Haig Zsolt

Az információs hadviselés kialakulása, katonai értelmezése

A társadalmi érintkezés folyamán, a mindennapi életben állandóan információval találjuk magunkat szembe, hiszen információt szerzünk, tárolunk, feldolgozunk, továbbítunk, vagyis folyamatos információs tevékenységet folytatunk. Mindez megvalósulhat az egyes emberek agyi tevékenysége során, az emberek közötti kommunikáció révén, illetve a 21. század információtechnológiai eredményeinek felhasználásával gépi úton, a különböző információszerző, -feldolgozó, -tároló és -továbbító eszközök segítségével is.

A polgári életben a különböző versenyhelyzetekben (például a politikai életben, gazdasági szférában), valamint a katonai területen mind béke, mind válságidőszakban, illetve a háborús és nem háborús katonai műveletek során folyamatosan zajlottak és zajlanak különféle tudatos információs, vagy információalapú tevékenységek. Így például – egyebek mellett – a gazdasági és katonai hírszerzés, a félrevezetés, a megtévesztés, a propaganda tevékenység. Mindezen információs tevékenységek a történelem során már a régi korok háborúiban is jelen voltak. A különböző verseny- és konfliktushelyzetekben mindig is törekvés volt arra, hogy az egymással szembenálló felek több és pontosabb információra tegyenek szert a másik féllel szemben, azokat gyorsabban és hatékonyabban tudják felhasználni. Ez azt jelenti, hogy a másik féllel szembeni információs fölényre való törekvés mindig is folyamatosan jelen volt, ezek a tevékenységek azonban korábban nem képeztek olyan egységes rendszert, mint amit ma információs hadviselésnek nevezünk.

Mindezen tényezők arra ösztönözték a katonai teoretikusokat, hogy választ keressenek a kérdésre: hogyan lehet a különféle információalapú tevékenységeket összehangolni, egységes mederbe terelni az információs fölény megszerzése és megtartása érdekében. Erre vonatkozóan már viszonylag korán történtek kísérletek: az információs hadviselés, mint összehangolt információs tevékenységek első definícióját az USA védelmi minisztériumának magyar származású kutatója, *Thomas P. Rona* alkotta meg egy, a Boeing vállalat számára 1976-ban készített kutatási jelentésében. [1] Ebben az információs eszközök és módszerek olyan mindenidejű (békeállapottól békeállapotig tartó) és minden szintű (stratégiai, hadműveleti és harcászati) alkalmazását értelmezi, amely lehetővé teszi a kitűzött célok elérését.

Látható tehát, hogy az eddig is meglévő, de ez idáig egymástól elkülönülten (esetleg elszigetelten) létező információs tevékenységek szinkronizálására irányuló elmélet kidolgozására való törekvés már több mint 30 éve bekerült a köztudatba. Az információs hadviselés különböző elemei (például a felderítés, megtévesztés, félrevezetés) már az ókor háborúiban is megjelentek. Mindezek a közelmúlt háborúiban (I. és II. világháború, helyi háborúk) olyan további információs tevékenységekkel egészültek ki, mint például a pszichológiai hadviselés, az elektronikai hadviselés.

A folyamatos információs tevékenységek a hidegháborús szembenállásnak is fontos jellemzői voltak. Ennek igazolására számos példát lehet hozni, de talán számunkra a legismertebb a Szabad Európa Rádió (SZER) propagandatevékenysége, illetve ennek ellensúlyozására a „vasfüggöny" mögött folytatott ellenpropagandatevékenység és a SZER vételét megnehezítő, lehetetlenné tevő rádiózavaró tevékenység említhető, amelyek szintén információs tevékenységek voltak.

Az információs hadviselés teljes körű kialakulásához a végső lökést az információtechnológia rohamos fejlődése adta meg. Napjainkra az információ szerepe, jelentősége a társadalmi, gazdasági, politikai életben és a katonai műveletek vonatkozásában egyaránt alapvető fontosságúvá vált. Amennyiben nincs megfelelő mennyiségű, pontosságú és a valós helyzetet tükröző információ, akkor nem lehet megalapozott döntéseket hozni. Ez a felismerés ösztönözte a szakembereket, hogy megpróbálják ezt az egészet összehangolni. Az információs hadviselés kezdeti jegyei az első Öböl-háborúban, a '91-es „Sivatagi Vihar" műveletek során voltak megfigyelhetők, ahol első ízben lehetett felismerni azokat a jellegzetességeket, amelyek az információs hadviselés sajátosságait viselték magukon. Mindehhez pedig még hozzájárult a „CNN-jelenségként" ismert médiatevékenység is, amely az emberek lakóterébe hozta a háborút.

Az információs hadviselés korai felfogása

Mint korábban láttuk, az információs hadviselés egy korai definícióját már 1976-ban megfogalmazták. A következő, sokak által hivatkozott, elsősorban polgári megközelítés az amerikai védelmi minisztérium egyik kutatója, *Martin C. Libicki* nevéhez kötődik, aki 1995-ben írt egy tanulmányt What is Information Warfare? címmel. Libicki nem definiálja az információs hadviselést, viszont megadja azokat a területeket, amelyeket e tevékenység körébe sorol. Ezek az alábbiak:

- vezetési hadviselés;[1]
- hírszerzés-alapú hadviselés;[2]
- elektronikai hadviselés;[3]
- pszichológiai hadviselés;[4]
- hacker-hadviselés;[5]

---

1 Command and Control Warfare (C2W)
2 Intelligence Based Warfare (IBW)
3 Electronic Warfare (EW)
4 Psychological Warfare (PSYWAR)
5 Hacker Warfare (HW)

– gazdasági információs hadviselés;[6]
– cyberhadviselés.7 (Libicki, Martin C., 1995)

Jelenlegi értelmezésünkben e felsorolás nem ad egzakt kategorizálást, mivel több terület is átfedi egymást. Így például korábban az elektronikai hadviselés és a pszichológiai hadviselés a vezetési hadviselés részét képezte, vagy a hacker-hadviselés és a cyberhadviselés igen sok hasonlóságot mutat egymással. Mindezek alapján e felosztás nem igazán volt alkalmazható a katonai műveletekben az információs hadviselés értelmezésére.

