TÁMOP 4.2.2/B-10/1-2010-0001
Tudományos képzés műhelyeinek támogatása
Kockázatok és válaszok a tehetséggondozásban (KOVÁSZ)

# KRITIKUS INFRASTRUKTÚRÁK ÉS KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK

TANULMÁNY

*Írta:*

Haig Zsolt
Kovács László

*Lektorálta:*

Munk Sándor

*Szerkesztő:*

Ványa László

*Tördelő:*

Vass Sándor



A tanulmány a TÁMOP 4.2.2/B-10/1-2010-0001 Tudományos képzés műhelyeinek támogatása - Kockázatok és válaszok a tehetséggondozásban (KOVÁSZ) projekt támogatásával készült.

# TARTALOM

# BEVEZETŐ

A világ és a kor, amelyben élünk, korábban elképzelhetetlen technikai és technológiai alapokra épül. Eddig a történelemben sohasem látott eszközöket használunk már a mindennapjainkban is. Ezek az eszközök, rendszerek és eljárások számtalan előnnyel járnak a 21. század társadalma számára.

Az információs technológia, valamint a számtalan új kommunikációs technológia konvergenciája eredményeként kialakuló, úgynevezett infokommunikációs technológia az alapja az információs hálózatokra épülő új társadalmi rendnek, az információs társadalomnak.

Globális kommunikációs, avagy infokommunikációs hálózatokat, illetve eszközöket használunk számtalan helyen az iparban, a gazdasági életben, a kereskedelemben, az oktatásban, a kutatás-fejlesztésben, de még a kultúrában is.

A mindennapjaink részévé vált infrastruktúrák jelentős hányada egy, vagy több hálózat része, az esetek döntő többségében az irányítás, a felügyelet, vagy ezek összekapcsolt felügyelete számítógépes hálózatokon keresztül valósul meg.

Ma már szinte valamennyi nagyobb hálózat kapcsolódik az internethez, igénybe veszi annak szolgáltatásait, vagy éppen valamilyen szolgáltatást biztosítanak az internet felé. Az internet felől azonban fel kell készülni az esetleges támadásokra, amik lehetnek betörési kísérletek, de a belső hálózat tönkretételére irányuló próbálkozások is.

Célunk, hogy bemutassuk a kritikus infrastruktúrák és a kritikus információs infrastruktúrák osztályozását, csoportosításait, a legfontosabb hazai infrastruktúrákat, ezek felépítését, működését, valamint azokat a veszélyeket, amelyek e rendszereinket fenyegethetik, valamint, hogy a feltárt veszélyekre válaszul milyen védelmi megoldásokat alkalmazhatunk.

Jelen tanulmány a *TÁMOP 4.2.2/B-10/1-2010-0001 Tudományos képzés műhelyeinek támogatása – Kockázatok és válaszok a tehetséggondozásban (KOVÁSZ)* projekt támogatásával készült. Ennek megfelően tanulmányunkban – pontos irodalmi hivatkozásokkal – felhasználtuk mindazokat a tudományos igényű írásokat, valamint szakmai publikációkat, amelyek a

témában a korábban a Zrínyi Miklós Nemzetvédelmi Egyetemhez, illetve ennek jogutódjához a Nemzeti Közszolgálati Egyetemhez, az ott működő és a témát kutató csoportokhoz köthetőek.[1]

Tanulmányunkban az irodalmi hivatkozásokat, azok nagy száma miatt fejezetenként adjuk meg, hasonlóan az ábrák, képek és táblázatok is fejezetenként kerültek számozásra.

[1] Tanulmányunk melléklete egy olyan bibliográfiai felsorolást tartalmaz, amely alapvetően a kritikus információs infrastruktúrák témában a ZMNE-ne, illetve az NKE-n született tudományos publikációkat tartalmazza összefoglaló jelleggel.

# I. fejezet
# KRITIKUS INFRASTRUKTÚRÁK ÉS KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK ALAPJAI

## *1.1. Az információs társadalom*

### 1.1.1. Az információs társadalom kialakulása

A 21. század óriási kihívás elé állítja társadalmunkat. Az információs kor kihívása, illetve az ezen kihívásnak való megfelelés kényszere, a modern társadalmat gyökeresen átalakítja. Korunkban a tudás alapú társadalmat tekintjük az eddigi legfejlettebb társadalomnak. Az ipari termelési korszakot egyes országokban már felváltotta, számos országban, napjainkban folyamatosan felváltja az információs termelési kor.

Az ipari termelési korszakot felváltó információs termelési kor új társadalmi modellt hoz magával: tudásalapúnak is nevezett információs társadalom jön létre. Az információs társadalomban az információ válik az egyik legfontosabb tényezővé. Ebben a társadalomban már a mindennapi élet alapvető mozgatórugója, valamint társadalmi értéke az információ, a kommunikáció és a tudás.

Az információs ipari termelési korszak az emberi társadalomnak és technikai civilizációjának legújabb fejlődési korszaka, amely felváltja a megelőző gépipari termelési korszakot. A tudásra és tudományra épülő, magas gyártástechnikai színvonalat képviselő információs ipari termelési korszakban az előállított termékek és kifejlesztett szolgáltatások összetevőinek részaránya: 80 %-ban szellemi összetevő, vagyis tudás és tudományos hányad, 20 %-ban pedig anyagi és energia összetevő, vagyis hardver és hajtóerő. Az ipari társadalomban ez éppen fordítva volt. Az összetevők említett részesedési aránya törvényszerűen jelen van az információs társadalom minden területén.

Az a fejlődési szint, ami napjainkat jellemzi az információs ipari forradalom, a tudományok forradalma, az informatika forradalma és a kommunikációs forradalom, szinergikus hatásainak és egymásra épülő eredményeinek köszönhető. Mindezen komplex evolúciós és forradalmi fejlődések, fejlesztések és változások szoros kapcsolatban vannak az információs forradalommal. A modern kor információs forradalma a következőkkel jellemezhető:

- a digitális jelátvitel megjelenése;
- az informatika fejlődése, azon belül különösen a számítógép-hálózatok fejlődése;
- a tudomány fejlődése és a tudásipar kialakulása (információs robbanás);
- a multimédia megjelenése;
- a távközlési ipar fejlődése;
- a távközlés, rádió, televízió és számítógép összeolvadása (műszaki konvergencia);
- az atomi méretű, nanoelektronikai, és mikro-elektro mechanikai (Micro Electro Mechanical Systems – MEMS) gyártástechnológia megjelenése.

Az információs forradalom előfutárai azok a tudományos eredmények, tudományos áttörések voltak, amelyeket a jól felszerelt kutatóközpontokban, számos tudományágban és tudományterületen értek el. Ilyen típusú tudományos áttörések voltak tapasztalhatók:

- a kvantumfizikai kutatásokban;
- a mikroelektronikában elért eredmények területén;
- a nanotechnológiában;
- az anyagtudományokban, az új és összetett (kompozit) anyagok felfedezése terén.

Az információs forradalom tulajdonképpen az információs ipari termelési korszak motorjának szerepét tölti be, és a következő forradalmakkal van összefüggésben:

- tudományos forradalom (alapkutatás + alkalmazott kutatás + innováció);
- kommunikációs és médiaforradalom;
- gyártástechnológiai forradalom (High-Tech);
- számítástechnikai forradalom;

- számítógépes termelés és tervezés forradalma (CAD/CAM rendszerek);
- mikroelektronikai gyártási forradalom;
- nanotechnológiai gyártási forradalom;
- mikrobiológiai forradalom (génkutatás, génsebészet, sejtkutatás, klónozás, gyógyszerkutatás és gyártás stb.);
- robotgyártási forradalom (ipari, háztartási, katonai robotok). [1]

Az információs társadalom elmélete szerint a társadalomban az információ előállítása, elosztása, terjesztése, használata és kezelése jelentős gazdasági, politikai és kulturális tevékenység. Ennek a társadalomtípusnak a sajátossága az információ-technológia központi szerepe a termelésben, a gazdaságban és általában a társadalomban. Az információs társadalmat az ipari társadalom örökösének is tekintik. Szorosan kapcsolódik a posztindusztriális társadalom, a posztfordizmus, a posztmodern társadalom, a tudástársadalom és a hálózati társadalom fogalmaihoz. [2]

Az információs társadalom új társadalmi alakulat. A tudomány eredményeinek intenzív és folyamatos felhasználására alapozott, új típusú termelési és társadalmi alapmodell, amelyet tartalma alapján intenzív tudásgazdaságnak és tudástársadalomnak neveznek.

Való igaz, az emberiség minden társadalma tudástársadalom volt, de összetevőinek részarányát tekintve a tudás és a tudomány ilyen arányú megjelenését ez idáig sehol nem találjuk az írott történelem folyamán. Az információs társadalom a hagyományos gépipari társadalmat követő, és azt felváltó, a tudomány eredményeit intenzíven felhasználó, új és rendkívül magas gyártástechnikai kultúrát képviselő, számítógép-hálózat alapú termelési világkorszak és benne a rendkívül fejlett számítógépes új technikai civilizáció terméke. Ebben a társadalomban a meghatározó mozgatóerő és alapérték az információ és annak tömörített minőségi formája a szaktudás és a tudomány. [1]

Az információs társadalomnak napjainkra már igen terjedelmes szakirodalma van, amely mind mennyiségileg, mind tartalmi mélységében egyre bővül. Az információs társadalom

kialakulásának elméleti előfutárai közül kiemelkedik Alvin Toffler amerikai szociológus, aki több könyvet írt erről a témáról. Toffler alkotta meg a társadalmi fejlődés hullámelméletét, amely szerint az agráripari termelési világrendszert, a gépipari tömegtermelésre szakosodott termelési világrendszer, majd azt az információs ipari termelési világrendszer (a harmadik hullám) váltja fel. Elmélete szerint az emberiség történetében eddig két, a korábbi valóságot alapjaiban megrázó, átalakító hullámról beszélhetünk: a gyűjtögető életformát felszámoló mezőgazdaság (első hullám), illetve a mezőgazdaságot váltó ipar térnyeréséről (második hullám). Az iparra épülő második hullámú társadalmi formációt váltja az információ alapú, nyíltabb társadalmakat ígérő harmadik hullámú társadalom. [3]

Az információs társadalmat többen posztindusztriális társadalomnak tekintik. E nézet képviselője Daniel Bell amerikai szociológus is, aki a posztindusztriális társadalmat az indusztriális (ipari) társadalom alternatívájaként határozta meg. Szerinte a posztindusztriális társadalomban az elméleti tudás és az innovációs készség adja azt a stratégiai erőforrást, amit az ipari társadalomban a tőke és munkaerő jelentett. Habár minden társadalom működésében alapvető szerepet játszik a tudás, de a mérnöki tevékenység a tudománnyal összekapcsolva, csak az utóbbi fél évszázadra jellemző. Bell összehasonlította a posztindusztriális társadalom jellemzőit az indusztriális- és preindusztriális társadalommal, és az alapján látható, hogy a posztindusztriális társadalom legfontosabb változói az információ és a tudás. (1. táblázat)

A szakirodalomban sokféle elmélet található arról, hogy mit nevezünk információs társadalomnak. Jelenleg nincs általánosan elfogadott elmélet arra, hogy pontosan mi nevezhető információ társadalomnak és inkább mi nem. A legtöbb teoretikus egyetért azzal, hogy egy átalakulást látunk, ami valamikor az 1970-es évek és napjaink között kezdődött, és ami megváltoztatja annak a módját, ahogy a társadalmak alapvetően működnek. [2]

Az információs társadalom fogalma igen összetett, olyan folyamatosan gazdagodó gyűjtőfogalom, amelynek modellezése óhatatlanul leegyszerűsítésekhez vezethet. Neves társadalomtudósok kutatásai alapján az új társadalom egyszerre „komputópia” (Masuda), „globális falu” (Mcluhan), „posztindusztriális társadalom” (Bell), a „hiperrealitás világa” (Baudrillard), a

„harmadik hullám” társadalma (Toffler) „hiperhálózati társadalom” (Kumon), „kockázattársadalom” (Beck) stb.

1. táblázat. A társadalmi fejlődés jellemzőinek összehasonlítása [4]

| Jellemzők | Preindusztriális | Indusztriális | Posztindusztriális |
|---|---|---|---|
| **Termelési mód** | Kitermelő | Termelő | Feldolgozó; újrahasznosító |
| **Gazdasági szektor** | **Elsődleges**<br>Mezőgazdaság<br>Bányászat<br>Halászat<br>Favágás<br>Olaj és gáz | **Másodlagos**<br>Árutermelés<br>Gyártás<br>Tartós iparcikkek<br>Nem tartós iparcikkek<br>Építőipar | *Szolgáltatások:*<br>**Harmadlagos**: Közlekedés, Közüzemek<br>**Negyedleges**: Kereskedelem, Pénzügy, Biztosítás, Ingatlan<br>**Ötödleges**: Egészségügy, Oktatás, Kutatás, Kormányzat, Kikapcsolódás |
| **Átalakulást hozó erőforrás** | **Természetes energia**<br>Szél, víz, igásállatok, emberi izomerő | **Gyártott energia**<br>Áram, olaj, gáz, szén, atomenergia | **Információ**<br>Számítógépek, adatátviteli Berendezések |
| **Stratégiai erőforrás** | Nyersanyagok | Finánctőke | Tudás |
| **Technológia** | Kézműipar | Gépi technológia | Intellektuális technológia |
| **Tudásbázis** | Kézműves, fizikai munkás, gazda | Mérnök, betanított munkás | Tudós, műszaki és professzionális Foglalkozások |
| **Módszertan** | Józan ész, próba-szerencse; gyakorlat | Empiricizmus, kísérletezés | Absztrakt elméletek, modellek,<br>szimulációk, döntéselmélet,<br>Rendszerelemzés |
| **Időperspektíva** | Múltorientált | Ad hoc alkalmazkodó képesség, kísérletezés | Jövőorientált: előrejelzés és tervezés |
| **Tervezés** | Játék a természet ellen | Játék a mesterséges jövő ellen | Személyek közötti játék |
| **Vezérelv** | Hagyomány--központúság | Gazdasági növekedés | Elméleti ismeretek kodifikációja |

A tucatnyi megfogalmazás közül ki kell emelnünk Manuel Castells spanyol származású szociológusprofesszor definícióját, amely az új társadalmat, mint hálózatos társadalmat írja le: az információs társadalom *„olyan hálózatos társadalom, ahol a kulcsfontosságú társadalmi rendszerek és tevékenységek elektronikus információs hálózatok köré szerveződnek.”* [5] Ma-

nuel Castells információtechnológia paradigmájában az információ mellett a hálózatosítás, a hálózatok rugalmassága és konvergenciája a központi elem.

Az információs társadalom kialakulása során számos nehézséggel, különböző feltételek teljesítésével kell számolni, amelyeket gyűjtőnéven információs társadalmi küszöbszinteknek neveznek. Ezek az alábbiak:

- információtechnikai küszöbszint;
- társadalmi küszöbszint;
- védelmi küszöbszint.

Egy adott ország az információs társadalomba való átmenetet nehezítő technikai küszöböt akkor lépi át, ha kiépül az országos digitális infokommunikációs gerinchálózata (információs infrastruktúrája,), amely nagysebességű adatátvitelt tesz lehetővé. Az államvezetés, államigazgatás, az intézményrendszer, a vállalatok és a háztartások döntő többsége (70-90 %-ban) kapcsolódik valamilyen számítógép-hálózathoz, pl. az internethez, vagy a vállalati, intézeti intranethez.

Egy adott ország az információs társadalomba való átmenet társadalmi küszöbszintjét akkor lépi át, ha a foglalkoztatottak több mint 60 %-a már nem alacsony szervezettségi szintű munkát – hagyományos értelemben vett fizikai munkát – végez, hanem korszerű információtechnológián alapuló, alkotó, tervező, értéknövelő, intelligens szolgáltató tevékenységet, vagyis magas szervezettségű tevékenységet folytat.

Az információs társadalom felé való haladás folyamán – kezdetben – törvényszerűnek látszik, hogy a társadalom és a világ két részre szakadhat, ha a digitális ismeretek és eszközhasználat terén nem érvényesül az esélyegyenlőség és szabad hozzáférés. Ezt a jelenséget nevezik digitális szakadéknak, digitális tudásollónak, vagy megfogalmazójáról elnevezve Maitland–résnek. A kevésbé tehetős társadalmi rétegek és országok felemelése és támogatása ezen a téren az egész világ közös érdeke.

E kérdéshez szorosan kapcsolódik a digitális írástudás problémája is. A digitális írástudásról akkor beszélhetünk, ha a tanulók és az aktív dolgozók felhasználói szinten képesek használni a korszerű információtechnológiai eszközöket, vagyis megszerzik a digitális írni-olvasni tudás alapkészségét, és tanulásuk, illetve munkájuk folyamán a hálózatba kötött számítógépet aktívan használják.

A védelmi küszöböt egy fejlett ország társadalma akkor lépheti át, ha a védelmi szféra (fegyveres erők és rendvédelmi szervek) digitális híradással, fejlett hálózatos információs rendszerekkel, precíziós információszerző képességgel és célravezetéssel, rendelkezik. Mindehhez a személyi állomány információs ismereteit és alkalmazási készségét fel kell emelni az előzőekben említett társadalmi küszöbszint követelményeihez. [1]

A fent jelzett küszöbszintek teljesítése esetén *„információs társadalomról akkor beszélhetünk, amikor az információs ágazat társadalmi, gazdasági súlya dominánssá válik, az információ beépül az egyének, szervezetek és intézmények mindennapjaiba, és a társadalmi kommunikáció nagy része a digitális csatornákon zajlik. Az információ mind szélesebb körű és könnyű elérése, fokozott termelése és átalakítása segíti a társadalom megújulását, mobilizációját, utat nyit az egyéni kezdeményezőkészségnek, vállalkozó kedvnek, szélesíti a civilizációs termékek, kulturális javak fogyasztását, továbbá globálissá teszi az emberi tudás megszerzését és megosztását, és soha nem látott mértékben sokszorozza meg azt.”* [6]

Az információs társadalmat információra alapozott társadalomnak tekinthetjük, mivel

- az információ adja a társadalom gazdasági szükségleteinek az alapját;
- a társadalom és a gazdaság maga is információs értékeket termel és felhasznál,
- az információ fontossága meghaladja az áru, az energia és a szolgáltatások szerepét.

Társadalmi rendszerét tekintve globális, szabadpiacú, parlamenti demokráciára épülő, magántőkére alapozott, ultrafejlett kapitalista gazdasági rendszer, amely szaktudásra, tudományra és hálózatos információs rendszerre épül. Az információs társadalom nem államforma, hanem a korábbinál magasabb technikai és tudás színvonalú társadalmi életforma, igen fejlett

életmód. Elvileg minden társadalmi formációban megvalósítható, de a diktatúrával össze nem egyeztethető.

E társadalom a fejlett tudomány legújabb eredményeire alapozott. Számítógép-hálózatilag integrált társadalom, amely statisztikailag alátámasztott, tudományos, pontos és gyors döntések társadalma. Az információs társadalomban teljes körűen informatizált, szélessávú, nagy átviteli sebességű, multimédiás, digitális jelátvitelű – elektronikus („e" jelzővel ellátott) – államvezetés, államigazgatás, önkormányzati közigazgatás, bíróságok, rendőrség, határőrség, vám- és pénzügyőrség, adóhivatalok, vagyis elektronizált intézményrendszerek működnek.

Technológiai értelemben multimédiás, digitális jelátvitelű, nagysebességű, szélessávú gerinchálózattal, fejlett távközlési és informatikai szolgáltatással rendelkező társadalom, ahol a közügyeket, vállalati és magánügyeket az információs közműhálózaton (információs infrastruktúrán) keresztül közvetlen (on-line) hozzáféréssel távolból lehet intézni. A fejlett infokommunikációs hálózatok révén az információk megszerzése, feldolgozása és a megalapozott döntések továbbítása terén a világ és az eddigi történelem leggyorsabb társadalma.

Az információs társadalom legfontosabb jellemzői közé tehát az alábbiakat sorolhatjuk:

- az információ, amely mint a technológiai fejlődés alapja az ipari társadalomban is fontos szerepet kapott, most már önálló értékké válik;
- az információs társadalom középpontjában az információ feldolgozó technológia áll;
- az "érvényes tudás" felezési ideje (az az idő, mialatt elavulttá válik) a fejlődés gyorsulása miatt jelentős mértékben csökken (éves, esetleg hónapos nagyságrendre);
- állandó követelménnyé válik az élethosszig tartó tanulás, mely a munkavállalótól egyre inkább az ismeretterületek közti mobilitást követeli meg, az egy szakma elsajátításának hagyományos követelménye helyett;
- az információ hatalmi tényezővé válik, a hatalom azé lesz, aki az információt termeli és elosztja. [2]

### 1.1.2. Információs társadalom Magyarországon

Magyarország is elkötelezett az információs társadalom építése mellett. Ennek megfelelően először 2001-ben alkotta meg a kormány a *Nemzeti Információs Társadalom Stratégiát (NITS)*. E stratégia hét részben – Infrastruktúra-fejlesztési Program, Gazdaságpolitikai Program, Kultúra Program, Oktatási Program, Társadalompolitikai Program, Elektronikus Kormányzati Program, Önkormányzati Program – határozta meg azt az akciótervet, amely alapján a magyar társadalom is az információs társadalom építésének útjára léphet. [7] Fontos megjegyezni azonban, hogy e stratégia nem tartalmazott olyan akciótervet, amely felmérte volna azokat a veszélyeket, amelyek az információs társadalom kiépítése – illetve kialakulása esetén –, annak működése során jelentkezhetnek.

Az első magyar információs társadalom stratégiát két év múlva – 2003-ban – újabb stratégia követte, amely a *Magyar Információs Társadalom Stratégia* (MITS) címet viselte. „*A Magyar Információs Társadalom Stratégia (MITS) megalkotásának első célja mindenki előtt világossá tenni, hogy Magyarország számára nincs más alternatíva, mint belépni az információs korba annyira intenzíven és innovatívan, amennyire erőnkből telik. Csakígy, utat nyitva az új gazdaság előtt valósítható meg a fenntartható fejlődés.”* [6] A MITS rámutat, hogy *„a tudásalapú gazdaság és információs társadalom létrehozásával a legfőbb közös cél az egyén és a közösség életminőségének és életkörülményének javítása…”*. [6]

A célok megvalósításához a MITS kijelölte azokat a stratégiai irányokat, amellyel Magyarország részese lehet annak az európai fejlődési folyamatnak, amelyet az Európai Unió tagállamainak vezetői 2000-ben Lisszabonban határoztak meg. A 2000 márciusában megrendezett lisszaboni csúcson Európa állam- és kormányfői azt az új célt állították az Európai Unió elé, hogy 2010-re a világ legversenyképesebb, dinamikus tudásalapú társadalmává váljon, több és jobb munkahellyel, valamint nagyobb szociális kohézióval. [8]

A MITS a fejlődés kulcsának az infokommunikációs technológiák alkalmazásának kiterjesztését tekintette. E technológiák széleskörű alkalmazása, termelőerővé válása biztosítja a

gazdaság modernizálását, a hatékonyság és versenyképesség növelését, és ezen keresztül egy új fejlettségi szint, az információs társadalom megvalósítását. A stratégia áttekintette rendszerbe foglalta és koordinálta az információs társadalom kiépítésével kapcsolatos feladatokat, ami által felgyorsítja és hatékonyabbá teszi a felzárkózást. A MITS a társadalmi és gazdasági folyamatokon és az információ társadalmasításán alapuló modellje segítségével rendszerezte az információs társadalom megvalósításának feladatait.

