Haig Zsolt - Várhegyi István

A cybertér és a cyberhadviselés értelmezése[1]

A szerzők e cikkben bemutatják a hadviselés egy új színterét a cyberteret, és a cyberhadviselést. Az új fogalmak megismerése kedvező helyzetet teremt ahhoz, hogy felismerjük és megértsük a hadtudomány fejlődésének egyik új irányát. A cybertér és az abban folyó műveletek meghatározó hatással lesznek a társadalomra és a hadügyre egyaránt.

In this article the authors present the cyberspace as a new scene of warfare, and the cyberwarfare. The cognition of these new concepts creates a favorable situation, to recognize and understand one of the new trend of development of military science. The cyberspace and cyberwarfare will be a determining effect onto the society and military operations.

A cybertér katonai értelmezése

A haderő híradásának digitalizálása hozzájárult, majd viszonylag gyors átmenetet tett lehetővé először a vezetékes, majd a vezeték nélküli számítógép–hálózatok elterjedéséhez. Ezzel forradalmi átalakulás következett be a katonai vezetésben. Ettől kezdve a döntések előkészítését és a hadműveletek vezetését igen nagy teljesítményű, egymással hálózatba kapcsolt számítógépek támogatták. A számítógép-hálózatok harctéri megjelenésének köszönhetően napjainkban már számos olyan tényezőt lehet figyelembe venni, amelyek változó mértékben, de folyamatosan befolyásolják és alakítják a hadműveleti és harci helyzetet.

A katonai híradásban a digitális jelátvitelre történő gyorsütemű áttérés, továbbá a fedélzeti számítógépek miniatürizálásának eredményeképpen megjelentek a precíziós, nagy találati pontossággal rendelkező fegyverek és fegyverrendszerek, amelyek alapvetően megváltoztatták a hadviselés módozatait, lefolytatásának ütemét, és sebességét.

Napjaink nagy intenzitású katonai műveletei megkövetelik, hogy a szárazföldi csapatokat a levegőből, az űrből és a tengerről egyidejűleg és a távoli körzetekből egyaránt támogassák. Ehhez viszont olyan, egymással haderőnemi szinten is összekapcsolt számítógép–hálózatokra van szükség, amelyek e támogatást lehetővé teszik. E harctéri számítógép–hálózatok jelentős szerepet töltenek be a vezetés támogatásában. Alkalmazásuk jelentős lépéselőnyt biztosít a másik féllel szemben, az információs fölény és a vezetési fölény gyors kivívásában és tartós megőrzésében. [1]

A védelmi szektorban az információ felhasználása két nagy területre osztható: egyrészt az információt, mint a vezetés eszközét használják fel a hadviselésben, másrészt az információt, mint un. nem kinetikus energiát felhasználó „fegyvert” alkalmazzák az információs műveletekben. Mindkét felhasználásra jellemző — a szembenálló fél feletti információs fölény és vezetési fölény kivívása érdekében — az információs technológia vívmányainak jelentős mértékű kihasználása.

Az információs fölény elérése és megtartása szorosan függ a különböző szenzorok, felderítő eszközök és rendszerek minőségétől, a vezetési folyamat gyorsaságától, a végrehajtó erők képességeitől és az eszközök egységes hálózatba kapcsolásától. Mindez egy új típusú katonai vezetési filozófiát jelent, melyet hálózatközpontú hadviselésnek (Network Centric Warfare - NCW) — NATO terminológia szerint hálózat nyújtotta képességnek (Network Enabled Capability – NEC) — neveznek. Eszerint az erőforrások kihasználása sokkal hatékonyabb, ha a rendszerek egymással összekapcsolva működnek, egyes erőforrásokat megosztva használnak, mintha önállóan, elkülönülve léteznének. A koncepció lényege, hogy a katonai műveletekben résztvevők valós időben, a megfelelő tartalomban és felhasználható formában képesek hozzáférni a feladatuk végrehajtásához szükséges valamennyi fontos információhoz. Ez az új felfogású hadviselési forma a szenzorrendszereknek, a parancsnokok, illetve a végrehajtók kommunikációs és információs rendszereinek ugyanazon hálózatba integrálásával megnöveli a harci erőt és képességet. [1]

Az információs fölény kivívásához azonban nem elegendő a legkorszerűbb katonai infokommunikációs rendszerek vezetésben való alkalmazása, vagyis a hálózat nyújtotta képességek

[1] A cikk a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.

kihasználása. Ahhoz, hogy az információs fölényt elérjük és meg tudjuk tartani, szükséges e rendszerek védelme és a szembenálló fél hasonló rendszereinek támadása is. Napjainkban a hagyományos hadszíntereken folyó katonai tevékenységekkel párhuzamosan, az információs hadszíntéren támadó és védelmi jellegű információs tevékenységek — információs műveletek (Information Operations - INFOOPS) — is zajlanak.

Az információs műveletek azon koordinált tevékenységeket jelentik, melyek a szembenálló fél információira, távközlési információs rendszereire gyakorolt ráhatásokkal képesek támogatni a döntéshozókat a politikai és katonai célkitűzéseik elérésében úgy, hogy e mellett a saját hasonló rendszereket hatékonyan kihasználják és megóvják. [2] Az információs műveletek különböző elkülönülten is létező, komplex információs tevékenységek közötti integráló és koordináló tevékenység, melynek szükségességét és létjogosultságát az összehangolt információs tevékenységek nagyságrendekkel növelhető hatékonysága adja.

Az információs műveletek céljai elérése érdekében fizikai–, információs– és tudati (az emberi felfogóképesség és megértés) dimenzióiban fejti ki hatásait.

A fizikai dimenzióban folytatott információs műveleti tevékenységek a különböző információs infrastruktúrák, infokommunikációs rendszerek elemei elleni fizikai, pusztító, ún. „kemény típusú" („Hard Kill",) támadásokat, illetve azok fizikai védelmét jelentik.

Az információs dimenzióban folytatott információs műveleti tevékenységek a különböző információs folyamatok, adatszerzés, adatfeldolgozás, kommunikáció, stb. elektronikus úton való, „lágy típusú" („Soft Kill") korlátozó hatású támadását jelenti annak érdekében, hogy a célpontokra való közvetlen pusztító, romboló fizikai ráhatás nélkül közvetlenül befolyásoljuk azokat. Másik oldalról ide tartozik a szembenálló fél saját információs folyamatainkra irányuló hasonló támadásának megakadályozása is.