Egy másik, a témában neves szakértő, *Winn Schwartau* 1996-ban megjelent Information Warfare című könyvében más megközelítésben, a szereplők, illetve a szintek vonatkozásában osztályozta az információs hadviselést. E szerint három osztályt különböztet meg:

– Class 1: személyes információs hadviselés;[8]
– Class 2: vállalati információs hadviselés;[9]
– Class 3: kormányzati információs hadviselés.[10] (Schwartau, Winn, 1996)

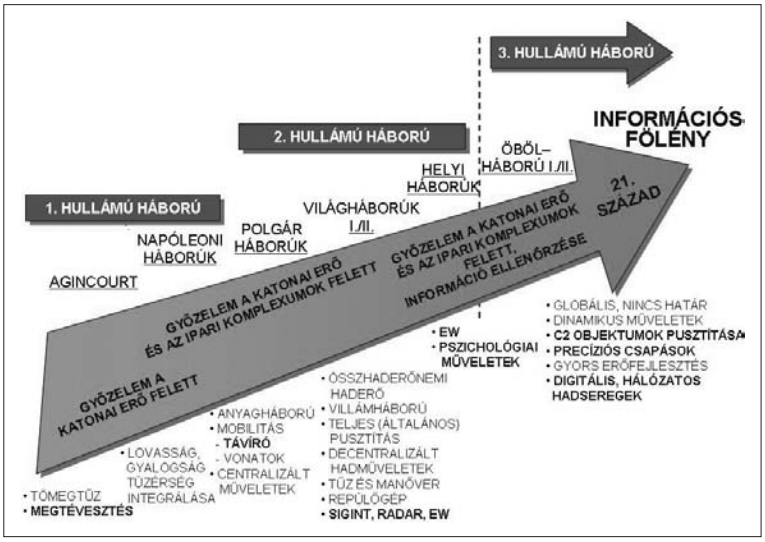
Értelmezése szerint a személyes információs hadviselés során az egyén a célpont, az egyes személyek adatai kerülhetnek veszélybe (például a személyiséglopás esetén, amikor az áldozat nemcsak pénzét, de hitelképességét, sőt, barátait is elveszítheti). A vállalti szintre jó példa lehet az ipari kémkedés, amely az egymással versenyhelyzetben lévő cégek, cégcsoportok között különböző formákban nyilvánulhat meg. A kormányzati szintű információs hadviselés a legszélesebb körű információs tevékenység, amely tetten érhető volt napjaink két, nagy nyilvánosságot kapott cybertéri konfliktusában: a grúz és az észt cybertámadás során.

Schwartau értelmezésének legfőbb jellegzetessége, hogy az információs hadviselést alapvetően csak a számítógép-hálózati környezetben zajló információs tevékenységekre vonatkoztatja, vagyis elsősorban az informatikai támadásokat és a védelmet érti alatta. (Ez a szemlélet egyébként az információs hadviselés polgári felfogásában folyamatosan tetten érhető.) Ebben a szférában többnyire nem számolnak olyan információs tevékenységekkel, mint – egyebek mellett – a pszichológiai hadviselés, a megtévesztés, az elektronikai hadviselés. Ennélfogva ez a felfogás is az információs hadviselés kereteinek a szűkítéséhez vezet, ami szintén alkalmatlan e tevékenység katonai műveleti környezetben való alkalmazhatóságára.

Az információs hadviselés katonai értelmezése: az információs műveletek

A háborúk megvívásában, a hadviselés formáiban, a haderők összetételében és technikai fejlettségi szintjeiben a 21. századra jelentős változások következtek be. Az új technikai eszközök hadszíntéren való megjelenése törvényszerűen magával hozta az

6 Economic Information Warfare (EIW)
7 Cyberwarfare (CW)
8 Personal information warfare
9 Corporate information warfare
10 Government information warfare



1. ábra. A háborúk hullámelmélet-szerű fejlődése
(Haig Zsolt–Várhegyi István, 2005)

új alkalmazási elvek kialakulását. A háborúk történetét a korszerű felfogás ugyanúgy hullámszerű fejlődésnek fogja fel, mint a társadalmi termelési világkorszakokat. Alapozva *Alvin Toffler* társadalmi fejlődési modelljére, a háborúk megvívása is a társadalmi fejlődés három hullámához köthető, és mindhárom hullámban jól meghatározhatók azok a tényezők, amelyek a katonai siker elérésének fontos zálogai lehetnek. (Toffler, Alvin, 1980; Haig Zsolt–Várhegyi István, 2005) Mindezt jól szemlélteti a háborúk hullámelmélet szerű fejlődését bemutató 1. ábra.

Eszerint minél magasabb fejlettségű haderőt vizsgálunk, annál magasabb gépesítettségének foka és információs fejlettsége.

A harmadik hullámban (ti. az információs társadalomban) jelentek meg azok az új típusú hadviselési módok, amelyekben központi szerepet játszik az információ, az információtechnológiára alapozott haderő kialakítása és az információs fölény kivívására való törekvés. Mindezek – amint azt korábban is jeleztük – az első Öböl-háborúban voltak elsőként tetten érhetők. Napjainkban a pusztításon alapuló műveletek átértékelődnek és egy másik gondolkodásmód kezd meghonosodni. Ez a hatékonyságot, a hatékonyságalapú műveleteket állítja előtérbe, amelyek fő célja, hogy minél kisebb erő és eszköz felhasználásával, illetve a lehető legkisebb veszteséggel (mind a saját, mind a szembenálló fél oldalán) lehessen katonai sikert elérni. Ezen hatásalapú műveletek egyik igen jó példája mindazon összehangolt információs tevékenységek összessége, amelyek fő célja az információs fölény kivívása és megtartása, és amelyet katonai értelmezésben *információs műveleteknek* nevezünk.[11]