A korszerűsítés két alappillérét a folyamatok korszerűsítésében és a szolgáltatások modernizálásában határozta meg. Előbbi a folyamatok belső működésének korszerűsítését, informatikai alapokra való helyezését jelenti ("back office"), míg az utóbbi ugyanezen folyamatok funkcióinak tökéletesítését ("front office"), a felhasználók széles köre számára elérhető elektronikus szolgáltatások kialakítását jelenti. [6] [9]

A MITS hat beavatkozási területet nevesített, úgymint:

- tartalom és szolgáltatások;
- infrastruktúra;
- tudás és ismeret;
- jogi és társadalmi környezet;
- kutatás-fejlesztés és
- esélyegyenlőség. [6] (2. táblázat)

Ezek alapján mindegyik beavatkozási területhez főirányokat kapcsolt. (3. táblázat)

A MITS célkitűzései a tervek szerint ezen főirányokba besorolható kiemelt központi programként (KKP), ágazati kiemelt programként (ÁKP), vagy ágazati programként valósultak meg.

*A programok együttesen „lefedik" a stratégiát, együttes megvalósulásuk biztosítja a stratégiai célok elérését. Minden program kapcsolatban áll a stratégia valamely „területével", de csak eggyel. Az adott területet egy program részben vagy egészben, de a teljes stratégiát, csak a programok összessége fedi le.*

2. táblázat. A MITS beavatkozási területei [6]

| Beavatkozási terület | Folyamatok informatizálása | Elektronikus szolgáltatások |
|---|---|---|
| **Tartalom és szolgáltatások** | Üzleti folyamatok újraszervezése; a távmunka és a távoktatás elterjesztése; elektronikus munkamegosztás; elektronikus elszámolási és fizetési rendszer használata; a kultúra digitalizálása, az egészségügyi-, oktatási-, közigazgatási folyamatok átalakítása; stb. | Üzleti tartalomszolgáltatás, a tartalomipar fejlesztése; közcélú, közhasznú információk nyújtása; online (köz)szolgáltatások megvalósítása, az e-közigazgatás bevezetése; stb. |
| **Infrastruktúra** | Országos szélessávú hálózat kiépítése; közösségi szolgáltató központok; alapinformációk, alapszoftverek biztosítása stb. | Országos szélessávú hálózat kiépítése; közösségi hozzáférés; stb. |
| **Tudás és ismeret** | A döntéshozók, szakemberek, állampolgárok ismereteinek bővítése stb. | A digitális írástudás széleskörű elterjesztése; élethosszig tartó tanulás; az infokommunikációs technológiák ismeretterjesztése; az információ „tudássá” alakításának képességére való felkészítés stb. |
| **Jogi és társadalmi környezet** | Informatikai biztonság; hitelesség, megbízhatóság, minőség; információs és kommunikációs ajánlások, szabványok, szakmai kódexek kidolgozása | A felhasználó védelem megoldása; az informatikai biztonság növelése; az informatika társadalmi elfogadtatása; az információs alapjogok rögzítése az alkotmányban; stb. |
| **Kutatás és fejlesztés** | Infokommunikációs technológiai K+F; nemzetközi kutatási együttműködés; a kutatóhelyek és a vállalkozások kapcsolatának fejlesztése stb. | Technológiai K+F; az információs társadalom elméleti és gyakorlati kutatása; speciális információtechnológiai szakmai kutatások; stb. |
| **Esélyegyenlőség** | Szolgáltatók esélyének növelése; a régiók, kistérségek modernizálása, az információs és tudásbeli esélyegyenlőtlenség mérséklése stb. | Az informatikailag hátrányos helyzetek, közösségek, térségek kezelése a felhasználók oldalán stb. |

3. táblázat. A MITS fő irányai és programjai [6]

| Beavatkozási terület | Fő irány | Programok | |
|---|---|---|---|
| | | KKP | ÁKP |
| Tartalom | Gazdaság | e-munka; e-üzlet; e-közlekedés; e-agrárium; | e-közbeszerzés, KKV- IT fejlesztése; Foglalkoztatás; GVOP 4.1; GVOP 4.2 |
| | Közigazgatás | e-kormányzat; e-önkormányzat; | Közbiztonság; Jogbiztonság; Építés- és közlekedéshatóság; Adó; Elektronikus adatszolgáltatás; Közportál; GVOP 4.3; e-közigazgatás |
| | Kultúra | Nemzeti Digitális Adattár; | Új kulturális értékek; Új közvetítő technológiák; Jövő Háza |
| | Oktatás | e-oktatás; | e-learning; Oktatási anyagok; Oktatói, hallgatói kártya |
| | Egészség | e-egészség portál; | Távdiagnosztika, távgyógyászat; Szociális portál OEP, ONYF; e-recept, e-kórlap, e-konzílium; HEFOP 4.4; HEFOP 5. |
| | Környezetvédelem | e-környezetvédelem; | Természetvédelem; Víz; Meteorológia |
| Infrastruktúra | Széles sáv | Közháló; NIIF; | Elektronikus Kormányzati Gerinchálózat (EKG); Speciális ágazati alhálók; Civil alháló; GVOP 4.4 |
| | Hozzáférés | eMagyarország-Pont; | Svéd modell |
| | Infrastrukturális szolgáltatások | Közcélú, közhasznú információk „infrastruktúrája” | |
| Tudás és ismeret | Tudás, ismeret | Digitális írástudás; | HEFOP 3. |
| Jogi- és társadalmi környezet | Jogi- és társadalmi környezet | e-biztonság; e-demokrácia; | Elektronikus aláírás és bizalmas dokumentumkezelés; Fogyasztóvédelem; eTár |
| Kutatás és fejlesztés | IT K+F | IT K+F | |
| Esély-egyenlőség | Esélyegyenlőség | e-ernyő | IT mentor; Eszköz |

*Minden programnak jól meghatározható (monitorozható), önálló célja van, amelynek megvalósulása alapvetően az adott programtól függ. Ez a cél egyértelmű kapcsolatban van a stratégia megfelel a „területével", megvalósulása egyértelműen a stratégia megvalósulását szolgálja*. [6]

A MITS célkitűzései és a célkitűzéseket megvalósítani szándékozó programjai teljes mértékben illeszkedtek az Európai Unió stratégiájához, és stratégiai programjaihoz, az eEurope+ illetve az eEurope 2005 akciótervekhez. Ez lehetőséget adott Magyarország számára, hogy kapcsolódjon a közösségnek az eEurope-ot támogató programjaihoz (pl. IST, eContent, eSafety, IDA stb.), és lehetővé tette, hogy az EU strukturális alapját forrásként felhasználhassuk az információs társadalom építéséhez. [6] [9]

A MITS célkitűzései helyesek voltak, a főirányokba besorolható KKP-k és ÁKP-k közül több eredményesen megvalósult, azonban részben a források hiánya, illetve az időközben bekövetkezett gazdasági válság több program megvalósításának gátat szabott.

Magyarország kormánya 2010-ben megalkotta a sorrendben harmadik információs társadalom építésével összefüggő stratégiáját (tervét). A dokumentum a „Digitális megújulás cselekvési terv 2010-2014" címet viseli, alcímében – „Az infokommunikációs ágazat cselekvési terve a társadalom és a gazdaság megújulásáért" – pedig tükrözi az információs társadalom építésének, fejlesztésének elősegítése és felgyorsítása érdekében megteendő feladatokat.

A Cselekvési Terv elkészítésekor figyelembe vették az Európai Unió célkitűzéseit, infokommunikációs programjait, azok közül is az európai digitális menetrendet.

Az Európai Unió 2010 márciusában mutatta be az „Európa 2020" – Az intelligens, fenntartható és inkluzív növekedés stratégiáját (COM(2010) 2020), amelynek célja a válságból való kiút megtalálása és az EU gazdaságának felkészítése a következő évtized kihívásaira. E stratégia összhangban a céljaival hét kiemelt kezdeményezést tartalmaz. Ezek egyike az európai digitális menetrend (COM (2010) 245), amely az infokommunikációs technológiák alkalmazásának kulcsfontosságú szerepét határozza meg Európa 2020-ra kitűzött céljainak sikeres megvalósításában.

Az európai digitális menetrend hét olyan kulcsfontosságú intézkedési területet nevesít amelyek az EU-ban jelenlévő problémakörök megoldására irányulnak. Ezek az alábbiak:

- élénk egységes digitális piac;
- interoperabilitás és közös szabványok;
- bizalom és biztonság;
- nagy sebességű és szupergyors internet-hozzáférés;
- kutatás és innováció;
- a digitális jártasság, a digitális készségek és a digitális inklúzió javítása;
- az infokommunikációs technológia előnyei az uniós társadalom számára.

A felsorolt intézkedések a jelenlegi problémákkal foglalkoznak, azokra nyújtanak lehetséges megoldásokat. Ugyanakkor a Bizottság közleménye hangsúlyozza, hogy a tapasztalatok és a gyors technológiai és társadalmi változások fényében a menetrend továbbalakítása várható. [15]

A Digitális Menetrend fő teljesítménycéljai az alábbiakban foglalhatók össze:

- 2013-ig alapszintű szélessávú internet lefedettség az EU teljes lakossága (100 %) számára;
- 2020-ig legalább 30 Mbps sávszélességű internetkapcsolat az EU teljes lakossága (100 %) számára;
- 2020-ig az európai háztartások 50 %-ában 100 Mbps-nál nagyobb sávszélességű internetkapcsolat biztosítása;
- 2015-ben a lakosság 50 %-a használja az internetet vásárlásra, 20 %-a pedig éljen a határokon átnyúló internetes vásárlás lehetőségével;
- 2015-ben a KKV-k 33 %-a végezzen internetes beszerzést, illetve értékesítést
- 2015-re a belföldi és roaming-tarifák közti különbség megszűntetése;
- 2015-ig a rendszeres internethasználók aránya 60 %-ról 75 %-ra, a hátrányos helyzetű felhasználók körében pedig 41 %-ról 60 %-ra növelése;

- 2015-re felére (15 %-ra) csökkentése azoknak arányát, akik még soha nem interneteztek;
- 2015-re a lakosság 50 %-a vegye igénybe az e-kormányzati szolgáltatásokat, és ezek több mint fele használja azokat nyomtatványok kitöltésére és visszaküldésére is;
- 2015-re valamennyi, a tagállamok által 2011-ig összeállítandó közös jegyzékben szereplő, határokon átnyúló alapvető közszolgáltatásnak online elérhetőnek kell lennie.
- az infokommunikációs technológia területén végzett K+F beruházások megduplázása (kb 11 milliárd EUR-ra növelése). [15]

A Digitális Megújulás Cselekvési Terv célcsoport szerinti bontásban tartalmazza a megvalósítandó akciókat.

A terv szándéka szerint, az elkövetkező években az egyes intézkedések különböző mértékben, az egymásra épülés és a megvalósítás szempontjait is figyelembe véve kapnak hangsúlyt.

A terv szerint 2011-ben az intézkedések a vállalkozások versenyképességének fokozására, az innováció, oktatás és képzés elősegítésére irányultak.

A cselekvési terv 2012-es fő célja: oktatási és képzési programokkal társuló közösségi programokkal a lakosság és a vállalkozások digitális készségének fejlesztése.

2013-ra válik elérhetővé országos szinten a lakosság és a vállalkozások információs írástudását elmélyítő programok beindítása.

1. Középpontban az ember – fő cél: az állampolgár esélyegyenlőségének, életminőségének javítása, versenyképességének fokozása, a társadalmi jólét növelése
2. Gyarapodó vállalkozások a munkahelyteremtés szolgálatában – fő cél: a vállalkozások alkalmazkodóképességének, versenyképességének növelése
3. Hatékonyan és biztonságosan működő, szolgáltató állam – fő cél: az állam egyszerűbb, átláthatóbb, biztonságosabb, olcsóbb, hatékonyabb működése
4. Fejlett és biztonságos infrastruktúra mindenkinek - fő cél: korszerű és biztonságos többfunkciójú infrastruktúra, amely a fentiek megvalósításának nélkülözhetetlen alapja [16]

Mindezek mellett a kormányzati e-közigazgatási koncepció és az informatikai fejlesztések eredményeként konkrét, központi programok mentén szervezetten folyik majd a kormányzati informatika átalakítása és fejlesztése. [16]

A Digitális megújulás - Magyarország középtávú infokommunikációs cselekvési terve négy intézkedési főirány mentén elemzi a jelenlegi helyzetet és fogalmazza meg a teendőket:

A tervben mind a négy kitörési pontban részletezve vannak az adott főirányhoz kapcsolódó fejlesztési irányok, amelyekhez hozzá rendeli a megteendő intézkedéseket és a kapcsolódó akciókat.

Így például a kritikus információs infrastruktúra védelemmel kapcsolatban két területen fogalmaz meg intézkedési tervet és hozzájuk kapcsolódó akciókat:

1. A hatékonyan és biztonságosan működő szolgáltató állam kitörési ponthoz rendelt közigazgatás információs rendszereinek biztonsága terén. Kapcsolódó akciók:
    - adatszabványok, információbiztonsági követelmények kompatibilitásának megteremtése az egészségügyi informatikában;
    - IT-biztonsági jogszabályok átdolgozása;
    - magas színvonalú informatikai biztonsági megoldások bevezetésének támogatása a kormányzat részére egységes szabályozás alapján.
2. Fejlett és biztonságos infrastruktúra mindenkinek kitörési ponthoz rendelt kritikus információs infrastruktúra védelme területén. Kapcsolódó akciók:
    - a kritikus információs infrastruktúra védelem vezetésének és a védelmi stratégia kidolgozásának kormányzati kézbe vétele, a vonatkozó EU irányelvnek megfelelően;
    - az állam vezetésével, kidolgozott módszertan alapján a nemzeti kritikus infrastruktúra, valamint az európai kritikus infrastruktúra elemek kijelölése, illetve a kijelölések folyamatos felülvizsgálata;

- a kritikus információs infrastruktúra védelmi szabályok és feladatok állami kijelölése;
- összkormányzati szinten a kritikus információs infrastruktúrák védelme területén a tudatosság növelés és az oktatás, továbbképzés. [16]

Az információs társadalom stratégiákon kívül Magyarország Nemzeti Biztonsági Stratégiája is kiemelt helyen kezeli az információs társadalmat és annak zavartalan kialakulását, működését.

*"Kiberbiztonság. Az állam és a társadalom működése – a gazdaság, a közigazgatás, vagy a védelmi szféra mellett számos más területen is – mind meghatározóbb módon a számítástechnikára épül. Egyre sürgetőbb és összetettebb kihívásokkal kell számolnunk az informatikai- és telekommunikációs hálózatok, valamint a kapcsolódó kritikus infrastruktúra fizikai és virtuális terében. Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem-állami – akár terrorista – csoportok arra használhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését. E támadások eredetét és motivációját gyakran nehéz felderíteni. A kibertérben világszerte növekvő mértékben jelentkező nemzetbiztonsági, honvédelmi, bűnüldözési és katasztrófavédelmi vonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelem feladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására Magyarországnak is készen kell állnia.*

*a) Elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális fenyegetések és kockázatok rendszeres felmérése és priorizálása, a kormányzati koordináció erősítése, a társadalmi tudatosság fokozása, valamint a nemzetközi együttműködési lehetőségek kiaknázása.*

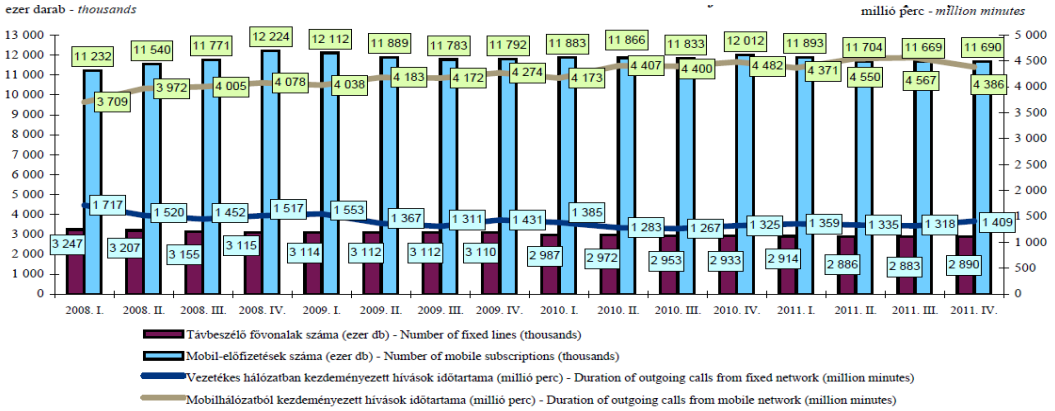
*b) A nemzeti kritikus információs infrastruktúra védelmének erősítése mellett szövetségeseinkkel és EU-partnereinkkel együtt arra törekszünk, hogy az információs rendszerek biztonsága erősödjön, valamint részt vegyünk a megfelelő szintű kibervédelem kialakításában."* [17]

Az információs társadalom „intézményesülésében” jelentős mértékben kivették részüket a különböző civil szervezetek, bár számuk nem túl magas, aktivitásuk azonban meghatározó. Ugyanakkor azt is látni kell, hogy a magyar információs társadalom fejlesztése a politika oldaláról nem élvez prioritást. Ezért minden olyan kezdeményezés, amely ezen az úton való előrehaladást segíti, támogatni kell.

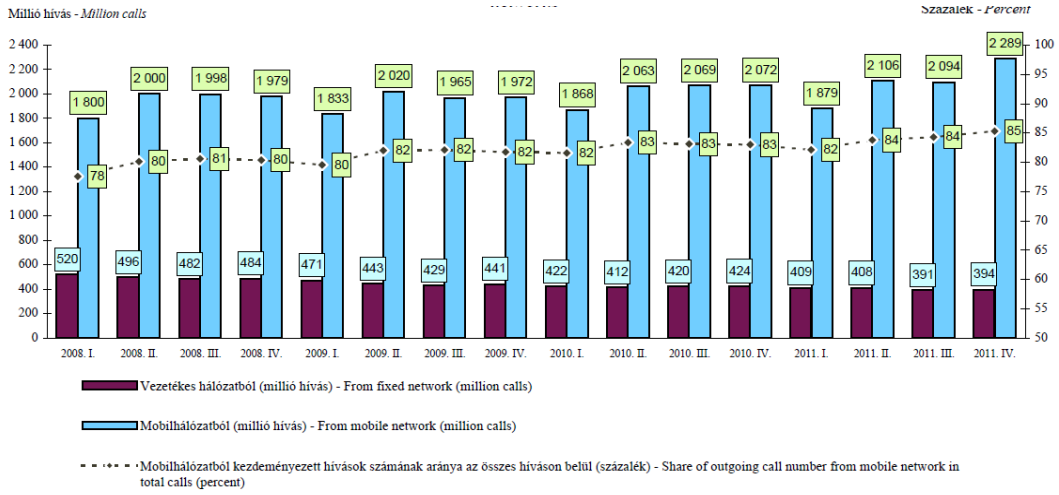
Az elmúlt több, mint tíz év információs társadalmának építési tendenciáját a hazai távközlési piac monopóliuma, majd liberalizációja határozta meg. A mobilkommunikáció területén igen éles verseny alakult ki az ezredfordulón, amikor háromszereplőssé vált a hazai piac. 2001 közepére a mobiltelefon előfizetések száma először haladta meg a vezetékes fővonalak számát.

A magyarországi internetpiac elmúlt 10 évét az előfizetések számának növekedése és az ADSL illetve más szélessávú technológiák elterjedése jellemezte. 2005-ben a szélessávú internet hozzáférések száma már meghaladta a modemes kapcsolatokét, mára pedig már jelentős többségben vannak a nagy sávszélességű kapcsolatok. [11]

Mindeközben az infokommunikációs technológia felhasználása örvendetesen növekszik hazánkban is. Mind többen ismerik fel a távközlés és mindenekelőtt az internet használatának szükségességét. A KSH negyedévente megjelenő gyorsjelentése szemléletesen mutatja az infokommunikációs technológia elterjedésének mértékét. A 2011. IV. negyedévi gyorsjelentés szerint a mobiltelefon piac telítődik, amit jól szemléltet, hogy a mobiltelefon-előfizetések száma egy év alatt 322 ezerrel csökkent: az állomány 2011. december végén kevesebb, mint 11,7 millió volt. A vezetékes telefonálás tekintetében az egy évvel korábbinál 43 ezerrel kevesebb, 2,9 millió vezetékes fővonal volt üzemben. A vezetékes vonalakról indított hívások száma 7%-kal csökkent, míg a hívások időtartama 6%-kal nőtt 2010 negyedik negyedévéhez képest. Az összes telefonbeszélgetésre fordított idő több mint háromnegyedét mobilkészülékekről indított hívások tették ki. (1.; 2. ábra)



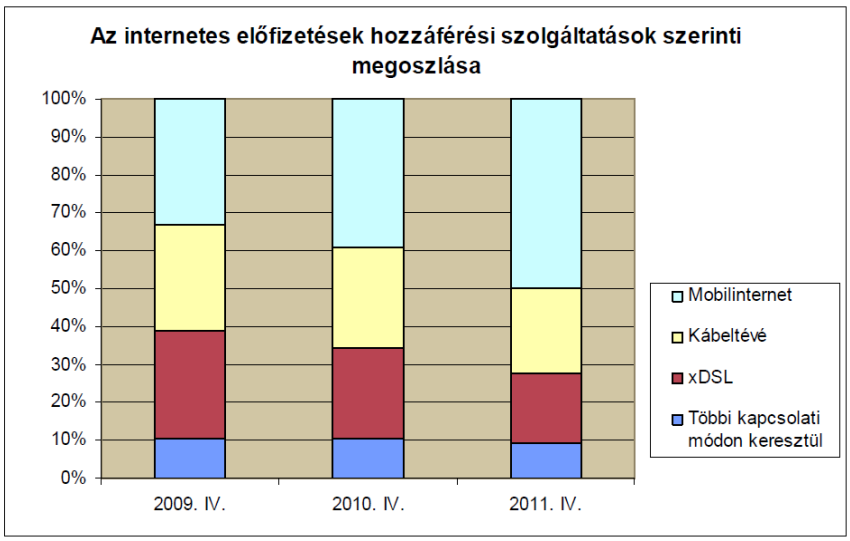

1. ábra. A vezetékes- és mobiltelefonálás fontosabb adatai (2011. IV. negyedév) [18]



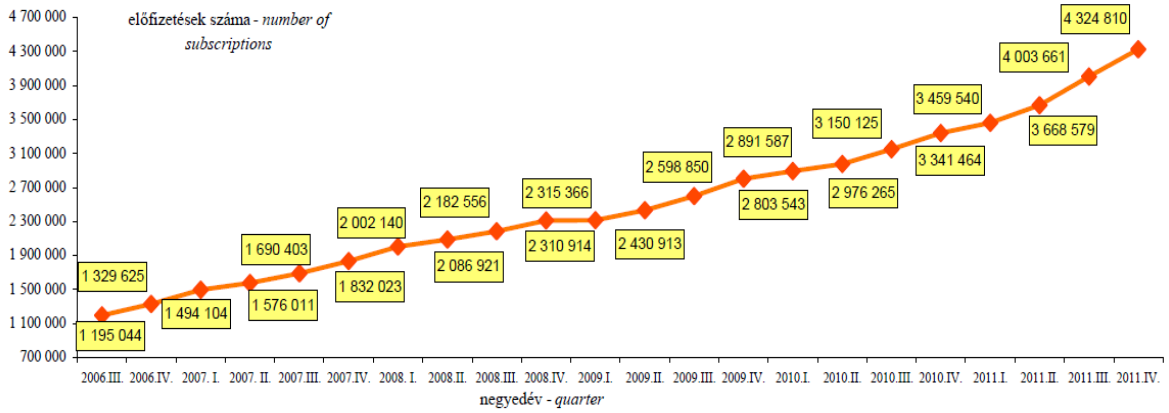

2. ábra. A vezetékes- és mobil hívások száma (2011. IV. negyedév) [18]

Az internetpiac bővülése folytatódott, az internet-előfizetések száma 2011 december végén meghaladta a 4,3 milliót, amely több mint negyedével meghaladja a 2010 azonos időpontjában mért szintet. Az összes internet-előfizetés 50%-a a mobilkategóriába tartozott, részaránya egy év alatt közel 11 %-al lett nagyobb. A vezetékes internet két legjelentősebb típusa közül éves szinten a kábelhálózatos előfizetések 8%-kal gyarapodtak, míg az xDSL-előfizetések

csoportja ennél kisebb mértékben növekedett. A szélessávú (kábeltévés és xDSL-) internetre történő előfizetések száma egy év alatt 5%-kal nőtt. (3.; 4. ábra) [18]




3. ábra. Internet előfizetések hozzáférési szolgáltatások szerinti megoszlása (2011. IV. negyedév) [18]




4. ábra. Internet-előfizetések számának változása (2011. IV. negyedév) [18]

Az eddigiekből világosan következik tehát, hogy maga az információs társadalom kialakulása és működése lehet az egyetlen út az Európai Unió, egy-egy európai régió, illetve Magyarország számára is a gazdasági versenyképességének fejlesztésében vagy megőrzésében.

