HADTUDOMÁNY
A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA

XVII. évfolyam **3. szám** **2007. szeptember**

Haig Zsolt

Az információs társadalmat fenyegető információalapú veszélyforrások[1]

A szerző e tanulmányban bemutatja az információs társadalom információtechnológiai függőségét, a fenyegetés új dimenzióit és a társadalom kritikus információs infrastruktúrákon keresztüli sebezhetőségét. Kategorizálja az információs támadás formáit, valamint bemutatja legjellemzőbb eszközeit és módszereit, majd végül javaslatokat fogalmaz meg a társadalom információbiztonságának erősítése érdekében.

Az információs társadalom nagyon fejlett, nagyon hatékony, ugyanakkor meglehetősen sebezhető társadalmi és gazdasági rendszer. E társadalom alapvető éltető eleme az információ, melynek mennyisége és minősége létfontosságú a felhasználók számára. Éppen ezért kíméletlen harc folyik az információ gyors megszerzéséért, biztonságos tárolásáért és mind hatékonyabb felhasználásáért. Az optimális mennyiségű és minőségű információ birtoklása jelentős mértékben járulhat hozzá a gazdasági haszon növeléséhez, az esetlegesen bekövetkező károk elhárításához, valamint két fél közötti verseny- esetleg konfliktushelyzetben a másik féllel szembeni fölény kialakításához. Mindezek alapján kijelenthető, hogy az információs társadalomban az egyének, gazdálkodó szervezetek, illetve a kormányzati szervek jelentős információfüggőségben szenvednek. Ez az információfüggőség egyúttal az információs technológiától való függőséget is jelenti, vagyis erősen függenek az információs környezet fejlett, ám erősen korlátozható vagy sebezhető integrált információs infrastruktúráitól, mint például a távközlési hálózatoktól és a számítógép-hálózatoktól.

Az információtól és az információtechnológiától való függőség azt is jelenti, hogy amennyiben az információhoz való hozzáférhetőség, illetve a technológia kihasználása valamilyen fenyegetés következtében korlátozottá válik, az kihatással van a különböző működési folyamatokra. Ezek a hatások mikro- és makroszinten egyaránt érvényesülnek, vagyis az egyének, kisebb szervezetek, intézetek szintjén éppúgy, mint össztársadalmi méretekben. Jelen írás az információs társadalom egészét érintő támadásokra, veszélyforrásokra koncentrál.

Az információs fenyegetések megjelenése

A hálózatok által átszőtt globális világ sosem volt olyan sebezhető, mint manapság. Ez a sebezhetőség a nyitottságból, a bonyolult technikai rendszerekből, az infokommunikációs rendszerektől való növekvő függésből, illetve az összefonódó és egymással összekapcsolt létfontosságú infrastruktúrákból eredeztethető. Egy olyan bonyolult, infokommunikációs rendszerekkel behálózott társadalomban és gazdaságban, ahol közel minden ügyünket a hálózaton keresztül intézzük, saját fejlettségünk csapdájába eshetünk. Ezt az ártó szándékú egyének, csoportok, terroristák is jól tudják, és mindent elkövetnek annak érdekében, hogy az információs társadalom működését és fejlődését csökkentsék, korlátozzák, vagy átmenetileg bénítsák. Egy hálózatilag fejlett ország vezetése, gazdasági rendszere, közlekedési- és szállítóhálózata, energiahordozó és -ellátó rendszerei, stb. megbénulhatnak, vagy működésük erősen korlátozottá válhat. Az egészségügyi ellátás akadozhat, a közbiztonság megszűnhet, és az addigi szervezett rendet káosz válthatja fel. [1]

Az információs társadalom nem hagyományos fenyegetésekkel szembeni kiszolgáltatottságát jól példázza a 2001. szeptember 11-i terrortámadás és annak hatása. E támadás hatását az ipari társadalom - ahol a világ gazdasági-,

pénzügyi- és tőzsdei rendszere kevésbé függött az infokommunikációs hálózatoktól - kevésbé érezte volna meg, a lélektani megrázkódtatástól eltekintve a fizikai és gazdasági hatás korlátozott lett volna. Ezzel szemben korunk hálózatokkal átszőtt világában a World Trade Center összeomlása a teljes globális gazdasági rendszert sokkolta. [2]

Az új típusú társadalom számos pozitív tulajdonságai mellett tehát újfajta kihívásokat, veszélyforrásokat is tartogat számunkra, melyeket folyamatosan szem előtt kell tartanunk. Mint ahogy azt a Magyar Köztársaság nemzeti biztonsági stratégiája is kiemeli: "Az informatikai infrastruktúra technikai és szellemi feltételeinek biztosítása mellett ügyelni kell e rendszerek védelmére és a megfelelő tartalékok képzésére is. Az informatika számtalan lehetőséget teremtett a társadalom számára, de fokozta annak veszélyeztetettségét is. A számítógépes hálózatok és rendszerek sebezhetősége, túlterhelése, az információlopás, a vírusterjesztés és a dezinformáció kockázati tényezőt jelent az ország számára." [3] Ezzel kapcsolatban mindenképpen meg kell jegyezni, hogy e veszélyeztetés nem csupán az informatika területén jelentkezik, hanem minden fajta integrált infokommunikációs rendszer (távközlési hálózatok, számítógép-hálózatok, távirányító-, távérzékelő-, távvezérlő rendszerek stb.) ki van téve az információs dimenzióból érkező fenyegetéseknek.

Természetesen akkor, amikor fenyegetésről, illetve fenyegetettségről beszélünk, meg kell határoznunk a fenyegetés szintjét, mértékét, esetlegesen komplexitását. E tekintetben különbséget kell tennünk a tekintetben, hogy e fenyegetések a társadalom egészének működését érintik-e, vagy csak a társadalom egyes szereplői (egyének, vállaltok, intézmények stb.) az elszenvedői eme veszélyeknek. Tisztában vagyunk azzal, hogy pl. egy vállalkozást érintő esetleges támadás milyen hatással lehet az adott gazdálkodó szervezet működésére, piaci helyzetére. Ugyanakkor ezt nem lehet egy szintre emelni azokkal a veszélyekkel, amelyek össztársadalmi szinten jelentkeznek, vagyis mindenki számára érezhető hatással bírnak. Ezek a veszélyek sokkal nagyobb horderejűek annál, minthogy pl. egy vállalat egy információs támadás következtében esetleg jelentős gazdasági haszontól esik el, vagy elveszíti piaci pozícióját.

Hiszen gondoljunk bele, hogy mi történne, ha valamilyen ártó szándékú csoport, esetleg terror szervezet fizikai, vagy elektronikai támadást (esetleg támadás sorozatot) intézne az információs társadalom egy vagy több fontos infrastruktúrája ellen. A hálózatilag összekapcsolt infrastruktúrákat ért információs fenyegetéseken keresztül egy információs technológiailag fejlett ország társadalmi, politikai, gazdasági és védelmi képessége erősen befolyásolhatóvá, fejlődése jelentősen korlátozható válna. Ez még inkább felerősödne, ha e támadások egymással összehangoltan, komplex információs támadások formájában, a célpontok körültekintő kiválasztásával kerülnének végrehajtásra.

A korszerű katonai műveletekben már megjelent egy teljesen újfajta elmélet, melyet *hatásalapú műveleteknek neveznek.* Ezen elv szerint a tervezők figyelembe veszik azt a láncreakcióhoz hasonlító elvet, miszerint a kezdeti közvetlen hatással (első csapással) törvényszerűen további közvetett károsító, korlátozó hatásokat lehet elérni, amely a teljes rendszerre különböző mértékű negatív hatást fejt ki. *Az előidézett hatások, vagyis az összhatás eredményének elemzése és értékelése képezi a hatásalapú műveletek lényegét.* Ez az új felfogás holisztikus elvű szemlélet alkalmazását igényli, amelynek lényege, hogy egy rendszeren belül az alkotó elemek kölcsönösen hatnak egymásra. [1] Ez még inkább így van az információs társadalomban, ahol a már említett információs hálózatoknak köszönhetően a különböző létfontosságú infrastruktúrák, rendszerek egymással szoros kapcsolatban állnak, az egyik rendszer működése alapvetően függ egy másiktól (lásd pl. a távközlési- vagy az informatikai hálózatok és a villamos energia hálózat viszonyát).

