Számítógép–hálózati hadviselés rendszere az információs műveletekben

Dr. Haig Zsolt mk. alezredes, egyetemi docens

A számítógépek megjelenése és hálózatba kapcsolása a katonai információs rendszerekben jelentős mértékben megváltoztatta a katonai műveletek vezetési folyamatát. Az információtechnológia e területének rohamos előretörését jól szemléltetik azok az új hadviselési elvek, melyeket a szakirodalomban hálózatközpontú hadviselésnek és információs műveleteknek neveznek. Az új technológia nagyarányú elterjedése természetszerűleg magával hozta e rendszerek támadhatóságának és védelmének problémáját is, melyet gyűjtőnéven számítógép-hálózati hadviselésnek neveznek. A cikk bemutatja eme új képesség helyét, szerepét az információs műveletek rendszerében, valamint a hálózatok támadásának és védelmének eszközeit és módszereit.

Bevezetés

A számítógépek elterjedésével és különösen azok hálózatba kapcsolásával nagymértékben megnőtt a vezetési és információs rendszerekhez való hozzáférés lehetősége, és ezzel egy teljesen újfajta támadási mód is kialakult. Az Internet ezt a tendenciát csak még jobban felerősítette. Ma már szinte valamennyi nagyobb hálózat kapcsolódik az Internethez, igénybe veszi annak szolgáltatásait, vagy valamilyen szolgáltatást biztosít az Internet felé. Az Internet felől azonban fel kell készülni az esetleges támadásokra is, amik lehetnek betörési kísérletek, de a belső hálózat tönkretételére irányuló próbálkozások is.

A számítógép–hálózati hadviselés (Computer Network Operations – CNO) az információs társadalom kialakulásával és fejlődésével hozható összefüggésbe. Napjainkban ezt a tevékenységi formát a szakirodalomban informatikai hadviselés, vírus hadviselés, cyber-hadviselés, hacker-hadviselés, stb. elnevezéssel illetik. Mindegyikre érvényes – az elnevezéstől függetlenül –, hogy ez a típusú hadviselési forma célját tekintve a számítógépes rendszerek működésképtelenné tételét, illetve ezzel ellentétesen, a saját rendszerek működőképességének biztosítását szolgálja. A másik nagyon fontos tényező, hogy az információs társadalom működéséből fakadóan ezek a számítógépek hálózatba kapcsolt rendszerek, és így a hadviselés más különböző folyamatai is a hálózatokon keresztül valósulnak meg.

1. Számítógép-hálózati hadviselés helye az információs műveletekben

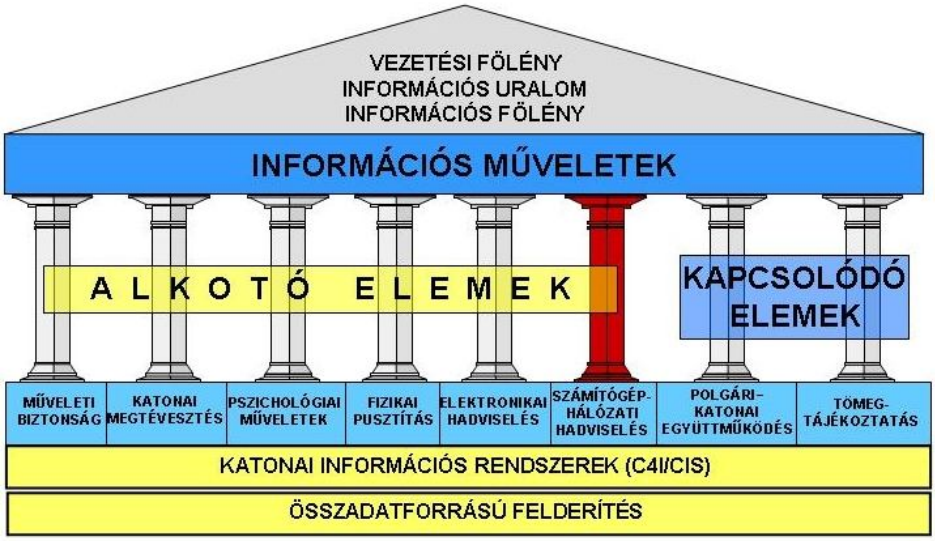
A védelmi szektorban az információt két területen alkalmazzák. Egyrészt az információt, mint a *vezetés eszközét* használják fel a hadviselésben, másrészt az információt, mint un. nem kinetikus energiát felhasználó *„fegyvert”* alkalmazzák az információs műveletekben. Az első esetben az információt a harc–hadművelet vezetése során, illetve a fegyverirányítás folyamatában használják fel, pl. a hálózatközpontú hadviselés keretében, míg a második esetben az információval harcolnak: védenek, vagy támadnak. Ez utóbbi tevékenységeket az e feladatra szakosodott információs harcosok végzik.

Az információs műveletek célja az információs fölény, információs uralom és végső soron a vezetési fölény kivívása, a saját oldali vezetési ciklus számára időcsökkentés, a szembenálló fél vezetési időciklusa tekintetében pedig időnövelés elérése érdekében, és ezek által a hadműveleti fölény elérésének elősegítése.[1] Megszerzésének és megtartásának két azonos fontosságú oldala van, úgymint: *kihasználni és megvédeni a saját információs képességeket,* illetve *gyengíteni az ellenség információs lehetőségeit.* Mindezek érdekében adott szervezetek béke, válság és konfliktus időszakában információs műveleteket hajtanak végre.

Az információs műveletek alkotó- és kapcsolódó elemei a következők:

- műveleti biztonság;
- katonai megtévesztés;
- pszichológiai műveletek;
- információs infrastruktúrák, vezetési objektumok fizikai pusztítása;
- elektronikai hadviselés;
- számítógép–hálózati hadviselés;
- polgári–katonai együttműködés;
- tömegtájékoztatás.

