MMXIV. II. ÉVFOLYAM I. SZÁM

NEMZETBIZTONSÁGI SZEMLE

KÜLÖNLENYOMAT

NEMZETI KÖZSZOLGÁLATI EGYETEM
NEMZETBIZTONSÁGI INTÉZET
BUDAPEST

Műholdas kommunikációs rendszerek támadhatósága

Szűcs Péter

Absztrakt

A műholdas távközlés a ma emberének már nem tudományos fantasztikum, ismert távközlési forma, még ha Magyarországon nem is elterjedt. Valószínűsítem, hogy a műholdas kommunikációs rendszerek támadási, zavarási lehetőségei viszont csak szűk szakmai körökben ismert. A Föld körül a világűrben 40 országnak van telepített eszköze, több mint 1000 aktív műhold működik különböző magasságú műholdpályán. Ez a „zsúfoltság" kihívást jelenet nem csak az üzemeltetőknek, hanem a rendszerek biztonságáért felelős szakembereknek is. Jelen cikkemben a tanult elektronikai hadviselési módszerek és a kutatásaim során feldolgozott szakirodalom alapján vizsgálom és bemutatom a műholdas távközlési rendszerek állóképességét, működési stabilitását a cikkben ismertetett támadási módszerekkel szemben.

Kulcsszavak: *műholdas kommunikáció, műhold pályák, műholdas távközlés, műholdas személyi kommunikációs rendszerek, zavarás, támadás, EMP, ASAT,*

Abstract

Nowadays satellite telecommunication is not a science fiction for everyday people but it is one way of telecommunications, even here in Hungary it is not very frequent one. However I presume that the methods of attacks and jammings of these satellite communications systems are known in a narrow professional circle. In the space around the world forty countries have installed systems and more than 1000 activated satellite systems operates on satellite orbits on different heights. This „traffic jam" is a challenge not only to the operators but to the security experts of these systems as well. In my essay - through the learned electronic warfare methods and the studied specialist literature in my researches - I scrutinize and present the stability of satellite telecommunications systems against the attacking methods.

Key words: *High Energy Radiofrequency Weapon, satellite personal communication system*

Bevezetés

Doktori tanulmányaim során sokszor találkoztam az információs társadalom, az információ fogalmának meghatározásával, amellyel egyet értetettem, hiszen a magam mérnöki létében, a társadalmi együttélés minden területén tapasztalom, hogy elterjedtek és egyre fontosabb szerepet játszanak az információs és kommunikációs technológiák. Castells szerint az információs társadalmat az elsősorban a gazdaságra jellemző, egységesítő hatású hálózati működési mód és a kulturális szférában meghatározó szerepet játszó különféle egyéni és csoportidentitások közötti konfliktus jellemzi, s ennek következtében bizonytalanná válik az emberi együttélés alapvető intézményeinek működése, az államtól a családig. Mindez átformálja a társadalom egész berendezkedését, s az egyes ember élete is egyre kevésbé válik belátható. [7: pp. 25-27]

Castells az információs társadalom emberre és a társadalomra gyakorolt hatását vizsgálta és nem tért ki a korra jellemző technológiákra. Véleményem szerint a technológiákra kiterjeszthetjük megállapításait, hogy nagy a veszélyeztetésük, ki vannak téve különböző emberi csoportok és érdekek támadásainak, és mint ahogy az embernél is kijelentette a technológiák élete sem belátható. Kutatási témám az információs társadalom által használt kommunikáció egy szeletét vizsgálja, kutatom a műholdas személyi távközlési rendszerek felderíthetőségét, és a dolgozatomban vizsgálni kívánom ezen rendszerek állóképességét a fizikai támadásokkal, elektronikai hadviselési tevékenységekkel szemben. Jelen cikkemben arra vállalkozom, hogy az elektronikai hadviselés ismereteim tükrében választ, vagy válaszokat adjak a kérdésre. Továbbá – a fellelt szakirodalom alapján - bemutatom, hogy a műholdas távközlési rendszereket hogyan, milyen eszközökkel és módszerekkel lehet támadni. Dolgozatomban nem kívánok foglakozni az úgynevezett kinetikus energián alapuló fegyverekkel és pusztító eljárásokkal. A kutatásaimban az alternatív vagy humán fegyverekkel és eljárásokkal, valamint az elektronikai zavaró megoldásokra fókuszálok. Érzékeltetni kívánom, hogy az információs társadalomban nem csak az ember, hanem a technológiák működése sincs biztonságban, sorozatos támadásoknak van kitéve.