A hatásalapú műveletek analógiáján tehát megállapíthatjuk, hogy amennyiben a támadó fél az információs társadalom elleni információs támadások megtervezésekor figyelembe veszi az információs rendszerek közötti igen szoros kapcsolódásokat, akkor a közvetlen első támadással elért hatás mind a konkrétan megtámadott rendszeren belül, mind pedig a rendszerek közötti kapcsolatokban másod, harmad és n-edik típusú és erősségű hatásokat vált ki. [1] Ennek felismerése azért is fontos, mivel ez rámutat arra a tényre, miszerint ezt az elvet felhasználva, a hálózatilag összekapcsolt társadalom rendkívüli mértékben sebezhetővé válik. Az információs társadalom és annak

védelmi rendszere olyan számítógép-hálózatokkal átszőtt hálózatos rendszerek komplexuma, amelyben e rendszerek biztonságos működése kölcsönösen függ a többi rendszer működésétől. Ennek következtében a rendszer bármelyik súlyponti elemének információs támadása, vagy védelme nemzetbiztonsági kérdés, amely védelmi síkon kihat az egész társadalomra. Elegendő egy kiválasztott - pl. a társadalom gazdasági élete, vagy közlekedése szempontjából fontos - infrastruktúrát információs támadással működésképtelenné tenni vagy működésében korlátozni, az éppen a hálózatoknak köszönhetően negatívan befolyásolja más hasonló fontossággal bíró elemek működőképességét is.

Napjaink egyik korszerű információalapú támadó és védelmi elmélete az *információs hadviselés* is ezt az elvet követi. Az információs hadviselés - illetve annak a NATO és tagországai katonai doktrínáiban elfogadott formája az információs műveletek - mindazon összehangolt, koordinált információs tevékenységeket jelentik, amelyek arra irányulnak, hogy a szemben álló fél információs rendszerei működésének korlátozásával befolyásolják a társadalom egészének vagy egyes területeinek működési folyamatait, illetve másik oldalról, hogy megteremtsék azokat a feltételeket, amelyek mentén a saját hasonló képességek fenntarthatók.

Az információs hadviselésnek és az információs műveleteknek napjainkra teljes mértékben kialakult az elmélete, többnyire letisztult az eszköz- és eljárásrendszere. Az információs hadviselés keretén belüli és az információs társadalom egésze ellen irányuló komplex információs támadás megvalósulhat *totális formában* polgári és katonai célpontok ellen egyaránt, *összpontosított módon* kiemelt célcsoportok ellen vagy *szelektív formában* egyes kritikusan fontos létesítmények ellen. A fenyegetések motiváló tényezői különböző politikai, gazdasági, pénzügyi, katonai, szociális, kulturális, ipari, etnikai, vallási, regionális vagy egyéni célok elérése lehet. Az információs rendszerek elleni fenyegetések, a konfliktus helyzetek-, a technikai lehetőségek-, és a motivációk szerint változhatnak. [4]

Egy ilyen támadás során az információs társadalom elleni veszélyek három területen jelentkeznek, úgymint: a tudati, a fizikai és az információs dimenzióban [1]

A tudati dimenzióban elsősorban a *humán típusú veszélyek* jellemzőek, míg a fizikai és az információs dimenzióban jelentkező veszélyek alapvetően *technikai, technológiai jellegűek.* Emellett persze meg kell említenünk az egyéb jellegű veszélyeket is, amelyek szintén a fizikai dimenzióban jelentkeznek, úgymint: *természeti és ipari katasztrófák illetve műszaki zavarokból* adódó veszélyek, amelyek szintén jelentősen befolyásolhatják a rendszerek és infrastruktúrák működését, és ezáltal kihatnak az össztársadalmi folyamatokra is.

A humán jellegű veszélyekkel mind az információs társdalom kialakulása, mind pedig a működése során találkozhatunk. *Ezek közé olyan jellegű veszélyforrások sorolhatók, mint pl.:*

- a digitális írástudatlanság;
- az információs szakadék;
- az információs technológia vívmányaihoz való hozzáférés hiánya;
- az innoválható tudás hiánya;
- a rejtett tudás kihasználatlansága;
- az információs túlterheltség hatásai;
- negatív hozzáállás, ártó szándékú tevékenység;
- az információs technológia eszközeinek használatával összefüggő pszichikai, fiziológiai és egészségügyi jellegű veszélyek;
- az információs technológiákkal szembeni idegenkedés, bizalmatlanság, iszony;
- az esetileg megjelenő prognosztizálható, vagy váratlan negatív jelenségek. [4]

Jelen tanulmányban a humán jellegű veszélyforrások bővebb kifejtésétől eltekintünk.[2] A felsoroltakon kívül ide tartoznak azon veszélyek is, amelyek az egyének - köztük a különböző szintű vezetők - gondolkodását, tudati

viselkedését, érzelmi állapotát próbálják meg befolyásolni. E befolyásoló tevékenység nem más, mint a *pszichológiai hadviselés.* A pszichológiai hadviselés keretében különböző audiovizuális berendezések (kihangosítók, hangosbeszélők) röplapok, és manapság egyre gyakrabban az Internet, az e-mail az SMS és MMS alkalmazhatók a tudati állapot befolyásolására. Az Internet ilyen célú felhasználását jól példázzák azok az egyre inkább terjedő web-lapok, amelyeken különböző terror szervezetek, csoportok próbálnak félelmet kelteni az olvasókban. A terrorizmus lélektani kapcsolódása egyértelmű, hiszen a különböző robbantásos, öngyilkos merényletek elkövetésével nemcsak a pusztítás a cél, hanem a lakosság megfélemlítése, folyamatos rettegésben tartása is. Számos módja van az Interneten keresztüli pszichológiai hadviselésnek, mint pl.: félretájékoztatások, fenyegetések kézbesítése, félelem elültetése képek, videó felvételek bemutatásával stb. illetve a cyber-terrorizmus lehetőségének bemutatása, a virtuális térben való támadás valószínűsítése, vagyis a "cyber-félelem" elterjesztése.

Egy másfajta megközelítésben a veszélyforrásokat osztályozhatjuk aszerint is, hogy a veszélyeztetés honnan eredeztethető, illetve, hogy a veszélyeztetők (fenyegetők, támadók) tevékenységüket mennyire szervezett keretek között hatják végre. E szerint eredetüket tekintve beszélhetünk külső és belső forrásból származó veszélyekről, strukturáltságukat tekintve, pedig magas szinten szervezett és alacsonyan szervezett fenyegetésekről.

A belső veszélyeket elsősorban a saját alkalmazottak, munkatársak okozzák, akik a biztonsági rendszabályok be nem tartásával, képzetlenségükkel, hanyagságukkal, illetve vélt vagy valós sérelmeik megtorlásaként veszélyeztetik az adott szervezet, intézmény, vállalat stb. infokommunikációs rendszereit. Ezek a veszélyek, amennyiben felfedésükre és elhárításukra nem helyeznek hangsúlyt, komoly biztonsági problémák forrásai is lehetnek.

A külső veszélyek közé mindazon fenyegetések tartoznak, amelyek valamilyen külső forrásból származnak, és a támadás célja anyagi- politikai-, gazdasági- vagy katonai előnyszerzés. E támadásokat általában az információs technológiához kiválóan értők hajtják végre. E támadók köre az infokommunikációs rendszerek elterjedésével és fejlődésével egyenes arányban napról-napra növekszik és bővül. Napjainkban ezek közé sorolhatjuk: a hackereket, crackereket, számítógépes bűnözőket, hacktivistákat, ipari kémeket, terroristákat, valamint a hírszerző szolgálatok-, illetve katonai és félkatonai szervezetek alkalmazottait.[3] [1; 5]

Magasan szervezett fenyegetéseket az előzőekben felsoroltak közül olyan szervezett csoportok, terror szervezetek, hírszerző szolgálatok, katonai és félkatonai szervezetek hajtják végre, akik képesek megszervezni akár egyszerre több fontos létesítmény elleni többirányú összehangolt támadást is. E támadások célja szinte minden esetben több mint anyagi haszonszerzés. Elsősorban gazdasági, politikai illetve katonai célok elérését szolgálják.

Ezzel szemben az *alacsony szervezettségű támadásokat* azon egyének, jogosulatlan felhasználók (hackerek, crackerek stb.) hajtják végre, akiket elsősorban anyagi haszonszerzés vagy a saját képességeik megmutatása motivál. Ebből adódóan látható, hogy a magasan szervezett fenyegetések nagyságrendekkel komolyabb biztonsági problémát jelentenek, mint az alacsonyan szervezettek. Ezek közül is külön kiemelendő a terrorszervezetek ilyen irányú képességei és lehetőségei, amelyeket napjainkban egyre komolyabban kell vennünk. Az információs terrorizmus sokkal veszélyesebb, mint az egyszerű hacker vagy cracker támadás, mivel minden esetben politikai tartalommal rendelkezik.

A potenciális információs veszélyforrások a különböző szereplők (versenytársak, ellenfelek, ellenségek) rossz szándéka, agresszív érdekérvényesítése, az üzleti és ipari kémkedés, a politikai és gazdasági befolyásolás, valamint a kialakított információs támadó képesség kombinációiból alakulhatnak ki. A fenyegetések sikeres realizálása esetén komoly vesztességek és/vagy károk érhetik az információs környezetet, benne az államot, a vállalatokat, a vállalkozókat és az egyéneket, összességében az információs társadalmat.