Az összetevő elemeken kívül az információs fölény kivívásában és fenntartásában fontos szerep hárul a *vezetési információs rendszerekre* és az *összadatforrású felderítésre*, melyek az információs műveletek támogató elemeit jelentik. (1. ábra)



1. ábra: Az információs műveletek elemei

Az információs műveletek nem más, mint 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 egymással összhangba hozott széles tevékenységi területen, számos külön–külön is alkalmazható információs vagy információalapú tevékenység révén érvényesülnek. Hatékony alkalmazásuk békeidőben elkerülhetővé teheti a pusztító katonai tevékenység szükségességét.

Az információs műveletek céljai elérése érdekében fizikai–, információs– és tudati dimenzióiban fejti ki hatásait. A számítógép-hálózati hadviselés ezek közül egyértelműen az információs dimenzióban érvényesül

Az információs dimenzióban folytatott információs műveleti tevékenységek a különböző információs folyamatok, adatszerzés, adatfeldolgozás, kommunikáció, stb. többnyire elektronikus úton való 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 folyamataira irányuló hasonló támadásának megakadályozása is.

A fentiekben leírtak alapján egyértelműen látszik, hogy napjainkra a számítógép-hálózati hadviselés szerves részévé vált az információs műveleteknek. Korábban e tevékenység nem jelent meg ezen integrált tevékenységi formában. Napjainkban azonban az informatika

fejlődése, a katonai vezetési rendszerekben a számítástechnika óriási térhódítása, valamint a különböző rendszerek hálózatba szervezése azt eredményezte, hogy e területen folytatott támadó és védelmi tevékenységek jelentősen hozzájárulhatnak az információs fölény kivívásához.
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.
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 az információs műveletek célkitűzéseinek eléréséhez. Természetesen az információs műveletek 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 hadviselést többféleképpen is osztályozhatjuk. A NATO-ban elfogadott osztályozás szerint a következő tevékenységeket foglalja magába:

- a számítógép–hálózati felderítés (Computer Network Exploitations – CNE);
- a számítógép–hálózati támadás (Computer Network Attack – CNA);
- a számítógép–hálózati védelem (Computer Network Defence – CND). [2]

A számítógép–hálózati felderítés és támadás megvalósítási formáiban számos hasonlóságot mutat, céljaiban azonban különbözik egymástól. Számos szakirodalom ezért egyként is kezeli azokat. A továbbiakban e két tevékenységet az egyszerűség kedvéért számítógép–hálózati ellentevékenység címen egy pontban tárgyaljuk.

2. Számítógép–hálózati ellentevékenység

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. [2]
A számítógép–hálózati ellentevékenység hatékonysága nemcsak a harctevékenységek során jelentkezik, hanem annak megkezdése előtt is, mivel jelentősen képesek akadályozni a szembenálló fél felkészülését, vezetési folyamatait, ugyanakkor nagymértékben csökkentik a saját erők felfedését. Ezen túlmenően az informatikai támadások mint un. „Soft Kill" támadások jelentősen csökkentik mindkét fél veszteségeit, elsősorban az élőerő veszteségét. Az informatikai támadásokkal el lehet érni az erők és eszközök más feladatokra való átcsoportosítását.
A számítógép–hálózati ellentevékenység a támadókkal, az alkalmazott eszközökkel, a hozzáférés módszereivel, az eredménnyel és a támadás céljával jellemezhetők. A támadók

köre egészen széleskörű lehet. A támadások származhatnak egyes személyektől, jogosulatlan felhasználóktól, csoportoktól, terroristáktól valamint különböző nemzeti szervezetektől külföldi hírszerző szolgálatoktól, katonai szervezetetektől. Szakértők véleménye szerint a rendszerbetörések nagy többségében, mintegy 70–90%-ban belső munkatárs, vagy volt munkatárs is közreműködik. Az ilyen betörőket, attól függően, hogy milyen a betörés jellege vagy célja, más–más nevekkel illetik. Ezek közül a legismertebbek a hacker, cracker, a phreak és a jerk.

A támadó információs műveleteknek - és így a számítógép-hálózati ellentevékenységnek is - kettős funkciójuk van: egyrészt minden lehetséges eszközzel *elfogni, felfedni*, másrészt *befolyásolni*, *tönkretenni* a másik fél információit. E kettős funkciót – a támadó jellegű információs műveletek nagyfokú hatékonysága érdekében – a *fizikai–, információs– és a tudati dimenzióban egyaránt, egymással összehangoltan* kell érvényre juttatni.

Az információs támadáson belül a számítógép-hálózati ellentevékenység az információs dimenzióban *közvetlen* és *közvetett* formában valósulhat meg. A *közvetlen információs támadás* – más néven belső vagy behatoló jellegű támadás – során a támadó fél egyrészt a különböző információbiztonsági rendszabályokat kikerülve bejut a számítógép–hálózatokba, hozzáfér különböző adatbázisokhoz stb. és ezáltal számára hasznosítható *információkhoz jut*. Másrészt megtévesztő információkkal, rosszindulatú szoftverek bejuttatásával *tönkreteszi, módosítja, törli* stb. a szembenálló fél számára fontos információkat. *A közvetett információs támadás* – más néven külső vagy szenzor alapú támadás – során a támadó fél hozzáférhetővé teszi az ellenség számára a saját félrevezető információit, ezáltal *megtéveszti a szembenálló fél felderítő rendszerét* és így befolyásolja a helyzetértékelését.[3]

Természetesen a közvetlen és közvetett támadást megfelelően összehangolva célszerű alkalmazni, ezáltal is erősítve egymás hatékonyságát. A felsorolt támadási funkciókat, formákat és konkrét tevékenységeket azok hatása és támadási szintje szerint a 1. táblázat szemlélteti.