A tudati (értelmi, kognitív) dimenzióban megvalósuló információs tevékenységek közvetlenül az emberi gondolkodást — észlelést, érzékelést, értelmezést, véleményt, vélekedést — veszik célba valós, csúsztatott vagy hamis információkkal. [1]

Az információs korszak, információs környezet, információs társadalom és a digitális, precíziós és hálózatos hadseregek megjelenése következtében, a katonai műveletek működési területei és tartományai tovább bővültek. A szárazföldi-, tengeri-, légi- és kozmikus hadszíntér mellett a hadviselés egy újabb tartománya jelent meg, melyet információs hadszíntérnek nevezünk. Az információs hadszíntér tulajdonképpen az információs műveletek működési környezete, melyben annak mindhárom dimenziója (fizikai-, információs- és tudati dimenzió) értelmezhető.

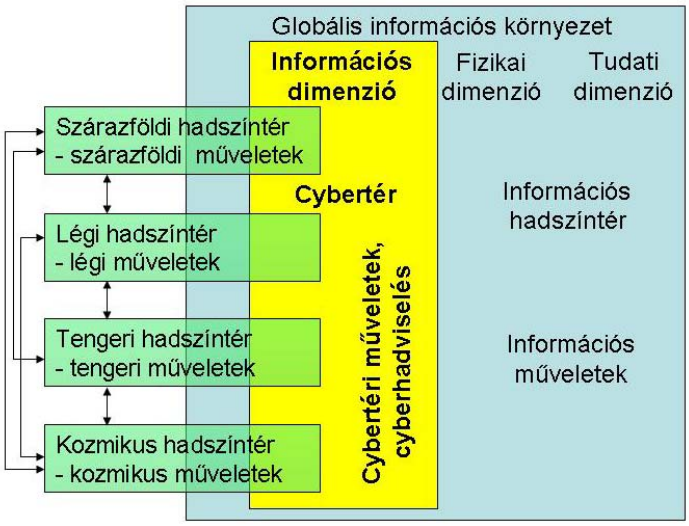
A harctéren a különböző hálózatba kapcsolt elektronikai rendszerek az információs hadszíntér azon részét használják, amelyben a különböző elektronikus információs folyamatok (elektronikai úton végrehajtott adatszerzés, adatfeldolgozás, kommunikáció stb.) realizálódnak, illetve az elektronikai rendszerek elleni tevékenység és a védelem megvalósul. Az információs hadszíntér ezen tartományát cybertérnek nevezzük. A cybertér tehát az információs hadszíntér azon tartománya, melyben csak az információs dimenzió értelmezhető.

Civil terminológia szerint a cybertér az elektronikus kommunikációs eszközök és rendszerek (számítógép-hálózatok, telefonvonalak, műholdas rendszerek stb.) és a rajtuk található szolgáltatások, információk alkotta virtuális tér vagy világ összefoglaló neve. A cybertér kifejezést — csakúgy, mint a virtuális valóság sok más szakkifejezését is — William Gibson alkotta meg a „Neuromancer" című novellájában, amelyben a globális internet társadalmát vetíti előre. E kifejezést igen gyakran alkalmazzák a virtuális valóság világára is.

A cybertér katonai értelmezése ettől eltérő, jóval tágabb. Az USA Nemzeti Katonai Stratégia a Cybertéri Műveletekhez (National Military Strategy for Cyberspace Operations) c. dokumentuma szerint a cybertér egy olyan tartomány, ahol hálózatos rendszerekben működő elektronikai eszközöket és az elektromágneses spektrumot használják fel az adatok tárolására, cseréjére és módosítására. [3] Meg kell azonban jegyezni, hogy egy hálózatban lévő különböző elektronikai eszközök, különböző vezetékes kapcsolaton keresztül is csatlakozhatnak egymáshoz. Így pl. az állandó helyű (stacioner) rendszerek elterjedt hálózati összeköttetési formája a vezetékes kapcsolat, azon belül is a leginkább elterjedőben lévő optikai kábeles csatlakozás. Ennek megfelelően a fenti értelmezést ki kell terjeszteni azon hálózatokra is, melyek elemei nem rádiócsatornán, hanem vezetéken (rézvezeték, optikai kábel stb.) vannak egymáshoz kapcsolva. Mindezeken túl az elektromágneses spektrum azért is szűkítése a cybertérnek, mivel azt a frekvencia spektrum más tartományaira is ki kell terjeszteni, ami pl. a

mechanikus rezgések és a részecskesugárzások fizikai tartományát is tartalmazza. A szeizmikus és akusztikus rezgések, valamint a részecskesugárzások felderítésére eszközök sokasága szolgál (szonárok, harctéri hangérzékelők, tüzérségi bemérő eszközök, speciális mikrofonok, sugárzásmérők, stb.), az ellenük vívott harcban pedig elektronikai hadviselési eszközöket (Electronic Warfare – EW) kell alkalmazni. [8] Az irányított energiájú fegyverek, amelyek jelentős része (pl.: az infrahangfegyverek, a hallható tartományú lökéshullám generátorok, a nagy energiájú részecske sugárzók, stb.) szintén a fizikai tartományokban működnek Ennek megfelelően helyesebb az elektromágneses spektrum helyett a teljes frekvencia tartományt értelmezni.

A cybertér a hadviselésnek a földi-, légi-, tengeri- és kozmikus színterekkel hasonlatos, azzal egyenértékű tartománya. Mint ahogy a tengeri hadszíntér jellemezhető a vízfelszínen vagy a víz alatt folytatott műveletekkel, vagy a légi hadszíntér a levegőben folytatott műveletekkel ugyanúgy jellemezhető a cybertér is a hálózatba kötött elektronikai rendszerekkel és a teljes frekvencia spektrum használatával (1. ábra).



1. ábra: A cybertér értelmezése

A cybertér meghatározásával kapcsolatban — civil értelmezés szerint — általánosan elterjedt nézet, hogy az a számítógép-hálózatokkal és az internettel van összefüggésben. A cybertér katonai értelmezése azonban kiterjeszti ezt a dimenziót, és nemcsak a számítógép-hálózatok működési környezetét érti alatta. Napjainkban a harctéren elektronikai eszközökből (pl. rádiók, radarok, navigációs eszközök, harctéri azonosító berendezések stb.) és számítógépekből olyan hálózatokat hoznak létre, ahol igen nehéz különválasztani egymástól a rendszert alkotó komponenseket. Amennyiben ezek elleni tevékenységről és a saját oldalon ezek védelméről beszélünk, akkor mindenképpen egy komplex rendszerként kell azokat értelmezni, melyeknek közös működési környezetük van. A harctéren ezek a hálózatos rendszerek (többnyire mobil rendszerekként) az elektromágneses energiát használják fel az adatok, információk megszerzésére, tárolására, továbbítására. Amennyiben ezek a rendszerek a teljes frekvencia spektrumot használják, akkor azon keresztül lehet hozzájuk férni is, vagyis felderíteni és támadni azokat.