A továbbiakban e tanulmány keretei között a technikai jellegű veszélyforrásokat, fenyegetéseket és azok célpontjait vizsgáljuk.

Az információs fenyegetések célpontjai - kritikus információs infrastruktúrák

Az előzőekben már több esetben is említésre kerültek azok a létfontosságú létesítmények, infrastruktúrák, amelyek információs veszélyeztetése jelentős hatással lehet a gazdaság, és a társadalom működésére. Az információs társadalomban mind az egyének, mind pedig a társadalom biztonsága jelentős mértékben függ a különböző, egymással szorosan összekapcsolódó infrastruktúráktól. Ezeket a különösen fontos infrastruktúrákat *kritikus infrastruktúráknak* nevezzük. A továbbiakban az információs fenyegetések oldaláról megvizsgáljuk ezeket az infrastruktúrákat.

A kritikus infrastruktúra meghatározásakor célszerű megvizsgálni, hogy a biztonság terén élenjáró Amerikai Egyesült Államok és az Európai Unió milyen fogalmi meghatározásokat alkalmaz.

Az USA meghatározása szerint: "a kritikus infrastruktúrák azok a valós és virtuális rendszerek, eszközök, amelyek alapvető fontosságúak az Egyesül Államok számára, és e rendszerek illetve eszközök működésképtelensége vagy megsemmisülése csökkentené a biztonságot, a nemzetgazdaság biztonságát, a nemzeti közegészséget és annak biztonságát vagy mindezek kombinációját." [6]

Az Európai Unió dokumentuma szerint: "a kritikus infrastruktúrákhoz azok a fizikai erőforrások, szolgáltatások és információtechnológiai létesítmények, hálózatok, és infrastrukturális berendezések tartoznak, melyek összeomlása vagy megsemmisülése komoly következményekkel járna a polgárok egészségére, biztonságára, védelmére vagy gazdasági jólétére, illetve a kormányok hatékony működésére." [7]

A fogalmi meghatározás alapján az Európai Unió illetékes bizottsága *a kritikus infrastruktúrák közé az alábbiakat sorolja:*

- energiatermelés és hálózat (áramszolgáltatás, olaj és gáztermelés, energiatárolók és finomítók, energiaátadó és elosztó rendszerek);
- kommunikációs és információs technológia (távközlés, műsorszórórendszerek, szoftver, hardver és hálózatok, beleértve az Internetet);
- pénzügy (bankügyletek, kötvények és befektetések);
- egészségügy (kórházak, egészségügyi és vérellátó intézmények, laboratóriumok és gyógyszertárak, kutató és mentőszolgálatok, mentők);
- élelmiszerellátás (élelmiszerbiztonság, termelés, nagykereskedelem és élelmiszeripar);
- vízellátás (gátak, víztározók, víztisztítás és vízhálózat);
- közlekedés (pl.: repterek, kikötők, vasúti és tömegközlekedési hálózatok, közlekedésirányító rendszerek);
- veszélyes áruk termelése, tárolása és szállítása (kémiai, biológiai, radiológiai és nukleáris anyagok);
- kormányzat (kritikus szolgáltatások, létesítmények, információs hálózatok, eszközök és jelentős nemzeti emlékhelyek műemlékek). [8]

Magyarország vonatkozásában kormányzati szinten deklarált kritikus infrastruktúra fogalommal jelenleg nem lehet találkozni. A terrorizmus elleni küzdelem aktuális feladatairól szóló 2112/2004. (V.7.) kormány határozat is csak abban a tekintetben foglalkozik e kérdéssel, hogy a kritikus infrastruktúra biztonságának erősítése mely területeken érvényesül. E szerint a következő területek sorolandók a kritikus infrastruktúrák közé: az energiaellátás; a közművesítés; a közlekedés és szállítás; a távközlés, elektronikus adatforgalom és informatikai hálózat; a bankrendszer; a szolgáltatások; a média; az ivóvíz és élelmiszer alapellátás, valamint az egészségügyi biztosítás. [9]

Mint látható, e kategorizálás részben megegyezik az USA és EU felsorolással, azonban egyes területeket, mint pl. a kormányzati-, és a védelmi szektort (honvédség, rendőrség, határőrség, katasztrófavédelem, vám- és pénzügyőrség) nem tartalmazza. E területek infrastrukturális elemei ugyanakkor elengedhetetlen részei egy ország kritikus infrastruktúráinak, hisz az állami- és közigazgatás, illetve az ország védelme kiemelt fontosságú. E létfontosságú

szerepet betöltő infrastruktúrák működése és működtetése nemzetgazdasági, nemzetbiztonsági, közbiztonsági és honvédelmi fontosságuknál fogva az ország biztonságát közvetlenül érintik.

A kritikus infrastruktúrák működésük során három alapvető funkciót látnak el. Egyrészt lehetővé teszik a nélkülözhetetlen javak előállítását, szállítását és a létfontosságú szolgáltatások folyamatos elérhetőségét. Így pl. az élelmiszer- és vízellátás, a közegészségügy, a mentő- és tűzoltószolgálatok biztosítják az ország túléléséhez nélkülözhetetlen javak és szolgáltatások igénybevételét. A gazdasági élet folyamatosságát olyan kritikus infrastruktúrák teszik lehetővé, mint az elektromos energiaellátás, az áru- és személyszállítás, vagy a bank- és pénzügyi rendszerek.

Másrészt biztosítják az összeköttetést és az együttműködés képességét. A kommunikációs és számítógép-hálózatok kötik össze, és azokon keresztül irányítják a társadalom és a gazdaság többi infrastruktúráját. Ebben az összefüggésben e rendszerek kritikus információs infrastruktúráknak is minősülnek.

Harmadrészt pedig hozzájárulnak a közbiztonság és az ország külső biztonságának megteremtéséhez. Egy ország azon képessége, hogy figyelemmel kísérje, időben felismerje a fenyegető veszélyeket, és hogy azokra megfelelőképpen reagálhasson, szintén a kritikus infrastruktúrák szolgáltatásain alapul. [10] Egyértelmű tehát, hogy e kritikus infrastruktúrák védelme és működésének fenntartása nemzetbiztonsági szempontból minden kormányzat alapvető és létfontosságú feladata.

Az elmúlt időszakban a különböző infrastruktúrák mindig is jó célpontjai voltak a különböző szintű és típusú támadásoknak. Amíg e támadások csak a fizikai dimenzióban realizálódtak, addig az országhatárok bizonyos védelmet jelentettek számukra. Az *információs dimenzió* megjelenése és egyre fokozódó előretörése, az infokommunikációs rendszerek globálissá válása azonban e viszonylagos letisztult helyzetet gyökeresen megváltoztatta. Napjainkban korlátozott erőforrások is elegendőek az infokommunikációs rendszerekre alapozott kritikus infrastruktúráink elleni támadások megtervezésére és kivitelezésére. A különböző egyéni aktivisták, jogosulatlan felhasználók és terroristák aszimmetrikus fenyegetései részben kibővítették, részben pedig felváltották a jól ismert háborús fenyegetettségeket. [11] E tekintetben kijelenthetjük, hogy a katonai és polgári természetű fenyegetések közötti hagyományos határvonal egyre inkább elmosódik.

Az információbiztonság szempontjából - mint ahogy fentebb már utaltunk rá - értelmeznünk kell a *kritikus információs infrastruktúrákat is*. Az információs társadalomban a kritikus infrastruktúrák nem egyeznek meg a kritikus információs infrastruktúrákkal. A kritikus infrastruktúrák védelmére vonatkozó európai programról szóló zöld könyv szerint: "Kritikus információs infrastruktúrák közé azok sorolandók, melyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, Internet, műholdak stb.)". [7] Mint a megfogalmazásból látszik, a dokumentum is különbséget tesz e két fajta infrastruktúra kategória között. Korábban egy ország kritikus infrastruktúrái fizikailag és logikailag is önállóak voltak, egymástól csekély mértékben függtek. Az információtechnológia fejlődése következtében azonban napjainkban e rendszerek már egyre inkább automatizáltak és egymással szoros kapcsolatban állnak. [12] Szinte minden fajta kritikus infrastruktúrát különböző szintű és rendeltetésű infokommunikációs rendszerek vezérelnek, irányítanak és ellenőriznek. Így tehát egy ország információtechnológiára alapozott infrastruktúrája joggal nevezhető a társadalom idegrendszerének, és ennek következtében az információs infrastruktúrák, illetve azok részei is a kritikus infrastruktúrák közé sorolandók. E megállapítás szerint, pl. egy ország nyilvános mobil távközlő hálózatai, mint önmagukban is kritikus infrastruktúrák, egyben kritikus információs infrastruktúráknak is minősülnek, illetve pl. az energiaellátó rendszert irányító, vezérlő számítógép-hálózat is ez utóbbiak közé sorolandó.