1. táblázat: A számítógép-hálózati ellentevékenység hatása és támadási dimenziói [3]

Funkció:	**ELFOGÁS, FELFEDÉS**		**BEFOLYÁSOLÁS, TÖNKRETÉTEL**					
Biztonsági jellemző:	**Bizalmasság** sérül		Adatok **sérülékenysége** nő Szolgáltatások **elérhetősége** csökken					
Forma:	**Közvetett**	**Közvetlen**	**Közvetett**			**Közvetlen**		
Támadó tevékenység: **Támadási szint:**	**Információ források felderítése**		**Megtévesztés**	**Zavarás**	**Pusztítás**	**Megtévesztés**	**Zavarás**	**Pusztítás**
Információs dimenzió	Hálózati topológia kívülről való feltérképezése Titkosítás megfejtés, dekódolás	Számítógép hálózatok adataihoz való rejtett hozzáférés Trójai programok alkalmazása Jelszólopók telepítése	Megtévesztő e–mail üzenet továbbítása Megtévesztő hálózati tevékenységek folytatása	Hálózatok adatokkal való mesterséges túlterhelése (FLOOD ATTACK), ezáltal a hálózati hozzáférés akadályozása		Trójai programok bejuttatása megtévesztő tevékenység útján Működő programokkal (virulens ágensek) adatok módosítása	Rosszindulatú szoftverekkel, programokkal (férgek, vírusok stb.) hálózati szolgáltatásokhoz való hozzáférés megakadályozása, adatok, adatbázisok tönkretétele	

A számítógép–hálózati ellentevékenységek fajtái az alábbiak lehetnek:

- illetéktélen hozzáférés az információkhoz (adatlopás);
- illetéktelen adatbevitel;
- rosszindulatú szoftverek bevitele;
- információs környezetszennyezés. [4]

Az illetéktélen hozzáférés az információkhoz az egyik legelterjedtebb fajtája a támadásoknak, amely a számítógép–hálózati felderítéssel hozható összefüggésbe. Az adatbázisokban rendszerezett információk mind anyagi mind erkölcsi értelemben sokat érnek. Annak érdekében, hogy ezekhez az adatbázisokhoz, információkhoz a jogosult felhasználók hozzáférjenek, valamilyen szintig hálózaton keresztül is elérhetővé kell számukra tenni őket. Ebben az esetben azonban megnyílik az út az illetéktelen felhasználók számára.
Az illetéktelen felhasználók – adatlopók, számítógépes kémek – a hálózaton található biztonsági rendszerek hiányosságait, vagy a legális belépéshez szükséges kritikus információk jogosulatlan megszerzésével megnyílt lehetőségeket használják ki annak érdekében, hogy az adott helyen meglévő információt megszerezzék. [4]
A hálózatok lehallgatása rendkívül jelentős, mivel ezúton tömegével lehet a hálózati belépéshez szükséges jelszavakat illetéktelenül megszerezni. A hálózatok lehallgatásra alkalmasak a szabadon elérhető un. „anonymous" FTP helyekről letölthető szoftverek, melyeket egyébként a hálózati menedzserek hálózatmonitorozásra, a forgalom analizálására fejlesztettek ki. E szoftverek használata kezdetben meglehetősen erőforrás–igényesnek számított, de az utóbbi idők átlagos PC–i már képesek futtatni ilyen programokat, így a lehallgatás széles körben elérhetővé vált. A hálózat kivitelezése, topológiája nagyban befolyásolja a lehallgatás lehetőségeit, azonban ez idáig a lehallgatás elleni védelem nemigen volt szempont a hálózattervezéskor. Szerencsére korunk új technikái, melyeket a nagyobb hálózati teljesítményigények miatt alkalmaznak, nagyban nehezítik a lehallgatást.
Számos adatátviteli mód nehezen hallgatható le (ISDN, GSM, optikai átvitel, vagy a szinte lehallgathatatlan szórt spektrumú átvitel), de a tökéletes megoldást csak a teljes adatforgalom titkosítása jelentheti. Több operációs rendszer és hálózati alkalmazás eleve titkosított formában küldi át a jelszavakat, vagy ún. titkosított, egyszer használatos jelszavakat használ. A jelszavak titkosítása azonban önmagában még nem megoldás, hiszen a titkosított jelszót elfogva, azt újra lejátszva beléphetünk egy rendszerbe anélkül, hogy a jelszót tudnánk. Ezért a mai rendszerek különböző módszereket alkalmaznak a titkosított jelszó újrafelhasználásának megakadályozására is. [5]
Az információkhoz való illetéktélen hozzáférés egy különleges módja a *Van Eck–Monitoring,* ami azt a jelenséget használja ki, hogy minden fajta elektromágneses rendszer, pl. a számítógép képernyője, kábelei, hardver elemei bizonyos mennyiségű és intenzitású elektromágneses sugárzást bocsátanak ki. Ezek érzékeny vevőkkel detektálhatók, értékelhetők és belőlük az információk helyreállíthatók. [6]
Az illetéktelen adatbevitel során a felhasználó adatbázisát próbálják meg módosítani, és ezáltal károkat okozni. A különböző adatbázisokba strukturált információk és azok megbízhatósága egy adott rendszer működéséhez elengedhetetlen fontosságúak. Abban az esetben, ha illetéktelen adatbevitel történik, akkor ezek az adatok a valóságostól eltérőek lesznek, információ tartalmuk hamissá válik. Ha a felhasználók ezt továbbra is megbízható, hiteles információnak tartják, abban az esetben óriási anyagi károk keletkezhetnek, illetve nagyfokú bizalmatlanság alakul ki az információs rendszerrel szemben.
Az illetéktelen adatbevitel – mint veszélyforrás – akkor is fennáll, ha nem szándékos adatbevitelről beszélünk. A jogosultság ellenőrzésén túl komoly szervezési, programozási feladat az adatok előzetes szűrésére, ellenőrzésére szolgáló lépések beiktatása a munkafolyamatba. [4]
Rosszindulatú szoftverek bevitelével a támadó képes zavart előidézni, túlterhelni, működésében akadályozni, és akár működésképtelenné tenni a felhasználó számítógépét. Minden olyan szoftver rosszindulatúnak tekinthető, amely nem az információs rendszer működésének a biztosítása céljából kerül az információs rendszerbe, és amelyek valamilyen módon az adott információs vagyon ellen irányulnak.