Az internet sebezhetősége manapság nagyon sokak számára ismert. Az információs társadalom működése alapvetően függ attól, hogy igen sok 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 hálózatba szervezett rendszer is működik, melyek nem csatlakoznak az internethez. A katonai vezetési rendszerek döntő többsége elszigetelt, zárt hálózatokként működnek, közvetlenül nem kapcsolódnak a világhálóhoz. Ha csökkenteni akarjuk az ellenség vezetési és fegyverirányítási képességeit, akkor ezeket a hálózatokat a cybertérben elektronikai úton a teljes frekvencia tartományban kell elérni. [3]

A cyberhadviselés

A cyberhadviselés organikus fejlődését jól mutatják azok a szervezeti és műveleti változások, amelyek ezen a téren a fejlett haderőknél nyilvánosságra kerültek. A fejlett haderőkben felismerték, hogy a cybertér egyre növekvő szerepet tölt be a modern hadviselésben. Felismerték, hogy amennyiben nem tesznek lépéseket a cyberhadviselési erők felállítására, abban az esetben jelentős hátrányba kerülnek a harctéri helyzetfelismerés, a vezetés, a precíziós csapásmérés terén. Ennek megfelelően a világ több országában megindultak a cyberhadviselés fejlesztésére irányuló törekvések. E kérdésekkel intenzíven foglalkoznak Kínában, Oroszországban, az USA-ban és még számos fejlett haderővel rendelkező országban.

A cyberhadviselés megjelenése a különböző haderőkben

A cyberhadviselési képességek kialakításánál vélhetően döntő szerepet játszott az Észtország elleni 2007 tavaszán bekövetkezett intenzív cybertéri támadássorozat, mely a második világháborús emlékmű eltávolításával hozható összefüggésbe. Észtország rendkívül fejlett információs infrastruktúrával rendelkezik. A közigazgatás, a bankrendszer, a gazdaság nagymértékben függ az internettől. Észtország az elsők között volt a világon, ahol az emberek a nemrégiben tartott parlamenti választásokon akár az interneten is leadhatták szavazataikat. A közel két hétig tartó támadás során a támadók megpróbálták megbénítani a különböző észt honlapok működését, megakadályozva, hogy a felhasználók elérhessék azokat, sőt, egyes esetekben azok tartalmát is igyekeztek megváltoztatni. A parlament, kormányhivatalok, minisztériumok, bankok, telefontársaságok és médiacégek szerverei elleni tömeges támadások eredményeként az internet szolgáltatás akadozott, egyes esetekben hosszabb-rövidebb időre leállt. A célpontok kiválasztása, a támadások összehangoltsága, precíz kivitelezése és hatékonysága arra mutatott, hogy e támadások hátterében szervezett erők állnak. Néhány esetben szakértők megállapították, hogy a támadások orosz szerverektől indultak, amit természetesen az orosz hatóságok tagadtak.

Ez a békeidőben példa nélkül álló cybertámadás felrázta az USA és a NATO illetékes szakértőit is. Megállapítást nyert, hogy már békében is lehetséges olyan nagyságrendű internetet bénító támadás, amely akár egy hagyományos támadó hadművelet bevezető szakaszának (az első csapás kezdeti tevékenységének) is felfogható. A kínai támadó hadászati elgondolás (doktrína) katonai információs hadviselési felfogása szerint a cybertéri műveleteket — a meglepetés és a kezdeti cyberfölény kivívása érdekében — az első csapás időszakában, elsősorban annak bevezető szakaszában lehet eredményesen alkalmazni. [5]

Az Észtország elleni cybertámadásnak az eredményessége jóval meghaladta azokat a veszélyszinteket és jelentős károkat okozó eredményeket, amelyeket korábban a magányos rosszindulatú támadók (crackerek, számítógépes bűnözők) tevékenysége idézett elő. Tekintettel arra, hogy az ilyen típusú támadások azonnali és rendkívül súlyos károkat idézhetnek elő, a cybertéri műveleteket — az USA részéről — rendkívül komoly fenyegetések kategóriái közé sorolják. Hangsúlyozzák, hogy az ilyen támadások nem maradhatnak megfelelő és arányos válasz nélkül.

Várhatóan az észt példa hatására — egyrészt a cybertéri támadó képesség megteremtése, másrészt a cybervédelem biztosítása érdekében — az elkövetkezendő években a cybertéri erők kialakítása, fejlesztése, majd hadrendbe állítása számos országban futótűzként terjedhet el. Törvényszerűen és kényszerítő jelleggel érvényesülni fog az a fejlesztési elv, miszerint a „cybertéri fegyverkezést" azért kell szorgalmazni, mert a potenciális ellenfélnek már van, vagy lehet ilyen jellegű képessége.

Az Amerikai Egyesült Államokban jelenleg felállítás alatt van a légierő cyber parancsnoksága (Air Force Cyber Command), mely a tervek szerint 2008. október elején kezdi meg működését. Jelenleg a 8. légierő parancsnokság alárendeltségében vannak olyan egységek, amelyek cybertéri műveleteket folytatnak. Ilyen pl. a 67. Hálózati Hadviselési Wing (67. Network Warfare Wing) öt századdal, amelyek naponta támadó és védelmi jellegű cyberműveleteket hajtanak végre. [4]

A felállítandó cyber parancsnokság feladata, hogy a cybertérből fizikai csapásmérő eszközökkel (nagypontosságú önirányítású rakétákkal), elektronikai zavaró eszközökkel, lézer és irányított energiájú fegyverekkel, továbbá számítógép-hálózati támadó eszközökkel (rosszindulatú programokkal) és módszerekkel csapásokat mérjenek az ellenséges országok integrált légvédelmi

rendszerére, felderítő rendszereire, távközlési hálózataira és más hálózatalapú katonai vezetési rendszereire. Ezen túlmenően feladata, hogy a cyberhadviselés eszközeivel és módszereivel támadást intézzen az ellenséges ország kritikus információs infrastruktúráira, ezen belül kiemelten az internet hálózatra, a cellás rendszerű mobiltelefon hálózatokra, az energiaellátás irányító rendszereire stb.