Műholdas személyi kommunikációs rendszerek támadhatósága

Az információs társadalom természetesen a hadügyben is alapvető változásokat okoz. Megjelenik az információs hadviselés és annak NATO elvek szerinti katonai megjelenési formája az információs műveletek. Az információs műveletek "*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 e mellet 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 tevékenység.*" [9: p18]

A jövő háborúit és fegyveres konfliktusait az fogja megnyerni, aki megszerzi a másik féllel szembeni információs fölényt. Az információs fölény birtokában képesek vagyunk „látni" az ellenséget, pontosan meg tudjuk határozni jelenlegi helyét, erőinek összetételét, vezetésének rendjét. Mindezek birtokában lehetőségünk van feltárni gyenge pontjait, és a szükséges erőkkel és eszközökkel csapást mérni ezekre a pontokra. [1]

Az USA felső katonai vezetése 2013-ban vizsgálta a katonai műholdas kommunikációs rendszerek fenyegetettségét, és ugyanarra a megállapításra jutott, amelyet a fenti definíció megfogalmaz: Meg kell védeni a műholdas távközlési rendszerüket a különféle támadásokkal szemben, továbbra is fenntartani az információs fölényt. Az amerikai védelmi szféra - megvizsgálva műholdas rendszereit - a fenyegetési formákat három csoportba sorolta:

1. **Fizikai támadások** (ütközések, vagy létfontosságú alkatrészek tönkretétele, amely lehet irányított is egy arra alkalmas támadó műhold segítségével (pl: Kína ASAT program [188]), vagy irányított energiát alkalmazó támadások, mint például a nagy teljesítményű lézerek és mikrohullámú rendszerek, amelyek tönkreteszik a kritikus műholdas

[188] *ASAT,,parazita műhold" néven emlegetett programon a kínai űrkutatási akadémia (CAST) kis műholdak kutatóintézete dolgozik.*

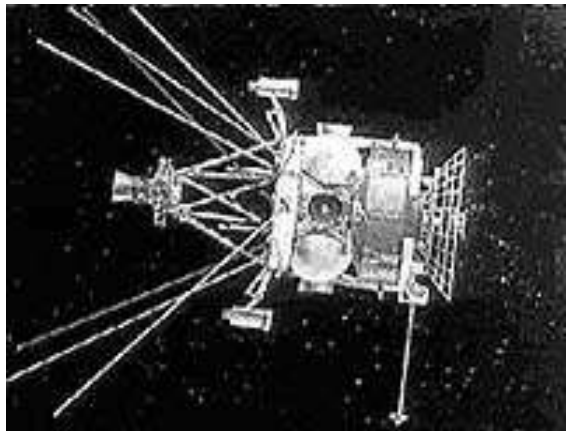
elemeket, mint például a napelem és érzékelők. Egy másik típusú fizikai támadás, amelyik nem közvetlenül a műholdra irányul, hanem a földi infrastruktúra támadásával-tönkretételével éri el a kommunikáció ellehetetlenítését, azonban az előző módszernél jóval olcsóbban.[2]

2. **Elektronikus támadások,** amelyek egyaránt támadhatják a rendszerek műholdas – és földi szegmensét az uplink és downlink csatornák zavarásával.[2]

3. **Kiber-támadás** a műholdak irányításának átvétele, pl. a kommunikáció leállítása, a műhold átmozgatása egy másik pályára, vagy akár a műhold által használt üzemanyag-ellátás megakadályozása, vagy károkozás a fedélzeti elektronikában.[2]

Ha egy civilt megkérdeznénk ki a világon a legnagyobb űrtevékenységgel foglakozó szervezet feltehetően a NASA-t válaszolná. Teljesen igaza lenne, ha csak a polgári alkalmazásokat vesszük figyelembe. Ám ha a katonai célú űrtevékenységet tekintjük, akkor az USA védelmi minisztériuma a DoD[189] a vezető. Az USA régtől fogva domináns szerepet élvezhetett a világűrben: fegyveres konfliktus esetén sem kellett félnie ellenséges kémműholdaktól. Ez a biztonság az ún. ASAT[1] technológiának köszönhetően azonnal megszűnne. Az USA a legnagyobb fizikai pusztítás lehetőségét a kínai ASAT rendszernek tulajdonítja. A műholdak elpusztítására már voltak kínai kísérletek: 2007-ben lelőtték egy rakétával saját időjárási műholdjaik egyikét. Bár erős nemzetközi kritikát kaptak érte, azóta is folytatják az anti-műhold fegyverrendszerek kutatását.[3]