### 1.1.3. Az információs társadalom információtechnológiai feltételei

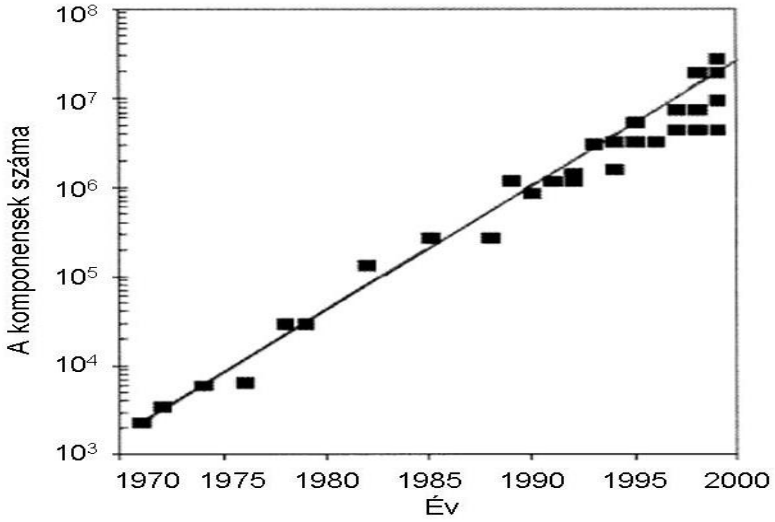
#### Gyártástechnológiai fejlődés

Az információs társadalom fejlődésének motorját az alap és alkalmazott tudományok terén folytatott kutatások képezik, amelyek eredményeit a gyártástechnológiában igyekeznek minél gyorsabban hasznosítani. A fejlettebb gyártástechnológiával nagyobb tudástartalmú termékeket, szolgáltatásokat és árukat lehet előállítani, amelyek versenyképessége és haszontermelő képessége jelentős mértékben javul. A nagyhatalmak közötti gazdasági és katonai verseny már eddig is – a jövőben pedig még inkább – a fejlett műszaki színvonalat képviselő gyártástechnológiák fejlettségi színvonalán dől el.

Az integrált áramköri technológia feltalálásától kezdve rohamosan ütemben fejlődött, és kialakult a mikroelektronikai ipar. Egyre több félvezető elem került az integrált áramkörökbe, egyre bonyolultabb áramköri és rendszertechnikai funkciókat lehetett egyetlen integrált eszközzel megvalósítani.

A fejlődés ütemét jól szemlélteti a Gordon Moore-ról (az Intel társalapítójáról) elnevezett törvény, amely megfigyelésen alapul és teljesen ad hoc keletkezett. E tapasztalati törvény kimondja, hogy egy integrált áramköri lapkára elhelyezett félvezető komponensek száma 18 havonta megduplázódik, miközben az áramkör mérete körülbelül a felére csökken. Ugyanilyen sebességgel csökken az egy komponensre eső költség is. (5. ábra)

Bár a Moore-törvény először egy megfigyelést és előrejelzést írt le, minél szélesebb körben lett ismert, annál inkább teljesítendő célként jelent meg az ipar számára. A Moore-törvény következményei az iparban jelentősen befolyásolják az alkatrészgyártókat. Egy termék (mint például egy CPU vagy egy merevlemez) kifejlesztésének átlagos ideje 2 és 5 év közé tehető.



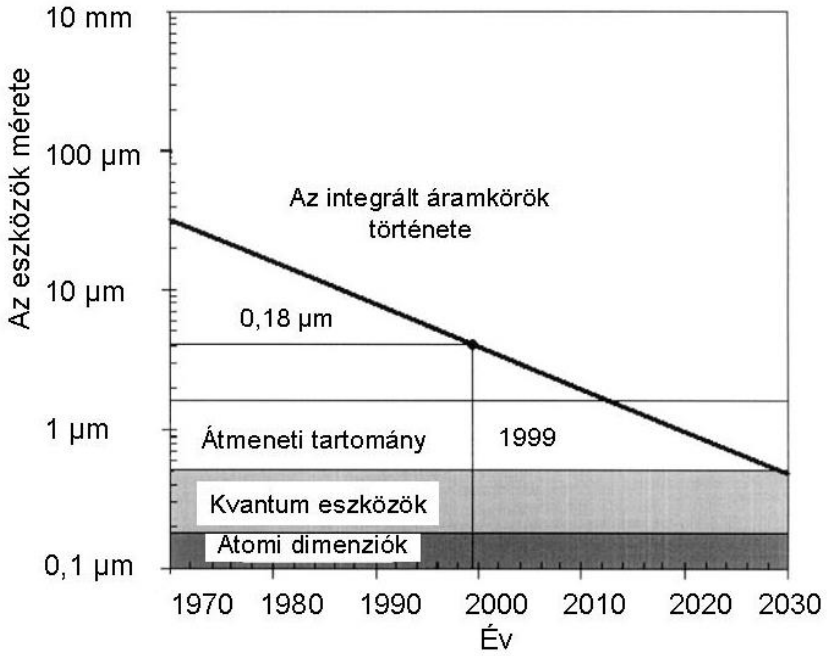

5. ábra. Moore-törvény: az egy lapkán lévő áramköri komponensek száma az idő függvényében [10]

Ennek következményeként a gyártók hatalmas nyomásnak vannak kitéve a határidőkkel kapcsolatban: egy főbb terméknél pár hét késés jelentheti a különbséget siker és kudarc vagy esetleg a csőd között. A „18 hónaponkénti megkétszereződésként" meghatározott Moore-törvény rendkívüli technológiai fejlődésre utal az elmúlt években. Rövidebb időskálára vetítve, a törvény heti 1%-os ipari növekedést jelent. A processzorpiacon szereplő gyártók számára ez azt jelenti, hogy a két vagy három hónapot késő, ezáltal 10-15%-kal lassabb, nagyobb méretű vagy kisebb tárolókapacitású termék általában eladhatatlan.

2004 utolsó negyedévében a processzorok 130 és 90 nm-es technológiával készültek. 2005 végen bejelentették a 65 nm-es gyártósorokat. Egy évtizede az integrált áramkörök 500 nm-es csíkszélességgel készültek. Egyes vállalatok azon dolgoznak, hogy a nanotechnológia segítségével képesek legyenek 45 nm-es vagy még kisebb csíkszélességű integrált áramkörök előállítására. [11]

A szilícium alapú technológia még nem érte el az elvi korlátait, de az évtized végére belép az úgynevezett átmeneti tartományba, amitől kezdve a hagyományos szilícium alapú techno-

lógiák mellett elkerülhetetlenné válik új eszköz(ök) megjelenése a gyakorlatban. A ma látható trendek alapján látható, hogy a szilícium alapú technológiák Moore-törvény szerinti fejlődése egyszer véget ér. Addig is azonban új paradigmák várhatók a szilícium alapú technológia területén is. A trendek arra utalnak, hogy tovább folytatódik a félvezető eszközök miniatürizálása a több milliárd eszközt tartalmazó és a több gigabit/s sebességű integrált áramkörök felé. Az új technológiáknak köszönhetően a közeljövőben elérhetőnek látszik a 2 nm-es szigetelővastagság, a 10 nm-es csatornaszélesség és a 20 nm-es csatornahossz. (6. ábra) [10]




6. ábra. Az integrált áramköri komponensek elemi méreteinek csökkenése az idő függvényében [10]

A fentiek alapján tehát megállapítható, hogy a mikroelektronikai alkatrész–tömörítési és kicsinyítési gyártástechnológia világa a mikrométeres tartományból, a nanométeres atomi méretek világába ment át.

A Moore- törvény mellett két másik tapasztalati törvény is jól jellemzi az infokommunikációs technológia fejlődési trendjét. Az egyik a Gilder-törvény a sávszélességről, ami kimondja, hogy a kommunikációs rendszerek teljes sávszélessége évente megháromszorozódik. A másik a Ruettgers-törvény a tárolási kapacitásról, amely szerint a memórialapkák tárolási kapacitása évente megkétszereződik. Ezen törvények érvényessége is már hosszabb ideje fennáll s az várhatóan fenn is marad az elkövetkező 10 évben.

Bár már többször megjósolták, hogy valamelyik tapasztalati törvény előbb-utóbb érvényét veszti, azonban ez még nem következett be. A következő tíz évben mind a sávszélesség, mind a tárkapacitás és a műveleti sebesség várhatóan a tapasztalati törvények szerinti exponenciális ütemben növekszik tovább. E fejlődésüknek kettős hatása lesz:

- a jövőben egyre inkább azzal számolhatunk, hogy a sávszélesség és a tárkapacitás szinte korlátlanul rendelkezésére áll majd a felhasználóknak;
- a műveleti sebesség fokozódásával a számítási teljesítmény átlépi – részben már át is lépte – azt a határt, amely felett lehetővé lesz csomagkapcsolt valósidejű jelfolyamok továbbítására is.

A két trendből együttesen következik, hogy a közel százharminc éves vonalkapcsolt technológiát a legtöbb hálózatban lavinaszerűen felváltja a csomagkapcsolás és ennek jelentős hatása lesz a szolgáltatók üzleti modelljeire is.

A gyártástechnológiában a mikrotechnológiát fokozatosan felváltja a nanotechológia. A nanoinformatika különböző módokon valósul meg: elektromos-, mágneses-, kémiai- biológiai-, esetleg kvantumos jelenségek felhasználásával jelentősen nagyobb sebességek, kisebb méretek és alacsonyabb költségek elérésével. [12]

Az atomi méretek elérésének lehetősége az elektronikai alkatrészek előállítása terén újabb gyártástechnológiai szintáttörés eredményez, és hatására a számítástechnikai iparban újabb technológiai korszak kezdődik. Az ilyen rendkívül kisméretű, ugyanakkor igen nagy teljesítményű nanoelektronikai eszközök előállítására képes nanoipari gyártástechnológiával rendel-

kező szuperhatalmak, az információs technológia területén abszolút csúcstechnikai és gyártástechnológiai fölényben, ún. technológiai felsőbbségben lesznek más ipari hatalmakkal szemben. Ennek hatását a globális és nemzeti biztonságra nem kell külön hangsúlyozni. [1]

### Infokommunikációs technológiai trendek

Az adatok, információk megszerzését, előállítását, tárolását, feldolgozását, továbbítását biztosító különböző elektronikai, informatikai eszközök és rendszerek közötti legátfogóbb, legmeghatározóbb jelenség ezen területek konvergenciája, amit infokommunikációs konvergenciának nevezzük. Az infokommunikációs konvergencia szerepe döntő az információs társadalom kiépítésében és fejlesztésében, mivel nem szűkül le a technológia szintjére, hanem mind szélesebb köröket von hatása alá, társadalmi jelenséggé válik. Ezt a folyamatot a digitális technológia hatalmas léptékű fejlődése váltotta ki. Az említett eszközök és rendszerek közös technológiai alapja kialakult.

A digitális technológia elterjedésével megkezdődött a számítógép, a vezetékes és vezeték nélküli távközlési eszközök, továbbá az elektronikus média műszaki közeledése, technikai konvergenciája, majd közös termékben való összeolvadása. A műszaki fejlesztések lehetővé tették az áttérést a multimédiás jeltovábbításra a kommunikációs csatornán. Ezáltal megvalósul a beszédhang, zene, szöveg, rajz, álló– és mozgókép egy csatornán történő továbbítása. Lehetővé vált korábban elkülönült információ kezelésmódok összekapcsolása és kombinálása, infokommunikációs alkalmazások és ezekre épülő vállalkozások létrejötte. Ilyen infokommunikációs alkalmazások a különféle audiovizuális/multimédia szolgáltatások, internet-alkalmazások, elektronikus tartalomszolgáltatások és tulajdonképpen az ún. információs társadalmi szolgáltatások. [13]

A világméretű infokommunikációs hálózatok megjelenése – Internet-I és Internet-II vagy Grid, az elektronikus levelezés (E-mail, Fax, SMS, MMS) szolgáltatásokkal – megteremtették a lehetőséget az új típusú globális gazdaság, az elektronikus tőzsdék, az elektronikus pénzpiac, az elektronikus kereskedelem és más, igen fejlett társadalmi tevékenységek világméretű

kialakítására. Ez a műszaki és technológiai lehetőség képezi, a gazdasági globalizmus alapját. [1]

Az infokommunikációs rendszerek konvergenciáján belül különbséget teszünk:

- szolgáltatások konvergenciája;
- hálózatok konvergenciája és
- készülékek konvergenciája között.

Szolgáltatások konvergenciájakor egy infokommunikációs rendszer szolgáltatásában különféle információs tartalmak jelennek meg (pl. a multimédia-termékek).

A hálózatok konvergenciája azonos technológiai alapokat, szolgáltatások együttes kiszolgálását lehetővé tevő kapacitásokat és hálózati funkciókat jelenti. E területen a teljes konvergencia megvalósítását lehetővé tévő szélessávú internethálózatok állnak.

A készülékek konvergenciája a korábban külön álló készülékek funkcióinak egybeépülését jelenti (pl.: a PDA-kba beépülő mobiltelefon, vezeték nélküli internet, navigáció). [13]

Az információs társadalom működésének alapja az infokommunikációs rendszereken alapuló információs infrastruktúrák egymásba kapcsolódó komplex rendszere. A rendszerek komplexitását bizonyítja, hogy a távközlési, informatikai rendszerek, a hozzájuk kapcsolódó távérzékelő, távfelügyeleti, navigációs rendszerekkel, szenzorhálózatokkal és más elektronikai rendszerekkel egységes rendszert képeznek, ami által képesek teljes hatékonysággal működni. Ez azt jelenti, hogy az infokommunikációs rendszerek jóval többet jelentenek, mint csak az informatikai és távközlési rendszerek konvergenciájából kialakuló rendszerek. Ebbe beletartoznak mindazon rendszerek is, melyek az érzékelés, irányítás, vezérlés funkcióit látják el. Így pl. e kategóriába sorolhatók azok a repülőtéri leszállító és irányító rendszerek is, amelyek a távközlési rendszereken és a számítógép-hálózatokon keresztül csatlakoznak más rendszerekhez.

Ennek megfelelően igen korszerű, igen fejlett információtechnológián alapuló infokommunikációs rendszerekkel látják el a különböző kormányzati, gazdálkodó, védelmi szerveze-

teket, intézményeket, illetve a vállalatokat. Amennyiben e szervek ezeket az információs rendszereket megfelelően tudják működtetni, ki tudják használni a bennük rejlő lehetőségeket, és ugyanakkor a biztonságos működtetésüket is meg tudják teremteni, akkor ez egy igen komoly erősokszorozó, hatásnövelő képességjavító és integráló hatású tényezővé válik.

Az infokommunikáció legtöbb területén létrejönnek olyan alkalmazások, amelyekkel a korlátlan sávszélességet kihasználva a távoli tároló- és számítási teljesítmény tetszőleges időben elérhető. Kialakulnak az elosztott feldolgozó rendszerek, amelyekben a személyes adatokat is távoli szervereken tárolják.

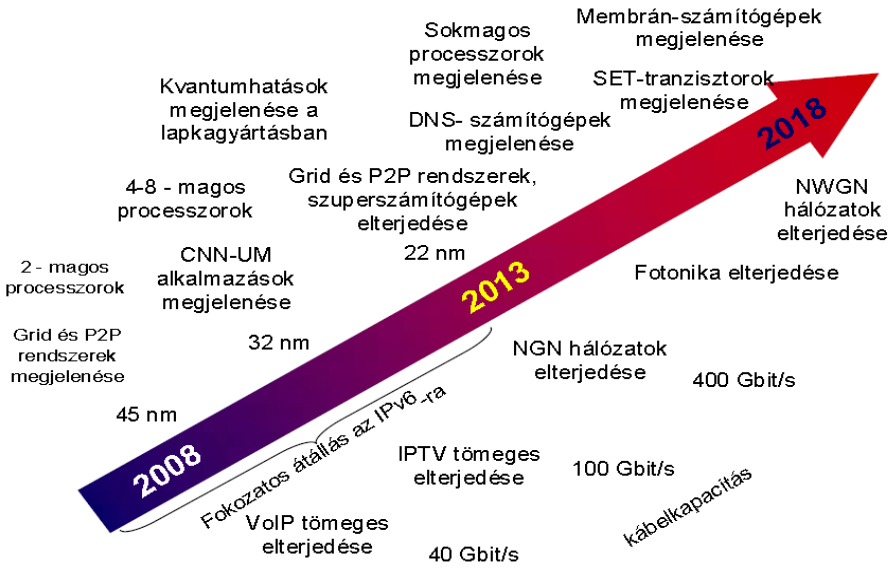
A hálózati technológia fejlődése, a sávszélesség növekedése lehetővé teszi, hogy gyakorlatilag minden számítógép mindig kapcsolatban lehessen a világhálóval, azaz a világ összes többi számítógépével. Ehhez szükség van a nagyobb címzési lehetőségeket és fokozott átviteli biztonságot megvalósító új internet protokoll (IPv6[2]) elterjedésére is. A teljes összekapcsoltság következtében:

- a felhasználók a világon tárolt bármilyen információhoz hozzájuthatnak, és bárkivel kapcsolatba léphetnek;
- az informatikai eszközök felhasználhatják egymás erőforrásait, így egy feladat megoldásában több – akár a világ különböző pontjain elhelyezkedő – számítógép vehet részt.
- Az infokommunikációs technológiai fejlődésére az alábbiak a jellemzőek:
- az infokommunikációs eszközök teljesítmény paraméterei (műveleti sebesség, tároló kapacitás, memória kapacitás, sávszélesség stb.) tovább növekednek;
- az eszközök összekapcsoltsága teljessé válik, ezáltal az információhoz való hozzáférés még könnyebbé és még teljesebb körűvé válik;
- információ-feldolgozó és adatátviteli kapacitások megjelennek a környezet tárgyaiban is, sokszínűvé válnak az ember-gép kapcsolat eszközei;

[2] Az IPv6 (Internet Protocol version 6; 6-os verziószámú Internet Protokoll) egy csomagkapcsolt hálózati rétegbeli protokoll, melyet az IPv4 továbbfejlesztésére találtak ki. Az IPv4 32 bites címzése helyett az IPv6 128 bitet használ címzésre.

- az infokommunikációs rendszerek egyre intelligensebbé válnak, aminek következtében a "gépi gondolkodásmód" egyre jobban közelít az emberihez, mind az információ feldolgozásban, mind az ember-gép kommunikációban;
- a rendszerek működésében egyre nagyobb szerep jut a szolgáltatások különböző fajtáinak;
- az infokommunikációs eszközök általános összekapcsoltsága révén fokozott mértékben együttműködnek egymással az infokommunikációs rendszerek felhasználói is;
- az infokommunikációs rendszerek működésének minden szempontból való biztonságossága egyre növekvő kihívást jelent. [14]

Összességében az infokommunikációs technológia fejlődésének fontosabb állomásait a 7. ábra szemlélteti.




7. ábra. Az infokommunikációs technológiai fejlődés várható tendenciája [12]

## *1.2. Az információs társadalom infrastruktúrái*

Az információs társadalom kiépítése, majd zavartalan működése azonban feltételez számos nélkülözhetetlen rendszert és eszközt – *infrastruktúrát* –, amelyek a társadalom és a gazdasági élet funkcióit támogatják, vagy ezeken keresztül valósulnak meg a különböző – a társadalom működése szempontjából elengedhetetlen – funkciók, illetve feladatok.

Ennek megfelelően először azt kell tisztáznunk, mit is értünk infrastruktúra alatt.

Amennyiben a szó eredeti jelentését akarjuk tisztázni, akkor először érdemes a Magyar Értelmező Kéziszótár (MÉK) meghatározását megvizsgálni. A MÉK szerint az infrastruktúra olyan angolszász eredetű szó, amely jelentése „*a társadalmi, gazdasági tevékenység zavartalanságát biztosító alapvető létesítmények, szervezetek (pl. lakások, közművek, a kereskedelem, a távközlés, az oktatás, az egészségügy stb.) rendszere.*" [19]

Egy másik meghatározás szerint az infrastruktúra nem más, mint „*egy adott rendszer (termelő vagy elosztó, szolgáltató rendszer, tudományos, állami, magán, nemzeti vagy nemzetközi szervezet, ország, város, vagy régió stb.) rendeltetésszerű működéséhez feltétlenül szükséges intézetek, intézmények, felszerelések és berendezések és a működtetést ellátó személyzet szabályszerűen működő összessége. Az infrastruktúra tehát a fizikai építményekből és berendezésekből és azokat szakszerűen működtetni tudó szakszemélyzetből áll.*" [1]

1997-ben egy, az akkori amerikai elnök, Bill Clinton utasítására létrehozott bizottság a következőképpen definiálta az infrastruktúra fogalmát (természetesen az Egyesült Államok vonatkozásában): „*Az infrastruktúrák olyan egymástól függő hálózatok és rendszerek összessége, amelyek meghatározott ipari létesítményeket, intézményeket (beleértve a szakembereket és eljárásokat), illetve elosztó képességeket tartalmaznak. Mindezek biztosítják a termékek megbízható áramlását az Egyesült Államok védelmi és gazdasági biztonságának fenntartása, valamint a minden szinten zavartalan kormányzati munka és a társadalom egésze érdekében."* [21]

Amennyiben az információs társadalom szempontjából vizsgáljuk az infrastruktúrák kérdését, akkor az infrastruktúra fogalmán belül általános feladatú és információs rendeltetésű infrastruktúrát különböztethetünk meg.