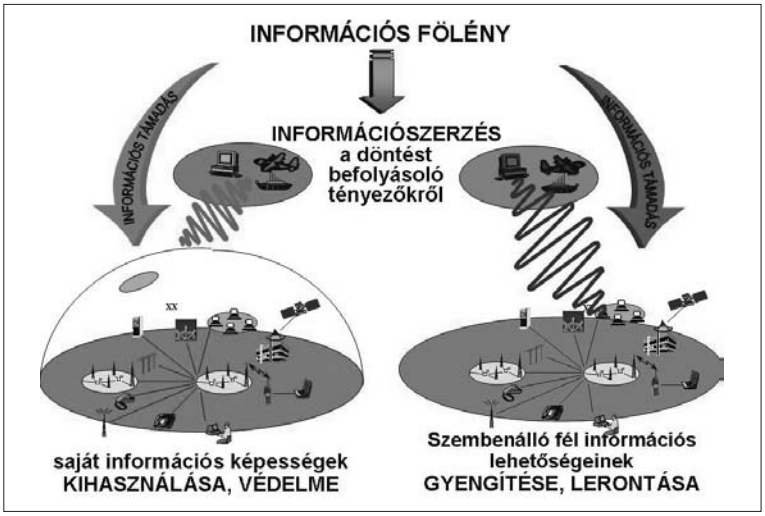
11 Information Operations – INFOOPS (USA rövidítés szerint: IO)

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 birtokosa képes információs rendszereit és azok képességeit kihasználva hadműveleti fölényt elérni, és a hadműveleti helyzetet folyamatosan úgy alakítani, irányítani, hogy emellett az ellenséget megfossza ugyanezen képességeitől.

Hogyan lehet kivívni és megtartani az információs fölényt? Az információs fölény alapját mindenekelőtt az adja, hogy a döntést befolyásoló tényezőkről elegendő, pontos, és valós idejű információval kell rendelkeznünk. Ezek a katonai műveletekben három terület köré csoportosíthatók: az ellenség helyzete, a saját kötelékek helyzete, valamint a harctéri környezet, ahol a katonai művelet zajlik. E három területről a felderítés és a saját kötelékek jelentései alapján juthatunk információhoz.

Másodsorban ki kell építeni a saját információs rendszereinket. Ezeket a szembenálló fél azon komoly erőfeszítései ellenére is hatékonyan kell működtetni, hogy vagy magát az információtartalmat vagy az információs rendszereket, illetve a döntéshozó(ka)t megpróbálja korlátozni, összezavarni, és ezáltal számára kedvező helyzetet előidézni. Vagyis: 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, valósidejű elhatározás meghozatalára. A leírt folyamatot szemlélteti a 2. ábra.



2. ábra. Az információs fölény kialakítása
(Haig Zsolt–Várhegyi István, 2005)

Amennyiben információs fölényben vagyunk a szembenálló féllel szemben, akkor a mi döntési ciklusunk gyorsabb, a parancsnok által meghozott elhatározás a valós helyzethez jobban illeszkedő, objektívebb, pontosabb. Mindez azt eredményezi, hogy a feladat végrehajtását korábban tudjuk megkezdeni, ami a kezdeményezés megragadását is jelenti. Ez – mint tudjuk – a harctevékenység megvívásának egyik fontos alapelve.

A katonai műveletekben az információs fölény elérésének leghatékonyabb formája az új típusú, összehangolt, szinkronizált, információalapú tevékenységek összessége, amit információs műveleteknek nevezünk. E műveletek alapját egyrészt az összadat-forrású felderítés, másfelől a saját oldalon hatékonyan működtetett vezetési információs rendszer képezi. Az információs műveletek három dimenzióban érvényesülnek, úgymint:

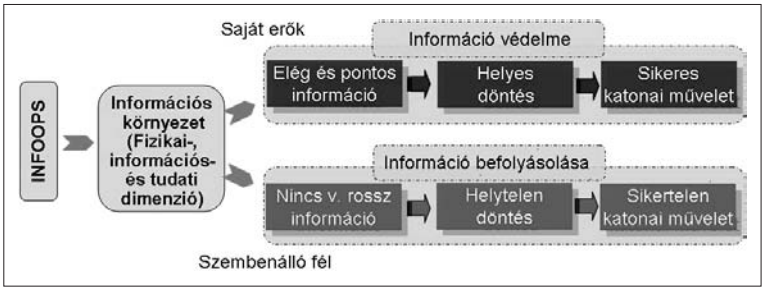
– a fizikai dimenzióban;
– az információs dimenzióban és
– a kognitív (tudati) dimenzióban.

A *fizikai dimenzióban* zajlanak a katonai műveletek, itt működnek a különböző információs infrastruktúrák, rendszerek. A különböző információs infrastruktúrák, információs rendszerek elemei elleni fizikai támadások, illetve ezek védelme ebben a dimenzióban valósul meg.

Az információs dimenzióban (amelyet katonai értelmezés szerint cybertérnek is neveznek) zajlanak a különböző információs folyamatok (adatszerzés, adattárolás, adatfeldolgozás, kommunikáció stb.), és többnyire azok elektronikus úton (a cybertérben) való támadását és a saját információs folyamatainkra irányuló támadások megakadályozását értelmezzük benne.

A kognitív (tudati) *dimenzióban* megvalósuló információs tevékenységek közvetlenül az emberi gondolkodást (véleményt, vélekedést) veszik célba, többnyire az elektronikus és a nyomtatott médián útján vagy közvetlen beszéd formájában. E dimenzióban a cél a döntéshozók közvetlen befolyásolása, ami egybeesik az információs műveletek információs fölényen keresztül elérni kívánt célkitűzésével, vagyis, hogy a döntéshozót olyan helyzetbe hozzuk, hogy saját oldalon optimális döntést hozhasson, másik oldalon pedig pontosan ellentétes hatást érjünk el. Ez pedig kihat a katonai műveletek sikerességére vagy sikertelenségére (lásd 3. ábra).