Rosszindulatú szoftvereknek (Malicious Software - MALWARE) általában azokat a programokat hívjuk, amelyek anélkül jutnak a számítógépbe, hogy arra a felhasználó engedélyt adott volna, vagy ennek az engedélynek a tudatában lenne. Bejutva a rendszerbe, ott végrehajtó objektumokat – programokat – módosíthatnak, illetve a gépben kárt okoznak, vagy okozhatnak. Ezek a szoftverek potenciálisan az alábbi károkat okozhatják:

- erőforrásokat foglalhatnak le (memória, lemezterület, processzorteljesítmény);
- adatvesztést, adatmódosítást, hardver hibát okozhatnak, és
- eltávolításuk időt és energiát igényel.

A MALWARE–ket számos módon lehet csoportosítani, egységes rendező elv nincs kategorizálásukra. Így e programok között megtalálhatók a mindenki számára közismert vírusok, a levélbombák, trójai programok, férgek, stb.

A rosszindulatú szoftverek információs rendszerbe való juttatásának több célja lehet. Egyes esetekben nem a konkrét károkozás a cél, hanem annak bizonyítása az elkövető részéről, hogy fizikailag (szoftveresen) be tud jutni az adott információs rendszerbe, felfedezi annak rejtett hibáit, és a bejutással – esetleg nagyon kis anyagi kár okozásával, pl. defacement, azaz adott internetes honlap arculatának módosításával, „átrajzolásával" – adja ennek tanúbizonyságát. E tevékenység az esetek jelentős részében nem okoz közvetlenül komolyabb anyagi kárt, hiszen a megváltoztatott oldal néhány órás munkával, viszonylag kis anyagi és energia ráfordítással visszaalakítható az eredeti formájába. Közvetetten azonban mégis komoly károkat idéz elő, hiszen az adott rendszert, vagy szolgáltatást használók körében komoly bizalomvesztéssel fenyegethet. Más esetekben a rendszerekbe való behatolás mögött konkrét cél, szándék húzódhat meg, amely megvalósítása a „nevelési célok" elérésétől az adatvagyon rombolásáig igen széles skálán mozoghat.

A rosszindulatú szoftverek hatékonyságuk, olcsóságuk miatt jelentős szerepet játszanak a katonai célú felhasználásokban is. Ma, amikor már a hálózatos vezetésről beszélünk, az elektronizált, számítógép–hálózatokkal átszőtt csapatvezetési és fegyverirányítási rendszerek elsődleges célpontokká váltak az ellenség vezetési rendszerei, vezetési folyamatai ellen vívott harcban. A támadási célú fejlesztésekkel párhuzamosan nagy jelentőségre tettek szert a védelmi célú megoldások, és a saját rendszerek támadhatóságát tesztelő, elemző alkalmazások is.

A hadviselés fegyvertárában tehát megjelentek a kibertérben – a számítógép–hálózatok világában – való csapásmérés eszközei, módszerei. Ezek alkalmazására ugyanakkor nemcsak a nagy, reguláris hadseregek képesek, hanem a fegyverzetben, anyagi erőforrásokban jóval szegényebb kis országok, politikai célokért küzdő csoportok, sejtek, vagy akár terrorista szervezetek is. [4]

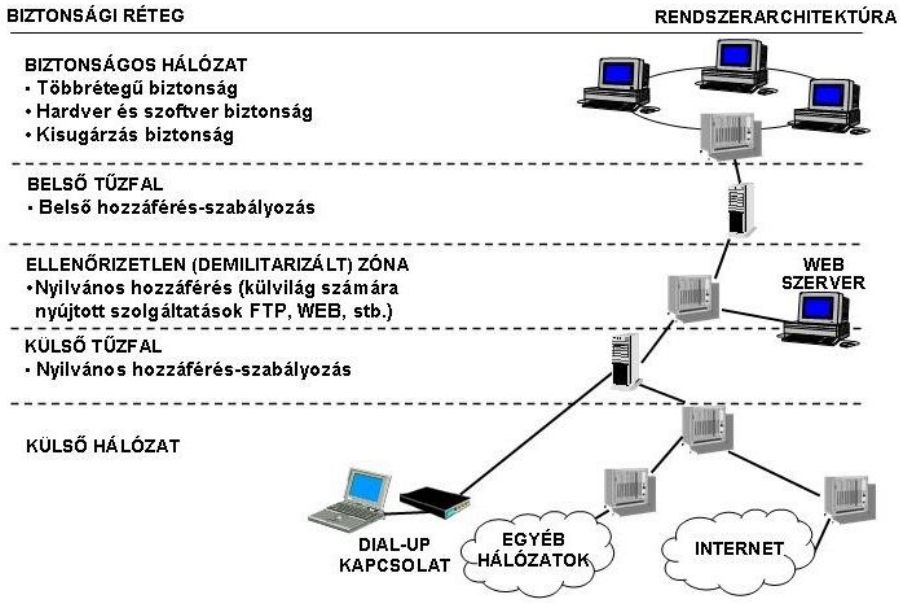
Az információs környezetszennyezésnek napjainkban minden számítógép felhasználó – aki a hálózatra kapcsolódik – akarva-akaratlanul, de áldozatul esik. Az adatvagyon területén megnyilvánuló környezetszennyezés elsősorban nem fizikai környezetszennyezés. Ez elsősorban olyan adatoknak és információknak az információs rendszerekbe való bejuttatását jelenti, amelyek egyrészt mennyiségüknél fogva, pl.: tömeges, nemkívánatos reklámok, ismertetők, „spam"-ek fizikailag terhelik, esetenként túlterhelik a hálózatot, ezáltal elérhetetlenné teszik a fontos, valódi információkat. Másrészről ideológiai, politikai, vallási, vagy egyéb tartalmuknál fogva károsan befolyásolhatják az információs társadalom tagjait, hiszen ezen a módon sokkal hatékonyabban és szélesebb körben eljuttathatók az információk, mint bármikor azelőtt. [4]