Az általános feladatú infrastruktúra fogalma alatt olyan állandóhelyű vagy mobil építmények, eszközök, rendszerek, hálózatok, az általuk nyújtott szolgáltatások, és működési feltételek összességét kell érteni, amelyek valamilyen társadalmi, gazdasági vagy akár katonai funkciók és rendszerek feladatorientált, zavartalan és hatékony működését teszik lehetővé. [1] Ilyen társadalmi funkciók lehetnek (természetesen a teljesség igénye nélkül, hiszen a társadalom különböző, szerteágazó területei számos egyéb funkcióval is bírhatnak):

- közigazgatási;
- szállítási;
- ellátási;
- hírközlési;
- vezetési;
- védelmi (ország védelem, rendvédelem, katasztrófavédelem, polgári védelem);
- oktatási;
- egészségügyi;
- tájékoztatási.

Az információs rendeltetésű infrastruktúrák olyan állandóhelyű vagy mobil létesítményeket, eszközöket, rendszereket, hálózatokat, illetve az általuk nyújtott szolgáltatásokat foglalnak magukba, melyek az információs társadalom működéséhez szükséges információk megszerzését, előállítását, tárolását, szállítását és felhasználását teszik lehetővé.

Mindezekből kitűnik, hogy az egyes infrastruktúrák egymást átfedő területeket is érintenek, illetve például az információs rendeltetésű infrastruktúrák – vagy azok egyes rész-elemei – sok esetben megtalálhatóak az általános rendeltetésű infrastruktúrákban.

Amennyiben tovább elemezzük az információs rendeltetésű infrastruktúrákat (információs infrastruktúrákat), megállapíthatjuk, hogy azok *„az információs társadalom működéséhez szükséges információk előállítására, szállítására és felhasználására különböző rendeltetésű, funkciójú és típusú infrastruktúrarendszerek, hálózatok állnak rendelkezésre. Ezek összessége képezi az információs társadalom komplex információs infrastruktúráját."* [22]

A felhasználók számára az információs infrastruktúra értéke – a fizikai összetevők mellett – jelentősen függ más elemektől is. Ezek az alábbiak [1]:

- az információ maga, mely formátumát tekintve lehet tudományos, gazdasági, politikai, védelmi és kulturális stb. felhasználású videó, kép, hang, szöveges információ, és amelyek hatalmas mennyiségben találhatók meg a különböző kormányzati, közigazgatási szerveknél, illetve minden nap egyre értékesebb információk termelődnek a laboratóriumokban, kutatóhelyeken és más intézményekben;
- szoftverek és alkalmazások, melyek a felhasználók számára lehetővé teszik az információs infrastruktúra szolgáltatásai által nyújtott információtömeg rendszerezését, megváltoztatását, tárolását stb.;
- hálózati szabványok (protokollok) és átviteli kódok, melyek alapján a különböző eszközök hálózatban működhetnek, és biztosítják a személyek, információhordozók, valamint a hálózatok biztonságát;
- az emberek – tágabb értelemben a humán szféra – melyek létrehozzák az információkat, kidolgozzák az alkalmazásokat, kutatják, fejlesztik és gyártják a különböző információs rendszereket, eszközöket, képezik saját magukat és másokat.

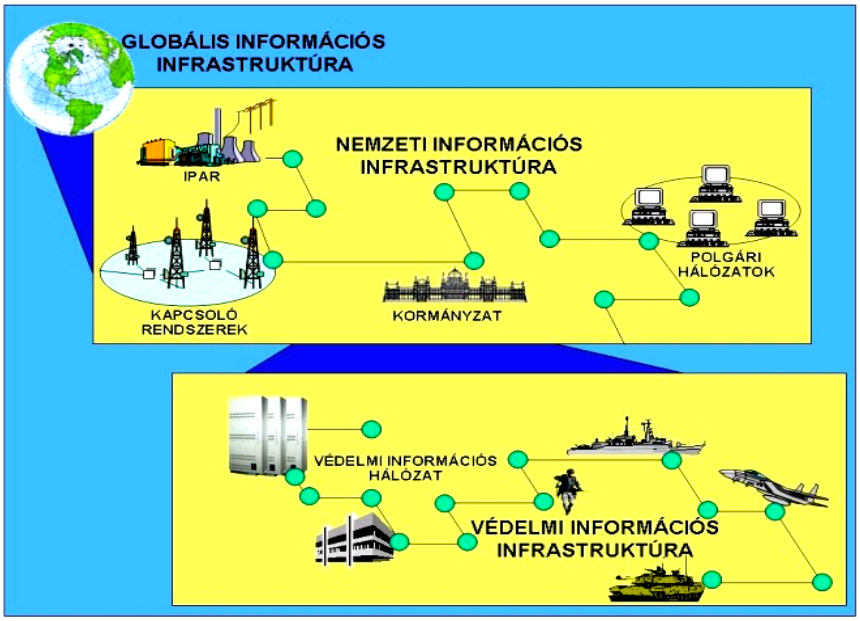
Az információs infrastruktúrák biztonságos üzemelése teszi lehetővé az információs társadalom feladatorientált (funkcionális), szervezett, szakszerű és hatékony működtetését. Az infrastruktúra fejlettségi szintje, korszerűsége, állapota, szolgáltatásainak minősége, hozzáértő kezelése és nem utolsósorban biztonsága alapvetően befolyásolja az információs társadalom működési mechanizmusát.

Az információs infrastruktúrákon belül különböző rendeltetésű és típusú infrastruktúra–halmazokat különböztethetünk meg. Rendeltetésük, feladatuk szerint az információs infrastruktúrákat az alábbi két nagy csoportra lehet osztani:

- funkcionális, alap információs infrastruktúrákra és
- támogató információs infrastruktúrákra.

Emellett felhasználás, alkalmazás szerint megkülönböztethetünk [1]:

- globális információs infrastruktúrát;
- nemzeti információs infrastruktúrát, és pl. ezen belül védelmi információs infrastruktúrát.




8. ábra. Az információs infrastruktúrák felhasználás szerinti osztályozása [1]

A funkcionális információs infrastruktúrákat feladatorientált információs szolgáltató infrastruktúráknak is lehet nevezni. Rendeltetésük, hogy fizikailag lehetővé tegyék a társadalom valamilyen információs funkciójának zavartalan működését, vagyis infrastrukturális alapon információs alapszolgáltatásokat végezzenek. Az információs társadalom információs infrast-

ruktúráin belül ezek az elsődlegesek. Biztosítják az információk megszerzését, előállítását, továbbítását, feldolgozását és felhasználását. A funkcionális információs infrastruktúrák rendszerint nagykiterjedésű, bonyolult szervezésű hálózatok vagy rendszerek formájában működnek. [1]

A támogató információs infrastruktúrák a kutató, fejlesztő és ellátó információs infrastruktúrák gyűjtő megnevezése, más néven háttér információs infrastruktúráknak is nevezhetők. [22] Ezek rendeltetése, hogy létrehozzák, és folyamatosan biztosítsák az alapvető információs szolgáltatásokat végző funkcionális információs infrastruktúrák zavartalan működéséhez és fejlődéséhez szükséges szellemi és anyagi alapokat, valamint támogató háttereket.

Az információs termelési korszak és az információs társadalom kibontakozásával kialakuló globális gazdaságot a globális információs környezet veszi körül. Ennek a globális környezetnek a műszaki alapját az a globális információs infrastruktúra képezi, amely nem más, mint azoknak a vezetékes és vezeték nélküli távközlési rendszereknek, valamint számítógéphálózatoknak összessége, amelyek a globális információcserét biztosítják.

E hálózatok digitális jeltovábbító közegei az optikai kábelek és rádiócsatornák, melyek a föld felszínén, a föld alatt, a tenger felszíne alatt vagy a föld körüli, közeli kozmikus térben – az űrben – továbbítják az információkat. Ebben a globális információs közműben egyre nagyobb szerepet tölt be az internet. A rohamos ütemben bővülő globális elektronikus kereskedelem és elektronikus pénzpiac egyre nagyobb mértékben veszi igénybe az internetet. A globális információs környezetben – az információs közművek hálózatán keresztül – a világ minden érintett globális, regionális és nemzeti szerve, intézménye és működési rendszere részt vesz.

A nemzeti információs infrastruktúra részét képezi a világméretű globális információs infrastruktúrának. Összetétele tulajdonképpen kicsinyített formában tükörképe a globális információs infrastruktúrának. [1]

A nemzeti információs infrastruktúra magában foglalja:

- a közszolgálati, kormányzati és magán célú, nagysebességű hálózatokat;
- az információ továbbítására szolgáló műholdas-, földi vezeték nélküli- és vezetékes rendszereket;
- számítógépeket, televíziókat, rádiókat és egyéb eszközöket, melyek segítségével az emberek képesek kihasználni az infrastruktúra adta lehetőségeket, valamint
- az embereket, akik létrehozzák, felhasználják és hasznosítják az információt.

A védelmi információs infrastruktúra átfogja a védelmi célú információk továbbítására, feldolgozására, az információ és adat tárolására, kezelésére, visszakeresésére és megjelenítésére szolgáló eszközöket. A Honvédelmi Minisztérium országos hálózatához kapcsolódnak az összhaderőnemi vezetési rendszerek, a csapatvezetési rendszerekhez, pedig a harctéri fegyverirányító rendszerek. A nemzeti védelmi infrastruktúra ezen túlmenően szervesen kapcsolódik a szövetséges védelmi infrastruktúrához, a védelmi információs közműhöz. [23]

### 1.2.1. Funkcionális információs infrastruktúrák

A funkcionális információs infrastruktúrák közé – fontossági sorrend nélkül – egyfajta felosztás szerint a következőket sorolhatjuk [22]:

- a nyílt előfizetői távközlési hálózatokat;
- a közszolgálati, közüzemi és közellátási érdekből üzemeltetett zárt távközlési különhálózatokat;
- a műsorszóró és tájékoztató hálózatokat;
- a vezetési rendszereket, hálózatokat (országos hatáskörű kormányzati, közigazgatási, rendőrségi, határőrségi, vámőrségi, honvédségi stb. hálózatok);
- a légi forgalmat, repülésirányítást és légi navigációt biztosító rendszereket;
- a légvédelmi fegyverirányítást biztosító rendszereket;

- a távérzékelést, távellenőrzést biztosító rendszereket;[3]
- a távirányító- és robotok vezérlését biztosító rendszereket;
- az informatikai hálózatokat.

Nyílt előfizetői távközlési hálózatok közé tartoznak a különböző rendeltetésű, fajtájú és típusú nyílt – előfizetési és használati díj ellenében – bárki számára hozzáférhető információátviteli hálózatok és rendszerek. Ezek a rendszerek jelek, jelzések, adatok, adatállományok, formalizált és szabad szövegek, elektronikus levelek, táviratok, üzenetek, képek, rajzok, mozgóképek, animációk, TV-adások, videokonferenciák és beszédalapú információk továbbítását végzik. Az információ továbbítására vezetékes és vezeték nélküli (rádió, rádiórelé, rádiótelefon, műholdas), vagy ezek kombinált rendszereit alkalmazzák.

A közszolgálati, közüzemi és közellátási érdekből üzemeltetett távközlési zárt különhálózatok az ország közüzemeinek, közlekedésének és más közellátó (logisztikai) és közrendvédelmi szerveinek – a nyilvános használat elől elzárt – belső, más néven szolgálati használatú, „zártrendszerű távközlési hálózatai". Ezeket a hálózatokat – az alaprendeltetésük mellett – válsághelyzetben, szükséghelyzetben, természeti katasztrófa idején, rendkívüli állapotban és háborúban fel lehet használni katonai célokra is, mint fontos tartalék távközlési hálózatokat. Ilyen fajtájú, zártüzemű távközlési külön-hálózatokkal rendelkeznek:

- a villamos energiatermelő, elosztó és ellátó hálózatok (energetikai rendszerek);
- az olaj- és gázipari ellátó rendszerek, (pl. szivattyú állomások, benzinkút hálózatok);
- a közlekedési hálózatok (vasúti-, közúti-, városi-, taxi-, légügyi-, vízügyi stb. hálózatok);
- a rendőrség, határőrség, vám- és pénzügyőrség;

[3] Azokat a vizsgálati módszereket jelöljük a távérzékelés gyűjtőfogalmával, amelyekkel a közelünkben vagy tágabb környezetünkben található tárgyakról vagy jelenségekről úgy gyűjtünk adatokat, hogy az adatgyűjtő (általában szenzornak nevezett) berendezés nincs közvetlen kapcsolatban a vizsgált tárggyal vagy jelenséggel. A fényképezés tipikusan távérzékelési adatgyűjtés, a tárgytól vagy jelenségtől meghatározott távolságra lévő fényképezőgép az objektíven keresztül beeső fényt (elektromágneses sugárzást) egy fényérzékeny lemezre (filmre) vetíti, ahol meghatározott kémiai folyamatok következtében kép keletkezik. [24]

- a polgári védelem és katasztrófa elhárítás;
- az árvízvédelem, vízügy;
- a tűzoltóság;
- a mentőszolgálatok (földi, légi, vízi) stb., és
- a közösségi kábel TV-s rendszerek.

Műsorszóró és lakossági tájékoztató hálózatok kategóriájába a közszolgálati, valamint a kereskedelmi (magán) médiumok, vagyis a földfelszíni, illetve műholdas rádió és TV állomások tartoznak. Híreket, politikai, gazdasági, kulturális és szórakoztató műsorokat szolgáltatnak, vagyis fontos, közérdekű közszolgálati kommunikációs feladatokat látnak el. Sajátos jellemzőjük, hogy adásaik az ország egész területén foghatók, és így katasztrófa, rendkívüli állapot stb. esetén országos riasztásra is felhasználhatók. [20]

Vezetési rendszerek és hálózatok kategóriájába tartoznak az országos hatáskörű kormányzati, közigazgatási, rendőrségi, határőrségi, vám- és pénzügyőrségi, honvédségi, katasztrófavédelmi stb. vezetési rendszerek és hálózatok. Rendszerint kombinált típusúak, vagyis távközlési és informatikai átviteli vonalakat egyaránt igénybe vesznek.

A vezetési rendszerek a vezetékes és az ún. hagyományos vezeték nélküli (rádió, rádiórelé, troposzféra) összeköttetéseken túl, cellás rendszerű rádiótelefon hálózatot (Global System for Mobile Telecommunication – GSM), egyéb korszerű digitális rádió rendszereket (Terrestrial Trunked Radio – TETRA)[4], személyhívó rendszereket és műholdas szolgáltatásokat is igénybe vesznek.

A légi forgalmat, repülésirányítást és légi navigációt biztosító rendszerek lehetnek polgári és katonai rendszerek. A katonai és polgári repülésirányító és navigációs rendszereket, valamint azok kiegészítő és kapcsolódó távközlő és adatátviteli elemeit napjainkban összevontan, közösen működtetik, melynek következtében jelentős erőforrásokat takarítanak meg. E rendszer elemei közé sorolhatók a repülőterek irányítótornyai, légtérellenőrző-, repülésirányító-,

[4] Magyarországon Tetra elven működik az Egységes Digitális Rádiórendszer, azaz az EDR, amelyet tanulmányunk későbbi fejezetében mutatunk be.

le-szállító-, gurító radarállomásai, navigációs berendezései, rádióállomásai. Ugyancsak ide tartoznak a repülő készenléti mentőszolgálatok, melyek légi katasztrófa esetén lépnek működésbe. A honi repülőterek (mind a polgári, mind a katonai) állandó kapcsolatban állnak egymással, és összeköttetésbe tudnak lépni a környező országok és a szövetségesek hasonló rendszereivel.

Légvédelmi fegyverirányítást biztosító rendszerek az ország légterének védelmére szolgálnak. A NATO csatlakozással hazánk a NATO egységes légvédelmi rendszeréhez (NATO Integrated Air Defence System – NATINADS) kapcsolódott, amelyben a légtér helyzetéről, állapotáról, megsértéséről szóló adatok azonnal a megfelelő légvédelmi harcálláspontra jutnak. Ebben az infrastruktúra osztályban is igen fontos szerepet kapnak azok a távközlési hálózatok, melyek az éjjel nappal üzemelő légi és földi légvédelmi vezetési pontokat, távol- és közel felderítő-, magasságmérő-, célmegjelölő- és tűzvezető radarállomásokat és egyéb más elemeket kapcsolnak össze.

A távérzékelést, távellenőrzést biztosító rendszerek közé tartoznak a műszeres (szenzoros) felderítő, ellenőrző és zavarelhárító rendszerek. Idesorolhatók továbbá az elektromágneses tartományban működő különféle műszaki ellenőrző, monitoring rendszerek is. Ezek a rendszerek a légvédelemhez hasonlóan folyamatosan működnek. Nemzetbiztonsági szempontból ezek a polgári és katonai rendszerek együttműködnek.

Távirányító- és robotok vezérlését biztosító rendszerek kategóriájához sorolható a polgári és katonai életben minden olyan rendszer, amelynek működését távolból irányítják, vagy a rendszer szenzorai országos vagy helyi központba továbbítják mérési adataikat. Ide tartoznak, pl. a pilóta nélküli repülőeszközöket vezérlő rádiós rendszerek.

Az informatikai hálózatok kommunikációs csatornákkal összekötött, egymással kommunikálni tudó számítástechnikai eszközök vagy csomópontok halmaza. A csomópontok számítógépek, terminálok, munkaállomások vagy különböző kommunikációs eszközök lehetnek, a térben tetszőlegesen elosztva. [20]

### 1.2.2. Támogató információs infrastruktúrák

A támogató információs infrastruktúrák közé a következőket sorolhatjuk:

- a villamosenergia-ellátó rendszerek;
- az elektronikai és informatikai kutató és fejlesztő intézetek;
- az elektronikai és informatikai vállalatok;
- a raktárakat, nagykereskedelmi ellátó vállalatok.

A villamosenergia-ellátó rendszerek közé a különböző erőművek (szén- és olajtüzelésű, gázüzemű, vízi-, szél-, nap-, biogáz- és atomerőművek), villamos energetikai hálózatok (távvezeték rendszerek), villamos energia transzformátorok és teherelosztók stb. tartoznak.

Az elektronikai és informatikai kutató és fejlesztő intézetek közé tartoznak az e tudományterületeken kutatásokat folytató egyetemek, főiskolák és más kutató-fejlesztő intézetek. Ezek vizsgálata megmutatja, hogy egy adott ország az elektronika és informatika terén milyen irányban fejlődik, és milyen képességekkel rendelkezik.

Az elektronikai és informatikai fejlesztő és termelő vállalatok működésén keresztül következtetni lehet az információs társadalom elektronikai és informatikai fejlettségre, teljesítő képességre. Fontos szempont, hogy egy adott ország, az elektronikai és informatikai eszközök területén önellátó-e, vagy erősen importra szorul.

A raktárak és nagykereskedelmi elosztó vállalatok közül azok sorolhatók e kategóriába, amelyek elektronikai és informatikai eszközök, alkatrészek országos tárolásával és ellátásával foglalkoznak. Közülük különösen fontosak azok, amelyek jelentős és kiterjedt nemzetközi kapcsolatokkal rendelkeznek. [1]

### 1.2.3. Kritikus infrastruktúrák

Ha az infrastruktúrákat abból a szempontból vizsgáljuk, hogy azok mennyire fontosak, akkor *kritikus* és sebezhető infrastruktúrákat különböztethetünk meg, melyek működése alapvető fontosságú és nélkülözhetetlen a társadalom működtetéséhez. Amennyiben ezek valamilyen

beavatkozás következtében működésképtelenné válnak, az beláthatatlan következményekkel járhat az ország gazdaságára és védelmére, azaz maga az ország biztonsága kerülhet veszélybe. Ezért alapvető fontosságú, hogy feltérképezzük, és pontosan behatároljuk e kritikus infrastruktúrákat, mivel egy információs támadásnak – azok információs rendszerein keresztül – potenciális célpontjai lehetnek. [1]

A kritikus infrastruktúrák működésük során három alapvető funkciót látnak el. Egyfelől 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.

Másfelől a kritikus infrastruktúrák biztosítják az összeköttetést és az együttműködés képességét. A kommunikációs és számítógép-hálózatok kötik össze és sok esetben rajtuk keresztül irányítják a társadalom és a gazdaság többi infrastruktúráját. Ebben az összefüggésben e rendszerek kritikus információs infrastruktúráknak minősülnek.

Harmadsorban a kritikus infrastruktúrák 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. [25]

Egyértelmű tehát, hogy e kritikus infrastruktúrák védelme és működésének fenntartása nemzetbiztonsági szempontból minden kormányzat alapvető és létfontosságú feladata. [26]

*„A kritikus infrastruktúrák veszélyeztetettségének feltérképezése, mérése, értékelése, s a szükséges védelmi intézkedések meghozatala előbb azt feltételezi, hogy a feltérképezéstől az intézkedésig egyetértés legyen abban, mi is az a kritikus infrastruktúra. Míg az infrastruktúra fogalma kellő körültekintés árán kielégítő pontossággal meghatározható, a kritikusság ismérvei sokrétűek, szerteágazóak, tudomány- és iparáganként változnak. Egy infrastruktúra tehát*

*nagyon sok szempontból lehet kritikus, kritikussá minősítéséhez viszont az is elég, ha csak egyetlen egy kritérium szerint az. A kritikus infrastruktúra fogalmának meghatározása ennek megfelelően nem egységes."* [27]

Mindezek alapján tehát a már a kritikus infrastruktúrák feltérképezése is meglehetősen nehéz és bonyolult feladat, mert „*ami kritikus* (infrastruktúra) *helyileg, az nem biztos, hogy kritikus az állam számára is. Ráadásul, erről gyakran még pontos információ sincs, hiszen jellemzően területi, vagy helyi szinten nem rendelkeznek szakszerű, tudományosan megalapozott kockázatértékeléssel."* [28]

Születtek azonban olyan módszerek, amelyek alkalmasak lehetnek a kritikusság mérésére az infrastruktúrák vonatkozásában is. Az egyik ilyen szerint három tényezőt kell figyelembe venni a meghatározáshoz. E három tényező a következő [29]:

- Hatókör: amellyel a kritikus infrastruktúra vagy annak részének elvesztését, elérhetetlenségét földrajzi kiterjedéssel méri. Ez lehet nemzetközi, nemzeti, regionális, territoriális vagy helyi.
- Nagyságrend: amely a veszteség vagy behatás mértéke a következőképp mérhető: Nincs hatás, minimális, mérsékelt vagy jelentős. A nagyságrend megállapításához a következőket is figyelembe lehet venni:
    - népességre gyakorolt hatása (az érintett lakosság száma, áldozatok, betegségek, súlyos sérülések, kitelepítések);
    - gazdasági hatás (GDP-re gyakorolt hatása, jelentős gazdasági veszteség, és/vagy termelés, szolgáltatás fokozatos romlása);
    - környezetvédelmi hatás (a lakosságra és lakókörnyezetére gyakorolt hatás);
    - interdependencia (a kritikus infrastruktúrák egyéb elemei között);
    - politikai hatás (az államba vetett bizalom);

- időbeli hatás: amely megmutatja, hogy az adott infrastruktúra vagy egyes elemének vesztesége mennyi ideig fejti ki komoly hatását (azonnal, 24–48 óra, egy hét, hosszabb időtartam).