A fentiek alapján megfogalmazhatjuk, mit is értünk általánosságban az információs műveletek fogalmán. Azért csak általánosságban adjuk meg az információs



3. ábra. Az információs műveletek hatásmechanizmusa

műveletek definícióját, mert a különböző országokban, katonai szövetségekben (például NATO), a haderőkben és azok doktrínáiban eltérő, különböző területeket jobban hangsúlyozó vagy másokat háttérbe szorító megfogalmazásokkal, értelmezésekkel is találkozhatunk.

Az információs műveletek tehát *a fizikai-, az információs- és a tudati dimenzióban 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 elérése és megtartása érdekében minden szinten (politikai, katonai [hadászati, hadműveleti, harcászati], gazdasági, kulturális stb.) és minden időben (béke, válság, háború) alkalmazott információs képességek közötti integráló, szinkronizáló és koordináló tevékenységek.*

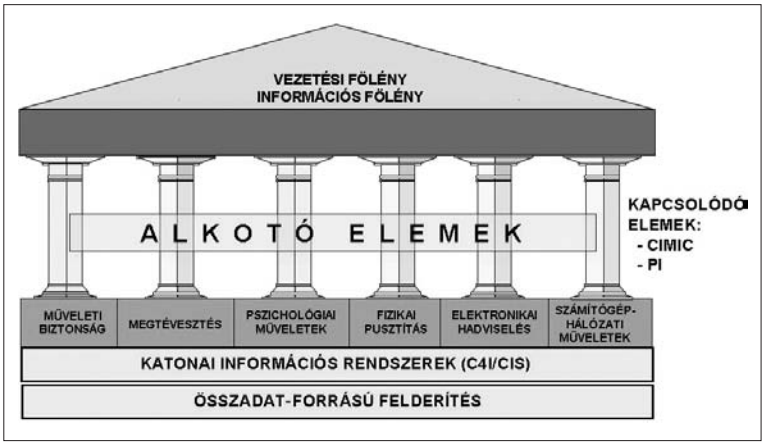
Mint arra már korábban utaltunk az információs műveletek a már korábban is létező és a katonai műveletekben alkalmazott információs tevékenységek közötti összhangot teremti meg. Ennél fogva összetevőit is ezek alkotják, kiegészülve olyan új képességekkel, amelyek csak az információtechnológia fejlődésével, illetve annak a harctéren való megjelenésével egy időben jelenhettek meg (például a számítógép-hálózatok harctéri megjelenése). Amint 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;[12]
– a katonai megtévesztés;[13]
– a pszichológiai műveletek;[14]
– a fizikai pusztítás;[15]
– az elektronikai hadviselés és
– a számítógép-hálózati műveletek.[16]

Az információs műveletek kapcsolódó elemei közé sorolják a civil-katonai együttműködést[17] és a tömegtájékoztatást,[18] mivel ezeknek nincs sem támadó, sem védelmi jellegű megjelenési formája. A hatékony információs műveletek végrehajtásának alapját minden esetben a saját katonai információs rendszerek és az összadat-forrású felderítés adja (ld. 4. ábra).

Itt kell megjegyezni ugyanakkor, hogy több országban eltérőek lehetnek a kategorizálások: például számos országban a fizikai pusztítást nem sorolják az információs műveletek közé, máshol (USA) pedig ún. támogató képességként értelmezik.

12 Operation Security – OPSEC
13 Military Deception – MILDEC
14 Psychological Operations – PSYOPS
15 Physical Destruction
16 Computer Network Operations – CNO
17 Civil-Military Cooperations – CIMIC
18 Public Information – PI



4. ábra. Információs műveletek elemei (általános megközelítés)

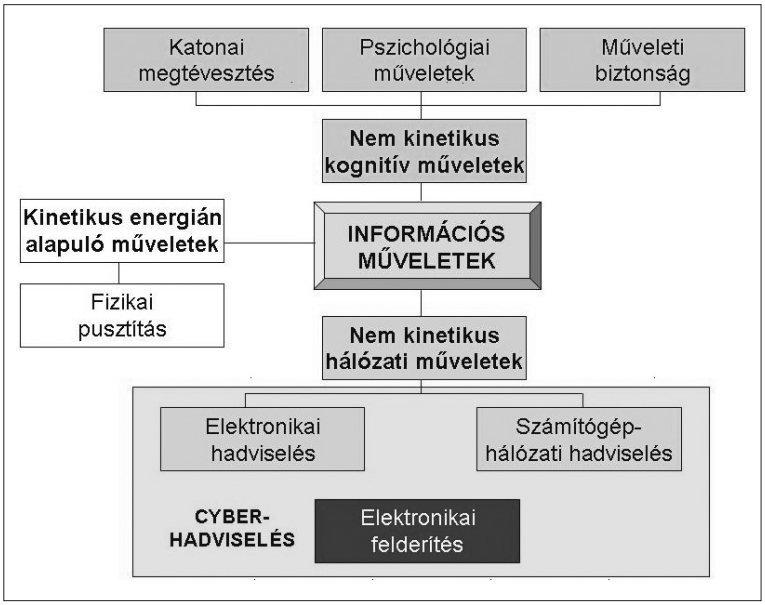
(E különbözőségek illusztrálására a későbbiekben röviden bemutatjuk az információs műveletek területeinek és összefüggéseinek néhány eltérő értelmezését.)

Anélkül, hogy részleteiben bemutatnánk, illetve elemeznénk az egyes területeket, világosan látszik, hogy a felsorolt tevékenységek egyértelműen köthetők az információhoz, információs folyamatokhoz. Az alkotóelemekként definiált területek mindegyikének van támadó vagy védelmi (esetleg mindkét) aspektusa. A területek egyenként is alkalmasak arra, hogy a fizikai, az információs vagy a tudati dimenzióban hatást gyakoroljanak az információs rendszerekre és folyamatokra, és ennek következtében befolyásolják a döntéshozókat a saját és a szembenálló fél oldalán egyaránt. Az információs műveletekben azonban mindezeket egy közös cél érdekében összehangolva, szinkronizálva nagyságrendekkel nagyobb hatékonyságot érhetünk el alkalmazásukkal. Ebben áll az információs műveletek lényege!