Az információs társadalom védelme szempontjából a legveszélyesebb fenyegetést azok jelentik, akik a számítógép-hálózati hadviselésben rejlő műszaki, technikai lehetőségeket szervezetten, valamely ideológiai, politikai, gazdasági, katonai vagy terrorista célból használják fel. Ahhoz, hogy egy ország egyrészt ne legyen kiszolgáltatva a támadásoknak, ne legyen védtelen, fel kell készülnie ennek a speciális területnek a művelésére, másrészt a

hagyományos fegyverzethez viszonyítva elenyésző beruházásokkal hatékony támadóeszköz birtokába is juthat. A kibertérben folytatott hadviselés támadó képességei a kizárólag védelmi doktrínával rendelkező országok fegyvertárában is helyet kaphatnak, mivel igen hatékony eszköze lehet az ellenséges támadás meghiúsításának, a támadó szándékú műveletek felfedésének, a támadó fél dezorganizálásának. [4]

3. Számítógép–hálózatok védelme

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. [2]
A megbízható számítógép–hálózatoknak rendelkezniük kell az információk *bizalmasságának*, *sértetlenségének* és *rendelkezésre állásának* követelményével. E követelmények teljesítése érdekében a hálózatot – biztonság szempontjából – többrétegűen kell kialakítani. A réteg koncepció lényege, hogy minden réteg biztonsága önállóan is biztosított, és a rétegek közötti információátvitel védelme érdekében a rétegekhez való hozzáféréshez különböző rendszabályokat alkalmaznak. Ilyen többrétegű hálózat biztonsági felépítést mutat be a 2. ábra.



2. ábra: Többrétegű hálózat biztonsági felépítése

A számítógép–hálózatok védelmének megvalósítása lehet *passzív és aktív*.
A *passzív védelmi* módszerek és eszközök lehetnek:

- a tűzfalak (Firewall);
- a vírusirtók (Antivirus Softwares);
- a hozzáférés szabályozás (Access Control) és
- a behatolás detektálás és adaptív válaszlépések (Intrusion Detection and Adaptive Response Tools).

Az *aktív védelem* módszerei közé sorolhatók:

- a megelőző támadások (Pre–emptive Attacks);
- az ellentámadások (Counterattacks) és
- az aktív megtévesztés (Active Deception). [7]

3.1 Passzív hálózatvédelmi módszerek

A számítógép–hálózat más hálózatoktól (pl. Internet) való elválasztásának az egyik elterjedt módja a *tűzfal*, amelyet a saját hálózat és az Internet közé építenek be, tehát az Internet, valamint a saját hálózat határfelületén dolgoznak. Feladatuk a határfelületen keresztül áramló *forgalom megszűrése*. Céljuk nem a támadás lehetőségeinek kiküszöbölése, hanem *akadály állítása* a támadás elé, a sikeres *behatolás valószínűségének csökkentése*. A tűzfal nem a védelem alapeszköze, inkább annak fontos kiegészítője.

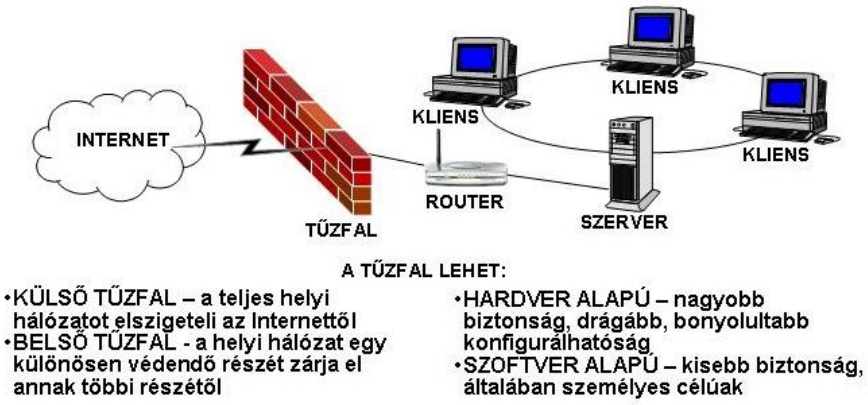
A tűzfal egyik típusa az ún. *külső tűzfal,* amely a teljes helyi hálózatot részben izolálja az Internettől, míg az ún. *belső tűzfal* a helyi hálózat egy különösen védendő részét zárja el annak többi részétől és így az Internettől is. Titkos, érzékeny adatok védelme vagy nagy üzembiztonságot kívánó hálózatok esetén elengedhetetlen a tűzfal használata. [5]

A tűzfalak működése azon alapul, hogy a rendszergazda beállíthatja, melyik IP–forgalmat engedje át, és melyiket tiltsa le a berendezés. Ha az üzenetek szűrése nincs körültekintően beállítva, a védelem hatékonysága máris csökken.

A tűzfalakról nemcsak a hálózat üzemeltetőinek kell tudniuk, hanem a felhasználóknak is, akik tűzfal mögül érik el az Internetet, illetve csatlakoznak rá. Ez azért fontos, mivel a tűzfal nem teljesen transzparens a felhasználók számára, azaz tisztában kell lenni a korlátozásokkal.

A tűzfal bizonyos protokollokat, az ún. biztonságos protokollokat átengedi, míg másokat, az ismeretlen vagy ún. veszélyes protokollokat nem. A tűzfal, korlátozva bizonyos portok elérését, további azonosítókat, jelszavakat is kérhet, s még számtalan módon szűrheti az információt. Fontos jellemzőjük, hogy rendszerint folyamatosan jegyzik a forgalom bizonyos adatait, a bejelentkező gépek, felhasználók azonosítóit, rendkívüli és kétes eseményeket, továbbá riasztásokat is adhatnak.