A parancsnokság a védelem terén is megteszi a szükséges lépéseket, amelynek keretében olyan eszközöket rendszeresít, melyekkel képes felderíteni és meghatározni az ellenséges cybertéri támadó eszközöket, és rendszereket, valamint védelmi eljárásokat dolgoz ki a saját hálózatos rendszereik védelme érdekében.

Természetesen nemcsak az USA, hanem Kína is felismerte a cybertér jelentőségét. Kína már több esetben kísérelt meg amerikai számítógépes rendszerek elleni támadást. Az egyik leghíresebb ilyen szisztematikus támadássorozat 2004-ben történt, és a támadások eredetét a dél kínai Guangdong tartományig lehetett visszavezetni. A támadások célpontjai amerikai katonai és ipari számítógép-hálózatok voltak.

A kínai hadsereg — a konfliktus kirobbanásának korai szakaszában — az „elektromágneses uralom" (Electromagnetic Dominance) elérése egyik döntő tényezőjének tartja a számítógép-hálózati hadviselés (Computer Network Operations - CNO) alkalmazását. Bár egyértelmű tények nincsenek arra vonatkozóan, hogy Kína rendelkezne számítógép-hálózati hadviselési doktrínával, ugyanakkor kínai katonai szakértők az integrált hálózati elektronikai hadviselés (Integrated Network Electronic Warfare) keretében látják megvalósíthatónak a harctéri hálózatos információs rendszerek működésének korlátozását. Ezen integrált tevékenység keretében elektronikai hadviselési erőket és eszközöket, számítógép-hálózati hadviselési eljárásokat és nagypontosságú irányított fegyvereket alkalmaznak a cél elérése érdekében.

A kínai haderőben információs hadviselési egységeket hoztak létre, amelyek számítógépes vírusokkal képesek támadni az ellenséges hálózatos vezetési rendszereket, illetve különböző rendszabályokkal biztosítják a saját rendszereik megbízható működését. Az elképzeléseket és fejlesztési eredményeket 2005-ben hadműveleti gyakorlatokon próbálták ki, amikor is számítógép-hálózati támadó műveleteket hajtottak végre a hálózatos vezetési rendszerek ellen, a feltételezett hadászati első csapás időszakában. [5]

A katonai elemzők hangsúlyozzák, hogy a katonai vezetési folyamatban a döntési időciklus időtartama az eddigi percekről napjainkban már másodpercekre rövidült, ezért igen nagy jelentősége van annak, hogy a hálózatos vezetés folyamatosságát biztosítsák. A cybertéri csapásokkal pontosan ennek a hálózatalapú vezetésnek és döntéshozatalnak folyamatosságát lehet korlátozni.

A cyberfölény

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

1. A különböző hálózatba kapcsolt elektronikai rendszerekkel az információ biztosítása a kialakult és a várható helyzetről. Ez egyrészt jelenti az ellenséges elektronikai rendszerek (rádióforgalmi rendszerek, légvédelmi rendszerek, számítógép-hálózatok stb.) felderítését, másrészt a saját erők helyzetéről szóló információk elektronikus feldolgozását, tárolását és továbbítását, harmadrészt pedig a harctéri környezetről szóló adatok (terepviszonyok, időjárás stb.) elektronikai rendszerekkel, eszközökkel való megszerzését, feldolgozását, továbbítását (pl. meteorológiai lokátorokkal adatok megszerzése, digitális térképi információk feldolgozása térinformatikai módszerekkel stb.).
2. Az ellenség elektronikus információs rendszerei működésének korlátozása, akadályozása. Ez alatt egyrészt az elektronikai hadviselés keretében végrehajtott ellentevékenységi módszereket értjük, mint pl. elektronikai zavaró eszközökkel az ellenséges híradás megbontása, légvédelmi radarrendszerek zavarása, különböző elektronikai megtévesztő tevékenységek folytatása vagy nagyenergiájú impulzus fegyverekkel (e-bomba) az ellenséges elektronikai eszközök, számítógépek tönkretétele. Másrészt a

számítógép-hálózati hadviselés keretében az ellenséges számítógép-hálózatokba való behatolást és ennek következtében pl. adatbázisok tönkretételét, módosítását, programfutási hibák előidézését jelenti.

3. A saját információs képességek kihasználása és megóvása az ellenség elektronikus úton végrehajtott különböző támadásaival szemben. Ez magába foglalja a saját hálózatos információs rendszereinkben rejlő lehetőségek maximális kihasználását, vagyis a hálózat nyújtotta képességek kialakítását és fenntartását illetve ezen rendszereink elektronikai- és számítógép-hálózati védelmét.

A cyberfölény fentiek szerinti értelmezése az információs fölényhez kapcsolódik, annak azon részét képezi, amely az információs dimenzióban realizálódik, és amelynek elérését a harctéren alkalmazott hálózatba kötött elektronikai rendszerek kihasználása, sajátoldali védelme és ellenség oldali támadása biztosítja. Cyberfölény nélkül a teljes információs fölény nem vívható ki és nem tartható meg. A cyberfölény kivívására irányuló képességek megteremtése döntő fontosságú napjaink katonai műveleteiben, ezért e feladatra való felkészülést a Magyar Honvédségben is fokozatosan meg kell kezdeni.

A cyberhadviselés értelmezése

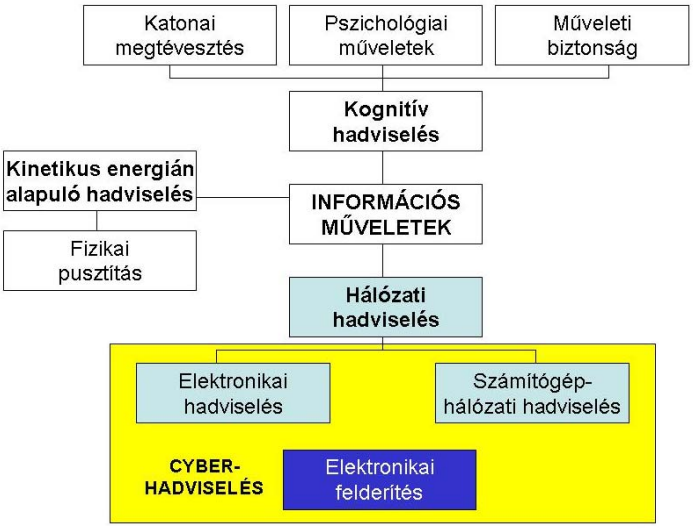
Mint ahogy a cyberfölényt az információs fölény részeként értelmezzük, úgy annak kivívása az információs műveleteken belül folytatott cyberhadviseléssel (Cyberwarfare), vagy más terminológia szerint cybertéri műveletekkel (Cyberspace Operations) valósítható meg.