Az információs műveletek egy újszerű megközelítés alapján három, egymástól jól elkülöníthető területre bonthatók, amelyek kapcsolódnak a már említett három (ti. a fizikai, az információs és a kognitív) dimenzióhoz. Ezek az alábbiak:

– a kinetikus energián alapuló hadviselés,[19] amelyet a fizikai dimenzióban hajtanak végre és az információs infrastruktúrák, infokommunikációs rendszerek elemeinek fizikai úton való pusztítását, rongálását, tönkretételét jelenti;
– a nem kinetikus energián alapuló kognitív hadviselés,[20] amely alapvetően a tudati, értelmi dimenzióban érvényesül, és a katonai megtévesztést, műveleti biztonságot illetve a pszichológiai műveleteket foglalja magába és
– a nem kinetikus energián alapuló hálózati hadviselés,[21] amely az információs dimenzióban realizálódik, és az elektronikai hadviselést valamint a számítógép-hálózati műveleteket tartalmazza. (Bourque, Jesse, 2007)

19 Kinetic Warfare
20 Cognitive Warfare
21 Network Warfare



5. ábra. Cyberhadviselés az információs műveletekben
(Haig Zsolt–Várhegyi István, 2008)

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, más szóval a cyberhadviselés. Mint ahogy az információs műveletek alapját képezik a katonai információs rendszerek, illetve az összadat-forrású felderítés, úgy a cyberhadviselés alapját is a hálózatokra épülő elektronikus információs rendszerek, és a különböző szenzorhálózatokra épülő elektronikai felderítés képezi (ld. 5. ábra). (Haig Zsolt–Várhegyi István, 2008)

Mint az ábrán látható, és tekintettel a cybertér katonai értelmezésére (amely tágabb, mint a civil felfogás) a cybertérben folytatott műveletek többet jelentenek a számítógép-hálózati műveleteknél. Ide sorolhatjuk például a rádióforgalmazások lehallgatását, a rádió-távközlő hálózatok, rádiólokátorok, navigációs rendszerek stb. elleni elektronikai ellentevékenység különböző formáit (például elektronikai zavarást, elektronikai megtévesztést, elektronikai pusztítást), a számítógép-hálózatok feltérképezését, azokba való bejutást és az adatbázisok tönkretételét, a szerverek túlterhelését vagy a rádió-távirányítású alkalmi robbanó eszközök[22] elleni tevékenységet is. A felsorolt cybertéri tevékenységek csak néhány kiragadott példák 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. (Haig Zsolt–Várhegyi István, 2008)

22 Radio Controlled Improvised Explosive Devices – RC-IED

Az információs műveletek az USA, a NATO és a Magyar Honvédség doktrínáiban

Az USA információs műveletek koncepciója

Az információs műveletek doktrínálisan elsőként az USA haderő doktrínáiban jelentek meg. Ebben nincs semmi meglepő, hisz az Egyesült Államok hadereje volt az, amelynek technikai, technológiai fejlettsége lehetővé tette a legkorszerűbb elvek elsőként való kipróbálását, és amely – ennek megfelelően – először szerzett tapasztalatokat e területen.

A vezetési rendszerek elleni összehangolt tevékenység igénye már az első Öböl-háborút megelőzően is megjelent doktrína formájában.[23] Ez azonban még csak a vezetési, irányítási és híradó rendszerek elleni tevékenységre helyezte a hangsúlyt. 1996-ban – többek között az Öböl-háború tapasztalatait is felhasználva – ezt fejlesztették tovább összhaderőnemi szinten vezetési hadviselési doktrínává,[24] amiben már nem csak az ellentevékenység, hanem a saját információs képességek védelme is megjelent. Ezzel párhuzamosan, szintén 1996-ban dolgozták ki a szárazföldi haderőnemnél az információs műveletek első doktrínáját[25] – amelyet 2003-ban dolgoztak át[26] – és amelyben már fellelhetők voltak a napjainkban elfogadott elvek.

1998-ban összhaderőnemi szinten is megjelent az információs műveletek doktrína első kiadása,[27] amelynek felülvizsgált és átdolgozott, ma is érvényben lévő 2. kiadása[28] 2006-ban jelent meg. Természetesen ezzel párhuzamosan, és az aktuális információs műveletekre vonatkozó doktrínával összhangban, megjelentek az információs műveletek elemeit alkotó különböző információalapú tevékenységek és képességek doktrínái is.[29]

Az USA összhaderőnemi információs műveletek doktrínája megadja az információs műveletek definícióját. E szerint az információs műveletek *„… az elektronikai hadviselés (EW), számítógép-hálózati műveletek (CNO), pszichológiai műveletek (PSYOP), katonai megtévesztés (MILDEC) és a műveleti biztonság (OPSEC) integrált alkalmazása, összehangoltan bizonyos támogató és kapcsolódó képességekkel, amelyekkel befolyásolja, megzavarja, lerontja, vagy korlátozza a szembenálló fél humán és automatizált döntéshozatali folyamatát, miközben megvédi a saját hasonló képességeket."*[30] (JP 3-13 Joint Doctrine for Information Operations, 2006)

---

23 JP 3–13 C3CM in Joint Military Operations (1987). (C3CM – Command, Control, Communications Countermeasures. A szerző megjegyzése)