Természetesen egy-egy infrastruktúrának nem minden eleme tekinthető kritikusnak, még abban az esetben sem, ha kritikus infrastruktúráról beszélünk. Ezért szükség lehet azonosítani és meghatározni azokat az elemeket, amelyek a legkritikusabbak, azaz amelyek támadásával, és amelyek kiesésével, részleges, időleges, vagy teljes működésképtelenségével a legjelentősebb mértékben okozhatók komoly humán (emberi élet) vagy anyagi (gazdasági) kár. Az infrastruktúrák méretének és összetettségének mérése lehetőséget teremthet beazonosítani ezeket a kritikus elemeket.

A kritikus infrastruktúrák meghatározása során a rendszerek priorálása is komoly segítséget nyújthat. Egyfajta ilyen prioritási rend kialakítása lehet a következő [33]:

1. Önmagukban kritikus létesítmények
2. Sérülésük több infrastruktúra működését is érinti
3. Interdependencia
4. Földrajzi elhelyezkedés
5. Tulajdonviszonyok

### 1.2.4. Kritikus információs infrastruktúrák

Korábban már idéztük: *„az információs társadalom működéséhez szükséges információk előállítására, szállítására és felhasználására különböző rendeltetésű, funkciójú és típusú infrastruktúrarendszerek, hálózatok állnak rendelkezésre. Ezek összessége képezi az információs társadalom komplex információs infrastruktúráját."* [22]

Ugyanakkor nyugodtan kijelenthetjük, hogy 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 azokat*

*kell sorolni, amelyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, internet, műholdak stb.)”*. [30]

Mint a megfogalmazásból látszik, már e dokumentum is különbséget tesz a 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. [31]

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. [26]

Mindezek alapján tehát fontossági sorrend, valamint a teljesség igénye nélkül egy ország kritikus információs infrastruktúrái közé a következők tartozhatnak:

- energiaellátó rendszerek rendszerirányító számítógép-hálózatai;
- kommunikációs hálózatok (vezetékes, mobil, műholdas);
- közlekedés szervezés és irányítás számítógép-hálózatai;
- pénzügyi-gazdasági rendszer számítógép-hálózatai;
- védelmi szféra riasztási, távközlési, számítógép-hálózatai;
- egészségügyi rendszer számítógép-hálózatai;
- kormányzati és önkormányzati számítógép-hálózatok.

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 di-

menzió 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. [32]

E tekintetben kijelenthetjük, hogy a katonai és polgári természetű fenyegetések közötti hagyományos határvonal egyre inkább elmosódik. [26]

# II. FEJEZET
# KRITIKUS INFRASTRUKTÚRÁK ÉS KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK MAGYARORSZÁGON

Az Európai Unió többi országához hasonlóan hazánkban is megtörtént azoknak a veszélyeknek a feltárása, amelyek egyrészt az információs társadalom alappilléreit, azaz az infrastruktúráinkat (kritikus infrastruktúráinkat), ezen belül kiemelten is az információs infrastruktúrákat (kritikus információs infrastruktúrákat), másrészt – illetve ezeken keresztül – a 21. század veszélyeiből következően egész társadalmunkat fenyegetik.

Ahogyan már korábban idéztük, Magyarország 2012-es új nemzeti biztonsági stratégiája is kiemelt helyen kezeli a cybertér, illetve az onnan a kritikus információs infrastruktúráinkat fenyegető veszélyeket. Mivel rendkívül új dologról van szó hazánk stratégiai gondolkodásában, ezért nem árt felidézni:

„*Kiberbiztonság. Az állam és a társadalom működése – a gazdaság, a közigazgatás, vagy a védelmi szféra mellett számos más területen is – mind meghatározóbb módon a számítástechnikára épül. Egyre sürgetőbb és összetettebb kihívásokkal kell számolnunk az informatikai- és telekommunikációs hálózatok, valamint a kapcsolódó kritikus infrastruktúra fizikai és virtuális terében. Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem állami – akár terrorista – csoportok arra használhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését. E támadások eredetét és motivációját gyakran nehéz felderíteni. A kibertérben világszerte növekvő mértékben jelentkező nemzetbiztonsági, honvédelmi, bűnüldözési és katasztrófavédelmi vonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelem feladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására Magyarországnak is készen kell állnia.*

*a) Elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális fenyegetések és kockázatok rendszeres felmérése és priorizálása, a kormányzati koordináció erősítése, a társadalmi tudatosság fokozása, valamint a nemzetközi együttműködési lehetőségek kiaknázása.*
*b) A nemzeti kritikus információs infrastruktúra védelmének erősítése mellett szövetségeseinkkel és EU-partnereinkkel együtt arra törekszünk, hogy az információs rendszerek biztonsága erősödjön, valamint részt vegyünk a megfelelő szintű kibervédelem kialakításában."* [1]

Mindezeken túl a magyar kormány már korábban meghatározta azokat az infrastruktúrákat, amelyekre elsősorban – a terrorizmus elleni harcban – a civil lakosság védelme érdekében különös gondot kell fordítani. Ezek a következők: [2]

- energiaellátás;
- közművesítés;
- közlekedés;
- szállítás;
- távközlés;
- elektronikus adatforgalom;
- informatikai hálózat;
- bankrendszer;
- szolgáltatások;
- média;
- ivóvíz;
- élelmiszer alapellátás;
- egészségügyi biztosítás.

## *2.1 AZ ENERGIAELLÁTÁS, MINT MAGYARORSZÁG KRITIKUS INFRASTZRUKTÚRÁJA*

Terjedelmi korlátok miatt a korábban említett kritikus infrastruktúrák közül csak a talán legfontosabb elem, az energiaellátás kerül bemutatásra jelen tanulmányban. Ennek megfelelően bemutatjuk a hazai villamosenergia-ellátást, annak kialakulását, főbb jellemzőit, illetve a másik igen fontos energiaellátó rendszert: a földgáz-ellátó rendszert.

Amint azt a *Magyarország energiapolitikai tézisei* című anyagban láthatjuk az energiaellátás a modern társadalmakban összetett, több technikai alrendszerből álló energiaellátási láncon keresztül valósul meg majdnem az összes energiahordozó esetében. A teljes ellátási láncra értelmezett ellátásbiztonság az egyes elemek megbízhatóságából vezethető le. [3]

Hazánk energiaellátása nagymértékben függ a külföldi energiahordozóktól, elsősorban a földgáztól és a nyersolajtól. Bár a magyar kormány (hasonlóan számos európai ország kormányához) többször is hangsúlyozta az energiafüggetlenség megteremtésének fontosságát, ez még nem valósult meg.

### 2.1.1. Villamosenergia-rendszer Magyarországon [4]

A magyarországi villamosítás története a XIX. század második feléig nyúlik vissza. Két évvel a világ első közcélú villamos művének New York-i üzembe helyezése után az Osztrák-Magyar Monarchiában, Temesvárott létesült általános célú villamos mű 1884-ben. A mai Magyarországon a mátészalkai villamosítás 1888-ban, Párizséval egyidejűleg indult el. Ettől az időtől számítjuk a magyar villamosenergia-ipar működésének kezdetét is.

A villamosítás rohamosan terjedt a századvég Magyarországán. A legjelentősebb lépés Budapest közcélú villamosítása volt, amely 1893-ban kezdődött, ezt követték a vidéki nagyvárosok.

1945-ben a villamosenergia-fogyasztás jelentősen visszaesett, hiszen a háború miatt megrongálódott számos közcélú és üzemi erőmű, valamint a villamos hálózat jelentős része.

Az 1948-ban következett be e területen az államosítás, amely után az Állami Villamossági Rt. alá tartozott a mintegy 300 közcélú rendszer. 1949-ben alapították meg a nagy és közép-erőművek központi irányító szervét, az Erőművek Ipari Központját. 1951-ben megalakult a hat, mai is működő regionális áramszolgáltató.

Az iparososítás éveiben a villamos-energia igények gyorsabban növekedtek, mint az erőművi kapacitás és bekövetkeztek a fogyasztói korlátozások. Az egyensúlyt tartósan csak 1954-re sikerült kialakítani.

1963-ban jött létre a francia villamos művek szervezetének mintájára a Magyar Villamos Művek Tröszt (MVMT), amely átvette az Erőmű Tröszt vállalatait, valamint a hat elosztó vállalatot is.

Az 1994-ben elfogadott új Villamos Energia Törvény és a kapcsolódó jogszabályok megalkotásával és az 1995 végén lezajlott privatizációval ismét új működési rend valósult meg. Újabb változást az EU-csatlakozáshoz szükséges előírások teljesítése, a kötelező piacnyitás bevezetése jelentett. [4]

A villamosenergia-ipar fejlődésének talán legjelentősebb lépésének tekinthető az addig függetlenül működő erőművek és az ellátott hálózat szinkron üzemben történő összekapcsolása. Ennek megfelelően jött létre 1949-ben az Országos Villamos Tehereloszto (amely jelenleg MAVIR ZRt. néven az MVM csoport részét képezi).

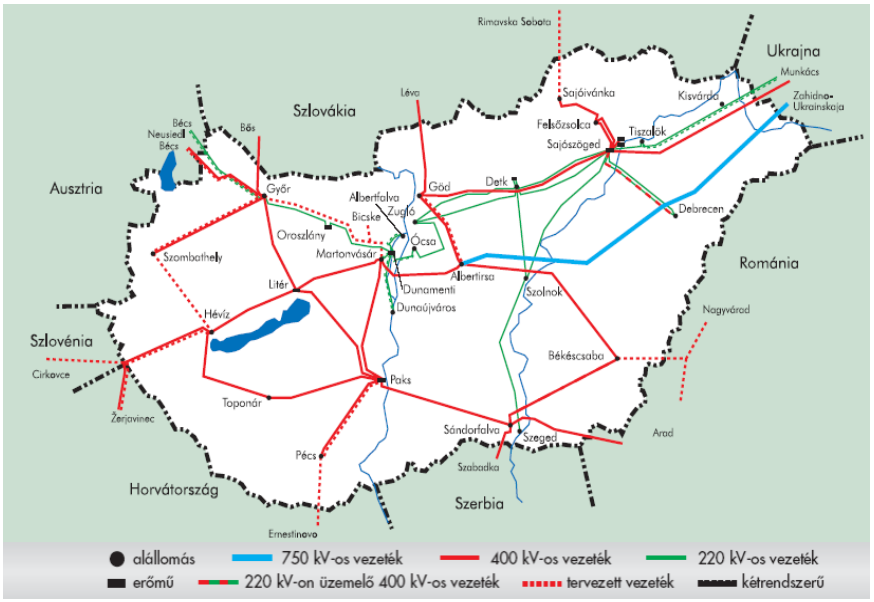
A Paksi Atomerőmű 1970-ben megkezdett beruházását 1971-74 közötti időszakra leállították. Ez tette lehetővé ugyanakkor a Tiszai Hőerőmű nagyblokkjainak indítását. A négyéves szünet igen előnyös volt a Paksi Atomerőmű reaktorainak végleges kivitelezésére. Az erőmű ma is a világ egyik legbiztonságosabb nukleáris létesítménye. [4]

1. kép. A Paksi Atomerűmű látképe [5]

Az energiarendszer korszerű folyamatirányító számítógépes rendszerének kialakítását az iparág elsőként valósította meg 1978-ban. Az automatikus terheléskorlátozás bevezetésének is köszönhető, hogy szemben más országokkal a magyar hálózaton rendszerbomlás sohasem következett be. A technikai fejlettség eredményeként az éves fogyasztói korlátozás 0,2 ezrelék alatt maradt. [4]

Hazánkban a villamos erőműveinknek teljesítőképessége több mint 8200 MW. Vannak azonban olyan áramtermelő egységek, amelyek hosszú ideje nem működnek, de a kapacitásmérlegben még számolnak velük. Ezek indítása azonban bizonytalan lehet. A csúcsfogyasztás időszakában azonban egyelőre a hazai fogyasztás kielégítésére elegendő 6300-6400 MW erőművi teljesítmény[5].

[5] Erre jó példa, hogy hazánk történetének egyik legmegelebb nyári napján 2007. július 20-án a legmagasabb villamosenergia-fogyasztás 6200 MWh volt. A napi csúcshőmérséklet Budapesten 40,3 C fok volt ezen a napon.




1. ábra. Magyarország villamos energia hálózata [6]

Az ország évi bruttó villamosenergia-fogyasztása 41-42 milliárd kWh. Ennek döntő hányadát négy erőmű adja. A Paksi Atomerőmű termelése mintegy 14 milliárd kWh. A Mátrai Erőmű lignittel üzemel, ezért ez is viszonylag olcsón termel. Szénhidrogénnel – alapvetően földgázzal – működik a Dunamenti Erőmű és a Tiszai Erőmű. Ugyancsak gázüzemű a csepeli erőmű, és gázzal üzemelnek a budapesti (a kelenföldi, az újpesti és a kispesti) fűtőerőművek is. Szenes erőművünk egy van, az oroszlányi erőmű a pusztavámi barnaszénnel működik. A gáztüzelésű erőművek jóval – mintegy 40-50 százalékkal – drágábban termelnek villamos energiát, mint a lignittüzelésű erőmű vagy az atomerőmű. A hazai erőművek listáját és működési adatait mutatja be az 1. táblázat.

Alternatív energia terén hazánkban ma még csak a biomassza van jelen nagyobb arányban, és a biomassza területén is alapvetően a fát, mint fosszilis energiahordozót találjuk meg túlnyomó részben. Az energiatermelésben Magyarországon a biomassza részesedése közel 4 százalék. A biomasszát, azaz a fát úgynevezett fluidágyas kazánokban tüzelik el.

1. táblázat. *A Magyarországon található erőművek adatai* [7]

| Erőmű neve | Létesítés időszaka | Teljesítmény (MW) | Blokkszáma (db) | Egységteljesítmény (MW) | Fűtőanyag |
|---|---|---|---|---|---|
| Mátravidéki Hőerőmű | 1947–1953 | 128 | 4 | 32 | lignit |
| Komlói Erőmű | 1950–1952 | 7 | 1 | 7 | barnaszén |
| Tatabányai Erőmű | 1950–1954 | 21 | 2 | 17,4 | barnaszén |
| Diósgyőri Keleti Erőmű | 1951–1955 | 12 | 2 | 6 | kohógáz, tüzelőolaj |
| Dorogi Erőmű | 1954–1955 | 3 | 1 | 3 | barnaszén |
| Dunai Vasmű Erőműve | 1950–1956 | 84 | 5, 21 | 5, 16 | barnaszén, barnagáz, kohógáz |
| Inotai Hőerőmű | 1950–1954 | 120 | 6 | 21 | barnaszén |
| Tiszapalkonyai Hőerőmű | 1952–1959 | 200 | 4 | 50 | barnaszén, földgáz |
| Borsodi Hőerőmű | 1951–1957 | 200 | 8 | 5, 32 | barnaszén |
| Kísérleti Atomreaktor | 1957–1959 | - | 1 | - | urán |
| Pécsi Hőerőmű | 1955–1966 | 215 | 6 | 23, 30, 50 | földgáz, biomassza (fa) |
| Ajkai Hőerőmű | 1957–1962 | 100 | 3 | 33 | barnaszén |
| Tiszai Vízerőmű (Tiszalök) | 1956–1959 | 12 | 3 | 4 | víz |
| Kvassay Vízerőmű | 1958–1961 | 1 | 2 | 0,5 | víz |
| Oroszlányi Hőerőmű | 1957–1963 | 200 | 4 | 52 | barnaszén |
| Dunamenti Hőerőmű I. | 1960–1973 | 600 | 7 | 25, 21, 41 50, 150 | gudron[6] tüzelőolaj, földgáz |
| Tatabányai Hőerőmű (Bánhida) | 1963–1967 | 100 | 1 | 100 | barnaszén |
| Kispesti Fűtőerőmű | 1965–1971 | 12 | 1 | 12 | barnaszén |
| Mátrai Erőmű (Gagarin) | 1965–1973 | 800 | 5 | 100, 200 | lignit, barnaszén |
| Kelenföldi FIAT Gázturbina | 1969–1972 | 32 | 1 | 32 | gázolaj |
| Inotai Gázturbinás Csúcserőmű | 1971–1975 | 200 | 2 | 100 | gázolaj |

[6] A gudron (vagy gudrun) olyan lepárlási maradék, amelyet úgy állítanak elő, hogy az ásványolajból nemcsak a fehérárukat, hanem a könnyebb olajpárlatokat is ledesztillálják. [8]

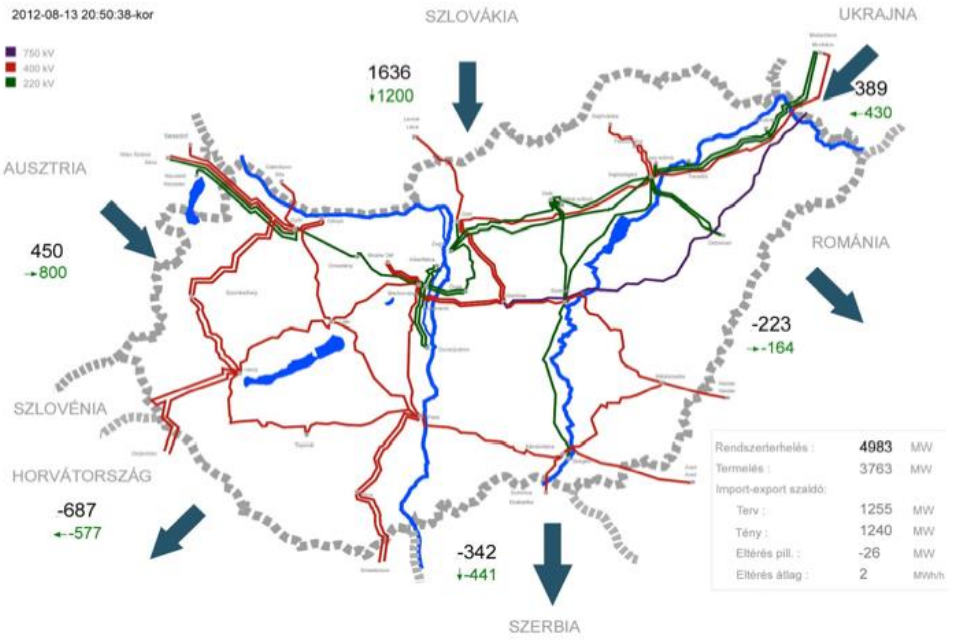
| Erőmű neve | Létesítés időszaka | Teljesítmény (MW) | Blokkszáma (db) | Egységteljesítmény (MW) | Fűtőanyag |
|---|---|---|---|---|---|
| Dunamenti Hőerőmű II–III. | 1969–1976 | 1290 | 6 | 215 | gudron, tüzelőolaj, földgáz |
| Paksi Atomerőmű | 1973–1986 | 1760 | 4 | 440 | urán |
| Tiszai Hőerőmű | 1971–1979 | 860 | 4 | 215 | gudron, tüzelőolaj, földgáz |
| Győri I. Fűtőerőmű fluidtüzelésű k. | 1984–1987 | - | 1 | - | barnaszén |
| Dunamenti Gázturbinás hőhasznosító blokkok | 1989–1998 | 385, 145, 156, 60 | 4 | 24 | földgáz |
| Kelenföldi Gázturbinás Erőmű | 1990–1996 | 136 | 1 | 136 | földgáz, gázolaj |
| Gyorsindítású Gázturbinás Erőművek (Litér, Sajószöged) | 1995–1998 | 240 | 2 | 120 | gázolaj |
| Lőrinci Gázturbinás Erőmű | 1997–2000 | 150 | 1 | 150 | gázolaj |
| Csepeli Gázturbinás Erőmű | 1995–2000 | 390 | 2 | 118, 136 | földgáz, gázolaj |
| Debreceni Kombinált Ciklusú Erőmű | 1999–2000 | 99 | 1 | 99 | földgáz |
| Nyíregyházi Kombinált Ciklusú Erőmű | 2006–2007 | 49 | 1 | 49 | földgáz |

Pécsett egy 50 MW-os erőmű működik fával. Fatüzelésű kazán található még Ajkán is, ugyanakkor vegyes tüzeléssel – fával és szénnel – üzemel a Borsodi és a Tiszapalkonyai Erőmű. Az oroszlányi erőmű széntüzelésűről vegyes tüzelésűre való átalakítása folyamatban van.

A hazai villamosenergia-fogyasztás nem egyenletes. Éjszaka általában keveset fogyasztunk, reggel hét óra körül nagyon gyors a fogyasztás felfutása, aztán az évszaktól, időjárástól függően alakul a délutáni-esti csúcs, és este tizenegy óra után megint lecsökken a fogyasztás. A maximum és minimum között gyakran 1000-1200 MW teljesítménykülönbség is van. Ez óriási kihívás elé állítja az egész villamosenergia-rendszert az erőművektől a rendszerirányítóig.

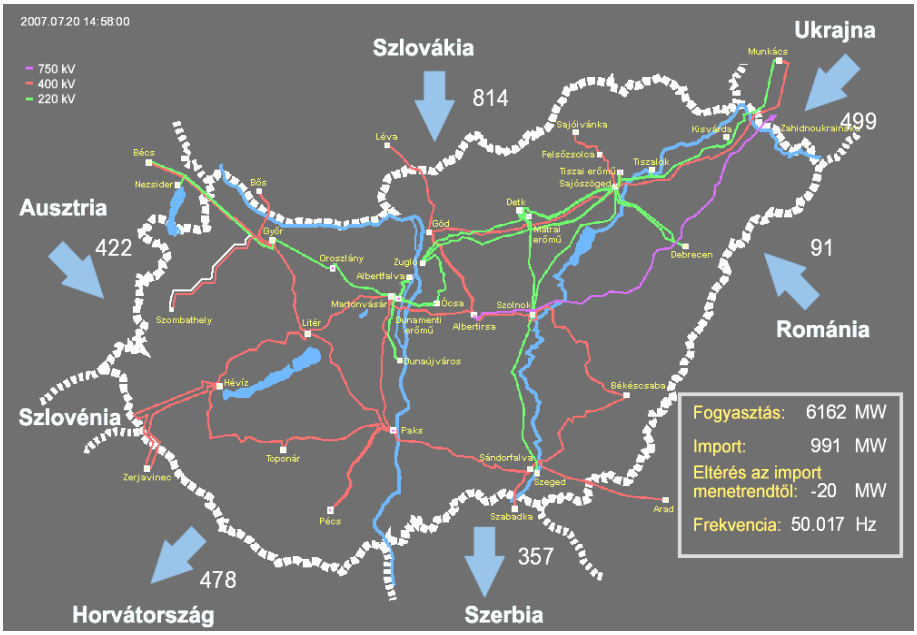
2003. január 1-jén az áramszolgáltatásban is megtörtént a liberalizáció, azaz a piacnyitás. Elsősorban azok a fogyasztóknak van lehetőségük olcsóbb áramot vásárolni a piacon, amelyek többé-kevésbé folyamatosan működnek. A piacnyitás óta sokkal nagyobb feladat hárul a rendszerirányítóra a közüzemi erőművek szabályozásában.