A tűzfal szerepét játszhatja egy intelligens router, megfelelő konfigurációjú Unix gép, vagy több is ezek közül. Internet tűzfalnak egy PC–n futó szoftver is kiválóan megfelelhet (3. ábra). [5]



3. ábra: Tűzfal

A tűzfallal való hálózatvédelem tehát összességében az alábbiakat jelenti:

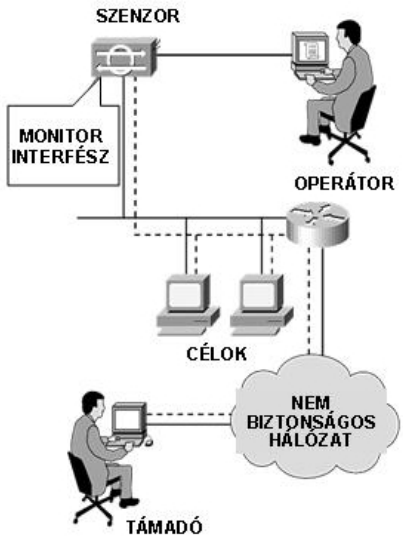
- ellenőrzési pontok létesítésével mind a kimenő, mind a bejövő forgalom megfigyelhető, szűrhető és erről statisztika készíthető;
- a rendszerben az egyetlen támadható gép a tűzfal, a védett hálózat gépei a külső hálózatról nem láthatók, így közvetlenül nem is támadhatók;
- a betörésgyanús tevékenység észlelhetővé válik, hatékony figyelő/riasztó rendszer alakítható ki;

- lehetőség van a felhasználók szigorú azonosítására nagy biztonságot nyújtó, egyszer használható jelszavas rendszerekkel;
- a szolgáltatások egyetlen ponton engedélyezhetőek a biztonsági politika igényei szerint;
- alkalmazásonként finoman szabályozható és naplózható az engedélyezett műveletek köre;
- a védett hálózat struktúrája, Internet címei és minden egyéb információja elrejthető a külvilág elől;
- lehetőséget nyújt automatikus titkosításra, vagyis egy szervezet Internetre csatlakozó telephelyei között az érzékeny információk nem nyíltan, hanem a tűzfalak által titkosítottan áramlanak. [8]

A tűzfalak alkalmazása sem ad azonban százszázalékos megoldást, mert a tűzfalak ugyanis tipikusan a feladó és a címzett címe szerint, valamint a portok címe szerint végzik el a beállított szelekciót. Ha a behatoló képes olyan megtévesztő üzeneteket előállítani, melyeket a tűzfal átengedhetőnek minősít, akkor megtörtént az első lépés a védelem feltörése terén.
A tűzfalak természetesen egyre megbízhatóbban tudnak védekezni a behatolók ellen, a baj csak az, hogy közben a behatolók módszerei is finomodnak. A megoldás kézenfekvő: olyan külön hálózatot kell építeni, amely úgy működik, mint az Internet, de teljesen független tőle, nincs köztük semmilyen kapcsolat. Ezeket a hálózatokat nevezzük *Intranet* hálózatnak. Az Intranet hálózat tehát nem más, mint egy TCP/IP protokollt használó, a web–technológia előnyeit és eredményeit teljes mértékben kihasználó számítógép–hálózat, mely azonban nincs kapcsolatban az Internettel. A katonai belső hálózatok Intranet típusúak.
A vírusirtók elsősorban a vírusazonosító adatbázisaik alapján, illetve heurisztikus vagy egyéb módszerek segítségével ismerik fel a rosszindulatú programokat. Ezeket a programokat a rendszer működése szempontjából mindenképpen blokkolni kell. [9] A napjainkban alkalmazott vírusirtók erre alkalmasak, bár meg kell jegyezni, hogy 100%–os biztonságot azok sem nyújtanak. A vírusirtók működésének hatékonyságát nagymértékben befolyásolja vírusazonosító adatbázisuk frissessége. Nem véletlen, hogy napjaink elterjedt vírusirtó szoftverei már lehetővé teszik az adatbázis automatikus, napi frissítését is.
A vírusirtók lehetnek háttérben állandóan futó, illetve alkalmilag elindítható programok.
A háttérben állandóan futó víruskeresők jellemzője, hogy a számítógép indításával egyidőben azok is elindulnak és a beállított paramétereknek megfelelően, folyamatosan ellenőrzik az operációs rendszer működését, a használatba vett lemezek boot szektorát, automatikusan ellenőrzik az összes megnyitott fájlt, keresik azokat a rosszindulatú programokat, melyek az adatbázisukban tárolt vírus–adatállományokkal megegyeznek. Természetesen ezek a szoftverek alkalmasak arra is, hogy rendszeres időközönként, vagy a felhasználó által meghatározott időben a számítógép összes lemezét vagy csak egyes meghatározott lemezeket, objektumokat teljes ellenőrzésnek vessenek alá. A vírusok keresése önmagában nem elegendő, ezért e szoftverek alkalmasak azok eltávolítására, törlésére, esetleg karanténba helyezésére, ahol már kárt nem okozhatnak. [9]
A folyamatos, és a háttérben futó automatikus vírusellenőrzés jelentős erőforrásokat köt le. Az erőforrások jobb kihasználása érdekében, a hálózat központi szerverein telepített vírusellenőrzés is igen hatékony védelmet biztosít, amennyiben a munkaállomások adatállományaikat hálózati (a szerver hatáskörébe tartozó) meghajtókon hozzák létre és tárolják. Ilyen rendszereken viszonylag csekély a vírustámadások kockázata. Ebben az esetben a munkaállomásokon elegendő az alkalmilag futtatandó vírusirtókat telepíteni és használni.
Az *alkalmilag futtatandó vírusirtók* csak akkor lépnek működésbe, ha a felhasználó elindítja, és meghatározza az ellenőrizendő lemezeket, objektumokat, fájlokat. Ezeknek a víruskeresőknek a folyamatosan futókkal szemben jóval kisebb az erőforrásigényük. Ezért