24 JP 3–13.1 Joint Doctrine Command and Control Warfare (1996)

25 FM 100–6 Information Operations (1996)

26 FM 3–13 Information Operations: Doctrine, Tactics, Techniques and Procedures(2003)

27 JP 3–13 Joint Doctrine for Information Operations (1998)

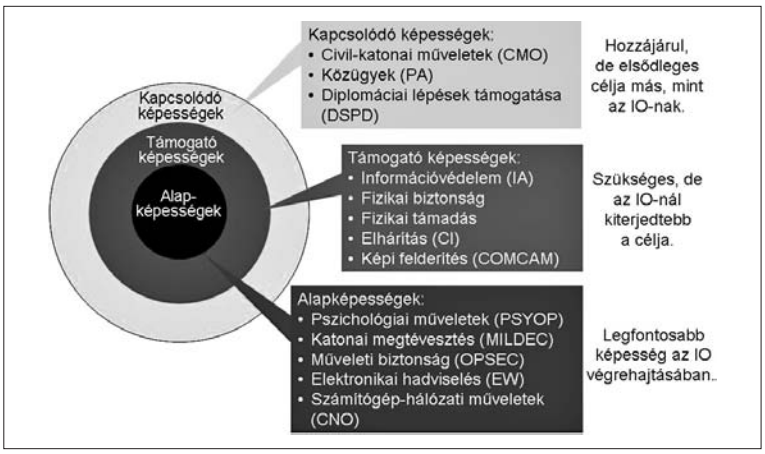
28 JP 3–13 Joint Doctrine for Information Operations (2006)

29 Például: JP 3–53 Joint Doctrine for PSYOPS (2003); JP 3–57.1 Joint Doctrine for Civil Affairs (2003); JP 3–61 Joint Doctrine for Public Affairs (2005); JP 3–13.4 Joint Doctrine for Military Deception (2006); JP 3–13.1 Joint Doctrine for Electronic Warfare (2007)

30 A szerző fordítása

A doktrína az alábbi képességeket nevesíti (ld. 6. ábra):
– Alapképességek:
  = pszichológiai műveletek (PSYOP);
  = katonai megtévesztés (MILDEC);
  = műveleti biztonság (OPSEC);
  = elektronikai hadviselés (EW);
  = számítógép-hálózati műveletek (CNO).
– Támogató képességek:
  = információ védelem (IA);[31]
  = fizikai biztonság;[32]
  = fizikai támadás;[33]
  = elhárítás (CI);[34]
  = képi felderítés (COMCAM).[35]
– Kapcsolódó képességek:
  = civil-katonai műveletek (CMO);[36]
  = közügyek (PA);[37]
  = diplomáciai lépések támogatása (DSPD).[38]

(JP 3-13 Joint Doctrine for Information Operations, 2006)



6. ábra. Az USA információs műveletek képességei
(Az Information Operations Fundamentals felhasználásával szerkesztette a szerző)

31 Information Assurance – IA
32 Physical Security
33 Physical Attack
34 Counterintelligence – CI
35 Combat Camera – COMCAM
36 Civil-military Operations – CMO
37 Public Affairs – PA
38 Defense Support to Public Diplomacy – DSPD

A definícióban előtérbe kerül a már korábban is említett információs tevékenységek közötti koordináló, integráló funkció úgy, hogy emellett hangsúlyozza a különböző támogató és kapcsolódó képességekkel való szoros összhangot. Kiemeli, hogy az információs műveletek az említett képességekkel a szembenálló fél és a saját döntési folyamatra gyakorolnak hatást. Bár ez a definícióból nem derül ki, más helyeken fő célként az információs fölény kivívását és fenntartását fogalmazza meg.

Mint látható a doktrína alap-, támogató és kapcsolódó képességeket nevesít. Az *alapképességek*[39] közé azok tartoznak, amelyek integrált és szinkronizált tervezése, illetve végrehajtása az információs környezetben kiemelt fontosságú. A *támogató képességeknek*,[40] bár más (akár szélesebb körű) katonai céljuk lehet, mint az információs műveleteknek, ugyanakkor az információs környezetben érvényesülnek és hatást is gyakorolhatnak arra. A *kapcsolódó képességeknek*[41] vannak közös kapcsolódási pontjaik az információs műveletekkel, azonban elsődleges céljaik és az alkalmazott rendszabályaik jól elkülönítik és elhatárolják azokat az információs műveletektől. Ennek eredményeként a parancsnoknak és törzsének koordinálnia kell az információs környezetben zajló e tevékenységeket az információs műveletekkel. (JP 3-13 Joint Doctrine for Information Operations, 2006)

A NATO információs műveletek doktrínája

A NATO információs műveletekkel foglalkozó irányelveit először 1998-ban adták ki, amelyet 2002-ben, 2005-ben, majd 2007-ben vizsgáltak felül és dolgoztak át.[42] 2009-ben jelent meg a NATO információs műveletek doktrínája,[43] amely egységes keretbe foglalja a NATO ez irányú elveit.

NATO-meghatározás szerint:

„a. Az információs műveletek 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 NAC[44] *által jóváhagyott felek akaratára, helyzetmegértési folyamatára és képességeire, és ez által támogassa a Szövetség missziós célkitűzéseit.*

b. Az információs tevékenységek hatást gyakorolnak az információra és/vagy az információs rendszerekre. Azokat bármilyen szereplők végrehajthatják, és védelmi rendszabályokat tartalmaznak."[45] (AJP-3.10 Allied Joint Doctrine for Information Operations, 2009)

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

---

39 Core capabilities
40 Supporting capabilities
41 Related capabilities
42 MC 422/3 NATO Military Policy on Information Operations
43 AJP–3.10 Allied Joint Doctrine for Information Operations (2009)
44 NAC – North Atlantic Council (Észak Atlanti Tanács)
45 A szerző fordítása

– 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*, valamint
– 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. (AJP-3.10 Allied Joint Doctrine for Information Operations, 2009)

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

– pszichológiai műveletek (PSYOPS);
– megjelenés, viselkedés, arculat (PPP);[46]
– műveleti biztonság (OPSEC);
– információbiztonság (INFOSEC);[47]
– megtévesztés;
– elektronikai hadviselés (EW);
– fizikai pusztítás;[48]
– kulcsfontosságú vezetők kezelése (KLE);[49]
– számítógép-hálózati műveletek (CNO);
– civil-katonai együttműködés (CIMIC).