[189] *Department of Defense*



1. ábra ASAT műhold [4]

A néhány centiméteres műholdak az idegen műholdakra akaszkodnak, és háborús esetben zavarják ezek működését, vagy szétrombolják őket. Az egységeknek kicsinek kell lenniük már csak azért is, hogy lehetőleg feltűnés nélkül megközelíthessék áldozataikat, és nem utolsó szempont az sem, hogy egy kis tömegű műhold feljuttatása kisebb költséggel bír. Ezt követően hosszabb ideig csendben kell együtt repülniük, anélkül hogy zavarnák a „gazdaegység" működését. Célpontként felderítő, navigációs vagy kommunikációs műholdak jöhetnek szóba, esetleg lézerfegyverrel felszerelt műholdak, sőt, egész űrállomások is. A paraziták révén a civil műholdak működése is zavarható, tekintve, hogy, a kiberhadviselésben a civil és katonai területek között eltűnnek a határok. Az apró műholdak alkatrészei, úgymint napelemek, áramforrások, kamerák, meghajtó rendszer, vezérlőegység, netán fegyverek, megfelelően kicsiknek kell lenniük. Összeszerelve néhány száz gramm és néhányszor tíz kilogramm között lehet a súlyuk. A földi tesztek során kiderült, hogy az ilyen eszközök rendkívül hatékonyak lehetnek. Egy jól elhelyezett parazita a gazdaműholdat egy percen belül képes megsemmisíteni. [4]

A fenti kínai törekvésekből is látszik, hogy a robotikának és a méretcsökkentésnek mekkora szerepe van a műholdas technológiákban és ezen belül a támadó műholdak kivitelezésében. A műholdas szegmens fizikai támadására alkalmas űreszközök alkalmazása azonban jóval magasabb fejlesztési és üzemeltetési költséget jelent, mint ha a támadást a földi szegmens esetében alkalmazzuk. Másik szempontból nézve, azonban megállapítható, hogy a műholdas szegmens jóval kevésbé védett a fizikai támadásokkal szemben, mint a földi szegmens, amelyik jól megtervezett és megszervezett fizikai védelemmel rendelkezhet.

Az irányított energiájú fegyverek népes csoportját képezik azon eszközök, amelyek nagyteljesítményű elektromágneses energia előállításával és a célra irányításával képesek azokban működési zavarokat, megfelelő energiaszint esetén végleges meghibásodásokat okozni. Ezen eszközöket a szakirodalom rádiófrekvenciás fegyvereknek, nagy energiájú rádiófrekvenciás fegyvereknek[190] nevezi. Attól függően, hogy az eszköz hány alkalommal használható, megkülönböztetjük azokat, amelyek csak egyszeri működésre képesek és akkor véglegesen megrongálódnak. Ezeket impulzusbombának nevezzük, az irodalomban előfordul az E-bomba megnevezés is. Ezen fegyverek mindegyike alkalmas a műholdas rendszerkülönböző részeiben végleges, vagy részleges károkat ejteni.[6: pp 25-29.]

A fenti felsorolás alapján a fizikai támadásokhoz tartozik az EMP[191] fegyverekkel való támadás. A fizikai működése az atombomba hatásának ismeretével egyidős. Az EMP hatásait először nagy tengerszint feletti magasságban robbantott nukleáris fegyvereknél figyelték meg. Ezek a hatások nagyon rövid fel- és lefutó karakterisztikát (néhány 100 ns), de igen intenzív elektromágneses impulzust eredményeznek, melyek a forrástól távolodva csökkenő értéket mutatnak. Az EMP hatása egy elektromágneses lökéshullámban érvényesül. A mező által létrehozott elég erős, meredek karakterisztikájú több ezer voltos feszültségnek nem védett elektromos vezetők, huzalozás, nyomtatott áramköri vezetők vannak kitéve.