Hazánk pillanatnyi villamosenergia-fogyasztását mutatja egy átlagos nyári napon a 2. ábra.




2. ábra. A pillanatnyi villamosenergia-fogyasztás Magyarországon 2012. 08. 13-án [9]

Amennyiben összehasonlítjuk a 2. ábrán szereplő fogyasztást – 4983 MW – amely megfelel egy átlagos nyári nap villamosenergia-fogyasztásának, a 3. ábrán szereplő fogyasztási adattal, amely 6162 MW, akkor jól látszik, hogy hazánk energiafogyasztása ugrásszerűen megnőhet.




3. ábra. Pillanatnyi villamosenergia-fogyasztás az egyik legmelegebb napon Magyarország történetében 2007. 07.20. 15.00
(Napi csúcshőmérséklet Budapesten 40,3 C fok) [10]

A 3. ábrán szeplő adat azért ilyen magas, mert ezen a napon volt Magyarország történetének egyik legmagasabb átlaghőmérsékletű napja. Ezen a napon, Budapesten a napi csúcshőmérséklet meghaladta a 40 C°-ot.

Hazánkban a villamosenergia-szolgáltatás rendszerének irányítását a MAVIR Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zártkörűen Működő Részvénytársaság (MAVIR ZRt.) végzi. A MAVIR létrehozását megelőzően az Országos Villamos Teherelosztó 1949 novembere óta látta el a rendszerirányítás műszaki feladatait.

2006. január 1-től pedig az integrált átviteli rendszerirányító (Transmission System Operator – TSO) létrejöttével az Országos Villamostávvezeték Rt. (OVIT Rt.) Üzemviteli Igazgatósága és a Magyar Villamos Művek Rt. (MVM Rt.) Hálózati Igazgatósága átkerült a rendszerirányítóhoz.

A MAVIR ma a következő fő feladatokat látja el [10]:

- gondoskodik a magyar villamosenergia-rendszer megbízható, hatékony és biztonságos irányításáról, a szükséges tartalékokról az erőművekben és a hálózaton;
- felügyeli és gyarapítja a hálózati vagyont, elvégzi a megfelelő, üzembiztos ellátáshoz szükséges felújításokat, karbantartásokat és fejlesztéseket;
- biztosítja a villamosenergia-piac zavartalan működését, további bővítését, az egyenlő hozzáférést a rendszerhasználók számára;
- összegzi a villamosenergia-ellátás szereplőitől kapott adatokat;
- tájékoztatja a piac szereplőit;
- összehangolja a magyar villamosenergia-rendszer működését a szomszédos hálózatokkal;
- koordinálja a nemzetközi szakmai együttműködéseket;
- a jövőbe tekintve elkészíti a hálózatfejlesztési stratégiát és javaslatot tesz az erőműpark fejlesztésére.

### 2.1.2. Földgázszállító- és ellátó rendszer Magyarországon [11] [12]

A villamosenergia-rendszer mellett az egyik legfontosabb hazai kritikus infrastruktúra az energiaellátás területén a fölgázszállító- és ellátó rendszer. Nagyon szoros a kapcsolat a villamosenergia-előállítás és a földgázellátó-rendszer között, hiszen a Paksi Atomerőművet leszámítva a hazai legnagyobb erőműveink – Dunamenti, Csepeli, Kelenföldi, Tatabányai, Pécsi – többsége fölgáz felhasználásával termel áramot.[7]

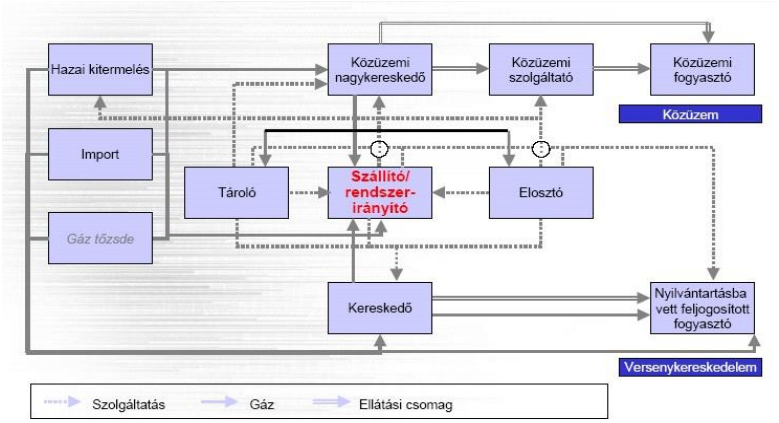
A magyarországi földgázszállítás közel 70 éves múltra tekinthet vissza. Az ország gáz-energiával történő ellátásához tudni kell, hogy hazánk éves földgáz szükséglete bár az elmúlt években némileg csökkenő tendenciát mutat, de 2010-ben megközelítette a 12,2 milliárd $m^3$-t.

[7] Természetesen ezek az erőművek más energiaforrás – pl. kőolaj – felhasználásával is képesek villamos energiát termelni, mint ahogy azt a 3. táblázat is mutatja, mégis a működésük alapvetően a földgázra alapul.

Arányait tekintve, ebből kb. 2,8 milliárd $m^3$ a hazai termelésű, míg kb. 9,6 milliárd $m^3$ import, amely beregdaróci és mosonmagyaróvári átvétellel kerül beszállításra az országba, elsősorban az orosz piacról. Amennyiben összehasonlítjuk a hazai kitermelés adatait, illetve az importból származó földgázszükségletünket, világosan látszik, hogy nagyon erősen függünk az orosz beszállítótól.[8]

Ha folyamatában vizsgáljuk a gáz útját a forrásoldaltól a felhasználóig, akkor jelenleg az alábbi főbb gázpiaci szereplőkkel találkozunk:

- az államközi szerződéseket lebonyolító földgáz nagykereskedő társaság;
- földgázértékesítő társaság, (a MOL Rt. hazai termelési, gázellátási, gázszállítási-rendszerirányítói, gáztárolói szervezetei)[9];
- gázszolgáltató társaságok;
- fogyasztók, (ipari nagyfogyasztók, közüzemi és lakossági fogyasztók);
- valamint a felügyeletet ellátó Magyar Energia Hivatal.




4. ábra. A hazai gázpiac kapcsolatai [11]

[8] Ez az erős függés nemcsak Magyarország esetében jelentkezik, hanem például Németország, Franciaország vagy akár Ukrajna esetében is.

[9] 2005-ben a német tulajdonú E.ON Ruhrgas megvásárolta a MOL földgáz kereskedelmi-értékesítési tevékenységét, így az különvált a MOL tulajdonában maradt gáztermelési és szállítási üzletágtól.

A gáz felhasználását tekintve a gázértékesítő a teljes mennyiség kb. 26 %-át közvetlen eladással értékesíti a (nagy)fogyasztóinál, míg kb. 74%-a pedig viszonteladókon (gázszolgáltatókon) keresztül kerül értékesítésre. Ebből is látszik, hogy mindkét értékesítési irány jelentős súllyal bír a folyamatosan egyensúlyozandó országos gázmérlegben. Nagyságrendjét tekintve az ország átlagos napi fogyasztása kb. 50,0 millió $m^3$/nap, melynek regisztrált minimum értéke kb. 10,0 millió $m^3$/nap, maximum értéke, pedig közel 86,0 millió $m^3$/nap volt ezidáig. [12]

A földgázellátás folyamata alapvetően a következő elemekből épül fel:

- a földgáz határon keresztül történő szállítása, importja illetve exportja, (tranzitja);
- az országhatáron belül a földgáz nagynyomású távvezetéki rendszeren történő szállítása;
- a hazai termelésű gázok betáplálása a gázszállító nagynyomású vezetékrendszerébe;
- a földgáztárolók ki és betárolása a gázszállító nagynyomású vezetékrendszerébe, illetve abból;
- a kiemelt ipari nagyfogyasztók közvetlen ellátása, kiszolgálása a gázszállító rendszeréről;
- a gázszolgáltatók hálózatának ellátása, forrás oldali betáplálás a gázszállító vezetékrendszeréből;
- az ipari, mezőgazdasági, közüzemi és lakossági fogyasztók gázellátása a szolgáltatók elosztóhálózatáról.

Az országba belépő import gázok (Beregszász-Beregdaróc illetve Baumgarten-Mosonmagyaróvár) folyamatos átvételéhez, elszámolásához a MOL Rt. az eladó féllel közösen rendelkezik megfelelő műszerezettségi szintű átadó/átvevő állomásokkal, melyekről a technológiai mért paraméterek az OTR-II elnevezésű telemechanikai rendszeren keresztül kerülnek a gázszállító-rendszerirányító szervezethez.

A 20 éves hosszútávra szóló államközi szerződésben megállapított gázimport lebonyolítására, azaz az import gázok behozatalára, majd a folyamatos éves, havi, heti nominálására a

Panrusgáz Rt. jogosult. A társaság on-line, a szállítórendszerre vonatkozó információkkal nem rendelkezik. Az import és export kapacitás lekötésekhez az adatokat a MOL rendszerirányítójától és a földgázellátásért felelős szervezetétől kapja e-mail-ben, illetve faxos, nyomtatott formában papír alapú adathordozón. A rendszerirányító részéről végrehajtott hazai távvezetéki rendszer egyensúlyozásához szükséges input/output információk áramlása a Panrusgáz Rt.-n keresztül működik mind a külföldi eladó, mind a hazai szállító felé. [12]

Az országhatáron belüli nagynyomású földgázszállító vezetékrendszer összességében közel 5200 km hosszúságú, átlagos átmérője 300-800 mm, névleges nyomásfokozata 63,0 bar, tároló kapacitása kb. 48–50 millió $m^3$.

Az országba beszállított, a távvezetéki rendszerbe belépő import gáz kétirányú betáplálással biztosított. (Beregdaróc, Testvériség-vezeték és Mosonmagyaróvár, HAG-vezeték)

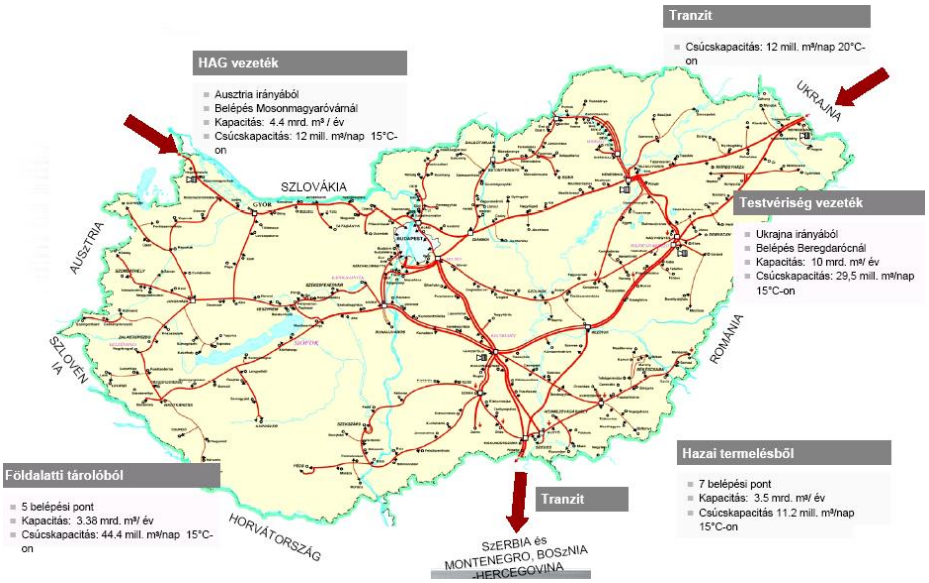
Betáplálási oldalon ezt a 8,0+2,0 milliárd $m^3$ éves gázmennyiséget egészíti ki a hazai, különböző régiókban megtermelt közel 3,0 milliárd $m^3$ éves volumen. A betáplálások földrajzi elhelyezkedése igazodik a termelési objektumokhoz, amely nagyon változatos és egyre csökkenő nagyságrendet mutat térben és időben egyaránt. Amíg öt évvel ezelőtt 56% volt az import/hazai arány, ez jelenleg már 78%-ot képvisel. [12]

A hazai földgázkitermelés főbb helyei [11]:

- Algyő;
- Hajdúszoboszló;
- Karcag/Bucsa;
- Kardoskút;
- Babócsa;
- Pusztaederics;
- Kenderes;
- Endrőd;
- Szank.

A hálózati veszteségek kompenzálása, a szállítási igények rugalmas kielégítése hat távvezetéki nyomásfokozó kompresszorállomással került biztosításra. Ezek a következők [11]:

- Beregdaróc (orosz/ukrán eredetű földgáz szállítására);
- Nemesbikk (orosz/ukrán/hazai termelés/tárolói gáz szállítására);
- Városföld (orosz/ukrán/hazai termelés/tárolói gáz szállítására);
- Mosonmagyaróvár (Ausztria irányából érkező földgáz szállítására);
- Hajdúszoboszló (orosz/ukrán / hazai termelés/tárolói gáz szállítására).




5. ábra**.** Magyarország földgázszállító-rendszere [11]

*A földgázszállító rendszer input oldala*

A hazai termelésű gázok rendszerbe történő betáplálása a gázátadó állomásokon, azaz az úgynevezett „0”-pontokon történik. Itt történik meg a betáplált mennyiségek hiteles mérése, a termelőtől történő átvétele. Ennek eszközei túlnyomórészt a szűkítő elemes mérési elven alapuló térfogatáram mérő mérőhidak, kisebb részt pedig turbinás mérőművek. Minden átadás-átvételi ponton az effektív térfogatáramok nyomás és hőmérséklet kompenzációs eszközökkel vannak normál állapotra *(101,325 kPa és 15,0 °C)* átszámítva, mely az elszámolás alapját

képezi a két fél között. Az elszámolást nagymértékben megkönnyíti a legtöbb betáplálási pont esetében, a bányászati területen kiépített folyamatirányító, mérésadatgyűjtő rendszerekkel illetve a Plant Information System-mel (PI), mint az üzemi operatív vezetői rendszerrel való „közvetett kommunikációs kapcsolata" a szállítói mérőrendszernek. Ez az OTR-től független kommunikációs kapcsolat, de legtöbb esetben „0"-ponti adatgyűjtő, kommunikációs bővítő rendszereken keresztül történik az adatátvitel. [12]

*A földgázszállító rendszer output oldala*

Az output oldalt a szállítóvezeték rendszerről leágazást jelentő gázátadó állomások jelentik, melyekről az alábbi fogyasztói, szolgáltatói körök ellátása történik meg:

- kiemelt ipari nagyfogyasztók, (jelenleg a MOL Rt.-nek 26 ilyen fogyasztója van);
- a gázszolgáltató társaságok elosztó rendszere, (jelenleg a MOL Rt.-nek mintegy 400 db, a szolgáltatókat ellátó átadó állomása van).

Mivel ezen átadóállomások mindegyike MOL tulajdonban van, ezért műszakilag nagyon hasonlítanak az input oldali „0"-pont-nál leírtakhoz. A MOL joghatással járó elszámolási méréseinek technikai körülményei, valamint azok kapcsolata az OTR-II országos telemechanikai rendszerrel megegyezik a „0"-pontokéval. A MOL Rt. Földgázszállítás-Rendszerirányítás szervezete ezek alapján rendelkezik on-line térfogatáram, mennyiség és nyomás paraméterekkel a siófoki diszpécserközpontjában. Innen történik a teljes földgázrendszer egyensúlyozása közvetett módon, a hat Távvezetéki Üzemen végrehajtásában. [12]

A földgázellátásról szóló törvény értelmében a földgázszállítás rendszerirányítási engedélyese a MOL Rt. A rendszerirányítás három napos, folyamatosan „gördülő" tevékenység. Ez a következőket jelenti [11]:

Gáznap előtt:

- nominálások fogadása, összesítése;
- hidraulikai vizsgálatok;
- nominálások visszaigazolása;

Gáznap:

- szállítatói megrendelések teljesítése;
- fogyasztás-forrás egyensúlyozása;
- szükség esetén a megszakítások és korlátozások elrendelése;

Gáznap után:

- a szállítatói megrendelések mennyiségi és minőségi allokált elszámolása;
- információ és adatszolgáltatás.

A *rendszerirányítás* feladatainak ellátása érdekében a társaság informatikai rendszert üzemeltet.

2004-ben a Synergon Informatika Rt. és leányvállalata, a Synergon Atos Origin Kft. (SAO) szerződést kötöttek a MOL Földgázszállító Rt. Informatikai Platformjának továbbfejlesztésére. A Synergon-csoport a megoldás infrastrukturális korszerűsítését végezte, míg alvállalkozásban az Atos Origin Spanyolország saját szoftvermegoldását fejlesztette a Gáztörvénynek és az Üzemi Kereskedelmi Szabályzatnak történő megfelelőség, az új funkcionális igények és a szigorúbb biztonsági elvárások érdekében. A Synergon-csoport integrált projekt keretében bővítette a szerverparkot, háttér (back up) rendszert alakított ki, Exchange szervert és tűzfalakat implementált Az Atos Origin az általa tervezett szoftvermegoldást, a MOL Földgázszállító Rt. igényei szerint, a Synergon-csoport szakembereinek részvételével készülő specifikációk alapján fejlesztették tovább.

A MOL Földgázszállító Rt. 2004 januárjától üzemelteti a piaci szereplők gázszállítási és gázfelhasználási tevékenységét támogató Informatikai Platformot, amely egyfelől az egyes szállíttatók által adott időszakra (nap - hét - hó) vonatkozó gázigényét rögzíti, másfelől a ténylegesen elszállított gázmennyiség allokációját teszi lehetővé. A földgázpiac működését támogató Informatikai Platform megvalósítását az Atos Origin Spanyolország (korábban Schlumber-ger/Sema) végezte. A Synergon-csoport 2004 közepétől látta el a rendszer üzemeltetési feladatait. [13]

Hazánk öt földalatti gáztárolóval rendelkezik:

- Hajdúszoboszló;
- Zsana;
- Pusztaederics;
- Kardoskút-Pusztaszőlős;
- Algyő-Maros-1.

A földalatti gáztárolók nagynyomású távvezetéki rendszerhez való kapcsolata méréstechnikai, telemechanikai, adatforgalmi kapcsolat terén nagyban hasonlít a hazai termelésű gázok betáplálási pontjainál leírt műszaki tartalomhoz, mivel ugyanazon „0”-pontokhoz csatlakoznak.

Ma a MOL Nyrt. 26 kiemelt ipari nagyfogyasztó[10] gázenergiával történő ellátását végzi közvetlenül saját távvezetéki rendszeréről Az ellátásuk MOL-os gázátadó állomásokon keresztül történik, melyekről a szállító-rendszerirányító on-line technológiai *(térfogatáram, integrált mennyiség, nyomás, alkalmanként minőségi paraméterek)* adatokkal rendelkezik saját telemechanikai rendszerén keresztül. [12]

A gázátadó állomások feladata a földgáz mennyiségének, minőségének, nyomásának, hőmérsékletének a hiteles mérése, a nyomás szabályozása, és a túlnyomás elleni védelem, szükség esetén a gáz melegítése és szagosítása. A távvezetékhez kapcsolódó gázátadó állomásokon történik a földgáz [11]:

- átadása az átvevőknek;
- mennyiségi paraméterek mérése az OMH által vizsgált mérőeszközökön;
- átadási nyomás szabályozása a szerződésekben rögzített paramétereknek megfelelően (jellemző 3-28 bar);
- mechanikai szennyeződések kiszűrése (98%-os szűrés 5 mikron nagyságig);

[10] Ezek a nagyfogyasztók elsősorban olyan ipari komplexumok, erőművek, amelyek fogyasztás meghaladja az 500 $m^3$/órát, és működésük kiemelten fontos a nemzetgazdaság szempontjából.

- melegítése az állomási berendezések megfelelő működése érdekében, hogy a kimenő földgáz hőmérséklete 0 °C, illetve efelett legyen;
- szagosítása egyedi szagosítású állomáson.

Kevés kivételtől (a MOL KTD regionális termeléséből történő betáplálása) eltekintve a mai gázszolgáltató társaságok elosztó hálózatába történő forrás oldali betáplálás a MOL Rt. nagynyomású szállítóvezetéki rendszeréről történik gázátadó és nyomáscsökkentő állomásokon keresztül.

Az átadó állomások MOL tulajdonú távvezetéki leágazást jelentő csomópontok, melyeken a nyomás csökkentése, valamint a térfogatáram és a primer/szekunder oldali nyomások mérése, táv-adatátvitele megtörténik az OTR-II rendszer felé. Az ezután következő kül- és belterületi csővezetéki hálózat és részegységei képezik a szolgáltatók működési területét és/vagy tulajdonát. Az elosztóhálózatokban az alábbi nyomásfokozatú rendszerek találhatók meg:

- nagynyomású ($p > 25$ bar);
- nagyközépnyomású ($25 \text{ bar} > p > 4$ bar);
- középnyomású ($4 \text{ bar} > p > 0{,}1$ bar);
- kisnyomású ($0{,}1 \text{ bar} > p$).

Néhány olyan műszaki megoldás, amely az elosztóhálózatokon belüli biztonságos rendszer egyensúlyozást szolgálja [12]:

- diszpécsertermi folyamatmegjelenítő rendszerre épülő on-line adatgyűjtő, telemechanikai rendszer, mely magába foglalja az átadási és fogyasztási helyek mennyiségi, minőségi és nyomás, valamint a nyomáscsökkentő állomások primer/szekunder nyomás paramétereit, és a főbb záró szerelvények helyzetjelzéseit;
- záró szerelvények, nyomásszabályozó ágak távműködtetési lehetőség a központi folyamatirányító rendszerről;
- korszerű, nyomás- és hőmérsékletkompenzációt biztosító térfogatáram mérő körök az (átadói) fogyasztói oldalon, korszerű, költségkímélő adatátviteli mód (pl: GSM SMS

alapú) a meghatározó, megszakítható fogyasztói pontok adatainak kvázi on-line feldolgozásához;

- az átadó állomások fogyasztási és technológiai adatainak transzparenssé tétele, az adatok allokálása az érintett szervezetek számára, (közvetlen OTR kapcsolat vagy internet alapú platformon történő adat közlés és adat elérhetőség);
- hálózat szimulációs és térinformatikai modell alkalmazása az elosztórendszer egyensúlyozásához;
- internet alapú nominálási gyakorlat a földgázszállító-rendszerirányító felé;
- központi diszpécseri irányító és hibaelhárítási ügyeleti rend fenntartása a zavarmentes, kiegyensúlyozott gázellátás érdekében;
- a Hivatal felé történő rendszeres adatszolgáltatás, mintavételi eljáráson alapuló gyakorlatának kidolgozása, alkalmazása;
- a fogyasztóközpontú szemléletre építő adatgyűjtés, hibabejelentés, call-center működtetés és minőségirányítási gyakorlat.

Az orosz gázszállítástól való függőségünket nagyon jól jellemzi az a helyzet, amely 2006 januárjában kialakult. Az orosz Gazprom 2006. január 1-jén leállította a gázszállítást Ukrajnának és Moldovának, mivel nem tudtak megállapodni a gáz árában.

