviselés tervezési folyamat szabja meg az elektronikai hadviselés eszközök feladat szerinti szervezetét, valamint az elöljáró parancsnoksághoz felterjesztésre kerülő elektronikai hadviselés támogatási kérelmeket.

6.2.2.2 Elektronikai hadviselés tervezési prioritások

A harcterületen elhelyezkedő nagyszámú, nagy fontosságú célobjektum jelentős igényt támaszt a katonai műveletek elektronikai hadviselési támogatásával szemben. Ezek az igények mindig nagyobbak, mint az elektronikai hadviselési csapatok meglévő képességei. Ezért a parancsnoknak sorrendet kell felállítania a célok között, meghatározva, hogy melyeket kell elsődlegesen támadni. Ezek a prioritások útmutatást adnak az elektronikai hadviselés tervezéséhez és az együttműködés megszervezéséhez.

Bár a harchelyzet változásai szükségessé teszik a prioritások gyakori megváltoztatását, a tervezés során a következő általános sorrendet kell figyelembe venni:

- először védeni kell a saját katonai információs rendszereinket. Ez megvalósítható részben az ellenség zavaróadói és célfelderítő rendszerei helyének meghatározásával és pusztításával, saját híradó rendszereink, illetve az elektronikai eszközök alkalmazására vonatkozó előírások szigorú betartásával. Az elektronikai zavarást is úgy kell megtervezni és végrehajtani, hogy az ne okozzon nem szándékos interferenciát a saját híradó-, felderítő- és fegyverirányító rendszerekben;
- másodszor pusztítani, vagy elektronikai úton korlátozni kell az ellenséges légvédelmi rendszer különböző elemeit. Az ellenséges légvédelem elleni tevékenység mind a szárazföldi csapatok, mind a légierő feladata. Először a saját légierő műveleteit közvetlenül veszélytető ellenséges légvédelmi rendszerek, és eszközök helyét kell meghatározni, majd megsemmisíteni, vagy zavarni. Másodszor, azonosítani kell az ellenség légvédelmének további kulcsfontosságú elemeit, meg kell határozni a helyüket, és le kell fogni azokat;
- harmadszor támadni kell az ellenség szárazföldi telepítésű csapásmérő rendszereit. A föld-föld rakéta, sorozatvető-, közvetett és közvetlen irányzású tüzér-, és páncéltörő eszközök és rendszerek a peremvonaltól olyan távolságban települ-

[255] FM 3-36, Electronic Warfare, Department of the Army, 2012. p. 4-12.

nek, hogy az elektronikai zavaróadóink hatni tudnak rájuk. Így lehetővé válik felderítésük, helymeghatározásuk, majd ez alapján pusztításuk és zavarásuk;
– negyedszer meg kell bontani az ellenség híradó rendszereit. Az elektronikai zavarás alkalmazása különösen hatékony lehet közvetlen harcérintkezésben, amikor az ellenséget arra kényszerítjük, hogy eltérjen a kidolgozott hadműveleti tervétől. Ezáltal csökkenteni lehet az ellenség manőverező képességét, az átcsoportosítás lehetőségét, és a tűzvezetést.

6.2.2.3 Elektronikai hadviselési erők harcrendje

Az elektronikai hadviselés erők a feladatuk végrehajtásához harcrendet vesznek fel. Az *elektronikai hadviselési erők harcrendje* az erők és eszközök szélességben és mélységben történő célszerű csoportosítása az elektronikai támogatás és ellentevékenység feladatainak sikeres végrehajtása érdekében. Az elektronikai hadviselés hatékony végrehajtása érdekében, a harcrend kialakításakor mindenkor az *elektromágneses hozzáférési követelményeket* figyelembe kell venni. Ez egyrészt azt jelenti, hogy elegendő térerősségű jel kell az ellenséges kisugárzások vételéhez, másrészt pedig elegendő térerősségű zavaró jelet kell biztosítani az ellenséges vevők bemenetén azok lefogásához.

A harcrendnek biztosítania kell:
– a kijelölt célterület fedését;
– a felderítési és zavarási lehetőségek maximális kihasználását;
– a rugalmas vezetést;
– híradás és együttműködés lehetőségeit más elektronikai hadviselési erőkkel;
– a terep adottságainak hatékony kihasználását;
– nagyfokú manőverezési lehetőséget;
– saját elektronikai rendszerek nem szándékos zavarásának kizárását; valamint
– az erők-eszközök megóvását, rejtését.

A harcrend méretét és a harcrendi elemek területi elhelyezkedését meghatározza:
– a kialakult harcászati-, hadműveleti helyzet;
– az összfegyvernemi kötelék műveleti területének méretei;
– az ellenséges célok valószínű területi elhelyezkedése;
– híradás és együttműködés lehetőségeit más elektronikai hadviselési erőkkel;
– a rendelkezésre álló technikai eszközök képessége; és
– a terepviszonyok.

A támadó jellegű elektronikai hadviselési eszközök (zavaróadók) a pusztítás szempontjából kiemelt fontosságú célok. Mivel nagy teljesítménnyel jellegzetes jeleket sugároznak ki, viszonylag könnyen felderíthetők és meghatározható a települési helyük.

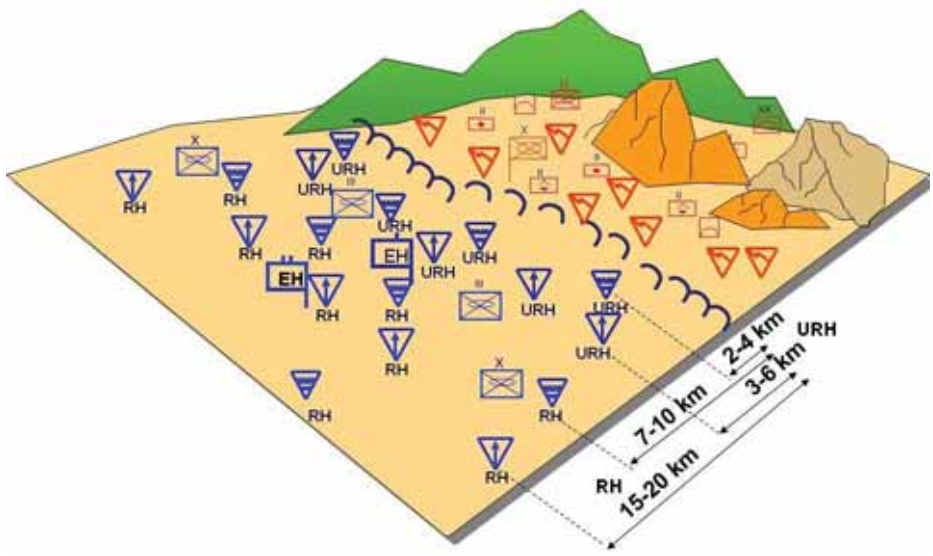
Az elektromágneses hozzáférhetőség és a terepviszonyok miatt az ultrarövid-hullámú (URH) és a magasabb frekvenciatartományokban működő földi telepítésű zavaróadókat a közvetett irányzású tűzfegyverek hatótávolságán belül kell telepíteni. Általában ezen eszközök gyenge páncélvédettsége nagyon sebezhetővé teszi őket, ezért a harcrend

megtervezésekor, a zavaró adók települési helyeit kellő körültekintéssel kell kialakítani. Azok helyes megválasztása, és a biztonsági rendszabályok szigorú betartása jelentősen növeli a túlélőképességüket.

Az álláskörletek nagybani helyét az Elektronikai Hadviselés Koordinációs Részleg koordinációja alapján az elektronikai hadviselési erők parancsnoka állapítja meg, egyeztetve annak az alakulatnak a parancsnokával, amelynek a műveleti területén települnek. A pontos települési helyet azonban a szakasz-, vagy csoportparancsnok határozza meg.

A kiválasztásnál alapvető szempontként figyelembe kell venni az ellenséges rádiók egymástól- illetve a harcérintkezés vonalától való távolságát, a terepet, az elektronikai láthatóságot, a technikai paramétereket és a kialakult harchelyzetet. Mivel az URH zavaráshoz szükséges az elektronikai átláthatóság, ezért az ilyen típusú zavaróeszközöket a csapatok első vonala mögött mintegy 2-4 km távolságra, kiemelkedő ponton kell telepíteni. A rövidhullámú zavaróadókat 7-10 km-re telepítik a harcérintkezés vonalától, de alkalmazhatók távolabbi álláskörletekből is. A földi zavaróadókat túlélőképességük növelése, illetve a zavarási feltételek biztosítása miatt sűrűn, lépcsőzetesen kell áttelepíteni. A rádiófelderítő és a rádió iránymérő eszközöket a zavaróállomások mögött és oldalt kell kijelölni. Az alkalmazott eszközök számára a harctevékenység minden fázisára fő és tartalék álláskörleteket kell kijelölni.

Többek között az előbb leírtak miatt a légi zavaró eszközök, és az egyszeri felhasználású zavaróadók hatékonyabban alkalmazhatók az ellenséges híradó- és fegyverirányító rendszerek ellen. (6.3. ábra)



6.3. ábra. **A földi telepítésű rádiózavaró eszközök harcrendje**[256]

[256] Szerkesztették a szerzők.

6.3 A harctér felderítő előkészítése

Az ellenség elektronikai helyzetértének ékelése, mint a harctér elektronikai előkészítése *(Electronic Preparation of the Battlefield – EPB)* nagymértékben támaszkodik a harctér felderítő előkészítésére. Ezért mielőtt az elektronikai helyzetértékelés tartalmát és végrehajtásának módszereit tárgyalnánk, röviden tekintsük át a harctér felderítő előkészítésének legfontosabb elemeit.

A harctér felderítő előkészítése, egy adott földrajzi területen az ellenség és a környezet elemzésének egy szisztematikus és folyamatos módszere. A harctér felderítő előkészítés, az információ feldolgozási szerepén túl, lehetőséget ad a helyzet- és a célértékelés komplexé tételére. A harctér felderítő előkészítés befolyásolja a helyzetértékelést, a célok meghatározásával kapcsolatos feladatok megtervezését, az adatgyűjtést, feldolgozást és a szétosztást. A harctér felderítő előkészítésének folyamata az alábbi négy fő fázisban zajlik:

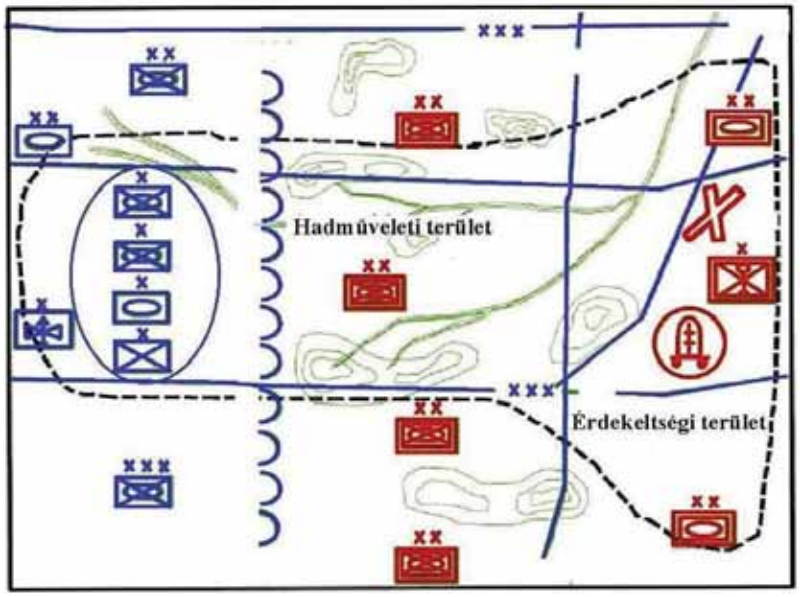
- a harctéri környezet meghatározása;
- a harctéri hatások elemzése;
- az ellenség értékelése; és
- az ellenség várható tevékenységének *(Course of Action – COA)* meghatározása.[257]