Itt kell megjegyezni, hogy vállalati és gazdálkodó szervezeti szinteken is találhatók olyan létfontosságú infrastruktúrák és szolgáltatások, amelyek védelméről kiemelt módon kell gondoskodni. Sok esetben ezek a vállalati- és állami kritikus információs erőforrások egybe eshetnek, és így védelmük is közös feladat. Az

információbiztonság szempontjából azonban mindenképpen meg kell különböztetni a gazdálkodó szervezetek információs rendszereit egy ország kritikus információs infrastruktúráitól, mert amíg ez utóbbiak veszélyeztetése esetén többnyire csak saját biztonságuk kerül veszélybe, addig az előbbiek nem megfelelő működése sokkal szélesebb körben érvényesül, az egész nemzet gazdasága és biztonsága kerülhet veszélybe.

Bár az információs társadalom zavartalan működésének megbontására irányuló támadások tényleges célpontjai a kritikus infrastruktúrák - hiszen ezek adják működésének alapját -, azonban az ellenük irányuló információalapú támadások és fenyegetések a különböző szintű és fontosságú infokommunikációs rendszereket érintik. Ezek a rendszerek mára a fenyegetések stratégiai célpontjaivá váltak, mivel a támadó fél kis erő- és eszközbefektetéssel igen jelentős károkat tud előidézni. Az infokommunikációs rendszerek globális jellegéből adódóan e rendszerek bárhonnan, bármikor elérhetők, és az információtechnológia vívmányait ellenük fordítva támadhatók. Miközben az informatikai és kommunikációs technológia konvergenciájából adódó közös platformok és alkalmazások lehetővé teszik az átjárhatóságot és a felhasználóbarát elterjedést, egyúttal jelentős mértékben növelhetik a kockázatokat is. Egyértelműen kijelenthető, hogy a kritikus információs infrastruktúrák közötti szoros kapcsolat jelentősen növeli az információs társadalom sebezhetőségét. Minél nagyobb e rendszerek integráltsága, komplexitása, minél kiterjedtebb a köztük lévő kapcsolatrendszer, annál nagyobb mértékben vannak kitéve az új típusú fenyegetéseknek, és ennélfogva annál erősebb a kényszer a védelem és biztonság megvalósítására.

Napjaink két legjelentősebb információtechnológiai vívmánya a távközlés és az informatika (hálózatok), amelyek a köztük lévő konvergencia következtében globálissá váltak. A globális hozzáférhetőség lehetővé teszi, hogy bárki bárhonnan kommunikálni tudjon. A különböző távközlési hálózatok (vezetékes, mobil, műholdas stb.) - az átjáróknak köszönhetően - teljes körűen integrálódtak egymásba, így minden további nélkül kapcsolat létesíthető analóg, digitális, vezetékes, mobil, vagy műholdas rendszereken keresztül. Ez mára - a konvergenciának köszönhetően - kiterjeszthető az informatikai hálózatokra is, különösen az Internetre.

A globalitás hatalmas előnyt jelent a felhasználóknak, ugyanakkor jelentős mértékben növeli az egyes rendszerek sebezhetőségét is. Az Internet korunk egyik legfőbb információforrása, így nem lehet csodálkozni azon, hogy a támadások zöme e globális infokommunikációs hálózaton keresztül történik. Az IP[4] alapú szolgáltatások rohamos terjedése pedig csak növeli e technológia támadhatóságát. Az Európai Bizottság közleménye is kihangsúlyozza, hogy a mobileszközök (3G-s mobiltelefonok, laptopok, PDA-k[5] stb.) terjedése és a mobilalapú hálózati szolgáltatások egyre növekvő száma új kihívásokat teremt az IP alapú szolgáltatások számára is. A különböző kommunikációs platformok és az informatikai alkalmazások minden új formája elkerülhetetlenül új lehetőségeket nyit meg a rosszindulatú támadások előtt. [13]

Az információs támadás eszközei és módszerei

Tekintettel napjaink információs fenyegetettségi tendenciáira, egyértelműen kijelenthetjük, hogy a támadások a célpontokat illetően két csoportra oszthatók, úgymint: a számítógép-hálózatok elleni fenyegetések illetve más infokommunikációs rendszerek elleni veszélyek. Célszerűnek látszana tehát a fenyegetéseket e szerint csoportosítani, azonban ez nem elég egzakt kategorizálás, hiszen a célpontok a legtöbb esetben komplexek, átfedik egymást, azaz egy-egy rendszer többféle komponenst is takarhat. Ez az átfedés alapvetően az információtechnológiai eszközök konvergenciájából fakad.

Egy másik csoportosítási elv szerint a fenyegetés módszerei szerinti célszerű kategorizálni az információs támadásokat. Eszerint az alábbi támadási módszerekről beszélhetünk: Számítógép-hálózati támadás, elektronikai felderítés, elektronikai támadás, fizikai támadás.

Számítógép-hálózati támadás

A számítógép-hálózati támadások alapvetően kettős célt szolgálnak. Egyrészt a hálózatok *felderítését,* az adatokhoz

való *hozzáférést*, másrészt pedig az adatok, információk *befolyásolását, tönkretételét*, a hálózatok működésének tényleges *akadályozását, megbontását.*

A hálózat felderítése tulajdonképpen olyan behatolást jelent a számítógépes rendszerekbe, hálózatokba, amely lehetővé teszi az adatbázisokban tárolt adatokhoz, információkhoz való hozzáférést, és azok saját célú felhasználását. A felderítés során lehetőség nyílik: a számítógépes hálózatok struktúrájának feltérképezésére; a forgalmi jellemzőik alapján hierarchikus és működési sajátosságainak feltárására; a hálózaton folytatott adatáramlás tartalmának regisztrálására, illetve az adatbázisban tárolt adatok megszerzésére, azok saját célú felhasználására.

E tevékenység során a rendszer nem sérül, és a benne tárolt adatok sem módosulnak, vagy törlődnek, viszont azok illetéktelen kezekbe kerülése jelentős veszteséget okozhat a támadást elszenvedőnek. Tehát e támadás során a rendszerben tárolt *adatok bizalmassága sérül*. Ezenkívül, ha figyelembe vesszük, hogy a megszerzett adatok birtokában a rendszer könnyebben támadhatóvá válik, akkor láthatjuk, hogy e tevékenység éppen olyan komoly veszélyforrás, mint a tényleges kárt okozó támadás.

A tényleges és egyértelműen észlelhető *kárt okozó támadás* olyan behatolást jelent a másik fél számítógépes rendszereibe, illetve hálózataiba, amelynek eredményeképpen tönkretehetők, módosíthatók, manipulálhatók, vagy hozzáférhetetlenné tehetők az adatbázisban tárolt *adatok, információk,* illetve a támadás következtében maga a *rendszer vagy hálózat sérül*. E tevékenység a hálózatokban folyó megtévesztő, zavaró tevékenységet illetve a célobjektumok program-, és adattartalmának megváltoztatását, megsemmisítését jelenti. Ennek következtében a rendszerben tárolt *adatok sérülékenysége nő, a szolgáltatások elérhetősége pedig csökken.*

Az ismertetett kettős célú (1. felderítés, hozzáférés illetve 2. befolyásolás, tönkretétel, akadályozás, megbontás) számítógép-hálózati támadások az információs dimenzióban közvetlen és közvetett formában valósulhatnak meg. *A közvetlen támadás* során a támadó fél egyrészt a különböző információbiztonsági rendszabályokat kikerülve bejut a számítógép-hálózatokba, hozzáfér különböző adatbázisokhoz, és ezáltal számára hasznosítható információkhoz jut. Másrészt megtévesztő információkkal, rosszindulatú szoftverek bejuttatásával tönkreteszi, módosítja, törli stb. a másik fél számára fontos információkat. *A közvetett támadás* során a támadó fél hozzáférhetővé teszi a másik fél számára a saját félrevezető információit, vagy megtévesztő hálózati tevékenységet folytat, és ezáltal félrevezeti és befolyásolja a helyzetértékelést, illetve hamis adatokkal túlterheli a rendszert, aminek következtében a hálózati hozzáférést akadályozza (táblázat). [14]

Számítógép-hálózati támadás [14]

Cél:	FELDERÍTÉS		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	Tönkretétel	Megtévesztés	Zavarás	Tönkretétel
Információs dimenzió	Hálózati topológia kívülről való feltérképezése Titkosítás megfejtés, dekódolás	Számítógép hálózatok adataihoz való rejtett hozzáférés Trójai programok alkalmazása Jelszó-lopók 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 támadás eszközei közé tartoznak a különböző kártékony, rosszindulatú programok, melyeket Malware-eknek nevezünk. A Malware azon szoftverek gyűjtőneve, melyek közös jellemzője, hogy anélkül jutnak a rendszerbe, hogy arra a felhasználó engedélyt adott volna. Minden olyan szoftver rosszindulatúnak minősíthető, amely nem a számítógépes rendszer vagy hálózat rendeltetésszerű működését biztosítja.