ezeknek elsősorban ott van létjogosultságuk, ahol kicsi a számítógép teljesítménye, és nincsenek az Internetre csatlakoztatva.
A heurisztikus víruskeresők kifejlesztése óriási lehetőségeket rejt magában, hiszen segítségével még fel nem fedezett vírusokat is felismerhetünk. A heurisztikus keresők nem a vírusadatbázisok alapján kutatnak vírusok után, hanem a vizsgált program viselkedése, működése, utasításai alapján próbálják eldönteni, hogy vírussal állnak–e szemben. A heurisztikus keresés általános formája, amikor a program olyan műveleteket figyel, amelyek általában vírusokban fordulnak elő. Gyanús művelet lehet például, a végrehajtható állományokba való írás. [9]
A hozzáférés szabályozás két leginkább alkalmazott módszere a *jelszó* és a *hitelesítés*.
Egy adott számítógéphez való hozzáférést sokszor kötik valamilyen *jelszóhoz*. Elvileg így csak az férhet a gépen lévő adatokhoz, információkhoz, aki ismeri az érvényes jelszót. Ha rosszul választjuk meg a jelszavunkat, akkor a gyakorlatban az ilyen jelszavas védelem nem sokat ér. A jelszó használatánál kétféle megoldás lehetséges. Alkalmazhatnak többször felhasználható és csak egyszer felhasználható jelszót. Az első esetben a jelszó hosszabb ideig lehet érvényben, a másik esetben egy adott jelszóval csak egyszer lehet belépni a rendszerbe. Ez az utóbbi nyilvánvalóan nagyobb biztonságot ad, de lényegesen bonyolultabb megoldásokat igényel.
A többször felhasználható jelszó biztonságát növelhetjük, ha jól választjuk meg a jelszavunkat. A jó jelszó nehezen kitalálható, könnyen begépelhető, könnyen megjegyezhető, igény szerint 5–10 karakter hosszú, tartalmaz betűket, számokat és/vagy írásjel karaktereket.
Biztonságosan védett számítógép–hálózatokban gyakran *többszintű jelszavas védelmet* alkalmaznak, azaz egymás után több jelszókérést kell kielégítenünk. Ez azt jelenti, ha belépünk egy többfelhasználós rendszerbe, akkor először a rendszer, utána pedig az adatbázis menedzsment rendszer kér jelszót. A jelszavas védelem más módszerekkel is kombinálható pl. PIN kártyával, ujjlenyomat ellenőrzéssel, írisz letapogatással stb., ez az ún. *többfaktoros védelem*.
Napjainkban előtérbe kerülnek az *egyszer használatos jelszavak*, melyek biztonságos úton, tehát olyan kommunikációs csatornán kerülnek továbbításra, amelyek nehezen hallgathatók le, az adatok módosíthatóságának esélye csekély, s az illetéktelen hozzáférés észlelhető. [5]
A *hitelesítés* a hálózati hozzáférés másik fontos módszere. Üzenetek, levelek, osztott dokumentumok és adatbázisok használata esetén fontos, hogy valóban a vélt személy küldte–e az üzenetet, végezte–e a módosítást, valamint illetéktelenek nem fértek–e hozzá az adatokhoz. Emellett fontos, hogy az adatok hitelességét ellenőrizni tudjuk, vagy kellő alapunk legyen abban megbízni.
A hitelességet legtöbbször az biztosítja, hogy csak az illetékes személy jogosult az adott művelet végrehajtására, pl. csak neki van hozzáférési joga.
A hitelesítés egyik leghatékonyabb módja a *kriptográfiai módszerek* alkalmazása. A rejtjelezés során az eredeti szöveget a küldő valamilyen eljárással titkosítja, és az eredményt továbbküldi. A visszafejtő egy másik eljárással a rejtjelezett szöveget átalakítja az eredetivé. A rejtjelezéssel a legtöbb esetben biztosítható a tartalom rejtettsége, érintetlensége, letagadhatatlansága és a forrás igazolhatósága. [5]
A hitelesség védelmére és bizonyítására a legajánlottabb módszer a *digitális aláírás*. A digitális aláírás gyakorlatilag az egyetlen jól bevált mód, amellyel egy teljes dokumentumról igazolni lehet nem csak annak hiteles aláírását, de a teljes dokumentum változatlanságát, azaz, hogy azt nem módosították az aláírása óta, valóban a keltezés idejében állították ki, stb. Nem mellékes, hogy ezzel az eljárással a titkosságot is biztosíthatjuk.
A digitális aláírás a papíralapú adathordozók esetében használt aláírás és pecsét tulajdonságait realizálja elektronikusan, tehát nem a hagyományos aláírás digitalizált változata (ahogy azt sokan hiszik). [4] A digitális aláírás egy olyan *titkosított karaktersorozat*, amelyet igen nagy

valószínűséggel csak a küldő kódolhatott, s ez magából a kódolásból következik. Keltezést, sorszámot a visszajátszás megakadályozására, a küldött üzenetből készült ellenőrző összeget stb. tartalmazhat. [5]
A behatolás detektálás és adaptív válaszlépések a hálózati biztonsági rendszer olyan aktív elemeit fogja össze, amelyek képesek a hálózatot fenyegető betörési kísérleteket észlelni, azonosítani, és a támadót elszigetelni. E módszer a betörési kísérleteket nem korlátozza csak a külső fenyegetésekre, hanem kiterjed a szervezeten belüli szabotázsakciókra is. A behatolás–védelmi rendszer (Intrusion Detection System – IDS) feladata a betörési kísérletek tényének feltárása. Ezek az eszközök azon az alapelven működnek, hogy a betörőket a hálózati forgalom elemzésével és a rendszerben észlelt abnormális események alapján azonosítani lehet. A hálózatban elhelyezett érzékelők és monitorprogramok ezeket az eseményeket időrendi sorrendben rögzítik, majd ezt az adatbázist a behatolás–védelmi rendszer elemzi. (4. ábra)



4. ábra: Behatolás detektálás

A támadások detektálása rendszerint a belső eseményszámlálók állítását, ill. e–mail riasztást eredményez, de van olyan rendszer is, amely képes a kapcsolatot törölni, vagy a tűzfalak konfigurációját megfelelően változtatni. [4]