A harctéri környezet meghatározása, a harc- (hadműveleti) terület és az érdekeltségi terület fizikai méreteinek kijelölését jelenti. Az adott szintű kötelék harcterületének határait (tűz, elektronikai hadviselés és manőver) az elöljáró határozza meg. Az érdekeltségi terület határa nincs meghatározva, erre a felderítő főnök tesz javaslatot a feladat, az ellenség, a terep, a saját erők és a rendelkezésre álló idő figyelembevételével és a parancsnok hagyja jóvá. A harcterület és érdekeltségi terület meghatározásának dimenziói a szélesség, mélység, légtér és az idő. (6.4. ábra)

A hadműveleti terület és az érdekeltségi terület fizikai dimenzióinak meghatározása alapvető az elektronikai hadviselés tervezéséhez is. *A hadműveleti terület* egy adott konfliktus területének azon része, mely szükséges a katonai tevékenységek megvívásához. A hadműveleti terület egy földrajzilag körülhatárolt terület, amelyet az elöljáró parancsnok jelöl ki az alárendelt parancsnok részére, amelyen belül önállóan hajtja végre a harctevékenységét. A kijelölésnél az elöljáró parancsnok figyelembe veszi a feladatot, az ellenséget, terepet, a saját erőket és a rendelkezésre álló időt.[258]

Az érdekeltségi terület az a terület, amely befolyásolja a parancsnok tevékenységét, beleértve a saját hadműveleti területet, valamint a szomszédokét és kiterjed az ellenség azon területére, ahol az éppen folyó, illetve a tervezett műveletek megvalósulnak. Az érdekeltségi terület átfedést jelent a szomszédokkal, elöljáróval valamint tartalmazza a hadműveleti terület mögöttes területét is.[259]

[257] FM 2-01.3 Intelligence Preparation of the Battlefield/Battlespace Department of the Army, 2009. p. II-1.
[258] FM 2-01.3 Intelligence Preparation of the Battlefield/Battlespace Department of the Army, 2009. p. II-3.
[259] U.o. p. GL-4.



6.4. ábra. **A hadműveleti terület és az érdekeltségi terület értelmezése**[260]

Az érdekeltségi területet annál is inkább figyelembe kell venni, mivel az elektromágneses hullámok terjedési sajátosságaiból adódóan mind az ellenség, mind a saját elektronikai hadviselési eszközök képesek a hadműveleti területen kívülről is felderíteni és zavarni a hadműveleti területen kívül elhelyezett elektronikai eszközöket.

Összességében a harctéri környezet meghatározása a következőket jelenti:

- a környezet fő jellemzőinek azonosítása;
- a hadműveleti terület határainak megállapítása;
- az érdekeltségi terület határainak megállapítása;
- az értékelésre rendelkezésre álló idő megállapítása.

A harctéri hatások elemzése során megállapításra kerül, hogy a harctéri környezet hogyan befolyásolja mind az ellenség, mind a saját csapatok tevékenységét. A harctéri hatások elemzése magába foglalja:

- a harctéri környezet elemzését, azon belül:
  - a terep elemzését;
  - az időjárás elemzését;
  - a harctér egyéb jellemzőinek elemzését; valamint
- a harctéri környezeti hatások leírását az ellenség és a saját csapatok tevékenységére.

[260] Szerkesztették a szerzők.

Az elektronikai hadviselés szempontjából a terep értékelésénél egyrészt figyelembe kell venni, hogy az hogyan tudja növelni az elektronikai hadviselés hatékonyságát, másrészt pedig hogyan használható fel a vezetési és fegyverirányítási rendszereink, eszközeink elektronikai védelmére az ellenséges felderítéssel és elektronikai hadviseléssel szemben.

A terep értékelésénél mind az ellenség, mind a saját csapatok vonatkozásában a következőket kell figyelembe venni:

– a terep optikai és elektronikai láthatóságát mind a kommunikációs, mind a nem-kommunikációs kisugárzó eszközök vonatkozásában;
– a növényzetet és azok hatását az elektromágneses hullámok terjedésére és az antenna rendszerek telepítésére;
– nagy kiterjedésű-, nagy magasságú objektumokat, mesterséges terepakadályokat, melyek szintén befolyásolják az elektromágneses hullámok terjedését;
– a különböző talajtípusokat, melyek hatással lehetnek az elektronikai eszközök működésére (például földelés, talaj vezetőképessége).

Az elektronikai hadviselés érdekében az időjárás értékelésénél mind az ellenség, mind a saját csapatok vonatkozásában a következőket kell figyelembe venni:

- szélsőséges időjárási viszonyok hatásait a nagy érzékenységű elektronikai eszközökre (például köd, pára, csapadék, por);
- elektromos viharokat és más elektromágneses jelenségeket;
- az elektronikai támogató és elektronikai ellentevékenységet végző repülőgépek tevékenységét befolyásoló időjárási hatásokat.

Korszerű elektronikai hadviselési vezetési rendszerekben – amelyek a térinformatika *(Geographic Information System – GIS)* elvét felhasználva digitális térképi alapon működnek – a terep és időjárási hatások értékelése nagypontossággal, kellő részletességgel és objektivitással valósul meg. A korszerű elektronikai hadviselési vezetési rendszerekről a későbbiekben szólunk.

Az ellenség értékelése kiterjed az ellenséges erők összetételének, szervezetének, alkalmazási eljárásainak, fegyvereinek és eszközeinek valamint a harcterületen található egyéb támogató rendszereknek a részletes tanulmányozására. Ennek a feladatnak az alapvető célja az ellenség lehetőségeinek és várható tevékenységének megállapítása.[261]

Elektronikai hadviselés tekintetében az ellenség értékelése tartalmazza:

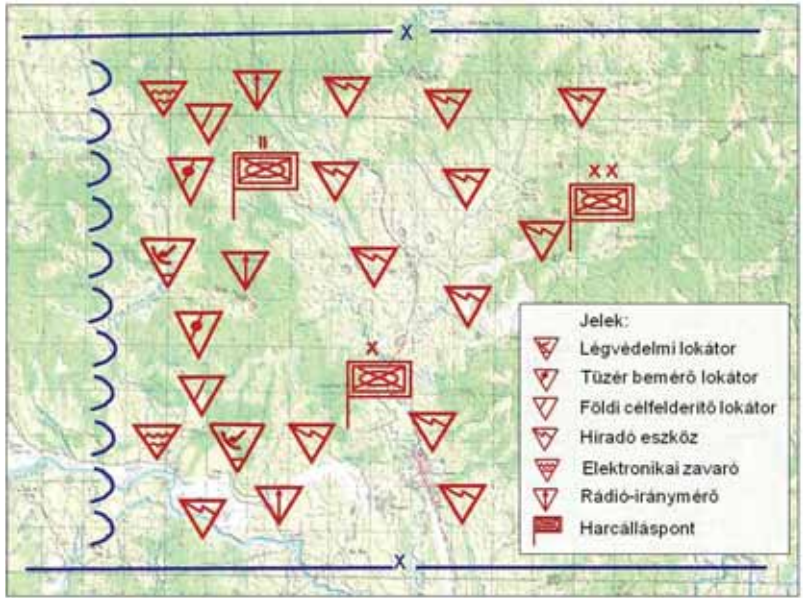
– az ellenség elektronikai harcrendi modelljének létrehozását, vagy aktualizálását, ezen belül:
– az ellenség elektronikai rendszerei harci alkalmazási elveinek grafikus formában való ábrázolását (elvi vázlatok);
– az ellenség elektronikai rendszerei harci alkalmazási elveinek és lehetőségeinek szöveges leírását;

[261] FM 2-01.3 Intelligence Preparation of the Battlefield/Battlespace Department of the Army, 2009. p. II-55.

– az ellenség nagy értékű célpontjainak (HVT) és nagy fontosságú célpontjainak (HPT) meghatározását (mennyiségi számvetések);
– az ellenség elektronikai rendszerei képességeinek meghatározását (képességi mutatók).

Az ellenség várható tevékenysége meghatározásának a célja megállapítani, hogy az előzőekben értékelt ellenség, a harceljárásait és képességeit hogyan fogja alkalmazni és kihasználni a terep és az időjárás által befolyásolt körülmények között. Az ellenség várható tevékenységének meghatározása az alábbiakat jelenti:
– az ellenség szándékának és végcéljának meghatározása;
  = az ellenség várható összes tevékenységének meghatározása;
  = minden egyes várható tevékenység elemzése és közöttük prioritások felállítása;
  = minden egyes várható tevékenység részletes kidolgozása;
– ezek alapján a kezdeti adatgyűjtési követelmények meghatározása.[262]

A harctér felderítő előkészítés során az egyes lépések eredményei vázlatokon kerülnek ábrázolásra. A vázlatok grafikus illusztrációi az ellenség összetételének, elhelyezkedésének, képességeinek és várható tevékenységeinek. Erre mutat egy példát a 6.5. ábra.



6.5. ábra. **Az ellenség elektronikai eszközeinek helyzet vázlata[263]**

[262] U.o. p. II-69.
[263] Szerkesztették a szerzők.

A harctér felderítő előkészítése során a következő vázlatok készülnek el:
- *az ellenség harcászati elveinek vázlatai*, amelyek az ellenség harcrendjének, elhelyezkedésének felépítését tartalmazzák, a különböző harctevékenységi formákban a terep és az időjárás figyelembe vétele nélkül;
- *helyzet vázlatok*, amelyek bemutatják az ellenség várható elhelyezkedését és tevékenységét figyelembe véve a terep és az időjárás befolyásoló hatását;
- *esemény vázlatok*, amelyek a harctevékenység fontosabb időszakai szerinti bontásban tartalmazzák a várható helyzetet;
- *elhatározást támogató vázlatok*, amelyek a harctér felderítő előkészítésének végeredményeként – az elhatározás szempontjai szerint – bemutatják azokat a legfontosabb területeket, ahol a kulcsfontosságú események történhetnek, és segítenek grafikusan megalapozni az elhatározás meghozatalát.

E vázlatok elektronikai hadviseléshez kapcsolódó részeit, az elektronikai helyzetértékelést végzők messzemenően felhasználják.

Az elektronikai hadviselésre tekintettel ezek a vázlatok a következők lehetnek:
- az ellenség kommunikációs rendszereinek és csomópontjainak, nem-kommunikációs (például radar, navigációs) eszközeinek, felderítő rendszerének és elektronikai hadviselési eszközeinek felépítését, alkalmazási elveit tartalmazó elvi vázlatok;
- az ellenség e rendszereinek, eszközeinek elhelyezkedését tartalmazó vázlatok figyelembe véve a terep és domborzat, valamint az időjárás hatásait;
- az ellenség e rendszereinek, eszközeinek helyzetét – a harc-, hadművelet kritikus időszakai szerinti bontásban (dinamikai helyzetben) – ábrázoló vázlatok.[264]

Hagyományos vezetési módszereket feltételezve az említett vázlatok általában fólián kerülnek ábrázolásra. Korszerű vezetési rendszerekben azonban – a számítógépes elemzés eredményeként – térinformatikai rétegmodelleken kerülnek kidolgozásra, és a törzsön belüli számítógépes hálózaton mindenki számára hozzáférhetővé válnak.