A Malware kifejezés számos rosszindulatú szoftvert takar. Napjainkban e szoftverek típusai és fajtái folyamatosan gyarapodnak, ezért egyértelmű kategorizálásuk szinte lehetetlen. A legismertebb ilyen programok: a vírusok, a programférgek, a trójai programok, a rootkitek, a böngésző eltérítők, a hátsó ajtó (backdoor) programok, a keyloggerek, a spam proxyk, a spyware és az adware programok, és a sort még folytathatnánk. Nem program típusú Malware-ek közé taroznak többek között a spam-ek, hoax-ok, és a phishing, amelyek szöveges információk formájában hordoznak veszélyt a rendszerre és felhasználójára.

Mindegyik Malware-nek megvan a maga speciális funkciója, ami a rendszer működésének megzavarástól az adatlopásig vagy a rendszer feletti vezérlés átvételéig terjedhet. Látható, tehát, hogy az előzőekben ismertetett számítógép-hálózati támadások minden típusánál (közvetlen és közvetett támadás, valamint felderítés és tönkretétel) alkalmazhatók a Malware-ek. A rosszindulatú szoftverek módosíthatják a programokat, erőforrásokat foglalhatnak le, adatokat módosíthatnak, hardverhibát eredményezhetnek, eltávolításuk pedig megfelelő eszközöket, időt és energiát, egyes esetekben pedig különleges szakértelmet igényelhet.

Alkalmazásuk az alábbi legjellemzőbb tevékenységeket indíthatják el a számítógépekben és a hálózatokban: automatikus tárcsázás; távoli bejelentkezés másik gépre; adatgyűjtés; adatok törlése, módosítása; adatokhoz való hozzáférés megtagadása; programfutási hibák; kéretlen reklámok megjelenítése; billentyűleütés figyelése; vezérlésátvétel, titkolt műveletek stb.

A támadás különböző módszerei ötvözve az eszközökkel lehetővé teszik a hálózatba való behatolást, működésének akadályozását, megbontását, illetve az adatokhoz való hozzáférést. A támadó egy távoli számítógéphez és annak adataihoz egy egyszerű, egylépéses folyamattal a legritkább esetben fér hozzá. Jellemzőbb, hogy a támadóknak számos támadási módszert és eszközt kell kombinálniuk, hogy kikerüljék mindazokat a védelmi eljárásokat, melyeket a hálózatok biztonsága érdekében alkalmaznak. A hálózatok támadására nagyon sokféle módszer létezik, így a támadóknak csak a megfelelő szakértelemre van szükségük, hogy a támadás eszközeit a megfelelő

eljárásokkal kombinálják. *Íme a sokrétű támadási formák közül néhány legismertebb:*

- Sniffing;
- Spoofing;
- Session Hijacking;
- Spamming;
- Man-in-the-Middle Attack;
- Denial-of-Service (DoS) Attack, stb.

E tanulmány terjedelme nem teszi lehetővé és nem is célja, hogy minden támadási módszert részletesen ismertessünk. Ezért a számos támadási módszer közül egy hálózati felderítésre és egy konkrét támadásra alkalmas eljárást mutatunk be röviden.

A sniffing (szimatolás) nem más, mint a hálózaton zajló információáramlás folyamatos nyomon követése, vagyis a hálózat felderítése. Az e célra alkalmas szoftver és hardver eszközökkel meg lehet figyelni az adatátvitel fő jellemzőit, mint pl., hogy honnan hová, milyen típusú és tartalmú adatok kerülnek továbbításra. Ezen túlmenően bizonyos típusú adatok kiszűrhetők a nagy adathalmazból, vagy e módszer alkalmazásával jelszavakhoz is hozzá lehet jutni. Az egyik ilyen ismert és vitatott működésű hálózatlehallgató eszköz volt a Canivore elnevezésű megfigyelőszoftver, amelyet az FBI leginkább e-mailek szűrésére használt. A Carnivore-val szembeni nagyfokú ellenállás miatt, a szövetségi nyomozóiroda e célra már kereskedelmi forgalomban is hozzáférhető szoftvereket használ.

A lehallgató (sniffer) egy olyan program, amelyet üzenetszórásos hálózatokban alkalmazhatnak az áramló információ illetéktelen megfigyelésére, kinyerésére. A sniffer program a hálózati kártyák meghajtóját megfelelő, ún. promiscuous módba (válogatás nélküli csomagelkapás) állítva képes az adott médián folyó minden forgalmat megfigyelni, elemezni. Ismertebb lehallgató programok, pl. az Ethereal, vagy a tcpdump, amelyek segítségével a támadó a hálózaton átküldött jelszavakat, vagy egyéb bizalmas információkat ismerhet meg. [15]

A Denial of Service (DoS) támadások - ami magyarul szolgáltatás-megtagadással járó támadást jelent - kiemelt jelentőséggel bírnak az Internet biztonsági problémái között. A DoS támadások során a támadó célja, hogy megakadályozza a hálózat megfelelő, üzemszerű működését. Ezt úgy éri el, hogy a válaszadó rendszert hamis kérésekkel megbénítja, így az a más forrásból érkező valós kéréseket már nem tudja kiszolgálni. Ezek a támadások nehezen megelőzhetőek, és nehezen akadályozhatók meg, mivel igen nehéz annak eldöntése, hogy melyik kérés valós, és melyik nem. Ezzel szemben megvalósításuk nem túl bonyolult, mivel a támadónak csupán megfelelő mennyiségű automatizált rendszerre van szüksége, ami elégséges a cél megbénításához. [16] A DoS támadások többnyire un. elosztott támadások (Distributed DoS - DDoS), ahol több támadó együttesen kívánja előidézni a rendszer összeomlását.

A DoS támadásoknak két nagy típusa ismeretes: a protokolltámadások és az un. elárasztásos (flooding) támadások. Az első csoportba azok tartoznak, amelyek az adott alkalmazás vagy protokoll hiányosságait használják ki. A második esetben pedig igen sok kliens egyszerre küld nagy adatmennyiségeket a szerver felé, aminek következtében annak hálózati kapcsolatai és erőforrásai már nem bírják kiszolgálni a felhasználókat.

A DDos támadásoknál igen gyakran olyan gépeket is igénybe vesznek, amelyek nem is tudnak arról, hogy egy ilyen típusú támadás aktív részesei. Ebben az esetben egy automatizált alkalmazás felderíti az Interneten lévő sebezhető számítógépeket. Ezt követően automatikusan vagy elektronikus levelekben küldött, esetleg egyes honlapok látogatásakor "összeszedett" vírusokkal és trójaiakkal feltelepítenek rá egy rejtett támadóprogramot. Ezzel a kiszemelt gépet "zombivá" teszik. Ez annyit jelent, hogy azokat egy "mester-gép" távolról vezérli, utasítja a kiválasztott honlap elleni támadás megkezdésére. A zombik egyenként ugyan kevés adattal dolgoznak, de együttes

fellépésük hatalmas - bénító erejű - adatáramlást eredményez.

Napjainkban számos DDoS támadással találkozhatunk. Szinte naponta kapjuk a híreket, hogy különböző ismert és nagy forgalmú weboldalak DDoS támadás áldozatává váltak. A legutóbbi ilyen eset volt az orosz-észt cyber-háborúnak kikiáltott eset, amely a világsajtóban is nagy hírverést keltett.

Mint ismeretes, 2007. április 27-én zavargások törtek ki a tallinni szovjet hősi emlékmű eltávolítása miatt, az igen fejlett informatikai kultúrával rendelkező Észtországban. Az első túlterheléses (DDoS) támadások jelei néhány nappal az első tüntetések után jelentkeztek a parlament, kormányhivatalok, minisztériumok, bankok, telefontársaságok és médiacégek szerverei ellen. A célpontok kiválasztása, a támadások összehangoltsága, precíz kivitelezése és hatékonysága arra mutatott, hogy e támadások hátterében szervezett erők állnak. Néhány esetben szakértők megállapították, hogy a támadások orosz szerverektől indultak, amit természetesen az orosz hatóságok tagadtak. Ugyanakkor a megtámadott szerverek jellegéből adódóan nyilvánvaló, hogy a támadások célja egyértelműen a balti állam kritikus információs infrastruktúrájának bénítása volt. Az ország on-line adatforgalmát irányító kulcsfontosságú szerverek naponta omlottak össze, sok állami intézmény hálózatát kénytelenek voltak ideiglenesen leválasztani az Internetről. Az elektronikus banki forgalom és kereskedelem részint megszűnt, részint erősen akadozott. Egyes szakértők szerint a cyber-támadás sokkal súlyosabb gazdasági károkat okozott Észtországnak, mint amit azok a kereskedelmi szankciók okoztak volna, amikkel Oroszország a krízis első heteiben fenyegetőzött. [17]

Az Észtország ellen végrehajtott DDoS támadás is bizonyítja, hogy az információs támadások hatalmas kockázatot jelentenek az egyes országok kritikus információs infrastruktúráira, és azokon keresztül a nemzetek biztonságára.