Tekintettel a cybertér katonai értelmezésére — mely tágabb, mint a civil felfogás — a cybertérben folytatott műveletek a számítógép-hálózati hadviselésnél többet jelentenek. Ide sorolhatjuk pl. a távközlési hálózatok lehallgatását, zavarását, a navigációs rendszerek elleni elektronikai ellentevékenység különböző formáit, a számítógép-hálózatok feltérképezését, azokba való bejutást és az adatbázisok tönkretételét, a szerverek túlterhelését vagy az alkalmi robbanó eszközök (Improvised Explosive Devices - IED) elleni tevékenységet is. A felsorolt cybertéri tevékenységek csak néhány kiragadott példa arról a széles palettáról melyek támadó céllal alkalmazhatók az ellenség elektronikai rendszerei és számítógép-hálózatai ellen, illetve védelmi jelleggel a saját hasonló rendszereink megóvása érdekében.

Az információs műveletek egy újszerű megközelítés alapján három egymástól jól elkülöníthető területre bontható, mely három terület kapcsolódik a már említett három dimenzióhoz (fizikai, információs és tudati). Ezek az alábbiak:

- *kinetikus energián alapuló hadviselés* (Kinetic Warfare), amely a fizikai dimenzióban kerül végrehajtásra és az információs infrastruktúrák, infokommunikációs rendszerek elemeinek fizikai úton való pusztítását, rongálását, tönkretételét jelenti;
- *kognitív hadviselés* (Cognitive Warfare), amely alapvetően a tudati, értelmi dimenzióban érvényesül, és a katonai megtévesztést, műveleti biztonságot illetve a pszichológiai műveleteket foglalja magába;
- *hálózati hadviselés* (Network Warfare), amely az információs dimenzióban realizálódik, és az elektronikai hadviselést valamint a számítógép-hálózati hadviselést tartalmazza. [6]

Az információs dimenzióban megvalósuló hálózati hadviselés a fenti értelmezés — illetve a cybertér hálózatos rendszerekre való értelmezése — alapján nem más, mint a cybertérben megvalósuló műveletek összessége, vagyis más szóval a cyberhadviselés. Mint ahogy az információs műveletek alapját képezik a katonai információs rendszerek, illetve az összadatforrású felderítés, úgy a cyberhadviselés alapját is a hálózatokra épülő elektronikus információs rendszerek, és a különböző szenzorhálózatokra épülő elektronikai felderítés képezi. (2. ábra)



2. ábra: Cyberhadviselés és az információs műveletek kapcsolata [6 alapján szerkesztették a szerzők]

A cyberhadviselés célja a cyberfölény kivívása és fenntartása egyfelől a saját oldali elektronikus, hálózatalapú információszerző, információtovábbító, -feldolgozó rendszerek védelmével, másfelől a szembenálló fél hasonló rendszerei működésének zavarásával, korlátozásával, lefogásával, vagy akár elektronikus úton történő megsemmisítésével. A cyberhadviselést az erre a feladatra kijelölt, felkészített és a megfelelő technikai eszközökkel ellátott speciális erők végzik. A cybertéri erőknél elsősorban nem a létszám (a mennyiség), hanem a technikai eszközök fejlettségi szintje (vagyis a minőség) számít. Ezek alkalmazása során — az állandó és kényszerítő kihívások és változások közepette — a cybertéri erők mentális (tudati, gondolati), innovációs, kreatív és adaptációs képessége a döntő tényező.

A cyberhadviselési 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 hadviselés keretében alkalmaznak, valamint 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. Mindenképpen ide kell sorolnunk a harctéren egyre inkább elterjedőben lévő földi és légi robotok alkalmazását is, hiszen ezen eszközök vezérlése és a működési folyamataik alapvetően köthetők a cybertérhez, másrészt ezek az eszközök is hálózatba szervezhetők, aminek következtében alkalmazásuk hatékonysága növelhető.

A cyberhadviselésnek a fejlett haderőkben (pl. az USA-ban, Oroszországban, Nagy-Britanniában, Franciaországban, Németországban, sőt Kínában, Izraelben, Indiában, Iránban is) saját vezetési hierarchiájuk van, technikai eszközrendszerüket állandóan fejlesztik. Mivel teljesen új és folyamatosan fejlődő, változó feladatrendszer szerint működnek, a cyberhadviselési erők funkciója gyakran változik, vezetési rendszerük állandó fejlődésben és átalakulásban van. Különösen fontos a cybertéri kihívások hatásainak meghatározása, a cybertérben jelentkező új típusú veszélyek felismerése. Ezen a téren nem egyszerűen csak katonai kihívásokról van szó, hanem az információtechnológia, infokommunikáció legújabb vívmányainak versenyéről, gyakran feszített küzdelméről lehet beszélni.

A fejlett országok (elsősorban az USA) azon doktrínális elképzelései, miszerint a cybertéri műveletek kezdeti csapásait — a meglepetés fokozása és a kezdeti információs fölény megszerzése érdekében — a tervezett összhaderőnemi első csapás időszakában kívánják alkalmazni, minden bizonnyal átrendezi majd a katonai költségvetések fejlesztésre fordítható tételeinek eddigi prioritásait.

A cyberhadviselés támadó és védelmi jellegű lehet. A támadó cyberhadviselésnek kettős funkciója van: egyrészt felfedni, másrészt befolyásolni, tönkretenni a másik fél hálózatos információs rendszereit. E kettős funkciót — a támadó jellegű cyberhadviselés nagyfokú hatékonysága érdekében — az információs dimenzióban kell érvényre juttatni.

A cybertéri támadás közvetlen és közvetett formában valósulhat meg. A közvetlen cybertéri támadás során a támadó fél egyrészt a különböző információbiztonsági rendszabályokat kikerülve bejut a kommunikációs rendszerekbe és számítógép–hálózatokba, hozzáfér különböző adatbázisokhoz stb. és ezáltal számára hasznosítható információkhoz jut. Másrészt zavaró jelekkel, megtévesztő információkkal, rosszindulatú szoftverek bejuttatásával tönkreteszi, módosítja, törli stb. a szembenálló fél számára fontos információkat. A közvetett támadás során a támadó fél hozzáférhetővé teszi a másik fél számára a saját félrevezető információit, vagy megtévesztő hálózati tevékenységet folytat, és ezáltal félrevezeti és befolyásolja a helyzetértékelést, illetve hamis adatokkal túlterheli a rendszert, aminek következtében a hálózati hozzáférést akadályozza. A cybertéri támadás funkcióit, formáit és néhány jellegzetes tevékenységét az 1. táblázat szemlélteti.