6.4 Az elektronikai helyzetértékelés

6.4.1 Az elektronikai helyzet és az elektronikai helyzetértékelés értelmezése

Az elektronikai hadviselés megtervezése, megszervezése és megvívása során elengedhetetlenül szükséges az elektronikai helyzet folyamatos értékelése. A kialakult elektronikai helyzetet elsősorban az Elektronikai Hadviselés Koordinációs Részleg értékeli, de az

[264] Frater, Michael R. – *Electronic Warfare for the Digitized Battlefield*. Artech House, 2001. p. 270.

eredményes tevékenység érdekében Elengedhetetlenül szükséges, hogy minden fegyvernem és szakcsapat törzs is figyelembe vegye azt, és tervezőmunkája során értékelje a saját területének megfelelően.

Az elektronikai helyzetértékelés során összevetik az elektronikai hadviselési rendszer képességeit és korlátait a harctér felderítő előkészítés során meghatározott célpontokkal. Ennek eredményeként megtörténik azon fontos célpontok kijelölése, melyek a rendelkezésre álló elektronikai hadviselési eszközökkel befolyásolhatók. Ez megfelel a célkidolgozási eljárásban a nagy fontosságú célok kiválasztásának. Ezt a feladatot az adott szintű felderítő törzs hajtja végre, együttműködve az Elektronikai Hadviselés Koordinációs Részleggel.

Az elektronikai helyzet a hadműveleti területen (harctevékenységi körzetben) és az érdekeltségi területen adott időben érvényesülő tényezők hatásra kialakult olyan elektronikai erőviszony, amely befolyásolja a harctevékenység előkészítését, végrehajtását és eredményét. Más szavakkal elektronikai helyzet alatt a csapatok vezetését, a fegyverek irányítását, a felderítést és az elektronikai hadviselést végrehajtó, egymással szemben álló elektronikai rendszerek, illetve eszközök között adott időben és adott hadműveleti- és érdekeltségi területen kialakult helyzetet értjük.

Mivel a bennünket körülvevő elektromágneses tér állapota objektív és szubjektív tényezőktől függően állandóan változik, így a tér bizonyos tulajdonságai definiálják az elektronikai helyzetet, tehát azokat a körülményeket, amelyek befolyásolják az elektronikai hadviselést.

Ezek a tulajdonságok:

- az ellenség elektronikai objektumai, azok helyzete, kiterjedése, jellemzői;
- a saját elektronikai objektumok, azok helyzete, kiterjedése, jellemzői;
- a fenti objektumok és a valós fizikai környezet kölcsönhatásai (például a domborzat sajátosságai, hullámterjedési feltételek, időjárás, napszak).

Az elektronikai helyzetértékelés az elektronikai hadviselés megvívására hozott elhatározás kidolgozásának legjelentősebb mozzanata, amely a harcászati-, hadműveleti helyzet figyelembevételével, az elektronikai hadviselés megvívását elősegítő és hátráltató körülményeinek értékelésével, majd következtetések levonásával biztosítja az elektronikai hadviselés törzs részére, a legoptimálisabb elgondolás kialakítását az elektronikai hadviselés megvívására.[265]

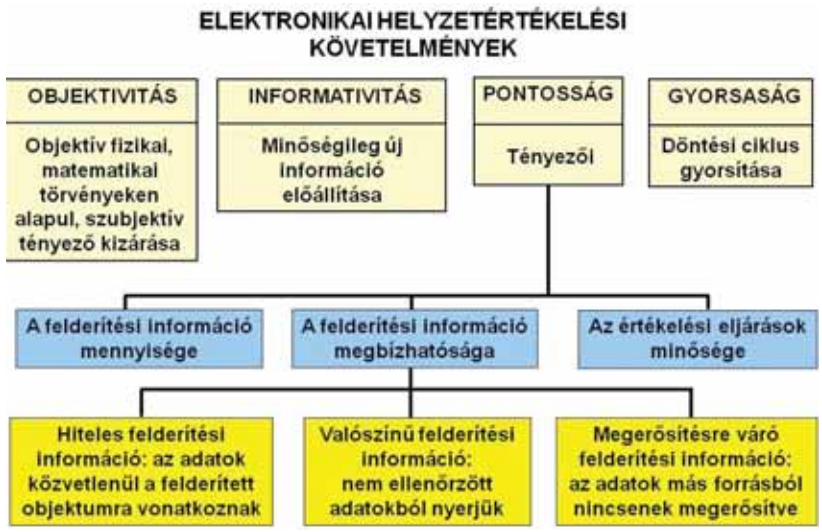
A megfogalmazásból egyértelműen kiderül, hogy az elektronikai helyzetértékelés egy döntés-előkészítő tevékenység, mely a következő részfeladatokat tartalmazza:

- az elektronikai helyzetet leíró modell kapcsolatrendszereinek, tulajdonságának definiálását, melyet egyszer kell végrehajtani, majd folyamatosan pontosítani (ellenség és saját elvi vázlatok kidolgozása, karbantartása);

[265] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 14.

– a modell adatokkal való feltöltését, aktualizálását, karbantartását, amelynek célja, hogy az minden időpillanatban a legjobban tükrözze a valós helyzetet (ellenség és saját helyzet és esemény vázlatok kidolgozása);
– az elektronikai helyzet elemzését, tulajdonságainak, kapcsolatrendszereinek, állapotának vizsgálatát, amely az értékelés eredményeként megfelelő következtetések, levonásához vezet.

Az elektronikai hadviselés megvívására hozott elhatározás alátámasztására az elektronikai helyzetértékelés egy sor követelménynek kell hogy megfeleljen. Ezek a követelmények a következők: *objektivitás, informativitás, gyorsaság, pontosság*. Mindezeket és tartalmunkat a 6.6. ábra szemlélteti.



6.6. ábra. **Az elektronikai helyzetértékeléssel szembeni követelmények**[266]

Az elektronikai helyzetértékelés olyan folyamatos tevékenység, amelyet a harc-, hadművelet előkészítése és megvívása során egyaránt végezni kell, csak más-más prioritások figyelembevételével.

6.4.2 Az elektronikai helyzetértékelés elemei, kiindulási adatai

Az elektronikai helyzetértékelés magában foglalja:
– az ellenség elektronikai helyzetének értékelését;
– a saját elektronikai helyzet értékelését;

[266] Szerkesztették a szerzők.

– valamint ezekkel párhuzamosan a környezeti tényezők (hadműveleti terület, idő, időjárás és egyéb tényezők) értékelését.

Az ellenség elektronikai helyzetének értékelése során tanulmányozni kell:
– a várható földi-, légi vezetési és fegyverirányító elektronikai rendszereket, objektumokat és eszközöket;
– a várható elektronikai objektumok mennyiségét, helyét, szerepét a vezetés és fegyverirányítás rendszerében, védettségüket, sebezhetőségüket, főbb jellemzőiket, települési helyüket;
– az ellenség ismert és várható elektronikai hadviselés erőinek, eszközeinek lehetőségeit, szakharcászati eljárásait;
– a polgári infrastruktúra felhasználásának lehetőségeit.

Az ellenség elektronikai helyzete értékeléséhez szükséges kiindulási adatok:
– az ellenség összfegyvernemi-, fegyvernemi- és szakcsapatainak elhelyezkedése;
– az ellenség szervezeti felépítéséről, struktúrájáról, harci technikai eszközeiről és azok alkalmazási elveiről ismert adatok (légierő, légvédelem, csapatok szervezeti felépítése, technikai eszközeinek mennyisége, minősége, harci lehetőségeik). Ezek az adatok nagyrészt már békeidőben rendelkezésre állnak (adattárakban, segédletekben), az értékelés végrehajtása előtt csak pontosításukra van szükség;
– a földrajzi környezet adatai. Ide értjük a domborzatot leíró adatokat, a fedettségre vonatkozó és a terepen található természetes, illetve mesterséges objektumokat leíró adatokat (például vizek, utak, hidak, vasutak, elektromos kábelek, ipari és adminisztratív objektumok, települések).

A saját elektronikai helyzet értékelése során tanulmányozni kell:
– a kapott feladatot, a saját erők elhelyezkedését;
– a saját elektronikai objektumok helyét, szerepét a csapataink vezetésében és a fegyverirányításban;
– a saját elektronikai objektumaink védettségét, sebezhetőségét;
– a saját elektronikai hadviselés erők képességeit, lehetőségeit;
– az elektronikai hadviselés feladatait végrehajtó egyéb erők és eszközök képességeit, lehetőségeit;
– az érdekeltségi területen a nem katonai célú frekvencia felhasználást.

A saját elektronikai helyzet értékeléséhez szükséges kiinduló adatok:
– a csapataink elhelyezkedése;
– a saját csapataink (azon belül az elektronikai hadviselés erők) szervezetéről, eszközeiről, lehetőségeiről, aktuális feltöltöttségéről, harcértékéről rendelkezésre álló adatok; valamint
– a földrajzi környezet adatai (hasonlóan az előzőekben leírtakhoz).

6.4.3 Az elektronikai helyzetértékelés módszere

Az elektronikai helyzetértékelés során az ellenség helyzetét, a saját helyzetet, illetve a környezeti tényezőket egymásra gyakorolt kölcsönhatásukban, az elektronikai hadviselés megvívása során végrehajtandó fő feladatoknak megfelelő fázisokban értékelik.

Ez azt jelenti, hogy a helyzetértékelés:

– az ellenség elektronikai objektumainak, eszközeinek elektronikai felderíthetősége;
– az ellenség elektronikai objektumaival, eszközeivel szembeni elektronikai ellentevékenység, és
– a saját elektronikai rendszereink, harci- technikai eszközeink elektronikai védelme alapján kerül végrehajtásra, mégpedig úgy, hogy minden fázisban egymással szembe kell állítani az ellenséges és a saját elektronikai helyzetet, mint ellentétes rendeltetésű tényezőket. (6.7. ábra)

6.7. ábra. **Elektronikai helyzetértékelés**[267]

Az értékelés során felhasználásra kerülnek a harctér felderítő előkészítése során elkészített vázlatok, melyek alapot szolgáltatnak az ellenség és a harctéri környezet további elemzéséhez.

[267] Szerkesztették a szerzők.

A fázisonként kapott részeredményeket – amelyek részben átfedhetik egymást – megfelelően súlyozni és összegezni kell, majd a részeredmények alapján következtetéseket kell levonni.

Az elektronikai támogató tevékenység tervezésekor az ellenség értékelése során meg kell határozni:

- a felfedett és a várható elektronikai objektumok mennyiségét, helyét, szerepét a vezetés és a fegyverirányítás rendszerében;
- az e rendszerekben működő elektronikai eszközök jellemzőit (például technikai paraméterek, frekvencia használat, hozzáférhetőség).

A saját csapataink értékelése során:

- tisztázni kell a saját elektronikai támogató-, felderítő erők és eszközök készenlétét, feltöltöttségét, technikai állapotát;
- meg kell határozni a saját elektronikai támogató, felderítő eszközök harci lehetőségeit (harci technikai paraméterek és az ellenség értékelése alapján).

Mindezek alapján meghatározható, hogy

- az ellenség mely elektronikai objektumait vagyunk képesek felderíteni, és ez alapján mely elektronikai eszközök fogják képezni az elektronikai támogató tevékenység célobjektumait;
- az elektronikai támogatást, felderítést milyen harcrendből lehet optimálisan végrehajtani;
- a harctevékenység (hadművelet) figyelembevételével, mi lesz az elektronikai támogatás, felderítés főerőkifejtésének iránya;
- milyenek lesznek a saját elektronikai támogató és felderítőerők vezetési és együttműködési lehetőségei (kivel, milyen területen, milyen módon kell együttműködni).