Az EMP pusztító jelentősége abban nyilvánul meg, hogy visszafordíthatatlan kárt tud okozni az elektronikus eszközök széles körében, és így akár a műholdas-, vagy földi szegmensben egyaránt. A műholdas kommunikáció szinte minden része kivétel nélkül célhardverekből épül fel, amely ezáltal különösen sebezhető az EMP fegyverek által. A fegyver erősségének függvényében tudunk egy rendszert részben, vagy teljesen hatástalanná tenni, melyet ez alapján elektromágneses keménységnek nevezünk. A kár ahhoz hasonlít, amikor a közelben becsapódik egy villám, ami megkövetelheti az egész rendszer-, vagy bizonyos részeinek cseréjét. Több ezer volt feszültség és 10-20 kA áram is indukálódhat az egyes helyiségekben a különböző falakon futó vezetékek által létrehozott hurkokban. Így veszélyben lehet például egy számítógép, melyhez az egyik fal mentén a telefonkábel, a másik mentén a villamos áramot vivő kábel fut. Az eredmény egy szétrobbant integrált áramkör lehet. A számítógépes adatfeldolgozó-, kommunikációs rendszerek, jelátvivő rendszerek bele vannak ágyazva a katonai felszerelé-

[190] *High Energy Radiofrequency Weapon – HERF*
[191] *Electromagnetic Pulse*

sekbe, mint processzorok, digitális vezérlő áramkörök és így potenciálisan ki vannak téve az EMP hatásainak. [5, 6]

A HERF fegyverek nagy teljesítményű irányított rádiófrekvenciás jelek sugárzásával képesek egy adott elektronikai rendszert megbénítani. A fegyvereknek jelentős hatása van minden olyan infrastruktúrára, amelyben elektronikai alkatrészekből álló berendezések üzemelnek. Ahhoz, hogy megóvjuk az elektronikus rendszereket, - jelen esetben ezen műholdas rendszereket - az adott támadással szemben valamiféle védelmet kell felépíteni a HERF fegyverek hatásai ellen. A HERF egy olyan fegyver, amely rádiófrekvenciás energiát használ rombolásra, és az elektromos rendszer megsemmisítésére. Bárhol alkalmazható, legyen az közeli terület, vagy távoli célpont. Ezeket az eszközöket két csoportra lehet osztani:

- Nagy Energiájú Mikrohullámú fegyver;
- Ultra Szélessávú fegyver.

Ezek nem nukleáris elektromágneses impulzust használnak, csak hasonló impulzusokat állítanak elő. A célpontnak teljesen mindegy melyikkel támadják, mert a hatás ugyanaz, tönkre teszi az elektromos rendszereket. Alkalmazásának lehetősége és a lehetséges célpontok száma egyre nagyobb. [5: pp. 145-146, 6: pp. 25-29]

Az utóbb bemutatott fegyverek többsége akár otthoni körülmények között is kis ráfordítással előállítható, ami korunk túlelektronizált világában nagy veszélyeket rejt magába. Ezen fegyverek használata beleillik az elektronikai támadások csoportjába. Az Interneten találhatók olyan kapcsolási rajzok, amelyek alapján egy jól felkészült szakember képes ilyen eszközt megépíteni. Az amerikai haditengerészet drónok elleni energiafegyvert állít hadrendbe, amelyet 2014-ben már használni is akarnak a Popular Science beszámolója szerint. A Kratos rendszer egy lézeres távmérővel beméri a célpontot, majd az energiafegyverrel tüzel a pilóta nélküli repülőgépre, tönkreteszi az elektronikáját. Így a drón nem képes már navigálni, sem a fő egységeit működtetni, és lezuhan. Szemben a ballisztikus fegyverekkel a hatás gyakorlatilag azonnali, itt nem lehet elkerülő manővereket tenni. Amit jól mértek be, annak vége. Ráadásul egy lövés kevesebb, mint egy dollárba kerül, és nincsenek eltévedt lövedékek sem. A fegyverrendszer fejlesztése hat évet vett igénybe. [8]

Az eszközt drónok elleni harcra fejlesztették ki, de a képességeiből következtethetünk, hogy az eszköz alkalmassá tehető többek között a műholdas rendszerek elleni fizikai pusztításra is, elsősorban a földi szegmens fizikai megsemmisítésére.