A képességeken, eszközökön és eljárásokon túl kiemeli a kapcsolatot a közügyekkel (nyilvánossággal, tömegtájékoztatással). (AJP-3.10 Allied Joint Doctrine for Information Operations, 2009)

Mint látható a NATO-doktrína fokozott hangsúlyt helyez 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 és a felsorolt képességek, eszközök és eljárások koordinációjának fő célja a különböző célcsoportok (saját erők, szembenálló fél és más, NAC által elfogadott felek) *akaratának, megértésének és képességének*[50] befolyásolása.

Szembetűnő ugyanakkor, hogy a NATO-doktrínában az információs műveletek célkitűzéseit nem fogalmazták meg egyértelműen, és az információs fölény kivívá-

46 Presence, Posture and Profile – PPP
47 Information Security – INFOSEC
48 Physical Destruction
49 Key Leader Engagement – KLE
50 will, understanding and capabilities

sára, és megtartására irányuló törekvés markánsan nem fogalmazódik meg.[51] E fölényképesség, mint célkitűzés egyértelműen háttérbe szorul, szemben az USA már korábban bemutatott doktrínájával, ahol ez kiemelt helyet és szerepet kap az egész doktrínában.

További észrevétel, hogy a felsorolt képességek, eszközök és eljárások több esetben nem egzaktak, több átfedés is megfigyelhető közöttük. Csak példaként lehet említeni a pszichológiai műveletek (PSYOPS); a kulcsfontosságú vezetők kezelése (KLE) és a megjelenés, viselkedés, arculat (PPP) képességek doktrínában való elkülönülését. Ha jobban belegondolunk, akkor felfedezhetjük, hogy e három terület az emberek gondolkodására, motivációjára, viselkedésére hat, és azt kísérli meg befolyásolni, ami végül is egyben a pszichológiai műveletek lényege. Egy katonai szervezet megjelenése (kiállása, ellenséges vagy barátságos viselkedése) jelentős pszichológiai befolyásoló hatással bírhat mind a szembenálló fél, mind a semleges érintettek irányába. Tehát e három terület egyként jelenik meg a pszichológiai műveletekben és külön választásuk ennél fogva zavaró lehet, félreértésekre adhat okot. De ugyanilyen problémás lehet az előbb említett három terület és a civil-katonai együttműködés (CIMIC) képességként való megjelenítése, ellentétben a közügyekkel (nyilvánosság, tömegtájékoztatás – PA), amely „csak" mint kapcsolódó terület jelenik meg. A szakértőkben joggal merülhet fel a kérdés: miért alapképesség például a CIMIC és miért nem az a közügyek (nyilvánosság, tömegtájékoztatás – PA)? Erre vonatkozóan egyébként az USA is megfogalmazza fenntartását a NATO AJP–3.10 doktrína első részében.[52]

Rendkívül fontos hangsúlyozni, hogy az információs műveletek képességeinek meghatározásakor *az egyértelműségre* kell törekedni, hisz az ilyen összemosódó területek, nem egyértelmű kategorizálások *erodálhatják az információs műveletek lényegének megértése irányba tett erőfeszítéseinket*.

Információs műveletek megjelenése a Magyar Honvédség doktrínáiban

Az információs műveletek elvei 2002-ben, a Magyar Honvédség (MH) összhaderőnemi doktrína első kiadásában jelentek meg először. A doktrína 2007-ben átdolgozott 2. kiadása a korábbinál bővebb tartalommal foglalkozik e kérdéssel. Ebben egy fejezet tárgyalja az információs műveletek fontosabb összefüggéseit, meghatározását és területeit.

Az MH összhaderőnemi doktrína alapján *„Az információs műveletek azon koordinált tevékenységeket jelentik, melyek a szembenálló fél információira, távközlési információs rendszereire (CIS) gyakorolt ráhatásokkal képesek támogatni a döntéshozókat a politikai és katonai célkitűzéseik elérésében úgy, hogy emellett a saját hasonló rendszereket hatékonyan kihasználják és megóvják."* (Ált/27, Magyar Honvédség Összhaderőnemi Doktrína, 2. kiadás)

51 Egy helyen kerül említésre a doktrínában: 1–4. oldalon

52 AJP–3.10, Record of Specific Reservations. xii oldalon

A doktrínában markánsan megfogalmazódik az információs fölény és végső soron a vezetési fölény kivívására és megtartására való törekvés, amely a hadműveleti fölény megszerzésének egyik fontos összetevője. Ennek elérése érdekében meghatározza az információs műveletek alapvető fajtáit, úgymint:

– a támadó információs műveleteket és
– a védelmi információs műveleteket.

E két fajta információs műveletben az információs fölény az alábbi területek összehangolt alkalmazásával érhető el:

– lélektani műveletek;
– katonai megtévesztés;
– műveleti biztonság;
– információbiztonság;
– fizikai megsemmisítés és
– elektronikai hadviselés.

(Ált/27, Magyar Honvédség Összhaderőnemi Doktrína, 2. kiadás)

Mint látható, e doktrínában foglaltak többnyire összhangban vannak az információs műveletek általános elméleti összefüggéseivel, és több területen kapcsolódnak más haderők (és részben a NATO) doktrináihoz. Jelenleg folyamatban van az összhaderőnemi doktrína átdolgozása, emellett előrehaladott állapotban van az MH információs műveletek doktrína kidolgozása is, ami a tervek szerint szoros összhangban lesz a NATO-doktrínával. A kidolgozók ebben, a NATO-doktrínához hasonlóan, hangsúlyozzák az információs műveletek döntéshozókra való befolyásoló képességét, a nem-kinetikus képességek fontosságát. Ugyanakkor remélhetően a doktrínában egyértelműen és egzaktul, egymást nem átfedő módon kerülnek meghatározásra az információs műveletek képességei.