Az elektronikai ellentevékenység tervezésekor, az ellenség értékelése során meg kell határozni:

- a felfedett és várható elektronikai objektumok mennyiségét, helyét, szerepét a vezetés és fegyverirányítás rendszerében;
- az ellenség nagy fontosságú elektronikai objektumait (HPT), azok sebezhetőségét;
- az ellenség elektronikai eszközeinek jellemzőit, különböző zavartípusokkal szembeni zavarvédettségét;
- a zavarás hatását a vezetési és fegyverirányítási rendszer működésére;
- a zavarás alóli kitérés lehetőségeit.

A saját csapataink értékelése során:

- tisztázni kell a saját zavaróerők és eszközök készenlétét, feltöltöttségét, technikai állapotát;
- meg kell határozni a saját zavaróeszközök harci lehetőségeit (a harci technikai paraméterek és az ellenség értékelése alapján);

– értékelni kell az elektronikai megtévesztésbe bevonható eszközök lehetőségeit;
– értékelni kell az elektronikai pusztításra alkalmazható fegyvereket, eszközöket.

Ezek alapján meghatározhatók
– az ellenség elektronikai objektumai zavarásának lehetőségei;
– az elektronikai zavarás célobjektumai;
– az elektronikai zavarás szempontjából optimális harcrend;
– az elektronikai zavarás főerőkifejtésének iránya;
– a saját elektronikai zavaróerők vezetési és együttműködési lehetőségei (kivel, milyen területen, milyen módon kell együttműködni);
– a vezetési és felderítő rendszerek megtévesztésének lehetőségei;
– valamint azon nagy fontosságú elektronikai objektumok melyeket a harc, hadművelet fő időszakaihoz kapcsolódóan, a tűzcsapásokkal és manőverekkel összhangban pusztítani kell.

Az elektronikai védelem tervezésekor az ellenség értékelése során meg kell határozni:
– hogy milyen irányított fegyverekkel lehet számolni, illetve ezek milyen irányítási móddal rendelkeznek és milyen irányból és terepszakaszokról várható ezek alkalmazása;
– hogy milyen (és mennyi) földi-, légi elektronikai zavaróeszközzel, -erővel kell számolni, ezek milyen harci technikai paraméterekkel rendelkeznek és milyen lesz ezen erők és eszközök várható csoportosítása;
– azokat a technikai felderítőeszközöket, amelyek alkalmazására számítani lehet, azok felderítési, adat-feldolgozási lehetőségeit, korlátait, megtévesztésük lehetséges módjait, illetve várható alkalmazásuk helyét és módját.

A saját elektronikai rendszereink, harci-technikai eszközeink értékelése során meg kell határozni:
– a saját vezetési és fegyverirányítási rendszereink felépítését, a bennük alkalmazott elektronikai eszközök harcászati-technikai paramétereit, azok sebezhetőségét, zavarhatóságát, zavarással szembeni védettségét;
– a fontosabb elektronikai objektumok fizikai sebezhetőségét, irányított fegyverekkel szembeni védettségét;
– az elektronikai védelem megvalósításához rendelkezésre álló technikai eszközöket, azok paramétereit, lehetőségeit;
– a legfontosabb elektronikai objektumainkat a korlátozások bevezetéséhez;
– a saját elektronikai objektumok felderíthetőségét, áruló jellemzőit;
– az álcázás, dezinformálás technikai és egyéb módszereit, a megvalósításban felhasználható eszközök lehetőségeit;
– a hadműveleti területre eső nem katonai célú frekvencia felhasználásokat.

Ezek alapján következtetések vonhatók le az elektronikai védelem különböző rendszabályaira, az álcázás módszereire, a szögvisszaverők, ködösítések alkalmazására, valamint a különböző korlátozások bevezetésére vonatkozóan.

Ilyen részletesen, minden területre kiterjedően az elektronikai helyzetértékelést csak a harc, hadművelet előkészítése során kell végrehajtani. A harc, hadművelet végrehajtása során csak a helyzet változásaira, a konkrétan végrehajtandó feladatra kell a helyzetértékelését elvégezni.

6.4.4 Az elektronikai helyzetértékelés eredményei

Az elektronikai helyzetértékelés a törzs munkarendjén belül, a cselekvési változatok kidolgozásának, elemzésének és összehasonlításának részeként zajlik. Az elektronikai hadviselés három területének megfelelően elvégzett értékelés eredményei alapján összegzett következtetéseket lehet levonni a törzs által kidolgozott cselekvési változatok elektronikai hadviselés támogatására. A levont következtetések alapján meg kell határozni:

- az ellenség várható elektronikai hadviselés tevékenységét;
- az ellenség vezetési és fegyverirányítási rendszereiben várható legfontosabb elektronikai objektumokat, elektronikai eszközöket, melyeket a harc, hadművelet sikere érdekében fel kell deríteni, illetve zavarással le kell fogni;
- az elektronikai ellentevékenység és elektronikai támogatás célszerű módját és lehetőségeit;
- a rendelkezésre álló elektronikai hadviselés erők szükséges csoportosítását, továbbá a felderítés, zavarás főerőkifejtésének irányait;
- az elektronikai védelem rendszabályait;
- az együttműködés feladatait a fegyvernemekkel a szomszédok- és az elöljáró elektronikai hadviselés erőivel és eszközeivel;
- a rendelkezésre álló elektronikai hadviselés erőkkel és eszközökkel az elektronikai hadviselés feladatai biztosításának feltételeit;
- a hadműveleti álcázás érdekében végrehajtandó feladatokat.

Az elektronikai helyzetértékeléssel párhuzamosan el kell végezni azokat a *számvetéseket***,** amelyek szükségesek például az elektronikai támogató és zavaró eszközök telepítéséhez, áttelepítéséhez és manővereihez, a felderítés és a zavarás hatótávolságának meghatározásához, az iránymérési zónák meghatározásához, összességében az elektronikai hadviselés irányításához.

Az elektronikai helyzetértékelés a különböző ismert, feltételezett, kapott és pontosított adatok (információk) alapján részletes, pontos számvetésekre kell hogy támaszkodjon, amelyek egyrészt bizonyító jellegűek, másrészt az egyes munkafolyamatok végrehajthatóságát biztosítják. Ezek a különböző számvetések, matematikai számítások képezik az elektronikai hadviselés szakértői rendszerének alapját.

A számvetések típusaira, sorrendiségére, illetve logikai folyamatára külön útmutató nincs, ugyanakkor a gyakorlati életben lényegében kialakult egy módszer, amely szük-

ségszerűen figyelembe veszi az időben végrehajtandó feladatokat, azok jellegét, nagyságrendjét és a tartalmukkal szemben támasztott követelményeket. A számvetések egyes részeit már békeidőben elő lehet készíteni.

A számvetések készítését az elektronikai helyzetértékelés során kell elkezdeni és a műveleti terv elektronikai hadviselési mellékletének elkészítéséig folytatni, illetve pontosítani kell. Az elkészített számvetések egy része az elektronikai hadviselés melléklet részét képezi, másik része pedig alátámasztja azt.

Az elvégzett elektronikai helyzetértékelés cselekvési változatonkénti eredményeit, következtetéseit a cselekvési változatok kiválasztása során kell jelenteni a parancsnoknak. A kiválasztást (döntést) követően a parancsnok által meghatározott változatnak megfelelően készül el a *műveleti terv elektronikai hadviselési melléklete*, amely részletesen tartalmazza a harc, hadművelet elektronikai hadviselési támogatására vonatkozó elgondolást, az elektronikai hadviselési csapatok alkalmazásának rendjét.

A melléklet kidolgozása során végső formába hozzák, illetve pontosítják az elektronikai helyzetértékelés során megkezdett, illetve elvégzett számvetéseket. Az elektronikai hadviselés melléklet *térképes és hozzá kapcsolódó szöveges részből áll***,** melyet a teljes műveleti időszakra kell elkészíteni. A melléklet általában a következőket tartalmazhatja:

- a kialakult helyzetet;
- az elektronikai hadviselés célját, feladatait;
- az elektronikai hadviselés megvívására vonatkozó elgondolást;
- a sikeres elektronikai hadviselési tevékenységek érdekében alkalmazott támogató tevékenységeket;
- az elektronikai hadviselés vezetésének rendjét, módszereit, a híradás kérdéseit.

Az elektronikai hadviselés melléklet a szükséges mértékben különböző táblázatokat és listákat, mint függelékeket tartalmazhat. Ilyen fontos mellékletek például az elektronikai hadviselési céllisták *(Electronic Warfare Target Lists – EWTL*) és zavarási tervek, korlátozott frekvenciák jegyzéke, amelyek alapvető fontosságúak az elektronikai támogató tevékenység és ellentevékenység összehangolásában és végrehajtásában.

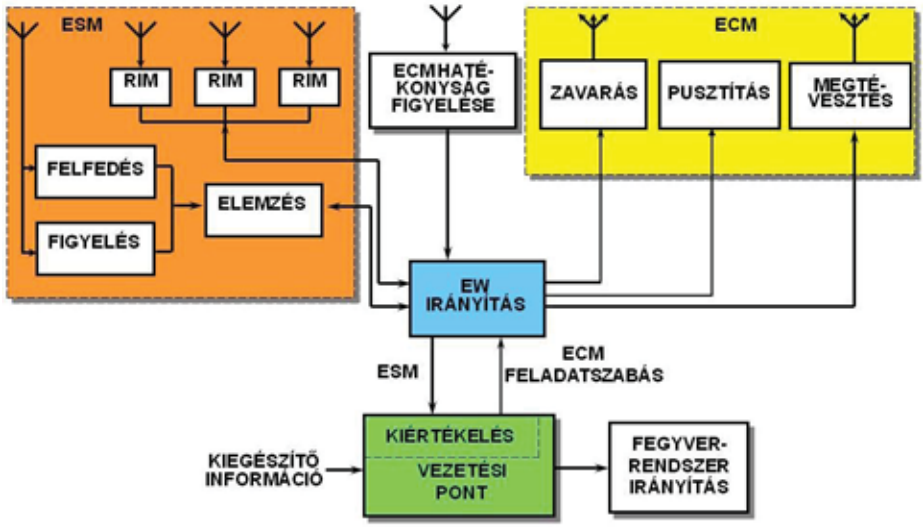
6.5 Az elektronikai hadviselés irányítása és hatékonyságának értékelése

Az elektronikai hadviselés hatékony irányítása alapvető követelmény a sikeres tevékenységhez. Az irányítást úgy kell megszervezni, hogy a zavarás a legfontosabb célok ellen irányuljon, ugyanakkor ne okozzon zavart a saját eszközeinknél, csapatainknál. Az elektronikai hadviselés általános irányítási folyamatát a 6.8. ábra mutatja.

Az irányítás történhet úgynevezett *pozitív* vagy *negatív módszerrel***,** illetve *kombináltan*. Leggyakrabban a kombinált módszert alkalmazzák, úgy, hogy maximális együttműködést biztosítanak a támogatott alakulat és az elektronikai ellentevékenységet végrehajtó erők között.

A pozitív irányítási módszer az alábbiak szerint valósulhat meg:

– speciális előre meghatározott egyedi frekvenciákon engedélyezik a zavarást, vagy kiadnak egy olyan frekvencia listát, amely tartalmazza a zavarható frekvenciákat. A többi frekvencián külön engedély nélkül tilos a zavarás;
– a zavarás engedélyezését az ellenség bizonyos speciális tevékenységéhez kötik, de a tiltott frekvenciákon ekkor sem lehet zavarni;
– közvetlen (központi) irányítást alkalmaznak, amely lehetővé teszi központilag a zavarás elrendelését és leállítását. Ehhez az irányítási módhoz stabil állandó híradás és az irányító parancsnok alapos szakmai felkészültsége szükséges.