Természetesen a közvetlen és közvetett cybertéri támadást megfelelően összehangolva célszerű alkalmazni, ezáltal is erősítve egymás hatékonyságát. Egy közvetett támadással el lehet terelni a felderítő rendszerek figyelmét, így a közvetlen támadás sikeresebben végrehajtható a megcélzott rendszerrel szemben. Ugyanakkor egy közvetlen módon végrehajtott támadás arra kényszerítheti a szembenálló fél hálózatos vezetési rendszerét, hogy pl. a döntési alternatívák kialakításakor, az összadatforrású felderítő rendszer helyett csak egy forrásból származó információkra, pl. csak a radarral végzett felderítésre támaszkodjon. Ez az egyforrású felderítő rendszer pedig a már említett közvetett támadással, pl. imitált célok elektronikai úton való létrehozásával (radarzavaró eszközzel) hatékonyan félrevezethető. [1]

1. táblázat: Cybertéri támadás funkciói, formái és tevékenységei

Funkció:	**FELFEDÉS**	**BEFOLYÁSOLÁS, TÖNKRETÉTEL**	
Támadó tevékenység:	**Hálózatos információs rendszerek felderítése**	**Hálózatos információs rendszerek**	
Támadás dimenziója:		**megtévesztése**	**zavarása, tönkretétele, pusztítása**
Információs dimenzió	Üzenetek, közlemények passzív módszerekkel való lehallgatása Hálózati topológia kívülről való feltérképezése Titkosítás megfejtés, dekódolás Elektronikai felderítő szenzorok alkalmazása Számítógép-hálózatok adataihoz való rejtett hozzáférés Trójai programok alkalmazása Jelszólopók telepítése	Megtévesztő e–mail üzenetek továbbítása Megtévesztő hálózati tevékenység folytatása Trójai programok bejuttatása megtévesztő tevékenység útján Működő programokkal adatok módosítása Hamis célok elektronikai úton való imitálása	Hálózatok adatokkal való mesterséges túlterhelése (DDoS Attack), ezáltal a hálózati hozzáférés akadályozása Szenzor adatok bejuttatása, melyek megzavarják az irányítási folyamatokat (pl. légvédelem) Nyílt forrású információkkal a figyelem elterelése Rosszindulatú szoftverekkel, (férgek, vírusok stb.) hálózati szolgáltatásokhoz való hozzáférés megakadályozása, adatok, adatbázisok tönkretétele Zavarással elektronikai rendszerek működésének akadályozása Nagyenergiájú impulzusokkal elektronikai eszközök tönkretétele

A cybertéri védelem arra irányul, hogy fenntartsa a saját hálózatos információs rendszereinkben a hozzáférhetőséget az információkhoz, információalapú folyamatokhoz, és biztosítsa ezen rendszerek hatékony használatát békeidőben, válság vagy konfliktus idején egyaránt. A hálózatos információs rendszerek védelme biztosítja a saját vezetési képességeink fenntartását azáltal, hogy kihasználja a saját rendszerekben rejlő lehetőségeket, illetve lehetetlenné teszi, hogy az ellenség beavatkozzon információs rendszereinkbe. Minimálisra csökkenti a saját hálózatos információs rendszereink sebezhetőségét és a közöttük fellépő kölcsönös zavarokat.

Természetesen a cybertéri védelem megvalósítható úgy is, hogy megakadályozzuk a szembenálló felet abban, hogy ellenünk alkalmazni tudja elektronikai támadó eszközeit. E megközelítés alapján a saját hálózatos információs rendszereink cybertéri védelme lehet támadó és védelmi jellegű. A támadó jellegű védelem a cybertéri támadás minden lehetséges eszközét és módszerét felhasználja, hogy csökkentse a szembenálló fél lehetőségeit a saját hálózatos információs rendszerek támadására. Így pl.

az ellenség rádiózavaró eszközeinek elektronikai úton való tönkretételével (pl. nagyenergiájú impulzus fegyverekkel) meg tudjuk akadályozni, hogy azokat a saját távközlési rendszereink ellen felhasználhassa. Ezzel szemben a védelmi jellegű tevékenység a saját rendszerek sebezhetőségét csökkenti, felhasználva a fent említett tevékenységek, és rendszabályok lehetőségeit. A hatékony cybertéri védelem összehangolt alkalmazása lehetővé teszi, hogy megvédjük saját hálózatos információs rendszereinket a szolgáltatásokhoz való hozzáférés megakadályozásától (Denial of Service– DoS), a jogosulatlan hozzáféréstől, zavarásától, módosítástól stb. [1]

A cyberhadviselés összetevői: az elektronikai felderítés; az elektronikai hadviselés és a számítógép-hálózati hadviselés.

Az elektronikai felderítés, mint információszerző tevékenység általában kettős céllal kerülhet végrehajtásra. Egyrészt az infokommunikációs rendszerekben tárolt és továbbított adatokhoz való hozzáférés és azok felhasználása céljából, másrészt a hatékony támadás kivitelezéséhez szükséges célinformációk megszerzése céljából. A kritikus információs infrastruktúrák elleni támadások hatékonysága nagymértékben függ attól, hogy a támadást elkövető tudja-e, hogy az adott objektum (rendszer) fizikailag hol helyezkedik el, milyen a strukturális összetétele, milyen hardver és szoftver elemekből áll, milyen célú és mennyiségű adatforgalom zajlik rajta keresztül, vannak-e gyenge pontjai, és ha igen hol, illetve kik az adott információs rendszer vagy hálózat üzemeltetői, és felhasználói. [7] Napjainkban e célra a legkülönfélébb módszerek és technikai eszközök alkalmazhatók, melyek jelentősen megnövelik, megsokszorozzák az emberi érzékelés határait. A 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. [8]

A korszerű elektronikai felderítésben egyre inkább jellemzővé válik, hogy az adatokat olyan eszközökkel szerzik meg, melyek az élőerőt nem veszélyeztetik. Ezek lehetnek egyrészt különböző hordozóeszközökön kijuttatott eszközök, mint pl. a pilóta nélküli repülőeszközön elhelyezett szenzorok, illetve a felderítendő objektum körzetébe letelepített úgynevezett felügyelet nélküli földi szenzorok. Ez utóbbiak olyan mini– mikro– és nanoméretű érzékelő- és mérőműszerek, amelyek a környezeti méret– és állapotváltozásokat, torzulásokat, ingadozásokat stb. képesek érzékelni, mérni, és automatikus úton jelenteni. E szenzorok olyan állapotváltozásokat mérnek, mint pl.: hőváltozások, mechanikai változások, akusztikus változások, vegyi állapotváltozások, mágneses változások, elektrooptikai változások, vagy esetleg biológiai változások.