3.2. Aktív hálózatvédelmi módszerek

Az aktív számítógép–hálózati védelem keretében a másik fél információs infrastruktúrája ellen alkalmazott megelőző támadások, ellentevékenységek és aktív megtévesztési formák jelentősen akadályozhatják hálózati támadó tevékenységét. Amennyiben elemezzük a sikeres hálózati támadás előfeltételeit és annak várható eredményeit, meghatározható, hogy milyen típusú aktív védelmi módszer alkalmazása vezet eredményre. Azt azonban meg kell jegyezni, hogy e tevékenységeket elsősorban válság és háború időszakában, már ismert ellenséggel szemben alkalmazhatjuk hatékonyan. Ahhoz, hogy e műveleteket hatékonyan alkalmazhassuk, ismerni kell a másik fél számítógép–hálózati struktúráját, a hálózatbiztonság terén alkalmazott módszereit, eszközeit, támadási képességeit. Mindezek egy ismert fél, pl. nemzeti szervezetek vonatkozásában jobban felmérhetők, mint egyes személyek, nem szervezett csoportok (hacker, cracker stb.) esetében. E felmérésben jelentős szerepet kap a számítógép–hálózati felderítés. Ezen belül kiemelten fontos annak meghatározása, hogy a

másik fél hálózati infrastruktúrája milyen módszerekkel támadható a leghatékonyabban, mielőtt azt különböző támadási céllal felhasználná. Ez a *megelőző támadás alapja.*
Amennyiben a megelőző támadás nem éri el célját, vagy nincs lehetőség annak végrehajtására, abban az esetben élni kell az *ellentámadás* módszerével. A hatékony ellentámadás végrehajtásához szükséges a támadás forrásának meghatározása. Ebben megint csak a hatékony hálózati felderítésnek van jelentős szerepe. A támadás forrásának nyomon követése és meghatározása jóval nagyobb erőfeszítést és szakértelmet kíván, mint maga az ellentámadás. Ha a hálózati felderítés sikeres, tudjuk, hogy kitől ered a támadás, és ismerjük annak hálózati felépítését, akkor viszonylag rövid idő alatt meg lehet tenni a megfelelő válaszlépéseket. A megelőző támadáshoz, és az ellentámadáshoz alkalmazott módszerek és eszközök az előzőekben leírtak közül kiválaszthatók.
Az aktív hálózati védelmen belül az *aktív megtévesztés* az előbb ismertetett két tevékenység, valamint a passzív védelem hatékony alternatívája lehet. Ahelyett, hogy hálózatunktól különböző módszerekkel megkísérelnénk távol tartani a betolakodókat, megkíséreljük átirányítani őket egy hasonló felépítésű és hamis adatbázisú hálózatba, amelyet kizárólag megtévesztés céllal működtetünk. Az aktív megtévesztés nem okoz tényleges károkat a támadó hálózatában, ugyanakkor erőforrásait leköti, és lehetőséget biztosít számunkra, hogy megfigyeljük támadási technikáit, elfogjuk támadó eszközeit (MALWARE–k). Ez lehetővé teszi, hogy ezek ellen – melyeket akár valós hálózataink ellen is alkalmazhat – megfelelő védelmet alakítsunk ki. Ezen túlmenően azzal, hogy a támadó irányába úgy tüntetjük fel, mintha támadása sikeres lenne, eltorzítjuk a támadás hatékonyságának értékelését is.
Az aktív megtévesztés alkalmazásának legegyszerűbb módja, ha a támadót egy felfedezhető csapda– vagy un. hátsó ajtón (trap door, back door) keresztül engedjük hozzáférni a virtuális hálózathoz. A hozzáférés megvalósulhat egy védtelen csatlakozó felületen (porton) keresztül, vagy egy cracker által könnyen feltörhető jelszóval védett felhasználói jogosultságon keresztül is. [7]
Természetesen az aktív hálózati megtévesztés – mint minden megtévesztő tevékenység – csak akkor éri el hatását, ha a támadó felé a virtuális hálózat egy valós adatbázissal rendelkező hálózat képét mutatja.

Összegzés:
A számítógép-hálózati hadviselés napjainkra az információs műveletek többi elemével egyenrangú fontossággal bír. Mindezt a különböző katonai információs rendszerek nagyfokú hálózatosítása indokolja. E tevékenység a korszerű katonai műveletekben – a másik fél számítógép-hálózatai támadásának és a saját rendszereink védelmének összehangolásával, és az információs műveletek más elemeivel való szinkronizálásával –jelentős mértékben járul hozzá az információs fölény eléréséhez, és így a vezetési folyamatok számunkra kedvező alakításához.
A számítógép-hálózati tevékenység azon információs műveletei tevékenységek közé tartozik, melyek, viszonylag kis költségráfordítással nagy hatékonysággal járulhatnak hozzá a műveletek sikeréhez. Ezáltal e tevékenység jól alkalmazható mindazon országok haderejében, melyek infrastrukturálisan és képzettségben felkészültek ezen igen fejlett támadó és védelmi eszközök, módszerek és eljárások alkalmazására. Így megítélésem szerint a Magyar Honvédség számára is alkalmazható információs műveleti tevékenységi forma lehet nem csak a védelem oldaláról, de a hálózatok terén is.

Felhasznált irodalom:

1. Haig, Zsolt–Várhegyi, István: A vezetési hadviselés alapjai. Egyetemi jegyzet, ZMNE, Budapest, 2000.
2. AJP–3.10 Allied Joint Information Operations Doctrine (draft). 2002. szeptember.

3. Waltz, Edward: Information Warfare Principles and Operaions. Artech House, Inc. Boston, London. 1998. ISBN: 0-89006-511-X.
4. 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
5. Dravecz, Tibor–Párkányi, Balázs: Hogyan védjük hálózatra kötött számítógépes rendszereinket? NIIF Információs Füzetek II./8. Budapest, 1996.
6. Az információs rendszereket fenyegető veszélyek, kihívások és a csökkentésükre, elhárításukra alkalmas intézkedések, rendszabályok és eszközök. Gazdasági Minisztérium kiadványa. 2001. december.
7. Holdaway, Eric J.: Active Computer Network Defense: An Assessment. Air Command and Staff College. Maxwell Air Force Base, Alabama, 2001.
8. Szirota, Csaba: Adatvédelem kérdései az Interneten, tekintettel az e-mail és World Wild Web-en keresztüli adatforgalomra. http://business.matav.hu/uzlet/sugoo/szanyek/dolgozat.html
9. antivirus.hu vírusvédelmi információs oldal. http://www.antivirus.hu.