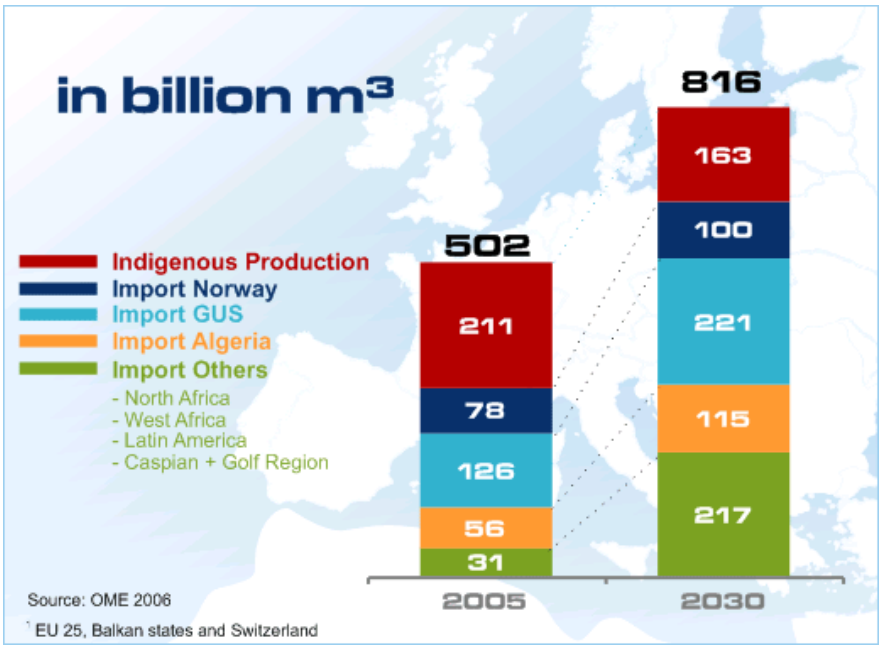
Ez azzal a következménnyel járt, hogy Ukrajna az országán keresztül haladó – Európának szánt – orosz gázt nem engedte tovább, azaz az úgynevezett tranzitgázt használta. Az ukrán-magyar határon ennek következtében közel 60 %-al kevesebb gáz érkezett Magyarországra. Ez jelentős kiesés volt, mely alapján a MOL felszólította nagyfogyasztóit, hogy térjenek át földgázról kőolaj felhasználására. Ennek megfelelően a tatabányai és a csepeli erőmű átállt a kőolajtüzelésre. Lakossági korlátozást – mivel másfél nap alatt rendeződött a helyzet, és a földgázszállítás visszaállt a normál mennyiségre – nem kellett elrendelni.

Egy hasonló – földgázhiány miatti – fogyasztói korlátozásra természetesen rendelkezésre állnak külön tervek. Ennek érdekében az Energia Hivatal minden évben úgynevezett *korlátó-*

*zási sorrendet* ad ki, rendelet formájában. E korlátozási sorrend első helyén azok a nagyfogyasztók – erőművek, nagy ipari létesítmények – vannak, amelyek képesek más, például kőolaj felhasználásával működésüket biztosítani. A lakossági fogyasztók, azaz a gázszolgáltatók részére biztosított földgáz korlátozása a lista utolsó harmadában szerepel.

Ez a – szerencsére nagyon rövid ideig tartó gázmennyiség csökkenés – azonban újra felhívta a figyelmet hazánknak arra a nagyfokú függőségére, amely az orosz piacról származó földgázzal kapcsolatosan fennáll. Ez nemcsak Magyarország vonatkozásában igaz, hanem számos nyugat-európai ország – pl. Németország – esetében is.

Ezért az Európai Unió közös energiapolitikát hirdetett, amelyben szerepet kap egy újabb, az orosz gázvezetékek alternatíváját jelentő gázvezeték megépítése is. Az új gázvezeték ötletét is magába foglaló úgynevezett *Nabucco* projekt már 2002-ben megszületett, hiszen az már akkor is jól látszott, hogy az egyszereplős, nem diverzifikált energiabeszállító hatalmas függőséget, és komoly biztonsági kockázatot jelent számos európai ország számára.




6. ábra. Európa földgázigényének várható alakulása 2005 és 2030 között [14]

A Nabucco projekt egy új csővezeték-rendszer kiépítését célozza meg Törökország és Ausztria között, Bulgárián, Románián és Magyarországon áthaladva. A projekt két igen komoly előnyt is magába foglal, úgy hogy mindeközben komoly pozitív hatást gyakorolhat az ellátás biztonságára. Az egyik ilyen, hogy új beszerzési forrást von be a gázellátásba, a másik előny pedig új tranzitútvonal biztosítása a gázszállításoknak Oroszország és Ukrajna kikerülésével. Az érintett öt gázipari cég egy projekttársaságot alapított a megvalósítására, bécsi székhellyel (Nabucco Gas Pipeline International). A projekt finanszírozása alapvetően magántőkéből történhet, közösségi pénzügyi forrás az Európai Beruházási Bank részéről érkezhet. (A MOL az FGSZ-en keresztül vesz részt a projektben).

A Nabucco projekt tervezett csővezetéke összességében közel 3300 km hosszú, a beruházás költsége kb. 4,6 milliárd euró volt az induláskor, ez azonban 22-26 milliárd Euróra kúszott fel az évek során. A tervek szerint a vezeték 2011-ben 8, 2020-ban 25,5 milliárd $m^3$, a csúcs-forgatókönyv alapján 2011-ben 13, 2020-ban pedig már 31 milliárd $m^3$ földgázszállítási kapacitással működhetett volna. A prioritást élvező, európai érdekű projekt szerepel a transzeurópai energiahálózatokról (TEN-E) szóló 1229/2003/EK határozatban is. A Nabucco csővezetékének tervezett nyomvonala a 7. ábrán látható. [15] A projekt azonban a folyamatosan emelkedő költségek miatt 2012-ben válságba jutott. [16]

A Nabucco projekttel párhuzamosan Oroszország is újabb földgázszállító csővezeték építéséről döntött. Az új csővezeték a *Kék Áramlat 2* (Blue Stream 2) nevet kapta.

Az orosz energiaipari óriás, a Gazprom egyébként már az 1990-es évek közepén, az Ukrajnán áthaladó európai szállítások növelése jegyében tervezte olyan, nagy kapacitású magyarországi és szlovéniai tranzitvezeték építését, amely Szlovákiából szállította volna az orosz gázt Olaszországba. Ezt a tervet azonban elvetették, miután a Gazprom megállapodott az ENI-vel az (Ukrajnát elkerülő) Kék Áramlat finanszírozásában, már akkor számolva esetleges meghosszabbításával. [17]


7. ábra**.** A Nabucco tervezett nyomvonala és a betáplálási pontok [14]

A Kék Áramlat csővezeték Oroszországot köti össze Törökországgal. Ennek meghosszabbítása a terv Dél-Európa, illetve Olaszország felé – Ukrajnát kikerülve – a Kék Áramlat két projektben. A Kék Áramlat, amely egy része a Fekete-tenger alatt fut, az egyik legmélyebben lévő tenger alatti csővezeték. A legmélyebben fekvő pontja 2,15 km mélyen van. Hossza jelenleg 1213 km, földgáztovábbító kapacitása pedig 16 milliárd $m^3$ évente.

Oroszország egy másik földgázvezetéket is támogat (sőt a Kék-Áramlat előtt priorizálja), amelynek neve Déli Áramlat. A Déli Áramlat 900 kilométeres tenger alatti szakasza az orosz fekete-tenger-parti Beregovajából indulna és innen a bulgáriai Várnáig menne.

Várnából vezeték délnyugati ága Görögországon és a Jón-tengeren keresztül Dél-Olaszországba tartana, úgy hogy görög javaslatra ez a vezeték láthatná el földgázzal a tervezett Görögország–Olaszország-gázvezetéket is. Az északnyugati ág Szerbián és Magyarországon keresztül az osztrák Baumgarten gáztárolóiig futna. [18]

Az eddig elmondottak alapján megállapíthatjuk, hogy hazánk számára ezen csővezetékek megépítése előnyt jelentene, hiszen csökkentené az egy helyről és egy beszállítótól való függőségünket a földgáz, mint energiahordozó tekintetében.

## *2.2. MAGYARORSZÁG KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁI*

Hazánk kommunikációs infrastruktúrája fejlett, számos olyan rendszerrel rendelkezik, amelyek világviszonylatban is korszerűnek mondhatóak. Ezen információs infrastruktúrák átszövik – interdependenciában vannak – számtalan egyéb, köztük kritikusnak is minősíthető infrastruktúrával.

A magyarországi kritikus információs infrastruktúrák közül jelen tanulmány a kommunikációs infrastruktúrákat (azon belül is a vészhelyzeti EDR rendszert, és a mobil kommunikáció rendszereket), valamint a hazai internetet mutatja be.

### 2.2.1. Kommunikációs infrastruktúra Magyarországon

Amennyiben a Magyarország esetében megvizsgáljuk a kritikus információs infrastruktúrák közé tartozó *távközlési és kommunikációs hálózatokat*, akkor ezeket az alábbi három nagy csoportra oszthatjuk:

- közcélú hálózatok;
- különcélú hálózatok;
- zártcélú hálózatok.

A *közcélú hálózatok* ma már alapvetően piaci alapokon nyugvó, liberalizált szolgáltatásokat és infrastruktúrákat jelentenek. E hálózatok fejlődési üteme követi a világ fejlődési tendenciáit. Ma már több vezetékes és mobil távközlési szolgáltató hálózata lefedi az ország egész területét. A szolgáltatók egyebek mellett vezetékes távközlési szolgáltatásokat, GSM, vagy UMTS szolgáltatásokat, VoIP lehetőségeket, különböző optikai illetve hagyományos hálózatokon szélessávú adatátviteli szolgáltatásokat, rádió és televízió műsorszórást biztosítanak.

A *különcélú hálózatok* valamely szervezet, vagy vállalat funkcionális feladatait támogatni, illetve irányítani hivatottak. Ilyen különcélú hálózat többek között a MÁV, a MOL, vagy az

MVM saját, vagy vállalkozásokban a részükre biztosított irányító, ellenőrző adat és távbeszélő hálózatai.

A *zártcélú hálózatok* körébe a védelmi, illetve a nemzetbiztonsági feladatokat ellátó szervezetek saját kommunikációs és adathálózatait sorolhatjuk. Ilyenek a Belügyminisztérium, az Országos Katasztrófavédelmi Főigazgatóság (OKF), vagy a Honvédelmi Minisztérium (HM) különböző hálózatai.

### *Az Egységes Digitális Rádiórendszer (EDR)*

Az 1990-es évek végére a készenléti szervek által használt URH diszpécser rendszerek már nem elégítették ki a készenléti feladatok ellátásához szükséges, egyre növekvő kommunikációs feladatokat. Ezek a rendszerek korszerűtlenek voltak, nem feleltek meg korunk kommunikációs rendszereivel szemben támasztott követelményeknek. Az alkalmazott URH rendszerek még az 1970-es években telepített infrastruktúrához nyúltak vissza, a felhasznált készülékek jelentős hányada rossz állapotban volt. A rendszerek műszaki megoldásai (analóg átviteli út) nem biztosítottak adatátvitelt, amelyre pedig egyre nagyobb igény jelentkezett. A készenléti kommunikációs rendszerek minőségi jellemzőit csak egy új, nagykapacitású és megbízható digitális rádiótávközlési rendszer bevezetésével lehetett növelni. [19]

A Magyar Kormány az 1031/2003. kormányhatározattal rendelte el a készenléti és a kormányzati felhasználói kör rádiókommunikációs igényeinek kielégítése céljából, a Schengeni Egyezmény követelményeinek megfelelő, és az Európai Távközlési Szabványosítási Intézet szabványa szerint működő egységes digitális rádiótávközlő rendszer kiépítését. 2005 októberében a Miniszterelnöki Hivatal EDR Kormánybiztosa és a T-Mobile Magyarország Rt. - Magyar Telekom Rt. konzorcium megkötötte az EDR létrehozására kiírt nyílt, kétfordulós, tárgyalásos közbeszerzési eljárás szerződését.

Az EDR-t a készenléti felhasználói kör a nem polgári célú frekvenciagazdálkodás feladatait ellátó hatóság-szervezetéről, valamint a nem polgári célú frekvenciagazdálkodás rendjéről

szóló 279/2001. kormányrendelet hatálya alá tartozó szervezetek, az Országos Mentőszolgálat, valamint az Országos Környezetvédelmi, Természetvédelmi és Vízügyi Főigazgatóság rádió távközlési igényeinek kielégítése céljából került kiépítésre.

A TETRA szabvány szerint épülő EDR jelentősen javítja az érintett szervek belső híradását, lehetővé teszi a szervek egymás közötti hatékony kommunikációját, ezzel nagymértékben hozzájárulva a reagáló képesség fokozásához, az együttműködés hatékonyságának növeléséhez.

A világon ma már közel ezer TETRA rendszer működik. A rádiórendszer szabványa európai uniós ajánlás, amelyet már számos európai országban alkalmaznak. Ennek megfelelően a szabvány alapján kialakított rendszer alkalmas arra, hogy a schengeni határokhoz tartozó országok rendvédelmi szerveinek együttműködését is támogassa.

A rendszert elsősorban a készenléti és kormányzati szervezetek (rendőrség, mentők, tűzoltóság, határőrség, stb.) speciális igényeihez tervezték. Ezt a célt szolgálják a TETRA szolgáltatásai és a rendszer többi jellemzője is.

A rendszer egyik legfontosabb funkciója a csoportkommunikáció, melynek során tetszőleges számú fél vehet részt csoporthívásban. A csoportok kialakítása számos előre beállítható paraméter figyelembevételével és dinamikus módon szabályozható. Emellett természetesen hagyományos hívások is kezdeményezhetőek. Az egyes felhasználókhoz vagy csoportokhoz egyéni jogosultságok és prioritások rendelhetők, amelyek megszabják, hogy ki milyen szolgáltatást vehet igénybe illetve, hogy hálózati csúcsterhelés esetén kinek legyen elsőbbsége a hívás lebonyolítására. A TETRA rendszerben, ha egy hívás lebonyolításához nincs elég kapacitás, a hívás nem bontódik, hanem várakozik a szabad kapacitásra.

A TETRA gyors hívásfelépítési időt (300 ms) biztosít, mely kritikus fontosságú lehet a készenléti szervek kommunikációjakor. A vészhívások segítségével a felhasználó minden körülmények között elérheti a hívott felet. A rendszeren átvitt információtartalom magas szintű védelmét biztosítja a titkosítás, akár a rádiós közegen, akár a teljes úton. A rendszer fontos követelménye a megbízhatóság kritikus és extrém körülmények között is. A biztonságot szol-

gálják a felhasználók jogosultság vizsgálatai, a különböző biztonsági és hitelesítési algoritmusok, a lehallgatás elleni védelem.

A közvetlen módú működés (DMO) lehetővé teszi a rádiósan nem lefedett területen történő kommunikációt. A hálózat szabványos interfészeken összekapcsolható más távközlő hálózatokkal, így telefonhívásokat indíthatunk akár GSM, akár vezetékes telefonokra.

A TETRA a beszédkommunikáción túl lehetőséget biztosít adatkommunikációra, valamint megoldott a két átviteli mód együttes használatba vétele is. Az SDS-nek (Short Data Service) négy típusa (adathossza) létezik. Az ún. státusz üzenetek – előre definiált szöveges üzenetek – speciálisan a készenléti szervezetek gyors és egyszerű információcsere igényeihez igazodnak. Az adatátvitel a kor igényeinek megfelelően általában IP alapú csomagkapcsolt technológiával történik. Az adatátvitel során 28,8 kbit/s adatsebesség érhető el.

Az alapszolgáltatásokon túl számos, a készenléti szervek igényeihez igazodó kiegészítő szolgáltatásra van lehetőség. Például a dinamikus csoportképzés lehetővé teszi a csoportok dinamikus létrehozását, vagy akár egy adott felhasználónak egy már létező hívásba való későbbi belépését. A rendszer többféle behallgatási funkciót biztosít. További kiegészítő szolgáltatások a hangrögzítés, a rövidített hívószám használat, a terület kiválasztás, és természetesen a hagyományos távbeszélő szolgáltatások, mint például a hívószámkijelzések, hívószám-korlátozások, hívásátirányítások, hívástartás, hívásvárakoztatás.

A hálózat a felhasználói igényeknek megfelelően rendkívül rugalmasan alakítható. A rendszeren virtuális magánhálózatok hozhatók létre, melyeken belül az egyes szervezetek teljes értékűen, és maximális biztonsággal kommunikálhatnak egymás zavarása nékül. Így az egyes felhasználói csoportok egyazon hálózati infrastruktúrát használva mégis teljesen különválasztva tudnak működni.

A rendszer szabvány szerint a 380-470 MHz-es frekvenciasávban működik, de vannak olyan változatai is, melyek a 800/900 MHz-es sávban üzemelnek. A Π/4 DQPSK moduláció és a TDMA hozzáférési rendszer, melyet a TETRA alkalmaz, számos előnnyel rendelkezik. A rendszer a frekvenciaspektrumot és a hálózat erőforrásait hatékony, gazdaságos módon hasz-

nálja ki. Mivel a rádiós interfész szabványosított, ezért több gyártó készülékeit is használni lehet azonos infrastruktúra alatt.

A TETRA fejlesztése folyamatos. A jelenleg alkalmazás alatt lévő TETRA Release 1 hálózatok mellett folyamatosan történik a TETRA Release 2 fejlesztése is, a TEDS (TETRA Enhanced Digital Service), illetve a TAPS (TETRA Advanced Packet Service) kidolgozásával. [20]

Az EDR magyarországi felhasználói között szerepel a Magyar Rendőrség, a Magyar Honvédség, az Országos Katasztrófavédelmi Főigazgatóság, a Nemzeti Adó- és Vámhivatal, a Büntetésvégrehajtás, az Országos Mentőszolgálat és az Országos Környezetvédelmi, Természetvédelmi és Vízügyi Főfelügyelőség, valamint a Nemzetbiztonsági Szolgálatok. [21]


2. kép. EADS THR 880i és TMR 880
Magyarországon alkalmazott TETRA rendszerű készülékek [22]

A gyakorlati felhasználás során a TETRA rendszer számos előnye mutatkozik meg a régi, analóg rendszerekkel szemben. A TETRA rendszer automatikusan gondoskodik a rádió forgalom információvédelméről. Nem csak a kommunikáció minősége, hanem biztonsága is sokkal magasabb szintű lesz azáltal, hogy az alapkódolás mellett további kódolási, titkosítási eljárások alkalmazása is lehetséges. A nagyobb frekvenciasáv miatt országos lefedettséget biztosít a

hálózat, még az eddig problémás vételi helyeken is (pl. metró, alagút). A beszéd mellett adatok, rövid státusz üzenetek átvitelére is alkalmasak a készülékek, melyek használatát számos programozási lehetőség tesz még egyszerűbbé. [23]

### *Kereskedelmi mobil kommunikáció Magyarországon*

Magyarországon a kereskedelmi mobiltelefon szolgáltatás 1990-ben jelent meg, akkor még analóg mobiltelefon rendszerrel. 1993-ra épült ki az első, akkor már digitális mobiltelefon rendszer, amely a GSM szabványt használta.

Az azóta eltelt időszak hatalmas fejlődést hozott a mobiltelefon szolgáltatásban, nemcsak technikai hanem társadalmi téren is. A vezetékes telefon előfizetések számának drasztikus csökkenése volt tapasztalható, hiszen a GSM szolgáltatás mellett egyre inkább megjelentek a már nem csak hangátvitelre, hanem adatátvitelre is használható szolgáltatások és rendszerek, mint pl. GPRS, EDGE, UMTS és LTE szabványú adatátvitel.

A 8. ábra bemutatja a mobiltelefon előfizetések számának növekedését, és összehasonlítást ad a vezetékes előfizetések számának változásáról is 2008-óta.

| Időszak | | Bekapcsolt vezetékes fővonalak száma, ezer | | Mobil-előfizetések száma, ezer | | 100 lakosra jutó | |
|---|---|---|---|---|---|---|---|
| | | összesen | ebből ISDN | összesen | ebből feltöltőkártyás | fővonalak száma | mobil-előfizetések száma |
| 2008.[a] | J–M | 3 247 | 574 | 11 232 | 6 966 | 32,3 | 111,9 |
| | Á–Jú | 3 207 | 574 | 11 540 | 7 163 | 32,0 | 115,0 |
| | Jl–Sz | 3 155 | 571 | 11 771 | 7 227 | 31,4 | 117,3 |
| | O–D | 3 115 | 559 | 12 224 | 7 486 | 31,1 | 121,9 |
| 2009.[b] | J–M | 3 114 | 545 | 12 112 | 7 314 | 31,1 | 120,9 |
| | Á–Jú | 3 112 | 533 | 11 889 | 7 039 | 31,1 | 118,7 |
| | Jl–Sz | 3 112 | 523 | 11 783 | 6 845 | 31,1 | 117,6 |
| | O–D | 3 110 | 504 | 11 792 | 6 681 | 31,1 | 117,8 |
| 2010.[c] | J–M | 2 987 | 492 | 11 883 | 6 680 | 29,9 | 118,7 |
| | Á–Jú | 2 972 | 485 | 11 866 | 6 587 | 29,7 | 118,6 |
| | Jl–Sz | 2 953 | 459 | 11 833 | 6 449 | 29,5 | 118,3 |
| | O–D | 2 933 | 452 | 12 012 | 6 465 | 29,4 | 120,3 |
| | J–D | 2 933 | 452 | 12 012 | 6 465 | 29,4 | 120,3 |
| 2011. | J–M | 2 914 | 443 | 11 893 | 6 292 | 29,2 | 119,2 |
| | Á–Jú | 2 886 | 435 | 11 704 | 6 018 | 29,0 | 117,4 |
| | Jl–Sz | 2 883 | 429 | 11 669 | 5 887 | 28,9 | 117,1 |
| | O–D | 2 909 | 421 | 11 690 | 5 798 | 29,2 | 117,3 |
| | J–D | 2 909 | 421 | 11 690 | 5 798 | 29,2 | 117,3 |
| 2012. | J–M | 2 891 | 412 | 11 634 | 5 725 | 29,0 | 116,9 |
| | Á–Jú | | | | | | |

8. ábra. A hazai mobiltelefon előfizetések számának alakulása 2008-tól [24]

Az ábrán is láthatjuk, hogy ma Magyarországon több mint 11,5 millió mobiltelefon előfizető van, azaz több mint hazánk lakosságának száma.

Hazánkban jelenleg három nagy mobilszolgáltató nyújt kereskedelmi mobiltelefon szolgáltatást: a T-Mobile, a Telenor, illetve a Vodafone. E három mellett várhatóan a közeljövőben kezdi meg működését a negyedik nagy szolgáltató az MPVI Mobil Zrt., amely a Magyar Posta Zrt., Magyar Villamosművek Zrt., MFB Invest Zrt. konzorciuma. [25]

A nagy mobilszolgáltatók mellett alternatív – úgynevezett virtuális szolgáltatók is megjelentek, mint például a Tesco Mobile, amely a Vodafone támogatásával, illetve annak bázisán nyújtja a szolgáltatását.