Az információs rendszerek védelme gyakran olyan mértékű, hogy technikai eszközökkel nem vagy csak nagyon kis hatékonysággal lehet róluk megfelelő információhoz jutni. E probléma kiküszöbölésére terjedt el egy igen hatékony információszerzési forma, melyet a magyarra igen nehezen lefordítható Social Engineering-nek neveznek. A *Social Engineering* az emberek természetes, bizalomra való hajlamát használja ki a számítógép-hálózatokba való bejutáshoz. E tevékenység keretében a hálózat gyenge pontjaira vonatkozó adatokat, a legfontosabb jelszavakat, stb. attól a személytől szerzik meg félrevezetés, zsarolás, csalás, esetleg fenyegetés útján, aki azokat kezeli, vagy aki azokhoz hozzáfér. E tevékenység igen nagy szerepet játszik abban, hogy a támadó megkerülhesse a különböző biztonsági megoldásokat, mint pl. tűzfalakat vagy behatolás detektáló rendszereket.

Itt kell megemlíteni napjaink egyik leginkább fenyegető információs veszélyforrását a *cyber-terrorizmust,* vagy annak még tágabb értelmezését az *információs terrorizmust.* Természetesen itt nem egy újfajta eszközrendszerről vagy módszerről van szó, hanem az információs támadásoknak egy olyan szervezett keretek között végrehajtott formájáról, mely sokkal veszélyesebb, mint néhány hacker, vagy elszigetelt csoport számítógép-hálózatok ellen megnyilvánuló támadása. Jelentőségét az adja, hogy e támadások szinte kivétel nélkül politikai tartalommal bírnak, és céljaik elérése érdekében a fejlett országok információtechnológiai fejlettségét használják ki.

Megvizsgálva az információs terrorizmus jelenlegi helyzetét, megállapíthatjuk, hogy a különböző terrorszervezetek az információtechnológiát - azon belül is elsősorban az Internetet - szinte kizárólag propaganda célokra használják, és egyelőre kevésbé foglalkoznak annak támadó jellegű felhasználásával. Az elmúlt években a terrorista csoportok és más szélsőséges szervezetek egyre erőteljesebben, felkészültebben és nyíltabban használják az Internetet eszméik hirdetésére, kiképzési célokra, kapcsolattartásra, toborzásra és nem utolsó sorban pszichológiai hadviselésre.

A terrorszervezetek manapság egyre több számítógépes szakértővel rendelkeznek, ám ezeknek még hiányzik egyrészt a műszaki hátterük, másrészt a kellő motivációjuk ahhoz, hogy pl. egy ország ellen átfogó információs támadást intézzenek. Arról azonban nem szabad megfeledkeznünk, hogy a támadás lehetősége fennáll. Amint felismerik e támadásban rejlő politikai hasznot, és egy bombamerénylettel egyenértékűnek értékelnek pl. egy banki

információs rendszerbe való behatolást, vagy egy energiaellátó rendszer ellen indított információs támadást, várhatóan nagy erőfeszítéseket tesznek e fenyegetések konkrét megvalósítása irányába.

Az információs dimenzióban folytatott terrorizmus által okozott kár pontosan mérhető, és egyre inkább egyenértékűvé válik a nehezebben kivitelezhető, több és körültekintőbb szervezést igénylő fegyveres támadásokkal. A nemzetközi szervezetek szerint növekszik az információs terrortámadások által elérhető célpontok száma is, mivel az Internet használata egyre szélesebb körű a világon. Tehát belátható időn belül számolnunk kell azzal, hogy a terrorizmus a céljai elérése érdekében kihasználja az információs dimenzióban megvalósítható támadási módszereket és eszközöket, és az információs hadviselés teljes repertoárját alkalmazni fogja.

- *Az elektronikai felderítés,* mint információszerző tevékenység általában kettős céllal kerülhet végrehajtásra. Egyrészt az infokommunikációs rendszerekben tárolt és továbbított *adatokhoz való hozzáférés és azok felhasználása* céljából. Másrészt a hatékony támadás kivitelezéséhez szükséges *célinformációk megszerzése* céljából. A kritikus információs infrastruktúrák elleni támadások hatékonysága nagymértékben függ attól, hogy a támadást elkövető tudja-e, hogy az adott objektum (rendszer) fizikailag hol helyezkedik el, milyen a strukturális összetétele, milyen hardver és szoftver elemekből áll, milyen célú és mennyiségű adatforgalom zajlik rajta keresztül, vannak-e gyenge pontjai, és ha igen hol, illetve kik az adott információs rendszer vagy hálózat üzemeltetői, és felhasználói. [4] Napjainkban e célra a legkülönfélébb módszerek és technikai eszközök alkalmazhatók, melyek jelentősen megnövelik, megsokszorozzák az emberi érzékelés határait. A felderítés céljára alkalmazott technikai eszközök képesek a teljes frekvenciaspektrumban adatokat gyűjteni, azokat akár automatikusan is a fúziós technológián alapuló adatfeldolgozó központokba továbbítani, ahol értékes felderítési információkat lehet nyerni belőlük. [18]

A mai korszerű infokommunikációs eszközöket alapul véve kijelenthető, hogy az elektronikus úton végzett felderítő tevékenység jelentősen képes hozzájárulni a célpontul kiszemelt objektumok és rendszerek mindenoldalú feltérképezéséhez. E tanulmány keretiben nem vállalhatjuk fel az elektronikai felderítés teljes spektrumának bemutatását, így csak a legjellemzőbb rendszerekről teszünk említést.

A korszerű *rádióelektronikai felderítő eszközök* a teljes rádiófrekvenciás sávban lehetővé teszik a különböző aktív kisugárzás elvén működő elektronikai berendezések (rádiórendszerek, radarok stb.) felfedését, lehallgatását, helymeghatározását és technikai jellemzőik kiértékelését. Napjaink korszerű, kis valószínűséggel felderíthető elektronikai eszközei (pl. frekvenciaugratásos illetve szórt spektrumú rendszerek) sem jelentenek akadályt e rendszerek számára, mivel az új generációs felderítő vevők képesek detektálni e kisugárzásokat, és meghatározni a sugárforrás helyét, ami az esetleges fizikai vagy elektronikai támadás végrehajtásához szükséges.

Az elektronikai felderítés céljára felhasználható eszközök jelentős része kereskedelemi forgalomban szabadon hozzáférhető és megvásárolható. Ezekkel a berendezésekkel mindazon információs rendszerről beszerezhetőek a legfontosabb adatok, amelyek valamilyen elektromágneses kisugárzó eszközt alkalmaznak működésük során.

Azon infokommunikációs rendszerek esetében, amelyek nem vagy csak nagyon kis számban alkalmaznak elektromágneses kisugárzó eszközöket, vagy a védelmi szintjük igen magas fokú, az információk megszerzése természetszerűleg más forrásokra támaszkodik. Ilyen lehet pl. a különböző vezetékeken zajló adat vagy kommunikációs forgalom technikai eszközökkel való felderítése. Ezek az eszközök, amelyek a vezetékeken folyó elektromos jelek által keltett mágneses mezőt felhasználva indukciós módszerrel nyerik ki az információkat, szintén beszerezhetők kereskedelemi forgalomban is. [4]

A korszerű elektronikai felderítésben egyre inkább jellemzővé válik, hogy az adatokat olyan eszközökkel szerzik meg, melyek az élőerőt nem veszélyeztetik. Ezek lehetnek egyrészt különböző hordozóeszközökön kijuttatott

eszközök, mint pl. a pilóta nélküli repülőeszközön elhelyezett szenzorok, illetve a felderítendő objektum körzetébe letelepített úgynevezett *felügyelet nélküli földi szenzorok*. Ez utóbbiak olyan mini-, mikro- és nanoméretű érzékelő- és mérőműszerek, amelyek a környezeti méret- és állapotváltozásokat, torzulásokat, ingadozásokat stb. képesek érzékelni, mérni, és automatikus úton jelenteni. E szenzorok olyan állapotváltozásokat mérnek, mint pl.: hőváltozások, mechanikai változások, akusztikus változások, vegyi állapotváltozások, mágneses változások, elektrooptikai változások, vagy esetleg biológiai változások.