2. ábra Kratos rendszer [8]

Műholdas személyi kommunikációs rendszerek támadhatósági modelljének vizsgálata

Az általam vizsgált műholdas rendszerek mindegyike működési szempontból három alapvető részre tagolható, bontható. Ezek a részek a következők:

1. **Műholdas szegmens**, amely magába foglalja a LEO[192], MEO[193] vagy a GEO[194] pályán keringő távközlési műholdakat.
2. **Földi szegmens**, amely magába foglalja a műholdak irányítását, távvezérlését és pályán tartásának elemeit, illetve azokat a földi átjátszó állomásokat, amelyek összekapcsolják a műholdas rendszert a földi infrastruktúrával.
3. **Felhasználói szegmens**, amely magába foglalja a műholdas kommunikációs eszközökön kommunikáló felhasználói készülékeket.

Ez a három részes tagozódás alkalmas arra is, hogy ennek megfelelően vizsgáljam a rendszerek sebezhetőségét. A különböző részek sajátos technikai paramé-

[192] *Low Earth Orbit*
[193] *Medium Earth Orbit*
[194] *Geosynchronous Earth Orbit*

terei, működési sajátosságai, az egyes szegmensek földrajzi, fizikai elhelyezkedései – ezáltal a hozzáférés fizikai és anyagi lehetőségei –, mind-mind meghatározók az ellenük alkalmazott zavarási, vagy megsemmisítő eljárások szempontjából. A következő fejezetben ezen modell, és az USA felső katonai vezetésének 2013. évi megállapításai szerint vizsgálom a rendszerek sebezhetőségét, támadhatóságát.

A műholdas személyi kommunikációs rendszereket, ha a működési modell szerint vizsgáljuk a támadásokkal szemben, akkor megállapíthatjuk, hogy a földi szegmens a legjobban sebezhető rész. Itt érvényesül a bemutatott fegyverek, elektronikai zavarok hatása a legkönnyebben, nem beszélve arról, hogy tönkremenetele a rendszer teljes összeomlásához vezet. A kisugárzott impulzusok hatására a földi állomások elektronikus alkatrészeiben, illetve a számítógépes vezérlő részekben okoz maradandó sérüléseket, ezzel téve tönkre a rendszert. Globális rendszerek esetén viszont az irányító központok más földrészeken való elhelyezése miatt nehézségekbe ütközhet, a rendszer teljes megsemmisítése csak világméretű, globális akciókkal érhető el.

A második helyen a felhasználók készülékei sebezhetők a legjobban, azonban ez nem vezet a rendszer tönkremeneteléhez. Konfliktus esetén azonban egyes felhasználói kör kommunikációjának zavarása nagy nyereséggel járhat. Korunk válságövezeteinek többségére megállapítható, hogy a távközlési földi infrastruktúra nem, vagy részben kiépített, ezért a műholdas telefónia elterjedése ezekben az országokban jelentős. A különböző terroristatámadásoknál előszeretettel használják a telefonokat különböző házi készítésű robbanóeszközök aktiválására, éppen ezért is bír nagy jelentőséggel a felhasználói szegmens támadása. A doktori kutatásaimban a különféle műholdas rendszerekben kezdeményezett felmenő kommunikáció detektálása, iránymérési eredménye hatásosan alkalmazható a különféle elektronikai hadviselési eszközökkel való támadások előkészítéséhez, hatásos alkalmazásához.

Az űrszegmens műholdjai sebezhetők a legnehezebben, ez a legköltségesebb és legfejlettebb eszközökkel és módszerekkel lehetséges. A fent ismertetett fegyverek által a rendszer teljes leállásához több műhold együttes tönkremenetele szükséges. Minden rendszer köteles legalább 10% tartalékolást alkalmazni, tehát egyes műholdak tönkremenetele esetén lehetőség van a tartalék műholdak aktivizálására. A műholdak földtől való nagy távolsága tovább nehezíti, illetve drágítja a megsemmisítésére irányuló estleges próbálkozásokat. Az Iridium rendszer esetén 66 műhold biztosítja a globális lefedettséget, amelynél 6 műhold képez tartalékot. A rendszer szintű leálláshoz ezért legalább 7 műhold tönkretétele szükséges. Ez a rendszer leállás a GEO rendszereknél már 2 műholddal is

biztosítható. A műholdas szegmens támadásához a cikkben bemutatott kínai ASAT rendszer lehet az egyik példa. Természetesen nem a Kínai ASAT rendszer az egyetlen, amely ilyen képességekkel rendelkezik, kiemelésére azért került sor, mert napjainkban az USA katonai vezetése ezt a rendszert tarja legveszélyesebbnek a műholdas szegmens tekintetében.