Az elektronikai hadviselés azon katonai tevékenység, amely az ellenség elektronikai rendszereinek elektronikai úton való felderítésére, működésük korlátozására, illetve a saját hasonló rendszerek működésének fenntartására irányul. Az elektronikai hadviselés elektronikai támogató tevékenységre, elektronikai ellentevékenységre és elektronikai védelemre, mint egymást kiegészítő területekre osztható, melyekkel biztosítható az ellenség katonai információs rendszereinek elektronikai úton való támadása, illetve a saját hasonló rendszerek működésének biztosítása, az élőerő és a csapatok megóvása.

Az elektronikai támogató tevékenység — hasonlóan az elektronikai felderítéshez — az elektromágneses és más tartományú kisugárzások jeleinek érzékelésével, azonosításával és azok felhasználásával kapcsolatos tevékenység. Az elektronikai támogatás fontos információkkal szolgál arról, hogyan használja az ellenség a frekvenciaspektrumot, érzékeli, azonosítja és felhasználja az ellenség szándékos (pl.: rádióadás) és a nem szándékos (pl.: kipufogó gázok infravörös hullámtartományú) kisugárzásait. Ezek alapján képes különböző fenyegetések jelzésére, meghatározására, illetve elektronikai ellentevékenység hatékony végrehajtása érdekében célmegjelölésre.

Az elektronikai ellentevékenység az elektronikai hadviselés támadó fegyvere, ami abban nyilvánul meg, hogy minden olyan technikát, módszert és eszközt felhasznál, ami az elektromágneses és más irányított energiák felhasználásával képes működésképtelenné tenni az ellenséges elektronikai eszközöket. Az elektronikai ellentevékenységnek három területe van:

- az elektronikai zavarás, mellyel megakadályozhatjuk az ellenség elektronikai eszközeinek vagy rendszereinek hatékony működését;
- az elektronikai pusztítás, melynek során elektromágneses és egyéb irányított energiákat vagy az önrávezetésű fegyvereket alkalmazhatunk az ellenség elektronikai eszközeiben és az élőerőben tartós, vagy ideiglenes károkozás céljából;

– az elektronikai megtévesztés, amely az elektronikai kisugárzások manipulálásával, torzításával vagy meghamisításával éri el, hogy az ellenség saját érdekeivel ellentétesen tevékenykedjen**.**

Az elektronikai védelem az elektronikai hadviselés azon területe, amely biztosítja az elektromágneses, és egyéb fizikai tartományok saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok nem szándékos elektromágneses interferenciái ellenére. 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. [9; 10]

A számítógép–hálózati hadviselés egyrészt a szembenálló fél hálózatba kötött informatikai rendszerei működésének befolyásolására, lerontására, lehetetlenné tételére irányul, másrészt viszont a saját hasonló rendszerek működésének fenntartására törekszik. Látható tehát, hogy e tevékenység során itt is támadó és védelmi típusú műveletekről beszélhetünk. [8]

A számítógép–hálózati hadviselés magába foglalja:

– 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 védelem kérdéseit.

A számítógép–hálózati hadviselés jelentős mértékben járul hozzá a cyberhadviselés célkitűzéseinek eléréséhez. Természetesen a cyberhadviselés e kifinomult módja csak akkor és azon ellenség ellen alkalmazható, amely az információs technológia és technika egy bizonyos fejlettségi szintjével rendelkezik. Ez azt jelenti, hogy többek között rendelkezik azon számítógép–hálózatokkal, amelyek bizonyos sajátos módszerekkel támadhatók.

A számítógép–hálózati hadviselés körébe tartozik a számítógép–hálózati támadás és a számítógép–hálózati védelem. [11]

A számítógép–hálózatok támadása egyrészt a hálózatok feltérképezését, felderítését, másrészt pedig azok tényleges támadását jelenti. A számítógép–hálózati felderítés szoftveres vagy hardveres úton való behatolást jelent a szembenálló fél számítógépes rendszereibe, illetve hálózataiba, azzal a céllal, hogy hozzáférjünk az adatbázisaiban tárolt adatokhoz, információkhoz, és azokat felderítési céllal hasznosítsuk.

A számítógép–hálózati támadás szoftveres vagy hardveres úton való behatolást jelent a szembenálló fél számítógépes rendszereibe, illetve hálózataiba, azzal a céllal, hogy tönkretegyük, módosítsuk, manipuláljuk, vagy hozzáférhetetlenné tegyük az adatbázisaiban tárolt adatokat, információkat, illetve magát a rendszert vagy hálózatot. A támadás a számítógép–hálózati elemekben való fizikai károkozást is jelentheti, amelyet a szoftverek módosításával vagy manipulációjával lehet elérni. [11]

A számítógép-hálózati támadás eszközei közé tartoznak a különböző kártékony, rosszindulatú programok, melyeket Malware-eknek nevezünk. A Malware azon szoftverek gyűjtőneve, melyek közös jellemzője, hogy anélkül jutnak a rendszerbe, hogy arra a felhasználó engedélyt adott volna. Minden olyan szoftver rosszindulatúnak minősíthető, amely nem a számítógépes rendszer vagy hálózat rendeltetésszerű működését biztosítja.

A Malware kifejezés számos rosszindulatú szoftvert takar. Napjainkban e szoftverek típusai és fajtái folyamatosan gyarapodnak, ezért egyértelmű kategorizálásuk szinte lehetetlen. A legismertebb ilyen programok: a vírusok, a programférgek, a trójai programok, a rootkitek, a böngésző eltérítők, a hátsó ajtó (backdoor) programok, a keyloggerek, a spam proxyk, a spyware és az adware programok, és a sort még folytathatnánk. Nem program típusú Malware-ek közé taroznak többek között a spam-ek, hoax-ok, és a phishing, amelyek szöveges információk formájában hordoznak veszélyt a rendszerre és felhasználójára. A rosszindulatú szoftverek módosíthatják a programokat, erőforrásokat foglalhatnak le, adatokat módosíthatnak, hardverhibát eredményezhetnek, eltávolításuk pedig megfelelő eszközöket, időt és energiát, egyes esetekben pedig különleges szakértelmet igényelhet.