6.8. ábra. **Az elektronikai hadviselés általános irányítási folyamata**[268]

Az előre tervezett célok elleni tevékenység irányítása általában pozitív irányítási módszerrel történik.

A negatív irányítás azon alapul, hogy kidolgozzák és közzéteszik a *Korlátozott Frekvenciák Jegyzékét.* Ez a lista koordinálja az elektromágneses spektrum használatát, és minimumra csökkenti a saját rendszereket fenyegető nem szándékos zavarás hatását. A negatív irányítási módszert elsősorban a harc kezdetén alkalmazzák, amikor még egyáltalán nem, vagy csak kis mértékben áll rendelkezésre megfelelő adatbázis a tevékenység támogatására.

Az Elektronikai Hadviselés Koordinációs Részleg felelős a Korlátozott Frekvenciák Jegyzékének összeállításáért és egyeztetéséért a Hadműveleti-, a Felderítő-, valamint a Híradó és Informatikai Főnökséggel/Részleggel.

[268] Szerkesztették a szerzők.

A Korlátozott Frekvenciák Jegyzéke alapvető jelentőségű a nem szándékos interferenciák elkerülése érdekében és segítséget nyújt a korlátozottan rendelkezésre álló elektronikai hadviselési erőforrások hatékony alkalmazásában. A jegyzéket a törzseknek folyamatosan pontosítani kell, ami biztosítja a támadó és védelmi jellegű elektronikai hadviselési-, rádióelektronikai felderítő (SIGINT) valamint a vezetési és fegyverirányítási eszközök frekvenciaszükségletét.

A korlátozott frekvenciáknak három kategóriájuk van, amelyeket az elektronikai ellentevékenység irányítása során maximálisan figyelembe kell venni. Ezek a következők:

- *„TILTOTT" frekvenciák (TABOO frequencies):* azok a saját csapatok által használt frekvenciák, amelyeken a zavarás, vagy egyéb szándékos interferenciák létrehozása tilos. Ezeket a frekvenciákat általában az elöljáró adja meg. E frekvenciák közé tartozhatnak például a légvédelmi riasztó rendszerben használt radar és híradó rendszerek frekvenciái, a saját vezetési és irányítási rendszereink frekvenciái, a légvédelmi rakéta irányítási frekvenciák, vagy a kutató-mentő és segélykérő frekvenciák. Ezenkívül e frekvenciák közé tartoznak a nemzetközileg ellenőrzött vagy kormányszerződésben elfogadott frekvenciák is, mint például a műsorszóró frekvenciák vagy a polgári légi és hajózási irányító frekvenciák;
- *„VÉDETT" frekvenciák (PROTECTED frequencies):* azok a saját csapatok által használt frekvenciák, amelyeken a különböző interferenciákat minimálisra kell csökkenteni;
- *„FELÜGYELT" frekvenciák (GUARDED frequencies):* az ellenség által használt frekvenciák, amelyek információforrásként szolgálnak, ezért zavarásukat a felderítő törzzsel mindenkor egyeztetni kell. Az ilyen frekvenciákon csak akkor lehet zavarni, ha a parancsnok mérlegelés után megállapította, hogy nagyobb a zavarással elérhető harcászati, hadműveleti nyereség értéke, mint az elveszett információ jelentősége. Ezek a frekvenciák általában időhöz kötöttek, mivel az ellenség elhelyezkedése és tevékenysége a harc-, hadművelet során változik.[269]

Az elektronikai hadviselés hatékony irányításának és koordinálásának alapvető feltétele a biztonságos, megbízható híradás. Ennek érdekében többcsatornás vezetékes, rádió és rádió-relé összeköttetést kell szervezni:

- a vezetéshez és a technikai kiszolgáláshoz;
- a zavaró tevékenység irányítására;
- tájékoztatásra és értesítésre a felderítők, zavarók és iránymérők között földön és levegőben egyaránt;
- a zavarók közötti együttműködésre;
- a harctevékenységgel kapcsolatos információk továbbítására;
- technikai helyzet jelentésre; illetve a
- szaktevékenység jelentésére.

[269] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, MH kiadvány, p. 13.

Az elektronikai hadviselés hatékonyságát a harctevékenységek során folyamatosan értékelni kell. Az értékelés során – amelyet az Elektronikai Hadviselés Koordinációs Részleg végez – mind a technikai hatékonyságot, mind a szaktevékenységnek az ellenségre gyakorolt általános hatását elemezni kell.

Az elektronikai ellentevékenység hatékonysága csak közvetett módon értékelhető (például forgalmazás, radar kisugárzás megszűnése, frekvenciaváltás észlelése) mivel például a zavarás hatása az ellenség területén elhelyezkedő vevőkben érzékelhető.

Ha az elektronikai támogatás és az ellentevékenység nem érte el a kívánt eredményt, meg kell állapítani annak okát. Újra vizsgálva a zavarandó célokat, megállapítható, hogy újabb zavaróadókat kell e alkalmazni ellenük, vagy célszerűbb a célobjektumok más módon való lefogása (például tűzcsapással történő pusztítása). Ha a sikertelenség oka az elégtelen vagy téves információ, az információ hiány megszüntetése érdekében az elektronikai felderítési követelményeket és prioritásokat felül kell vizsgálni. Az értékelésnek döntő szerepe van a hatékony elektronikai hadviselési tevékenységben. Ez mutat rá az erős és gyenge pontokra, segíti az elkövetkező műveletek szakszerűbb megtervezését és végrehajtását.

6.6 Az elektronikai hadviselés vezetési rendszere

6.6.1 Térinformatikai alapú vezetési rendszer

Az elektronikai hadviselés vezetésének nagy mennyiségű hiteles adatokra, részletesen kiértékelt információkra kell támaszkodnia. Figyelembe véve az információ mennyiségét, a nagyszámú számításokat, a terepnek az elektronikai hadviselésre gyakorolt hatását, a helyzet kiértékelésére és a döntés meghozatalára rendelkezésre álló időt, megállapíthatjuk, hogy az elektronikai hadviselés széles körű feladatainak körültekintő megtervezését, a tevékenységek végrehajtásának hatékony vezetését kizárólag *automatizált vezetéstechnikai eszközökkel* lehet megvalósítani.

Mivel az elektronikai helyzet folyamatosan változik és mindez térben és időben történik, leszögezhetjük, hogy e tényezőknek a figyelmen kívül hagyása alapjaiban befolyásolhatja az elektronikai hadviselés sikerét. A hagyományos vezetési módszerekkel és eszközökkel a terep kiértékelése, az elektronikai felderítésre és zavarásra gyakorolt hatásának figyelembe vétele lehetetlen.

A terep ugyanakkor nemcsak az elektronikai hadviselésre gyakorol hatást, hanem az egész katonai művelet megvívására is. Az alárendeltek részére történő feladatszabás és a tőlük érkező jelentések, valamint a csapatok- és törzsek közötti együttműködés mindmind térbeli adatokon alapulnak. Ezért is van kiemelt jelentősége a harctér felderítő előkészítés során a terep értékelésének.

Az adatok nagy száma, azok pontos kiértékelése és a lerövidült reakcióidő miatt nélkülözhetetlen a különböző felderítési adatok digitális feldolgozása és az így képződött információk terephez, tereptárgyakhoz, vagy objektumokhoz történő kapcsolása. Napjainkban a helyhez kötött információk jelentős mennyisége miatt azok feldolgozására

számítógépen alapuló információs rendszereket használnak. Ilyen információs rendszerek a *térinformatikai rendszerek (GIS)*, amelyeknek legfőbb jellegzetessége, hogy egy adott földrajzi környezethez tartozó és különböző forrásokból származó adathalmazhoz integráló adatbázist, az adatbázis elemeinek és a köztük lévő kapcsolatok elemzéséhez pedig azok kezelésére alkalmas rendszert teremt, lehetővé téve az időbeni változások vizsgálatát is.

A térinformatikai rendszerek alapját a *digitális térkép* képezi, amely különböző rétegekből áll, és amelyek tematikusan magukba foglalják a terepet jellemző objektumokat. A digitális térkép – a hagyományos papírtérképhez hasonlóan szintvonalak formájában tartalmazhatja a terepre vonatkozó magassági adatokat. A különböző magassági adatokkal való műveletek végzéséhez (földfelszínelemzés, láthatóság vizsgálat) azonban a domborzat adatait a *digitális domborzati modell* tartalmazza, mégpedig úgy, hogy az egyes koordinátákhoz tartozó magassági adatokat rácshálózat formájában tárolja, mely rácshálózat méretei az alkalmazástól függően változhatnak.[270]

A digitális térkép és a hozzá kapcsolódó digitális domborzati modell együttesen képezik a térinformatikai rendszerek háromdimenziós, térbeli viszonyítási alapját. A digitális domborzati modell teszi lehetővé a katonai vezetési rendszerek – így az elektronikai hadviselés vezetési rendszere – számára szükséges háromdimenziós elemzéseket, műveleteket, ezen kívül alapját képezheti egyes korszerű fegyverrendszerek irányításának.

6.6.2 Az elektronikai hadviselés vezetési rendszerének adatbázisa

Az elektronikai hadviselés térinformatikai alapú automatizált vezetési rendszerének hatékonysága nagyban függ az adatok mennyiségétől, minőségétől és az adatelemzés hatékonyságától. Ez azt jelenti, hogy az adatok tárolása és azok kezelése kiemelt jelentőségű a pontos helyzetértékelés szempontjából. Az elektronikai hadviselés térinformatikai adatbázisa egy *grafikus adatbázisból*, illetve a grafikus adatbázis megfelelő rétegeihez kapcsolódó *leíró adatbázisból* áll. *A grafikus adatbázis* alapját a digitális térkép és a digitális domborzati modell képezi. A digitális térkép és a digitális domborzati modell adja azt az egységes viszonyítási rendszert, amely alapján az elektronikai hadviselés vezetése és tágabb értelemben a különböző törzsek közötti együttműködés (adatok, helyzetértékelési eredmények cseréje) és a hadművelet vezetése megvalósul.

A grafikus adatbázis elemei közé sorolhatók az ellenség alkalmazásának elvi vázlatai is, amelyek a harctér felderítő előkészítése és az elektronikai helyzetértékelés során kiinduló adatokként kerülnek felhasználásra.

Ezen kívül a grafikus adatbázisba tartoznak azok a felderítés és a hadműveleti helyzet alakulásának függvényében *folyamatosan változó,* úgynevezett *aktuális grafikus adatok*, amelyek csak az adott műveletre érvényesek. Ezen adatoknak a tereppel és az elvi vázlatokkal való összevetése alapján készíthetők el azok a helyzet-, esemény- és a döntés-

[270] Detrekői, Á. – Szabó, Gy.: *Bevezetés a térinformatikába*. Nemzeti tankönyvkiadó, 1995. p. 250.

támogató vázlatok, amelyekről a harctér felderítő előkészítésének tárgyalása során már szóltunk, és amelyek az elektronikai helyzetértékelés kiinduló elemeit képezik. A grafikus adatbázis említett elemei rétegenként kerülnek megjelenítésre.