Összegzés, következtetések

Összegzésként megállapítható, hogy az információs műveletek olyan információalapú tevékenységek összességét, integrált, koordinált alkalmazását jelentik, amelyek több, egymástól látszólag szerteágazó területet fednek le. Az információs dimenzióban, a tudati térben és a fizikai valóságban egyaránt alkalmazhatók olyan információalapú eljárások, amelyek a különböző szereplők (szembenálló fél, saját erők, semleges érintettek stb.) befolyásolásra alkalmasak.

Mindezt már az MH is felismerte, és megtette a kezdeti lépéseket az információs műveleti képességek fejlesztése, és a doktrína kidolgozása terén. Ezek a lépések azonban még csak azokon a területeken láthatók, amelyek különböző technikai, információtechnológiai képesség meglétét különösebben nem igénylik (lásd: CIMIC, PSYOPS stb.). Mindennek az alapja, hogy az MH jelenleg elsősorban ezekkel a képességekkel rendelkezik, és e területeken tud jelentősebb eredményeket felmutatni (lásd például az MH afganisztáni tartományi újjáépítő csoportját).

Ugyanakkor az információs rendszerek támadhatósága és védelme terén lenne mit tennünk. Az egyik ilyen terület az elektronikai hadviselési képességeink növelése. Mint tudjuk, egy bizonyos fejlettségi szinten ez a képesség a 2000-es évek elejéig megvolt az MH-ban. Napjainkban azonban például a rádió-távirányítású alkalmi

robbanó eszközök elleni tevékenység megköveteli, hogy rendelkezzünk olyan zavaró eszközökkel, amelyekkel ezeket az eszközöket biztonságosan hatástalanítani tudjuk. Ezen túlmenően a korszerű hadviselés elveinek megfelelően, az információs fölény elérése érdekében egyéb, az információs dimenzióban alkalmazható, „hagyományos" értelemben vett elektronikai hadviselési képességeket (például korszerű elektronikai támogató és elektronikai ellentevékenységi eszközöket, rendszereket) is fel kell tudni mutatni.

A másik ilyen terület a számítógép-hálózati műveleti képességek megteremtése. Ennek hiánya miatt sok esetben találkozhatunk olyan nézetekkel, miszerint mivel ilyen képességgel az MH nem rendelkezik, ezért például a doktrínában sem kell azt megjeleníteni. Az igazsághoz azonban hozzátartozik, hogy a számítógép-hálózati műveleti képesség három nagyon fontos, egymással összefüggő területet jelent. Jelenti a számítógép-hálózati rendszerekbe való behatolást alapvetően felderítési céllal (vagyis az információk megszerzését, adatbázisokhoz való hozzáférést). Második területe a számítógép-hálózatok támadása, ami konkrétan az adatbázisokban tárolt adatok lerontását, törlését, hamis adatok bevitelét, programfuttatási hibák és ennek következtében a rendszer működésképtelenségének előidézését eredményezi. Harmadrészt pedig jelenti a védelem területét, tehát a meglévő saját számítógépes rendszereink működésének a biztosítását. Ez utóbbi terület, a számítógép-hálózatok védelmének kérdése, mindenféleképpen indokolt, fontos kérdés, hiszen akár a békeidejű vezetési rendszerekben, akár a harctérvezetési rendszerekben a számítógép-hálózatok az MH-ban is elterjedőben vannak. Tehát ezek védelme alapvető fontosságú a hatékony vezetési és irányítási megvalósításához.

A másik kérdés a támadó képesség fejlesztése mind elméleti, mind gyakorlati vonatkozásban. Ez az a terület, amely nem igényel nagy, vállalhatatlan költségbefektetést, technikai eszközpark kialakítást. Ehhez olyan jól képzett szakemberek kellenek, akik a magyar civil és katonai számítógépes szakértők köréből kerülhetnek ki, akik már több esetben bizonyították alkalmasságukat, tudásukat. Ezeknek a szakembereknek a szakirányú felkészítése, ún. etikus hackerekké válása jelentős előrelépés lehetne e téren, és alkalmasak lehetnek arra, hogy például az ország biztonsága szempontjából, de akár a katonai műveletek sikeressége szempontjából is, a cybertérben számítógép-hálózati támadó feladatokat hajtsanak végre. Tehát nem feltétlenül költségigényes eszközbeszerzéseken múlik ennek a képességnek a megteremtése, hanem alapvetően azoknak a szakembereknek a meglétén, felkészítésén, akikből jó néhány van a civil szférában, de talán az MH kötelékében is.

Az MH információs műveleti képessége így válhat teljes értékűvé, egy olyan erősokszorozó területté, amelynek alkalmazásával – és kevesebb hagyományos értelemben vett pusztító képesség igénybevételével – a katonai műveletek hatékonysága akár nagyságrendekkel is növelhető, és a siker biztosítható.

FELHASZNÁLT IRODALOM

Rona, Thomas P.: Weapon Systems and Information Warfare. Boeing Aerospace Co., Seattle, WA, 1976

Libicki, Martin C.: What is Information Warfare? National Defense University. 1995

Schwartau, Winn: Information Warfare: Cyberterrorism: Protecting your Personal Security in the Electronic Age, Thunder's Mouth Press, 2nd edition, 1996. ISBN 1-56025-132-8

Toffler, Alvin: The Third Wave. Bantam Books, 1980. ISBN 0-553-24698-4

Haig Zsolt–Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó. 2005. ISBN 963 327 391 9

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

Haig Zsolt–Várhegyi István: A cybertér és a cyberhadviselés értelmezése. Hadtudomány 2008. Elektronikus szám. ISSN 1215-4121 http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf

JP 3-13 Joint Doctrine for Information Operations. 2006

Information Operations Fundamentals. http://iase.disa.mil/eta/io-fundamentals/IO_Fundamentals/mod1/module.htm (letöltve: 2011. 04. 14)

AJP-3.10 Allied Joint Doctrine for Information Operations. 2009

Ált/27 Magyar Honvédség Összhaderőnemi Doktrína, 2. kiadás. A Magyar Honvédség kiadványa, 2007