A felügyelet nélküli szenzorok számos előnyös tulajdonsággal bírnak, mint pl. hogy a telepítés után a nagyon kis méretüknek köszönhetően alig felderíthetők, illetve hogy nagyon kis áramfelvételük miatt a saját akkumulátoraikról igen hosszú ideig képesek működni. [18]

- *Elektronikai támadás:* Az elektromágneses környezetben működő elektronikai eszközök párosulva bizonyos természeti jelenségekkel (hullámterjedési sajátosságokkal) gyakran forrásai különböző káros, (szándékos és nem szándékos) elektromágneses kisugárzásoknak. Ezeket ún. *elektromágneses környezeti hatásoknak* nevezzük.

Az elektromágneses környezeti hatások közé a következők sorolhatók:

- elektrosztatikus kisülések, melyek különböző elektromos potenciálú testek közötti elektrosztatikus töltés átvitelt jelenti;
- nagy energiájú elektromágneses impulzusok, melyek általában földfelszín feletti nukleáris robbantások során keletkeznek;
- irányított energiájú eszközök által keltett pusztító, rongáló hatások;
- szándékos elektronikai zavarok;
- nem szándékos interferenciák.

Mint a felsorolásból is kitűnik az elektromágneses környezeti hatások egy része szándékos tevékenységek következménye, amelyeket az elektronikai támadás eszközeivel és módszereivel lehet elérni. Az elektronikai támadás minden olyan technikát, módszert és eszközt felhasznál, ami az elektromágneses és más irányított energiák felhasználásával képes lerontani az ellenség infokommunikációs rendszereinek hatékonyságát, csökkenteni vezetési és irányítási lehetőségeit, működésképtelenné tenni fontosabb technikai eszközeit és megtéveszteni információs rendszereit.

Ezek az eszközök minden esetben valamilyen energiát sugároznak ki, sugároznak vissza, vagy vernek vissza a célobjektum működésének akadályozása, korlátozása vagy rongálása érdekében. E tevékenység az elektronikai hadviselés egyik alapvető összetevője, melynek körébe az elektronikai zavarást, elektronikai megtévesztést és az elektronikai pusztítást soroljuk.

Az elektronikai zavarás az elektromágneses energia szándékos kisugárzását, visszasugárzását vagy visszaverését jelenti abból a célból, hogy a különböző fajtájú infokommunikációs rendszerek rendeltetésszerű működését megakadályozzuk, korlátozzuk, vagy túlterheljük. Az elektronikai zavarás mind aktív (zavarójelet kisugárzó, vagy visszasugárzó), mind passzív (elektromágneses hullámokat visszaverő) eszközökkel megvalósítható.

Az elektronikai zavarok olyan elektromágneses sugárzások, melyek a berendezések vevőegységére hatva torzítják a megfigyelt és a végberendezés által rögzített jeleket, információkat, megnehezítik, illetve kizárják a rádióforgalmazás lehetőségét, az adatátvitelt, a cél felderítését, csökkentik a felderítő eszközök megkívánt hatótávolságát és az automatizált vezetési rendszerek pontosságát, megtévesztik a kezelőket.

Az elektronikai zavaráshoz erre a célra tervezett és szerkesztett berendezésekre, úgynevezett zavaróállomásokra,

speciális sugárzókra vagy visszaverő eszközökre van szükség. Az esetek túlnyomó többségében ezek bonyolult, és drága berendezések, amelyek rendszerint az egyes országok elektronikai hadviselési erőinek kötelékében találhatók meg. Számolni kell ugyanakkor azzal is, hogy hozzáértő szakemberek képesek előállítani egyszerűbb kivitelű, korlátozott képességekkel rendelkező eszközöket, amelyek pl. nem reguláris erők, vagy akár terroristák kezében az ismertetett zavarási feladatokra hatékonyan felhasználhatók. [4]

Az elektronikai megtévesztés hamis jelek szándékos kisugárzását, visszasugárzását vagy visszaverődését jelenti, amely megtéveszti, félrevezeti, az elektronikai rendszerben működő humán, vagy gépi döntéshozatali folyamat működését. E tevékenység során a cél, hogy az adott rendszerbe bejuttatott jelek, információk szintaktikailag és szemantikailag is egyaránt helytállóak legyenek, megfeleljenek a helyzetnek, ugyanakkor hamis voltuk miatt hibát okozzanak, helytelen döntéseket eredményezzenek a megtámadott rendszerben. Mindemellett olyan veszélyek is kialakulhatnak, mint például egy repülőtér közelében elhelyezett és ott működésbe hozott hamis jeladó, amely a valóságostól eltérő adataival látja el a körzetében repülő repülőgépeket. [4]

Az elektronikai megtévesztés során alkalmazható eszközök és eljárások az alábbiak lehetnek:

- infracsapdák, válaszadók, hamiscél generátorok, melyek megtévesztő kisugárzásokat hoznak létre;
- különböző imitációs technikai eszközök, melyek helyettesítik a rádiólokátor-, navigációs- és kommunikációs kisugárzásokat;
- dipólok és egyéb visszaverő eszközök, amelyek álcáznak, vagy hamis célokat hoznak létre;
- rádióhullámokat elnyelő anyagok, védő festékek és bevonatok, melyek csökkentik a hatásos visszaverő felületet;
- hőenergiát elnyelő vagy szétszóró anyagok, védő festékek és bevonatok, melyek csökkentik az infravörös kisugárzásokat.

A hatékony elektronikai megtévesztés feltétele egyrészt, hogy a másik félnek érzékelnie kell a megtévesztő jeleket, másrészt pedig e tevékenységeknek - hogy a félrevezetést ne lehessen felfedezni - valóságosnak kell látszaniuk. Ennek érdekében az elektronikai megtévesztés részletes és alapos tervezést, koordinációt és végrehajtást igényel.

Az elektronikai pusztítás, rongálás az elektromágneses és egyéb irányított energiák, alkalmazását jelenti abból a célból, hogy a megtámadott elektronikai eszközökben tartósan, vagy ideiglenesen kárt okozzanak.

Az elektronikai eszközökben, számítógépekben használt mikroprocesszorok miniatürizálása következtében a vezetőrétegek vastagsága rendkívüli mértékben lecsökkent. Ez a nagymértékű csökkenés azt eredményezheti, hogy megfelelő nagyságú sztatikus - külső vagy belső forrásból származó - túlfeszültség hatására villamos átütés jöhet létre a rétegek között, amely roncsolja, és így javíthatatlanná teszi az alkatrészeket. [4]

Az elektromágneses impulzus (EMP) elvén működő fegyverek tulajdonképpen ezt használják ki. Képesek megfelelő nagyságú elektromágneses tér létrehozására, és mindezt irányítottan, célzottan a mikroprocesszorokat, illetve mikroelektronikai áramköröket tartalmazó eszközök közelébe juttatni. Ezek az eszközök alkalmazhatók bombaként (E-bomba) amely egy bizonyos magasságban berobbantva, közel kör alakú területen működő összes elektronikai berendezést tönkre teszi. Másik alkalmazási mód, amikor az eszköz, pl. a nagy energiájú rádiófrekvenciás fegyver (HERF) az adott célpont felé irányítva nagy energiájú impulzusokkal rongálja a berendezéseket. Ez utóbbi előnye, hogy míg az E-bomba csak egyszer alkalmazható, addig a HERF eszköz többször is bevethető.

Napjainkban a nagy veszély abban áll, hogy az elektromágneses impulzus hatás elvén működő eszköz könnyen hozzáférhető elemekből alig 1000 dollárért, házilag is összebarkácsolható. Ezek teljesítménye természetesen ebben az esetben korlátozott, de ahhoz pontosan elegendőek, hogy egy-egy jól megválasztott helyre elhelyezve, kulcsfontosságú információs rendszereket részlegesen, vagy teljesen megbénítson. [4] Ezt természetesen jól tudják

a fejlett információs rendszerekkel rendelkező államok is. Talán éppen ezért Bush amerikai elnök nem sokkal az ikertornyok elleni támadást követően elrendelte a kritikus információs infrastruktúrák elleni esetleges támadásokkal szembeni védekezés stratégiájának kidolgozását.

- *A fizikai támadás* a fizikai dimenzióban fejti ki hatását, mégpedig a védő fél fizikai lehetőségeinek és képességeinek (katonai ereje, kritikus infrastruktúrái, stb.) támadásával. A fizikai erő alkalmazása a legalapvetőbb és a legrégebbi módja a támadásoknak, illetve a háborúknak. Amennyiben a korunkra jellemző aszimmetrikus hadviselés elméletét vesszük alapul, kijelenthetjük, hogy a kritikus infrastruktúrák fizikai támadása jelenleg a leginkább alkalmazott módszer, különösen a terrorista csoportok részéről.

Sajnálatos módon az információs rendszerek rendkívül gyors fejlődésével és elterjedésével nem tartott lépést e rendszerek védelmét szolgáló fizikai biztonsági megoldások fejlesztése illetve kiépítése. Rendkívül sok információs infrastruktúra (köztük jó néhány kritikus információs infrastruktúra), vagy az infrastruktúra egyes elemeinek fizikai védelme gyenge, hatástalan, esetleg primitíven kivitelezett. [4] Ez pedig rendkívüli mértékben megnöveli a fizikai sebezhetőségüket.