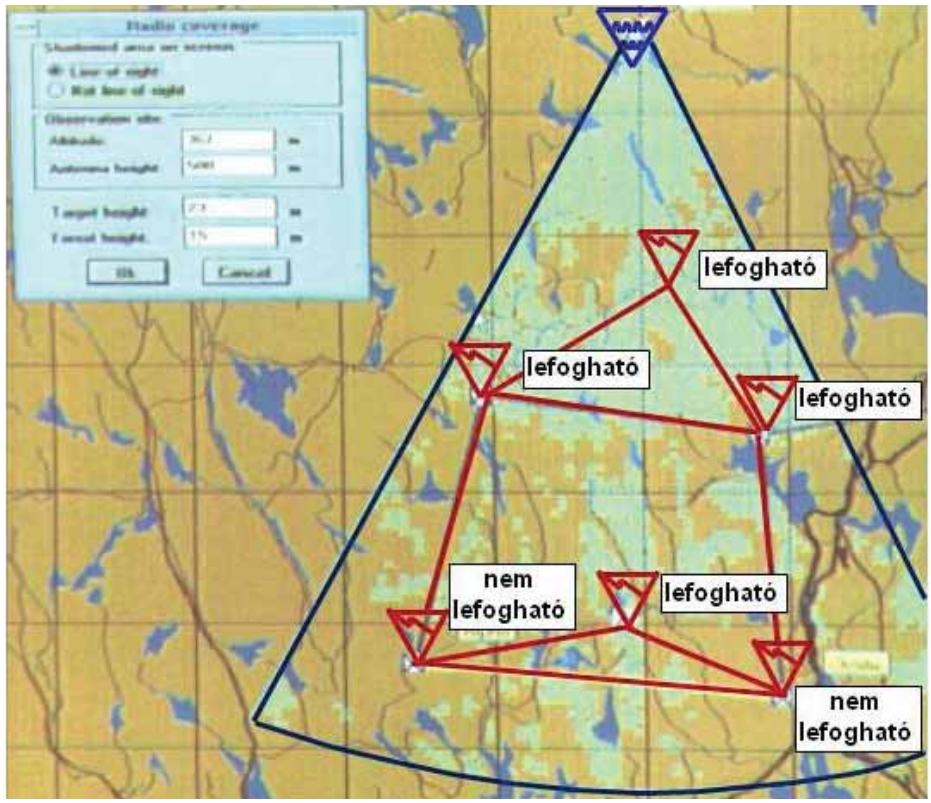
A grafikus adatbázishoz kapcsolódó *leíró adatbázis* tartalmazza minden olyan elektronikai eszköz adatait, amelyeket az elektronikai hadviselés vezetése, azon belül a tervezés, helyzetértékelés során figyelembe kell venni, illetve amelyekkel különféle számításokat, számvetéseket kell végezni. Az adatbázisban egyrészt a *saját elektronikai eszközeink adatait*, másrészt az *ellenség elektronikai eszközeinek adatait* kell tárolni, illetve az adott műveleti helyzetnek megfelelően aktualizálni.

A nagyvonalakban felvázolt grafikus és leíró adatbázis önmagában még nem biztosítja az elektronikai hadviselés tervezésének térinformatikai alapú végrehajtását. A térinformatika nyújtotta előnyöket az elektronikai hadviselés vezetése vonatkozásában csak úgy lehet érvényesíteni, ha a térinformatikai alapú adatbázis kezelésen kívül a tervezéshez felhasználunk különböző matematikai számításokat, illetve számvetéseket. Minél szélesebb körben támaszkodunk a matematikai modellre, annál inkább elvárható, hogy a helyzetértékelés eredményei a valóságot fogják tükrözni.

6.6.3 Az elektronikai hadviselés vezetési rendszerével szembeni követelmények

Az előzőekben leírtakat is figyelembe véve, a térinformatikai alapú elektronikai hadviselés vezetési rendszerrel szemben a következő követelmények fogalmazhatók meg:

- az adatbázisban tárolt adatok alapján határozza meg az ellenség elektronikai objektumainak mennyiségét egy adott területre vonatkoztatva (elektronikai objektum számvetés). Az adott terület lehet a teljes hadműveleti terület, az érdekeltségi terület, a főerőkifejtés vagy a főcsapás iránya, vagy bármilyen egyéb terület (sáv, szektor). Ezen belül legyen képes az elektronikai objektumok rendeltetés szerinti csoportosítására;
- az egyes elektronikai objektumokban jelenítse meg az ott lévő elektronikai eszközöket;
- egy adott elektronikai objektumról „felfűzhetők” legyenek az adott objektum belső rádióforgalmi rendszerei (például dandár harcálláspont belső RH és URH rádióforgalmi rendszereinek felépítése). Az eredmények mind grafikusan, mind táblázatos formában megjeleníthetők legyenek;
- az elektronikai eszközöket (objektumokat) legyen képes különböző szempontok szerint szelektálni és összegezni (például frekvencia, teljesítmény, hovatartozás) majd az eredményeket megjeleníteni;
- az URH és a rövidebb hullámhosszokon felderítés és zavarás vonatkozásában végezzen terepanalízist (terepfedettség, átláthatóság vizsgálat). Egy adott pontról vizsgálva meghatározott mélységig, – egyrészt az egyenes láthatóság alapján, másrészt az elektronikai láthatóság figyelembevételével – jelenítse meg a látható és a nem látható területeket; (6.9. ábra)



6.9. ábra. **Célobjektumok pontosítása terepanalízis alapú láthatóság vizsgálattal**[271]

- az ellenség elektronikai objektumainak rendszere-, a láthatóság vizsgálat eredménye- és az eszközök telepítési elvei alapján javasoljon optimális települési körzeteket az elektronikai támogató (felfedő, iránymérő, lehallgató) és zavaró állomások számára;
- az adatbázisban lévő technikai eszközök viszonylatában számoljon felderítési és zavarási távolságokat, mind az ellenség, mind a saját erők vonatkozásában;
- a különböző irányokban a jellemző paraméterekkel elvégzett felderítési és zavarási távolság számítások alapján, a terep domborzati viszonyai és a harcrend figyelembevételével, ábrázolja a felderítéssel és zavarással lefedhető zónákat;
- az ellenség meghatározott összeköttetési viszonylataira a zavaróállomások települési helyei figyelembevételével számítsa ki a le nem fogható zónákat, és ezeket jelenítse meg;

[271] Szerkesztették a szerzők.

– az iránymérő állomások települési helyei (iránymérési alap) és a rádiófelderítés fő iránya alapján határozza meg a pontos iránymérés zónáját. Ez alapján tegyen javaslatot az iránymérő állomások telepítési helyeinek esetleges módosítására;
– az elektronikai támogató- és a zavaró állomások települési helyei alapján, a frekvenciatartományok, hatótávolságok, elektronikai láthatóság figyelembevételével válogassa le az ellenség elérhető (felderíthető és lefogható) elektronikai eszközeit, majd ez alapján pontosítsa az elektronikai támogatás és a zavarás célobjektumait (HPT-k); (6.9. ábra)
– a harcrend, a célobjektumok és elektronikai eszközök elhelyezkedése, frekvencia-tartományok, hatótávolság és elektronikai láthatóság alapján a hadműveleti feladat függvényében készítsen feladatelosztást a felderítő és zavaró munkahelyekre. Az eredményeket az elektronikai hadviselési céllistákban és zavarási tervekben jelenítse meg;
– az ellenség és a saját felderítési és zavarási lehetőségek figyelembevételével, az ellentétes rendeltetésű eszközök szembeállításával készítsen elektronikai erőviszony számvetést;
– állásváltások, áttelepülések tervezésekor – figyelembe véve az eszközök telepítési és bontási idejét és a menettávolságot – készítsen manővertervet. Ezen belül határozza meg a technikai eszközök által járható legrövidebb útvonalat;
– az elektromágneses kompatibilitás biztosítása érdekében a frekvenciatartomány, a teljesítményviszonyok, az antenna paraméterek és a terepdomborzat figyelembevételével számítsa ki az elektronikai eszközök közötti minimális telepítési távolságokat, az eredményeket jelenítse meg;
– készítsen számvetést a passzív elektronikai zavaró eszközök alkalmazására, szögvisszaverők telepítésére az ellenség földi mozgócél felderítő lokátorainak paraméterei, illetve az álcázandó terület (útvonalszakasz, terepszakasz, hídátkelő) figyelembevételével;
– a tervezés eredményeként tegye lehetővé intézkedések, harcintézkedések, szöveges tervek, jelentések, esemény és döntéstámogató vázlatok meghatározott formában történő elkészítését, a parancsok, intézkedések eljuttatását a végrehajtókhoz, valamint szükség esetén papírtérkép készítését.[272,273]

6.6.4 Az elektronikai hadviselés vezetési rendszerének felépítése, kapcsolatai

Az elektronikai hadviselés vezetési rendszere nem egy önállóan működő rendszer, hanem szervesen kapcsolódik a többi törzs hasonló felépítésű rendszeréhez, és így az adott szintű parancsnokság vonatkozásában egységes összfegyvernemi (összhaderőnemi) ve-

[272] Detrekői, Á. – Szabó, Gy.: *Bevezetés a térinformatikába*. Nemzeti tankönyvkiadó, 1995. p. 250.
[273] Graham, A.: *Communications, Radar and Electronic Warfare*. Wiley Publications, 2011. p. 397.

zetési rendszert alkotnak. Külön ki kell hangsúlyozni az elektronikai hadviselés vezetési rendszer kapcsolatát az összadatforrású felderítő rendszer adatfúziós feldolgozó alrendszerével.

Az elektronikai hadviselés vezetési rendszerének párhuzamosan kettős feladatot kell megoldani. Egyrészt *harcvezetési rendszerként*, másrészt pedig *információ feldolgozó, kiértékelő és döntés-előkészítő rendszerként* kell funkcionálnia. A két rendszer ugyanabban a hardver és szoftver környezetben fut. Ez azt jelenti, hogy mind a műveletek előkészítésének időszakában, mind a harc, hadművelet megvívása során alkalmasnak kell lennie adatok fogadására, azok kiértékelésére, ezáltal a mindenkori aktuális helyzet folyamatos karbantartására. Ezenkívül képesnek kell lennie megfelelő protokollon keresztül kapcsolódnia az összhaderőnemi/összfegyvernemi vezetési rendszerhez. Ezáltal biztosítható az adatok és információk egységes viszonyítási rendszerben (digitális térkép) való cseréje, a mindenkori helyzet egységes értelmezése, illetve az adatbázisokhoz való hozzáférés.