Következtetés

A cikkem természetesen nem mutat be minden lehetséges támadó eszközt, amelyek még ezeken felül alkalmasak lehetnek a rendszerek támadására, elpusztítására. A cikk megírásával arra kívántam rámutatni, hogy az űrben működő civil vagy katonai távközlési rendszerek milyen mértékben vannak kitéve egy esetleges támadásnak, független attól, hogy ez egy katonai konfliktus, vagy egy hackertámadás.

A fenti vizsgálat alapján a következő megállapítások tehetők:

1. A **műholdas szegmens zavarása, elpusztítása bír a legkisebb valószínűséggel**, a fent ismertetett okok folytán. A műholdak ellen korlátozottan bevethetők a fizikai pusztítás, az elektronikai zavarás és a kiber-támadás módszerei és eszközei.
2. **A földi szegmens zavarása, fizikai rongálása végezhető el a legnagyobb valószínűséggel**, hiszen a támadó eszközök könnyen eljuttathatók közvetlen közelébe. Ezen műholdas alkotó elemek ellen a bevethetők a fizikai pusztítás, az elektronikai zavarás és a kiber-támadás módszerei és eszközei.
3. **A felhasználók készülékei sebezhetők a legjobban**, azonban ez nem vezet a rendszer tönkremeneteléhez. Konfliktus esetén azonban egyes felhasználói kör kommunikációjának zavarása nagy nyereséggel járhat.

Jelen cikkemben nem foglalkoztam azzal a fontos kérdéssel, hogy a most bemutatott eszközök és módszerek ellen hogyan lehet védekezni, hatásaikat csökkenteni. A védekezéssel kapcsolatos kutatásaimat a következő cikkben ismertetem. Az általam feldolgozott szakirodalom alapján viszont látom, hogy az egyre kreatívabb támadásokkal szemben már nem jelent védelmet egy meghatározott védelmi módszer, megoldást csak a komplex védelmi struktúrák jelenthetik.

Felhasznált irodalom:

[1] Dr Kovács László: Az elektronikai hadviselés helye és szerepe a jövő információs hadviselésében
http://www.zmne.hu/kulso/mhtt/hadtudomany/2001/2/04/t-05.htm (letöltve 2014. 01. 10.)
[2] Options for Military Satellite Communications Debated http://www.spacepolicyonline.com/news/options-for-military-satellite-communications-debated (letöltve: 2014. 01. 11.)
[3] Az amerikai katonaság tart a kínai űrprogramtól http://galaktika.hu/az-amerikai-katonasag-tart-a-kinai-urprogramtol/(letöltve: 2014. 01. 11.)
[4] Műholdparaziták http://index.hu/tudomany/muholdpara/ (letöltve: 2014. 01. 14.)
[5] Szűcs Péter: Műholdas személyi kommunikációs rendszerek állóképessége a rádiófrekvenciás-, nagyfrekvenciás- és elektromágneses impulzus fegyverek ellen, Repüléstudományi Közlemények Különszám 2. „Future Aviation Technologies" 2002. ISSN 1417-0604 p143-148 (pp. 145-146)
[6] Dr. Ványa László: Irányított energiájú fegyverek Egyetemi jegyzet Nemzeti Közszolgálati Egyetem 2013. p. 55 pp. 25-29
[7] Pintér Róbert (szerk.): Az információs társadalom - Az elmélettől a politikai gyakorlatig. Budapest 2007. ISBN 978 963 693 061 5 p.240 (pp. 25-27)
[8] Kratos defence and security solutions http://www.kratosdefense.com/ (letöltve:2014. 01. 14.)
[9] Haig Zsolt: Az információs hadviselés kialakulása, katonai értelmezése. Hadtudomány, XXI. évf. 1-2 sz. 2011., ISBN 1215-4121 pp. 12-28.