A rosszindulatú szoftverek ötvözve azok alkalmazásának különböző módszereivel lehetővé teszik a hálózatba való behatolást, működésének akadályozását, megbontását, illetve az adatokhoz való hozzáférést. A támadó egy távoli számítógéphez és annak adataihoz egy egyszerű, egylépéses folyamattal a legritkább esetben fér hozzá. Jellemzőbb, hogy a támadóknak számos támadási módszert

és eszközt kell kombinálniuk, hogy kikerüljék mindazokat a védelmi eljárásokat, melyeket a hálózatok biztonsága érdekében alkalmaznak. A hálózatok támadására nagyon sokféle módszer létezik (pl. Sniffing, Spoofing, Session Hijacking, Spamming, Man-in-the-Middle Attack és a leggyakrabban alkalmazott Distributed Denial-of-Service /DDoS/ Attack.), így a támadóknak csak a megfelelő szakértelemre van szükségük, hogy a támadás eszközeit a megfelelő eljárásokkal kombinálják. [12]

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 és információkat, illetve, hogy szándékosan lerontsák, működésképtelenné tegyék információs rendszerünket. [11]

A számítógép–hálózatok védelmének megvalósítása lehet passzív és aktív**.** A passzív védelmi módszerek és eszközök lehetnek: a tűzfalak; a vírusirtók; a hozzáférés szabályozás és a behatolás detektálás és adaptív válaszlépések.

Az aktív védelem módszerei közé sorolhatók: a megelőző támadások; az ellentámadások és az aktív megtévesztés. [13]

A cyberhadviselés során alkalmazott számítógép-hálózati védelem felsorolt módszereinek és eszközeinek együttes és komplex alkalmazása növeli a hálózatok biztonságát, vagyis az informatikai biztonságot. Eredményes védelem alkalmazása esetén biztosítható a számítógépes rendszerben tárolt adatok esetében a bizalmasság, titkosság (lehallgatás elleni védelem); a sértetlenség (adatok módosítása elleni védelem); az elérhetőség (adatok törlése elleni védelem); illetve a számítógépes rendszer által ellátott funkciók esetében az elérhetőség (szolgáltatás működésének megakadályozása elleni védelem) és a funkcionalitás (adott szolgáltatás megváltoztatása elleni védelem).

Összegzés

Az információs társadalom fejlődési ütemének felgyorsulása következtében egyre nagyobb szerepet töltenek be cybertérben működő a hálózatalapú elektronikai rendszerek. Napjainkban fokozottan gondoskodni kell a polgári és katonai hálózatos rendszerek több irányú védelméről, miközben megfelelő eszközökkel és eljárásokkal korlátozni kell a szembenálló fél ilyen irányú képességét. Ez olyan nemzetbiztonsági, polgári és katonai feladat, amelyre a lehető legrövidebb időn belül fel kell készülnünk. Ez egyrészt az ország biztonsága szempontjából is fontos, másrészt szövetségi tagságunkból adódó kötelezettség is, hiszen a különböző missziós feladatokban való részvétel megköveteli ezen képességünk meglétét

A felkészülés elméleti és gyakorlati lépéseket igényel. Jelenleg az elméleti felkészülési, felkészítési feladatokra helyeződik a hangsúly, ami azt jelenti, hogy a személyi állománnyal, parancsnokokkal, döntéshozókkal meg kell ismertetni ezen új típusú hadviselési forma lényegét, el kell fogadtatni fontosságát. A belátható jövőben (5-10 éven belül) azonban konkrét ellentevékenységi és védelmi eszközök beszerzését is meg kell kezdeni, és azok alkalmazására fel kell készíteni az állományt. A felkészítés során jelentős mértékben célszerű támaszkodni a polgári szférában e téren már elért eredményekre.

Meggyőződésünk, hogy a döntéshozóknak akkor tudunk érdemben segíteni, ha az e területen jelentkező problémát széles körben feltárjuk, majd terítjük (társadalmasítjuk), és folyamatosan jelezzük a téma további vagy váratlan fejlődését. Az ezredfordulón már részben sikerült a vezetők és a személyi állomány szemléletét átformálni a digitalizálást érintően, bízunk abban, hogy ugyanolyan sikereket érünk majd el a cybertéri feladatok vonatkozásában is.

FELHASZNÁLT IRODALOM

1. Dr. Haig Zsolt, Dr. Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005. 286 p. ISBN: 963-327-391-9
2. Magyar Honvédség Összhaderőnemi Doktrína. 2. kiadás. Magyar Honvédség kiadványa. MH DSZOFT kód: 11313. Budapest, 2007.
3. Fahrenkrug, David T.: Cyberspace Defined. http://www.au.af.mil/au/archive/0209/Articles/CyberspaceDefined.html (letöltve: 2008. 02. 24.)

4. Air Force Cyber Command. Frequently Asked Questions. http://www.afcyber.af.mil/library/factsheets/factsheet.asp?id=10688 (letöltve: 2008. 02. 24.)
5. Minnick, Wendel: Computer Attacks Form China Leave Many Questions. Defense News, August 13, 2007. p.: 13. ISSN 0884-139X
6. Bourque, Jesse: The Language of Engagement and the Influence Objective. The Journal of Electronic Defense. November 2007. Vol. 30. No.11. p. 30-35 ISSN 192429X
7. Dr. Haig Zsolt–Kovács László–Dr. Makkay Imre–Dr. Seebauer Imre–Dr. Vass Sándor–Ványa László: Az információs társadalom veszélyforrásai. A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban. Tanulmány. MEH Informatikai Kormánybiztosság, 2002
8. 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.
9. AJP–01 Allied Joint Operations Doctrine, September, 1999.
10. Magyar Honvédség Összhaderőnemi elektronikai hadviselés doktrínája. Honvédelmi Minisztérium, Honvéd Vezérkar, Felderítő Csoportfőnökség, Budapest, 2004.
11. AJP–3.10 Allied Joint Information Operations Doctrine (draft). 2002. szeptember.
12. Dr. Haig Zsolt: Az információs társadalmat fenyegető információalapú veszélyforrások. Hadtudomány, XVII. évf. 2007. 3. sz. 37-56p. Budapest. ISSN 1215-4121
13. Holdaway, Eric J.: Active Computer Network Defense: An Assessment. Air Command and Staff College. Maxwell Air Force Base, Alabama, 2001.