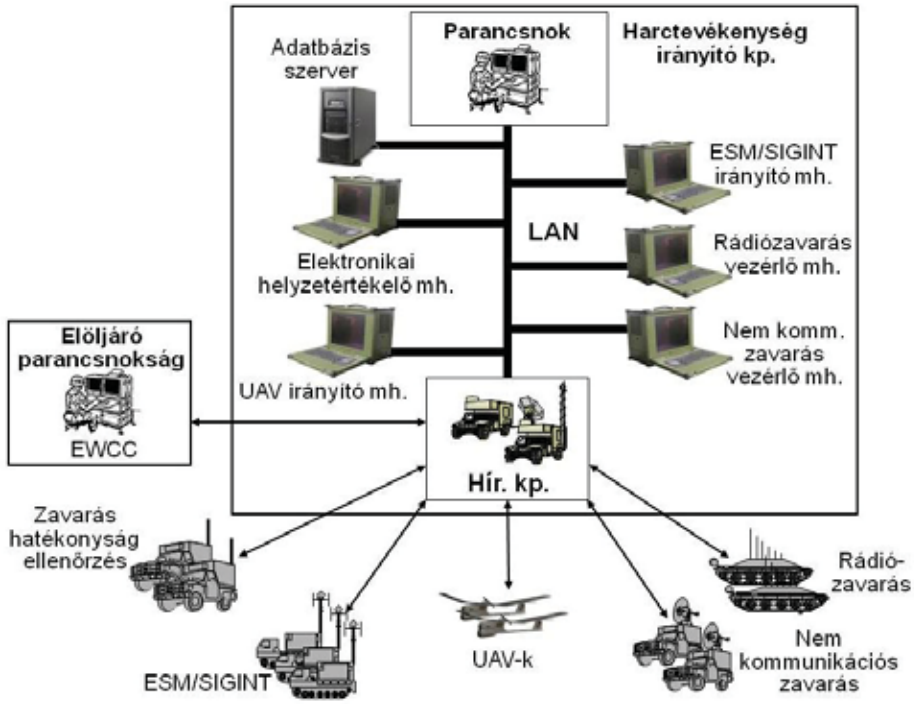
Az összhaderőnemi/összfegyvernemi törzs helyi hálózatához kapcsolódó elektronikai hadviselés vezetési rendszer maga is több munkahelyes helyi hálózat formájában épül fel. Ez lehetővé teszi a tervező munka során jelentkező szerteágazó értékelő-elemző tevékenységek párhuzamos végzését. Minden értékelő-elemző hozzáfér a rendszer adatbázisához, mely lehetővé teszi az elemzések során összefüggő grafikus és alfanumerikus adatok kiértékelését, szelektálását, a számítások, számvetések elvégzését és az eredmények rétegenkénti létrehozását.

A rendszer biztosítja a harctér felderítő előkészítése során kidolgozott, és az elektronikai hadviselés tervezéséhez – azon belül a helyzetértékeléshez – elengedhetetlen elvi-, helyzet-, esemény- és döntéstámogató vázlatokhoz való hozzáférést.

Az elektronikai hadviselés vezetési rendszeréhez vezeték nélküli adatcsatornán keresztül kapcsolódnak az alárendelt elektronikai hadviselési erők. Az alárendelt elektronikai hadviselés erők parancsnoka ezen keresztül kapja a harcfeladatokat és egyéb információkat, illetve ezen keresztül jelenti a feladat végrehajtását. Az alárendelt elektronikai hadviselési csapatok vezetési rendszerének és kapcsolatainak egy lehetséges változatát a szárazföldi haderőnem vonatkozásában a 6.10. ábra szemlélteti.

Az alárendelt elektronikai hadviselés erők szintén egy több munkahelyes helyi hálózattal rendelkeznek, ahol a kapott parancsok feldolgozása és az alárendeltek részére a feladatszabás történik. Ezen a szinten történik a harcfeladatok elosztása a felfedő, iránymérő és zavaró csoportok számára, a feladatszabás, az adatok előzetes feldolgozása, szűrése, a jelentések adatainak összeállítása, döntés-előkészítés a parancsnok részére.

A vezetési ponton belül létrehozott hálózatra kapcsolódik a parancsnok, ahonnan képes az elektronikai támogatás és az elektronikai ellentevékenység folyamatos irányítására. A hálózat további elemét képezi az elektronikai helyzetértékelő központ, amely folyamatosan nyilvántartja az aktuális elektronikai helyzetet, és elvégzi a harcászati- és forgalmi elemzéseket, valamint a technikai jelanalizálást. Az elektronikai támogatást és az elektronikai ellentevékenységet vezérlő munkahelyek szintén a vezetési ponton kapcsolódnak a hálózatra. Ezekről a központokról történik kommunikációs és a nemkommunikációs felderítés és zavarás, valamint a pilótanélküli felderítő repülőeszközök közvetlen irányítása pozitív irányítási módszert alkalmazva.



6.10. ábra. **Az elektronikai hadviselést végrehajtó erők vezetési rendszerének kapcsolatai**[274]

Az adatszerző és a zavaró munkahelyek rádiócsatornán keresztül csatlakoznak a vezetési pont hírközpontjába és azon keresztül az elektronikai támogatást és az elektronikai ellentevékenységet vezérlő munkahelyekhez.

Az elektronikai hadviselés fent ismertetett vezetési rendszerének felépítése egy általános változat, mely azonban eleget tesz a vele szemben megfogalmazott követelményeknek.

[274] Szerkesztették a szerzők.

FELHASZNÁLT IRODALOM

1 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról. Honvédelmi Közlöny, 2013. október 19., CXL. Évfolyam 10. sz., 1125. o., Magyar Közlöny Lap- és Könyvkiadó
2 AAP-6 NATO Glossary of Terms and Definition, NATO Standardization Agency, Brussels, 2006.
3 AJP-2.0 Szövetséges Összhaderőnemi Felderítő, Felderítés elleni védelem, és Biztonsági Doktrína, NATO HQ, Brüsszel, 2002
4 AJP-3.10 Allied Joint Doctrine for Information Operations, 2009.
5 Alberts, D. S. – Garstka, J. J. – Stein, F. P. *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series, Washington, 1999, ISBN 1-57906-019-6
6 Ált-4/457 A Magyar Honvédség Törzsszolgálati Szakutasítása. A Honvéd Vezérkar Hadműveleti Csoportfőnökség kiadványa
7 AN/ALQ-161A Defensive Avionics System http://www.fas.org/man/dod-101/sys/ac/equip/an-alq-161.htm (Letöltve: 2014.02.12.)
8 AN/ALQ-172 Countermeasures System (CMS) http://www.fas.org/man/dod-101/sys/ac/equip/an-alq-172.htm (Letöltve: 2014.02.12.)
9 AN/AQS-22 ALFS Sonar System (Letöltve: 2014.02.14.) https://www.defenseindustrydaily.com/154m-for-3-aqs-22-alfs-sonars-et-al-03643/
10 AN/TSC-93A and AN/TSC-93B Satellite Communications Terminals. https://www.fas.org/spp/military/program/com/an-tsc-93.htm (Letöltve: 2014.02.12.)
11 Balajti István, Vass Sándor. *Elektronikai védelem*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, Elektronikai Hadviselés Tanszék, J-1435. 2000.
12 Bourque, J. *The Language of Engagement and the Influence Objective*. The Journal of Electronic Defense, Vol. 30. No.11. pp. 30-35, November 2007, ISSN 192429X
13 Dr Carlo Kopp: Air Defence System Defensive Aids, Technical Report APA-TR- 2009-0604, June 2009, updated April, 2012 (Letöltve: 2014. 02.14.) http://www.ausairpower.net/APA-SAM-DefAids.html
14 Chopin, Ted – *Tradoc System Manager, Information Briefing* (Letöltve: 2014.01.15.) http://www.fas.org/irp/program/process/ASASBRF/sld009.htm
15 Davenport, T.H., Pusak, L.: *Tudásmenedzsment*, Kossuth, Budapest, 2000.
16 Detrekői Ákos, Szabó György: *Bevezetés a térinformatikába*. Nemzeti tankönyvkiadó, 1995. p. 250, ISBN: 9631883973
17 Elsworth, Adam T. ed.: *Electronic Warfare*. Nova Science Publishers, Inc. New York, 2010, p. 193, ISBN 978-1-61324-541-5
18 EMC villámvédelem és túlfeszültség-védelem V. rész (Letöltve: 2014. 01.23.) http://epa.oszk.hu/00000/00025/00001/feher.html
19 Fahrenkrug, D. T.: *Cyberspace Defined* (Letöltve: 2014.03.09.) http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm

20 Fenyves Péter: *A rádióelektronikai felderítés és az elektronikus célobjektum – tervezés hatékonyságának növelését biztosító fúziós elven alapuló adatfeldolgozási technológia vizsgálata* – kandidátusi értekezés, Budapest, 1994. p.45.
21 Ferenczi, G. – Szűcs, P. – Balog, K.: *Rádiólokáció alapjai*. Bolyai János Katonai Műszaki Főiskola, Budapest, p. 50, 1998.
22 FM 2-01.3 Intelligence Preparation of the Battlefield/Battlespace Department of the Army, 2009.
23 FM 24-33 Communications techniques: electronic counter-countermeasures http://www.globalsecurity.org/intell/library/policy/army/fm/24-33/fm243_2.htm (2014.01.23.)
24 FM 3-36, Electronic Warfare, Department of the Army, 2012.
25 Frater, Michael R. – *Electronic Warfare for the Digitized Battlefield*. Artech House, 2001, p. 270, ISBN: 1-58053-271-3
26 Gander. http://jproc.ca/rrp/gander.html (Letöltve: 2014.02.15.)
27 Géher, K. főszerk.: *Híradástechnika*. 2. kiadás. Műszaki Könyvkiadó, Budapest, 2000. p. 109. ISBN 963 16 3065 X
28 Graham, Adrian: *Communications, Radar and Electronic Warfare*. Wiley Publications, 2011, p. 397, ISBN. 9780470688717
29 Haig Zsolt, Fürjes János, Kovács László, Vass Sándor, Ványa László: *Felderítés hatékonyság minősítő eljárás kidolgozása: Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett integrált elektronikai felderítő és zavaró rendszerhez*, ZMNE, Budapest, 2008.
30 Haig Zsolt, Kovács László, Vass Sándor, Ványa László: *Felderítési és zavarási technikák vizsgálata: Tanulmány a Jedlik Ányos Program – 2. alprogram: Versenyképes Ipar NKFP_07_2-HT28_SAJ program keretében kidolgozásra tervezett integrált elektronikai felderítő és zavaró rendszerhez*, ZMNE, Budapest, 2008.
31 Haig, Zs. – Kovács, L. – Munk, S. – Ványa, L.: *Az infokommunikációs technológia hatása a hadtudományokra*. Nemzeti Közszolgálati Egyetem, 2013, ISBN: 978-615-5305-02-3
32 Haig, Zs. – Várhegyi I.: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005, ISBN 963-327-391-9
33 Haig, Zs. – Várhegyi, I.: *A cybertér és a cyberhadviselés értelmezése*. Hadtudomány, elektronikus szám pp. 1-12, 2008, ISSN 1215-4121 (Letöltve: 2014.03.09.) http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf
34 Hálózati szűrők (Letöltve: 2014.01.23.) http://cmswebdav.weidmueller.de/cms/gu_hu/letoltesek/katalogusok/Tulfeszultseg/E_Halozati%20szurok.pdf
35 Hóka, M.: *The Tactical Internet*. AARMS, Volume 2, Issue 2. pp. 271-282, MZNDU, Budapest, 2003, ISSN 1588-8789
36 Holdaway, E. J.: *Active Computer Network Defense: An Assessment*. Air Command and Staff College. Maxwell Air Force Base, Alabama, 2001.
37 Holics, L. szerk.: *Fizika*. Műszaki Könyvkiadó, Budapest, 1986. pp. 352-354. ISBN 963 10 7148 0
38 Illés Attila: *Lehetőségek a radarok ESM eszközök elöli rejtettségének növelésére* http://www.zmne.hu/tanszekek/ehc/konferencia/may/illes.htm (Letöltve: 2014.02.14.)