A pusztító, romboló, rongáló hatású fizikai támadások a földről, levegőből vízfelszínről és víz alól végrehajtott közvetlen és közvetett pusztító csapásokat, valamint a különböző speciális erők alkalmazását jelentik a kritikus információs infrastruktúra elemeivel szemben. A szembenálló fél információs rendszerei objektumainak egy adott ideig tartó vagy folyamatos pusztítása, rombolása vagy rongálása jelentősen hozzájárul a vezetési, irányítási képességek csökkentéséhez. A fizikai megsemmisítés alkalmazása az egyik legsúlyosabb veszélyforrás, az információs hadviselés un. "Hard Kill" típusú módszere, melyet kizárólag terrorcselekmények illetve katonai műveletek során alkalmaznak.

A kritikus információs infrastruktúrák rombolására alkalmazott pusztító erők és eszközök fajtája és típusa minden esetben az adott helyzettől függ. A cél elérése érdekében alkalmazhatók irányított rakéták, robotrepülőgépek, harci repülőgépek, harci helikopterek, pilóta nélküli harci repülőgépek, hagyományos tüzérségi fegyverek, robbanószerek stb., illetve kritikus információs infrastruktúrák ellen speciálisan felkészített különleges egységek, romboló csoportok.

A fizikai támadásnak azonban lehetnek finomabb formái is, mint pl. olyan nem pusztító, romboló eszközök alkalmazása, melyek az infrastruktúra vagy annak egyes elemei működését ideiglenesen bénítják. Ilyen lehet pl. az elektromos távvezetékekben rövidzárlatot okozó grafitbomba. Ezek a bombák ugyanúgy kerülnek alkalmazásra, mint hagyományos társaik, csak a robbanás következtében nem a kinetikus energia fejti ki a hatását, hanem a szétszóródó grafitszálak telepednek rá a távvezetékek lezáró ellenállásaira. Ennek következtében azok vezetővé válnak, és a földön keresztül rövidzárat okoznak a távvezeték hálózatban. Alkalmazásukra jó példa volt a balkáni konfliktus, amikor is e bombák az akkori Jugoszlávia területén összesen hét nagyobb központban okoztak súlyos energiaellátási zavarokat.

Összegzés

Információs társadalom a nagyfokú hálózatosítás következtében rendkívül sebezhető társadalom. Az eddig ismert hagyományos veszélyeken túl e társadalomban más típusú fenyegetésekkel is kell számolnunk.

E fenyegetések a társadalom működését lehetővé tevő kritikus információs infrastruktúrákon keresztül jelentkeznek. Ezért ezek meghatározása, egymás közötti kapcsolataik bemutatása, sebezhető pontjaik feltárása, és az ellenük alkalmazható támadás eszközeinek és módszereinek ismerete rendkívül fontos az átfogó biztonság

megteremtése érdekében.

Amennyiben - a kritikus információs infrastruktúrákon keresztül - az egész társadalom ellen átfogó és összehangolt információs támadást intéznek, az várhatóan az információs hadviselés elméletének megfelelően kerül végrehajtásra. Egy ilyen támadás hatására - az információtechnológiától rendkívüli mértékben függő társadalomban - megtörténhet a *teljes infokommunikációs rendszer összeomlása,* amit a médiában "Digitális Pearl Harbor" effektusnak neveznek. Ennek eredményeként megszűnhet az energiaellátás, az élelmiszer- és vízellátás, megbénulhat a közlekedés és szállítás, leállhat a bankrendszer és a piacgazdaságot működtető pénzügyi és árutőzsde működése, akadozhat az egészségügyi ellátás, és az ország biztonságát szavatoló védelmi szervek (honvédség, rendőrség, katasztrófavédelem stb.) működése. Bekövetkezhet a politikai, gazdasági, biztonsági összeomlás, vagyis a *teljes káosz állapota.*

Bár az ilyen típusú összehangolt információs támadásokra eddig még nem volt példa - egyelőre - a veszély ott leselkedik, a támadás lehetősége fennáll. Ezért az ilyen típusú veszélyekre, a fenyegetés eme újszerű formáira fel kell készülni. Ennek érdekében:

- ki kell dolgozni az ország - nemzetközi szinten is koordinált - *információbiztonsági stratégiáját;*
- az információs társadalom biztonságának fenntartásához szükséges új szervezetek, eljárások és speciális módszerek, alkalmazási kérdéseit *jogszabályi keretek között kell szabályozni*, és meg kell teremteni a jogharmonizációt a már meglévő hazai, nemzetközi és Európai Uniós jogszabályokkal;
- a biztonságot szavatoló szervezetek állományát *fel kell készíteni* az információs dimenzióból érkező veszélyekre, az általuk potenciálisan okozható károkra, a fenyegetések elhárítására illetve a támadás következményeinek felszámolására. A felkészítés érdekében, meghatározott időközönként *információbiztonsági szimulációs gyakorlatokat* célszerű levezetni;
- biztonsági szempontból *felül kell vizsgálni* az információs társadalom működését biztosító kritikus infrastruktúrák, szervezetek nyilvánosan hozzáférhető adatait, és ha szükséges azok nyilvános publicitását meg kell szüntetni;
- az információs társadalom tagjai körében pedig széleskörű és tudatos *tájékoztatást* kell folytatni az esetlegesen bekövetkező információs fenyegetésekkel kapcsolatosan, meg kell *ismertetni* velük az új típusú veszélyeket, és *fel kell készíteni* őket a védelem alapvető technikai eljárásaira és rendszabályira.

Végső összegzésként kijelenthetjük, hogy egy jól megszervezett, és összehangolt - az információs hadviselés eszközeit és módszereit alkalmazó - információs támadással egy információtechnológiától nagymértékben függő országnak igen komoly, rendkívül nehezen helyreállítható károkat lehet okozni. Ezért a biztonság eme új dimenziója *az információbiztonság* kiemelt szerepet kell, hogy kapjon biztonságpolitikai gondolkodásunkban.

FELHASZNÁLT IRODALOM

1. Haig Zsolt - Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005. ISBN 963 327 391 9

2. A hálózati társadalom sérülékenysége. http://www.nato.int/docu/review/2002/issue2/hungarian/features2.html (2007. 05. 20.)

3. A Magyar Köztársaság nemzeti biztonsági stratégiája. http://www.kulugyminiszterium.hu/kum/hu/bal/Kulpolitikank/Biztonsagpolitika/Nemzeti_biztonsagi_strategia.htm (2007. 05. 20.)

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. Kovács László: Az információs terrorizmus eszköztára. Robothadviselés 6. Tudományos szakmai konferencia, Hadmérnök különszám. 2006. ISSN 1788-1919

6. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. Public Law 107-56-oct. 26, 2001.

7. Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final.

8. Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the Fight Against Terrorism. Brussels, 20.10. 2004 COM(2004) 702 final.

9. 2112/2004. (V. 7.) Kormány határozat a terrorizmus elleni küzdelem aktuális feladatairól

10. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. http://www.whitehouse.gov/pcipb/physical_strategy.pdf (2007. 06. 25.)

11. Gerencsér András: Rövid összefoglalás kritikus információs infrastruktúrák védelméről. http://www.isaca.hu/addons/news_1626_CIIP_GerencserAndras.pdf (2007. 06. 18.)

12. Dr. Munk Sándor Információs színtér, információs környezet, információs infrastruktúra. Nemzetvédelmi Egyetemi Közlemények 2002. 2. sz. ZMNE, Budapest, 133-154. p. ISSN 1417-7323

13. A strategy for a Secure Information Society - "Dialogue, Partnership and Empowerment". Brussels, 31.5.2006. COM(2006) 251 final

14. Waltz, Edward: Information Warfare Principles and Operaions. Artech House, Inc. Boston, London. 1998. ISBN: 0-89006-511-X.

15. Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai. MTA SZTAKI, 2004.

16. Előházi János: Internetbiztonság. Robothadviselés 5. Tudományos szakmai konferencia, Bolyai Szemle 2006. 1. sz. ZMNE, Budapest, 160-178. p. ISSN 1416-1443

17. Magyar Narancs. http://www.mancs.hu/index.php?gcPage=/public/hirek/hir.php&id=14820 (2007. 06. 25.)

18. Ványa, László: Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre. Doktori PhD értekezés. ZMNE, Budapest. 2002.

vissza a szöveghez

1 A tanulmány a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.

2 Bővebben lásd a hivatkozott irodalmat.

3 Bővebb kifejtésük a hivatkozott irodalmakban megtalálható

4 Internet Protokoll

5 Personal Digital Assistant

vissza a szöveghez

« vissza a tartalomhoz