39 Istvánffy, E.: *Tápvonalak, antennák és hullámterjedés*. Tankönyvkiadó, Budapest, 1984. pp. 584-588.
40 John Frank: *Honing in Trouble*. New Geosearch software accelerates comprehensive intelligence analysis. ISR, 2003 september-october
41 Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms 2010.
42 Joint Publication 3-13, Information Operations, 27 November 2012, by United States Government US Army
43 Joint Publication 3-13.1, Electronic Warfare, 08 February 2012, by United States Government US Army
44 Joint Publication 3-60, Joint Targeting, 31 January 2013, by United States Government US Army
45 JP 6-02: A Hadműveleti/Harcászati Vezetési, Irányítási, Kommunikációs és Számítógépes Rendszerek Alkalmazásának Alapelvei, NATO HQ, Brüsszel, KIADÁS ÉVE????
46 Juhász József (szerk.): *Magyar Értelmező Kéziszótár*, Akadémiai Kiadó, Budapest, 1972.
47 Kovács László: *Az elektronikai felderítés korszerű eszközei, rendszerei és azok alkalmazhatósága a Magyar Honvédségben*. Doktori (PhD) értekezés, ZMNE, Budapest, 2003.
48 Kuehl, D.: *From Cyberspace to Cyberpower: Defining the Problem*. In: Cyberpower and National Security. ed. Kramer, F. D. et al., Potomac Books Inc. pp. 24-43, 2009, ISBN-10: 1597974234
49 Levityin, I.B.: *Infravörös sugárzástechnika*. Műszaki Könyvkiadó, Budapest, 1962.
50 Light-Weight Camouflage Screen System (Letöltve: 2014.01.23.) http://www.fas.org/man/dod-101/sys/land/lccs.htm
51 Magyar Értelmező Kéziszótár, szerk.: Juhász József, Akadémiai Kiadó, Budapest, 1972.
52 Magyar Honvédség Összhaderőnemi Doktrína 3. kiadás, 2012, A Magyar Honvédség kiadványa
53 Magyar Honvédség Összhaderőnemi Doktrína, HM, HVK, HCSF, 2002.
54 Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrína. Budapest, Honvédelmi Minisztérium Honvéd Vezérkar Felderítő Csoportfőnökség, 2005. MH DSZOFT kód: 11216
55 Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína 1. kiadás, 2004, A Magyar Honvédség kiadványa
56 Magyar Honvédség Összhaderőnemi Műveleti Doktrína 1. kiadás, 2013, A Magyar Honvédség kiadványa
57 Makraduli, Mario: *Direction Finding*. http://www.dtk.gov.mk/Portals/57ad7180-c5e7-49f5-b282-c6475cdb7ee7/INA_DF_makraduli.ppt (Letöltve: 2014.01.28.)
58 MC 422/3 NATO Military Policy on Information Operations
59 Munk Sándor: *A közös munkavégzés új lehetőségei a virtuális vezetési pontokon*. Új Honvédségi Szemle, 2000/2.
60 Munk, S.: *Az információs fölényről*. Hadtudomány, XI. évf. 3. sz. pp. 43-52, 2001, ISSN 1215-4121
61 Palij, A. I.: *Radioelektronnaja Borba*. Voennoje Izdatyelsztvo, Moszkva, 1989. ISBN 5-203-00176-6

62 Purdy, R. W. H.: *A hatásalapú műveletek áttétele a gyakorlatba*. Nemzetvédelmi Egyetemi Közlemények, 9. évf. 4. sz. pp. 9-16, ZMNE, Budapest, 2005, ISSN 1417-7323
63 QuickCam – Camouflage System. (Letöltve: 2014.01.23.) http://www.saabgroup.com/en/Land/Force_Protection/Signature_management/Static_Camouflage/Camouflage_Systems/Quick_Cam_camouflage_system/Features/
64 Rádiómérő módszerek és eljárások a Nemzeti Hírközlési Hatóság gyakorlatában http://meres.nhh.hu/u/document/200606/Korszeru_radiomeresek_az_NHH_gyakorlataban_6.pdf (Letöltve: 2014.02.20.)
65 Raytheon and US Navy begin MALD-J Super Hornet integration http://rpdefense.over-blog.com/article-raytheon-and-us-navy-begin-mald-j-super-hornet-integration-107847534.html (Letöltve: 2014.02.14.)
66 Rohde-Schwarz. *Radiomonitoring and Radiolocation*. Products catalog 2003/2004.
67 Seiferth, G.: *Hatásalapú információs műveletek*. Nemzetvédelmi Egyetemi Közlemények, 9. évf. 4. sz. pp. 17-23, ZMNE, Budapest, 2005, ISSN 1417-7323
68 Self-standing modular Faraday cage (Letöltve: 2014.01.23.) http://www.shieldingsystems.eu/index.php?p=Nieuws&id=159&Lang=2&gclid=COGyscOF-7oCFUiN3godAA8AHg
69 Ványa László: *Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre*. Doktori PhD értekezés. ZMNE, Budapest. 2002.
70 Várhegyi, I. – Makkay, I.: *Információs korszak, információs háború, biztonságkultúra*. OMIKK, Budapest, 2000, ISBN 963-593-238-3
71 Vass Sándor: *A Magyar Honvédségben az elektronikai harc – ezen belül az elektronikai védelem – számítógépekkel biztosított tervezése, különös tekintettel az elektromágneses kompatibilitás kérdéseire*. Budapest, Zrínyi Miklós Katonai Akadémia, kandidátusi értekezés.1995.
72 http://commons.wikimedia.org/wiki/File:Parabolic_antenna_types2.svg (Letöltve: 2014. 02. 14.)
73 http://htka.hu/2010/04/28/sajat-infracsapdaja-rongalt-meg-egy-ausztral-oriont/ (Letöltve: 2014.02.14.)
74 http://indolinkenglish.wordpress.com/2012/04/30/india-developing-anti-radiation-missile/ (Letöltve: 2014.02.14.)
75 http://jegyzet.sth.sze.hu/ftp/!Muinfo/!Felsobb_eves/Szakiranyos/_Kozlekedesi_szakirany/Technika.III/kt3.4.doc (Letöltve: 2014.02.18.)
76 http://punjab-pk.all.biz/prc-2505-vhf-frequency-hopping-transceiver-g35887#show0 (Letöltve: 2014.04.20.)
77 http://wiki.ham.hu/index.php/Oldals%C3%A1v (Letöltve: 2014.02.06.)
78 http://www.arbenelux.com/images/ETS_LogPer.jpg (Letöltve: 2014. 02. 06.)
79 http://www.ausairpower.net/XIMG/empfootprint.gif (Letöltve: 2014.02.14.)
80 http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm (Letöltve: 2014.03.09.)
81 http://www.dnjradio.com///images/sy4.jpg?osCsid=0a0cc1a017e479f98bee2001185d17f3 (Letöltve: 2014. 02. 06.)
82 http://www.fas.org/man/dod-101/sys/land/lccs.htm (Letöltve: 2014.01.23.)

83 http://www.fas.org/programs/ssp/man/uswpns/air/special/ec130.html (Letöltve: 2014.02.12.)
84 http://www.honvedelem.hu/cikk/35068_3d-s_radar_kisebb_energia_nagyobb_teljesitmeny (Letöltve: 2014.02.12.)
85 http://www.itu.int/osg/spuold/ni/images/codedivision.gif (szerzői szerkesztés)
86 http://www.lionhearth.com/VCP (Letöltve: 2014.01.23.)
87 http://www.npostrela.com/ru/products/75/567/ (Letöltve: 2014.02.12.)

ÁBRAJEGYZÉK

RÖVIDÍTÉSEK JEGYZÉKE

ABCS	Army Battlefield Command System
ACINT	Acustic Intelligence
AEW	Airborne Early Warning
AGM	Attack Guidance Matrix
ALE	Automatic Link Establishment
AM-DSB	Amplitude Modulation Double Sideband
AM-DSB/SC	Amplitude Modulation Double Sideband Suppressed Carrier
AM-SSB/SC	Amplitude Modulation Single Sideband Suppressed Carrier
ARM	Anti-radiation Missile
ASAS	All-Source Analysis System
ASK	Amplitude Shift Keying
ATM	Asyncronous Transfer Mode
AWACS	Airborne Warning and Control System
BIL	Band Interleaved by Line
C2	Command and Control
C4ISR	Command, Control, Communication, Computer, and Intelligence, Surveillance, Reconnaissance
CDMA	Code Division Multiple Access
CI/FP	Counter Intelligence and Force Protection
CIMIC	Civil-Military Cooperations
CIS	Communication and Information System
CMS	Countermeasures System
CNO	Computer Network Operations
COA	Course of Action
COMINT	Communication Intelligence
CW	Continuous Wave
DARPA	Defense Advances Researches Programme Agency
DBS	Direct Broadcasting Satellite
DDL	Dispersive Delay Line
DdoS	Distributed Denial of Service
DEC	Deception
DEW	Directed Energy Weapons
DS	Direct Sequence
ECM	Electronic Counter Measures
EH	Előretolt Harcálláspont
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMS	Electro-magnetic Susceptibility

EP	Electronic Protection
EPB	Electronic Preparation of the Battlefield
EPM	Electronic Protective Measures
ESM	Electronic Support Measures
EW	Electronic Warfare
EWCC	Electronic Warfare Coordination Cell
FDMA	Frequency Division Multiple Access
FFH	Fast Frequency Hopping
FFT	Fast Fourier Transformation
FH	Frequency Hopping
FISINT	Foreign Instrumentation Signals Intelligence
FSK	Frequency Shift Keying
FVP	Fő Vezetési Pont
GIS	Geographical Information System
GLONASS	GLObal'naya NAvigatsionnaya Sputnikovaya Sistema
HPT	High Payoff Targets
HPTL	High Payoff Target List
HTML	Hyper Text Markup Language
HUMINT	Human Intelligence
HVT	High Value Targets
IEW	Intelligence and Electronic Warfare
IMINT	Imagery Intelligence
INFOSEC	Information Security
IPB	Intelligence Preparation of the Battlefield
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
KLE	Key Leader Engagement
LASER	Light Amplification by Stimulated Emission of Radiation
LCSS	Lightweight Comouflage Screen System
LHK	Légi Hadműveleti Központ
LMKK	Légi Műveletek Koordinációs Központ
LOB	Line of Bearing
LPI	Low Probability of Interception
LPIR	Low Probability of Intercept Radar
LQA	Link Quality Analysis
MALD	Miniature Air-Launched Decoy
MASINT	Measurements Intelligence
MAWS	Missile Approach Warning System
MI	Military Intelligence
MIC	Military Intelligence Commander
MILDEC	Military Deception
MOVCS	Mozgó Vezetési Csoport
MTD	Moving Target Detector
MTI	Moving Target Indicator

MUSIC	Multiple Signal Classification
MVP	Mögöttes Vezetési Pont
MVR	Műveleti Vezetési Rendszer
NAC	North Atlantic Council
NAVSTAR GPS	NAVigation System using Time And Ranging
NBFM	Narrow Band Frequency Modulation
OPSEC	Operation Security
OSINT	Open Source Intelligence
ÖHP	Összhaderőnemi Parancsnokság
PAM	Pulse Amplitude Modulation
PD	Physical Destruction
PFM	Pulse Frequency Modulation
PI	Public Information
PN	Pseudo Noise
PPM	Pulse Position Modulation
PPP	Presence, Posture and Profile
PSK	Phase Shift Keying
PSYOPS	Psychological Operations
PWM	Pulse Width Modulation
RADAR	RADio Detection And Ranging
RADINT	Radar Intelligence
RC-IED	Radio Controlled Improvised Explosion Devices
RFL	Restricted Frequency List
RGB	Red-Green-Blue
SDR	Software Defined Radio
SEAD	Suppression of Enemy Air Defence
SEWOC	Signal Intelligence and Electronic Warfare Operations Centre
SFH	Slow Frequency Hopping
SIGINT	Signal Intelligence
SLC	Side Lobe Cancellation
SST	Spread Spectrum Technologies
TALD	Tactical Air-Launched Decoy
TCP/IP	Transmission Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TECHINT	Technical Intelligence
TH	Time Hopping
TI	Tactical Internet
WBFM	Wide Band Frequency Modulation