*A T-Mobile (Westel 900) története* [26]

1994. március 31-én 5,4 milliárd Ft alaptőkével indult a Westel 900 GSM Mobil Távközlési Rt. Ezt a tőkét 1997-re a tulajdonosok – MATÁV, Westel Rádiótelefon Kft és a US West – több mint 10 milliárdra emelték. A vállalat 1996 végére elnyerte az ISO 9001 minősítést.

A Westel technikai berendezéseit az Ericsson szállította. 1997-re 5 milliárd forintos hálózatfejlesztést hajtottak végre. A Westel szolgáltatásaival már az indulás évében lefedte az egy számjegyű főutakat, a megyeszékhelyeket, valamint a kisebb településeket.

1996 végére a szolgáltatások az ország 90 százalékán voltak elérhetőek. Az előfizetők száma meghaladta a 200 ezret.

2000-ben a Westel a WAP-szolgáltatást, március elején pedig az internetes online ügyfélszolgálatot indította be elsőként az országban. Az év végére közel 97 %-os lefedettség mellett, több mint 1,6 millió előfizetője volt a társaságnak.

2002-ben a cég a világon elsőként indított MMS (Multimedia Messaging Service) küldési szolgáltatást. Bevezették a GPRS szolgáltatást.

2004. május 3-tól a Westel 900 új neve T-Mobile Magyarország Távközlési Részvénytársaság lett.

2007-ben indították ez első mobiltelefonos televízió sugárzást.

A cég folyamatos technikai fejlesztéseket végez, ma már elérhető a 4g/LTE mobilinternet szolgáltatása is. A cégnek jelenleg több mint 4,5 millió előfizetője van.

*A Telenor (Pannon GSM) története* [27] [28]

1994. március 26-án indították kereskedelmi tevékenységüket Pannon GSM néven, 10,45 milliárd Ft alaptőkével. Tulajdonosai az északi országokból kerültek ki 25% magyar tulajdon mellett. A társaság finanszírozását a holland ING Bank végezte. A technikai hátteret a finn Nokia biztosította. A kezdeti 10,45 milliárd forint alaptőkét folyamatosan emelték 18 milliárdra, közben az előbb említett ING Bank nyújtott kedvező hiteleket.

Eleinte Budapest és környékére, majd a főutakra, vidéki nagyvárosokra terjesztették ki szolgáltatásaikat. Kezdetben műszakilag próbáltak a vetélytárs elébe kerülni, sokféle szolgáltatást vezettek be.

1995 márciusában a cég Magyarországon elsőként indított rövid szöveges üzenetküldés szolgáltatást, PannonHívó néven.

1996-ban beindult a konferenciahívás szolgáltatás. Megújult a hangposta-szolgáltatás: a Privát hangpostát a szolgáltató minden előfizetőjének díjmentesen a rendelkezésére bocsátotta. Székesfehérváron felavatták a Pannon GSM Rt. harmadik kapcsolóközpontját, valamint megkezdte működését a 4. kapcsolóközpont Szolnokon. 1996 decemberére az ország 99 %-át lefedi a szolgáltatásával. A Pannon GSM előfizetőinek száma az 1995-ös év végi adatokhoz képest több mint kétszeresére, 170 ezerre emelkedett. Négy kapcsolóközpont, 501 bázisállomás, 10 területi képviselet és több mint 500 Pannonos dolgozó biztosította az országos szolgáltatást.

1997-ben az előfizetői száma 260 ezerre emelkedett. A kapcsolóközpontok száma 7, a bázisállomások száma 664, a területi képviseletek száma 14 volt.

2000-re a Pannon GSM előfizetőinek száma meghaladta az 1,2 milliót. Országszerte több mint 1000 Pannon GSM bázisállomás működött, ebből 2000-ben 216-ot helyeztek üzembe.

Az év folyamán átadásra került egy mobil kapcsolóközpont, melyek száma így 10-re növekedett.

2002 januárjától a Pannon GSM részvényei 100%-ban a norvég Telenor távközlési vállalat tulajdonába kerültek.

A hangalapú szolgáltatások mellett egyre több teret kap az adat alapú kommunikáció, a mobilinternet szolgáltatás felfutó ágban e vállalt vonatkozásában is.

2006-ban aculatváltás következett be: bevezették az anyavállalata, a Telenor nemzetközi szinten is használt logóját. 2010 májusában a vállalat felvette a Telenor nevet. Előfizetőinek száma meghaladja a 3,6 milliót.

*A Vodafone története* [29] [30]

A Vodafone 1985. január 1-jén bonyolította le az első mobil hívást Nagy-Britanniában. Tizenöt év elteltével a hálózat a legnagyobb európai vállalattá, és világszerte a maga nemében az egyik legnagyobb céggé nőtte ki magát. A század fordulóján az Egyesült Királyság csaknem minden második lakosának volt mobiltelefonja - közülük minden harmadik a Vodafone ügyfele.

A Vodafone Magyarország Rt. 1999. július 7-én nyerte el a koncessziót magyarországi GSM 900/DCS 1800 mobil rádiótelefon hálózat kiépítésére. A Vodafone 150 millió euró értékű szerződést írt alá a Nokiával, a teljes 1800 MHz-es GSM-hálózat kiépítésére. A Nokia valósítja meg Vodafone magas szintű szolgáltatásához szükséges telefonközpontokat, bázisállomásokat, bázisállomás-kontrollereket és intelligens hálózati (IN) megoldásokat. Az együttműködés első szakaszában a Nokia közel 900 bázisállomást épített a cég számára, amely 2001 év végéig 1200-ra növekedett.

Még 1999 októberében aláírták a koncessziós szerződést. A szerződés értelmében a vállalat 15 éven keresztül jogosult a 900 és 1800 MHz-es frekvenciatartományban mobiltelefon szolgáltatást nyújtani magyarországi ügyfeleinek. Ezzel négyre nőtt a hazai mobiltelefon-

szolgáltatók száma. A hivatalosan Vodafone Magyarország Mobil Távközlési Részvénytársaság néven bejegyzett vállalat bejelentette, hogy VODAFONE márkanéven vezeti be szolgáltatását.

2001 szeptemberében a Vodafone megnyitotta új Hálózatfelügyeleti Központját, a Network Management Centert (NMC). A központ feladata a Vodafone hálózatának a nap 24 órájában, a hét 7 napján, történő nyomon követése és a fellépő rendellenességek azonnali kijavítása. Ide újonnan építettek be egy intelligens video falat, amely azt a célt szolgálja, hogy a hibákat nagyon rövid idő alatt be tudják határolni, és azokat gyorsan kijavítsák. Az ügyfélközpontú munka további elősegítésének érdekében Call Centert, valamint a legmodernebb technikát felhasználó tesztlabort üzemeltetnek a Hálózatfelügyeleti Központban.

2002-re a Vodafone előfizetők száma elérte az 500 ezret, amely 2003 májusára már meghaladta az 1 milliót.

2004 decemberében a szolgáltató megvásárolja a harmadik 3G licencet. Ezzel a Vodafone Magyarország Rt. jogosultságot szerzett a magyarországi UMTS tendert kiíró Nemzeti Hírközlési Hatóságtól a harmadik, úgynevezett B frekvenciablokk 15 éves használatára. A Vodafone Magyarország Rt. a licencért részben az UMTS árbevétel mértékétől függően, de összesen legkevesebb 16,5 milliárd forintot fizet majd az engedély teljes időtartama alatt. A 3G szolgáltatást 2005 decemberében indították be.

2007-ben a vállalat elindította a 3,5G szélessávú mobilinternetes szolgáltatását, amelynek maximális letöltési sebessége 1,8 Mb/s, feltöltési sebessége 384 kb/s volt.

2009-ben a Vodafone elsőként a hazai piacon, minden eddiginél nagyobb letöltési sebességet – 21 Mb/s – letöltési tesztet mutatott be.

### 2.2.2. Internet Magyarországon

Az IIF (Információs Infrastruktúra Fejlesztési) program 1985-ben indult, a SZTAKI (Számítástechnikai Automatizálási Kutató Intézet) akkori főigazgatója, Vámos Tibor akadémikus ötlete alapján. Az IIF a magyarországi kutatás-felsőoktatás-közgyűjtemények számítógép-hálózati hátterének megvalósítását tűzte ki alapvető céljaként.

Komoly kihívást jelentett ez a terv abban az időben, hiszen a minden hálózati termék szigorú embargó alá esett, azaz a fejlett nyugati technológiákat nem lehetett a keleti blokk (Szovjetunió és szövetségesei) számára eladni. Az embargóval sújtott termékek és technológiákat az úgynevezett COCOM[11] listák tartalmazták. [31]

Mivel 1988-tól az USA engedélyezte Európa számára is az internet technológiákat, így megkezdődhetett a kísérleti internet kapcsolatok felépítése, a név – domain name – szolgáltatás biztosítása és az internet címzések használata az elektronikus levelezésben. A MATÁV[12] korszerűbb, import csomagkapcsoló központokat szerezhetett be, melyekkel az adathálózat minőségét, teljesítményét és a szolgáltatások körét bővíthették. 1992-re a csomópontokba Unix-os szerverek (host computers) kerültek. Ezekhez alapértelmezés szerint tartozik a TCP/IP protokoll és a névszolgáltató szoftverrendszer. Elindult a HBONE (országos, bérelt vonalas, IP-protokollt alkalmazó gerinchálózat) ki-alakítása. Fontos cél volt, hogy a HBONE és a nagy nemzetközi hálózatok megbízható, nagy kapacitású vonalakkal való összekapcsolása is. [31]

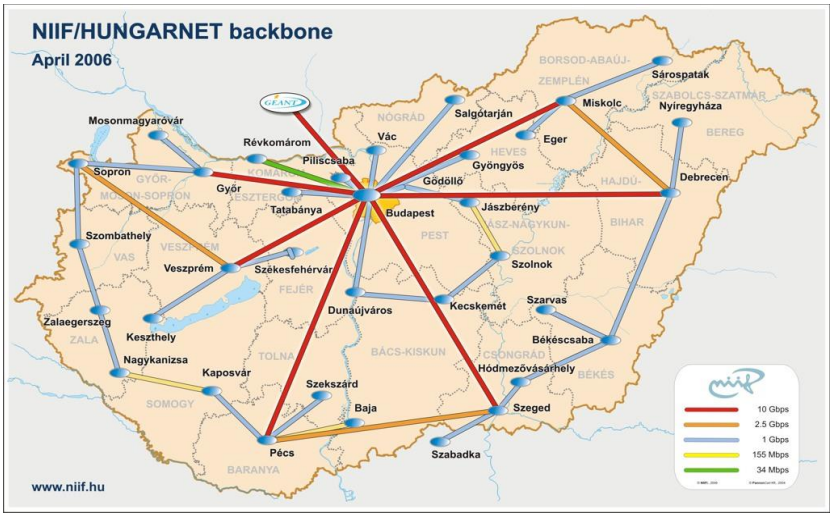
A HBONE különcélú (távközlő) hálózat. A HBONE a robusztus MAG-ból, valamint a MAG routereihez (közvetlenül vagy közvetve) kapcsolódó regionális központi routerekből áll,

[11] COCOM: Coordinating Committee for Multilateral Export Controls, azaz magyarul: Többoldalú Exportellenőrzési Koordináló Bizottság. Az akkori NATO tagállamok (Spanyolország és Izland kivételével) és Japán részvételével működő bizottság, székhelye Párizs volt. A bizottságot 1950-ben hozták létre. Ellenőrzésével megakadályozták egyes termékek, főként katonai felszerelések, fejlett technikájú műszaki berendezések, pl. számítástechnikai, híradástechnikai, navigációs stb. exportját a (volt) szocialista országokba. A bizottság ellenőrzése alá vont termékeket az ún. COCOM listák tartalmazták. [32]

[12] Magyar Távközlési Rt., napjainkban a vállalat neve Magyar Telekom.

beleértve az összekötő adatvonalakat is. A HBONE gerinc fő vidéki és budapesti vonalai valamint nemzetközi kapcsolatai gigabites sávszélességűek. A vidéki és nemzetközi gigabites kapcsolatok a legkorszerűbb DWDM[13] technológiára épülnek, melyet a HBONE alkalmazott legelsőként Magyarországon.

Kezdetben a HBONE csak három budapesti tudományos kutatásokat folytató intézetben lévő csomópontból (router-ből), és az azokat összekötő nagysebességű mikrohullámú kapcsolatokból, illetve a MATÁV Budapesten, a Városház utcai központjában lévő csomagkapcsoló központjából állt. Napjainkban a HBONE a budapesti magból és a több mint 20 helyen elhelyezett csomópontokból áll. Ma már a HBONE szolgálja ki a hazai felsőoktatást, kutatás-fejlesztést, könyvtárakat és közgyűjteményeket, egy átjárón keresztül számos kormányzati szervet, valamint jó néhány egyéb közintézményt is. [31] [34]




9. ábra. A HBONE Gerinchálózati topológia
(csak a nagy sávszélességű, hazai távolsági kapcsolatok kerültek feltüntetésre) [34]

[13] DWDM: Dense Wavelength Division Multiplexing — nagysűrűségű hullámhossz multiplexá-lás. Olyan hullámhossz multiplexáláson alapuló átviteli technológia, mely lehetővé teszi, hogy 8-tól akár 40-ig terjedő különböző frekvencián továbbítsunk információt az optikai kábelen keresztül. A DWDM technológia alkalmas arra, hogy SDH rendszerek átvitelét is ellássa, vagy azokat helyettesítse. [33]

Az IIF Program öt eredményes év – a hazai kutatói hálózat alapjainak megteremtése – után a 90-es évek elejétől már valamennyi érintett minisztérium és az OTKA (Országos Tudományos Kutatási Alap) támogató részvételével NIIF (Nemzeti Információs Infrastruktúra Fejlesztési) Programként folytatódott. [35]

A Nemzeti Információs Infrastruktúra Fejlesztési (NIIF) Program a magyarországi kutatói hálózat fejlesztésének és működtetésének programja. A Program a teljes magyarországi kutatási, felsőoktatási és közgyűjteményi közösség számára biztosít:

- integrált országos számítógép-hálózati infrastruktúrát;
- kommunikációs, információs és kooperációs szolgáltatásokat;
- élvonalbeli alkalmazási környezetet;
- tartalom-generálási, illetve tartalom-elérési hátteret.

A Program központi költségvetési támogatásra támaszkodik. A fejlesztési és működtetési feladatokat az NIIF Intézet (NIIFI) fogja össze, a Program Tanács irányítása és a Műszaki Tanács szakmai közreműködése mellett. A Program szorosan együttműködik a felhasználói közösséget tömörítő Hungarnet Egyesülettel.[14]

Az NIIF Program – a nemzetközi gyakorlatnak megfelelően – egyúttal élvonalbeli szerepet tölt be a legújabb hálózati technológiák magyarországi fejlesztésében és alkalmazásában is. Így a program meghatározó szerepet játszik az informatika országos fejlődésében. Korszerű, versenyképes infrastruktúrát és szolgáltatásokat biztosít a felsőoktatás és a kutatás számára, de egyúttal követendő példával is szolgál az országszerte folyó informatikai fejlesztésekhez. [36]

[14] A HUNGARNET Egyesület feladata a Nemzeti Információs Infrastruktúra Fejlesztési Program (NIIF) alkalmazói körébe tartozó felső-, és középfokú oktatási intézmények, akadémiai és más kutatóintézetek, közgyűjtemények (könyvtárak, levéltárak, múzeumok) társadalmi szervezeteként képviselni ezen intézmények információs infrastuktúrájának és országos számítógépes szolgáltatásainak összehangolt fejlesztését hazai és nemzetközi szervezetekben. Az Nemzeti Információs Infrastruktúra Fejlesztési Iroda (NIIFI) által létrehozott és üzemeltetett magyar kutatói, felsőoktatási és közgyűjteményi hálózatot (NIIF Hálózat) illetve az üzemeltető szervezetet (NIIFI) gyakran nevezik HUNGARNET-nek, különösen nemzetközi fórumokon. Pontosabb azonban az NIIF Hálózat ill. NIIF Iroda elnevezések használata. [39]

A Kormány 2003 decemberében fogadta el az Elektronikus Kormányzat Stratégia és Programtervet[15] (E-kormányzat stratégia). A Stratégiában meghatározott e-kormányzati programok és feladatok túlnyomó többsége 2006 végére teljesült. [37] [38]

Az E-kormányzat stratégia megvalósítása érdekében a Kormányzati Informatikai és Társadalmi Kapcsolatok Hivatala (KITKH), majd az **Elektronikuskormányzat-központ (EKK)** összkormányzati koordinációs tevékenységét a Kormányzati Informatikai Egyeztető Tárcaközi Bizottság (KIETB) segítette. A KIETB az 1991-ben létrehozott Informatikai Tárcaközi Bizottság (ITB) jogutódja. Tagjai a fejezeti jogkörű költségvetési szerveknek az informatika ágazati stratégiájának kidolgozásáért és végrehajtásáért felelős vezetői. A KIETB működését a 1054/2004 (VI. 3.) Korm. határozat szabályozta.

Mind a KIETB, mind az EKOB eredményesen látta el feladatait. A kibővült, valamint megváltozott feladatok figyelembe vételével, a koordinálás egyszerűsítése és átláthatóbbá tétele érdekében előkészítés alatt áll a két korábbi bizottság feladatait átvevő, új Közigazgatási Informatikai Bizottság létrehozása.

Az elektronikus közigazgatás megvalósításának alapját a **Központi Elektronikus Szolgáltató Rendszer** (Központi Rendszer) biztosítja, amely magába foglalja az **Elektronikus Kormányzati Gerinchálózatot (EKG)**, a **kormányzati portált**, a **kormányzati ügyféltájékoztató központot**, az ott megjelenő szolgáltatásokat és ügyintézési lehetőségeket, valamint azok fenntartóit és üzemeltetőit, továbbá biztosítja az ügyfelek számára az **elektronikus ügyfélkapu** létesítésének lehetőségét.

Az elektronikus kormányzás alapinfrastruktúráját a 1122/2001 (XI. 22.) Korm. határozatban megfogalmazottaknak megfelelően létrehozott Elektronikus Kormányzati Gerinchálózat (EKG) képezi.

Az EKG egy olyan informatikai hálózat, amelynek feladata, hogy a kormányzati és közigazgatási adatbázisokat, hálózatokat és informatikai rendszereket összekapcsolja a vonatkozó

[15] 1126/2003. (XII. 12.) Korm. határozat

kormányrendeletben meghatározott kormányzati körnek, - valamint a különböző kormányzati szolgáltatások elérhetőségét biztosítsa a civil szféra számára.

A kormányzati hálózat megvalósításának gondolata, az európai folyamatokkal összhangban, – már több programban megfogalmazódott, mielőtt 2000-ben kormányhatározat formájában is testet öltött.

Az EKG infrastruktúrájának megteremtésével válik lehetővé a kormányzati rendszerek elektronizálása és új, hatékony, távolról is elérhető szolgáltatási rendszerek bevezetése, egyszóval az e-kormányzat kialakítása. Ezek a szolgáltatások jelentősen közelítik egymáshoz az igazgatási munkát és a civil szférát, erőteljesen lecsökkentve az ügyintézéshez szükséges időt, nyílttá, átláthatóvá teszik a közszféra munkáját.

Az EKG célja és rendeltetése [40]:

1. Nagy sebességű, nagy üzembiztosságú és magas biztonsági követelményeknek megfelelő, egységes architektúrájú hálózati infrastruktúra biztosítása a civil szféra számára az állami intézmények által nyújtott szolgáltatások eléréséhez (Front-Office feladatok).
2. Az új infrastruktúrára épülő szolgáltatások és egyes eddig elszigetelt (pl. ágazati) hálózatok elérhetővé tétele a jogosult felhasználók számára (Back-Office feladatok).
3. A kormányzati szervek közötti kommunikáció, az adatátvitel költségeinek csökkentése, minőségi szintjének emelése.
4. Kormányzati szintű, több felhasználó által használt alkalmazások hatékony működtetése.
5. Olyan infrastrukturális háttér biztosítása, amely alkalmas az elektronikus ügyvitel és ügyintézés feltételeinek megteremtésére, a jövőbeli elektronikus közigazgatás koncepciójának, vagyis az állampolgár és a kormányzat újszerű kapcsolatának kiszolgálására.
6. A kétirányú kormányzati kapcsolatok biztosítása a brüsszeli adminisztráció rendszereihez (csak az EKG-n keresztül lehetséges).
7. A minisztériumok és a központi intézmények részére biztosítson védett, – security, – szolgáltatások nyújtása és elérése.

Az EKG fő célkitűzése, hogy a széttagolt, gyakran nem megfelelő kapacitású és biztonságú hálózatokat egy olyan nagy sávszélességű, üzembiztos, országos elérhetőséget biztosító és egységes gerinchálózat váltsa fel, amelyen különös figyelmet kap a hálózaton elérhető szolgáltatások üzembiztonsága. A gerinchálón minden intézmény kapcsolatrendszere önálló magánhálózatként kerül kialakításra a közös infrastruktúrán, ezzel is tovább növelve a biztonságot.

Az EKG hálózata – Magyarország EU-hoz való csatlakozásának előkészítését szolgálva – már 2004 februárjában kapcsolódott az Európai Unió TESTA hálózatához. A TESTA egy zárt, internettől független gerinchálózat, amely az Európai Unió adminisztrációja és a tagországok kormányzatai közötti információcserét teszi lehetővé.

A TESTA – az EU informatikai hálózata – a központi alkalmazások elérését biztosítja a tagországok számára. Az Európai Bizottság közigazgatási intézményeinek elektronikai adatcseréjét szolgáló összefüggő szektoriális hálózatok rendszere. Magyarországon az intézmények jelenleg a TESTA hat alkalmazását használják:

1. A menedékjogi kérelmek elbírálására illetékes hatóságok közötti információcserét biztosító kapcsolattartó rendszer (DUBLINET).
2. Export/import engedélyek kezelésének integrált rendszere (SIGL).
3. A menedékkérők és illegális emigránsok ujjlenyomatának nyilvántartását és összehasonlítását végző rendszer (EURODAC).
4. Polgári védelmi és környezeti katasztrófahelyzetek európai hálózata(i) (PROCIV-NET).
5. Újfajta élelmiszerek és élelmiszer-összetevők hálózata (NF-NET).
6. Európai Közúti Balesetek Adatbázis (CARE2).

Az IDA programoknak köszönhetően az elérhető alkalmazások ugrásszerű növekedése várható.

A kormányzati informatikai rendszerek üzemeltetésére a Miniszterelnöki Hivatal a Kopint-Datorg Rt.-vel kötött üzemeltetési megállapodást. A Kopint Datorg Rt munkatársai napi 24 órás rendszerfelügyeletet, intézménytámogatást és hibaelhárítást biztosítanak az infrastruktúra

felhasználóinak. Az EKG üzemeltetésével megbízott Kopint-Datorg Rt. a proaktív EKG HelpDesk támogatás mellett – jelentős szakmai segítséget is nyújt az intézményi hálózatüzemeltetés számára is.

A 2005. április 1-jétől igénybe vehető Ügyfélkapu biztosítja, hogy az ügyfél egyedileg azonosított módon biztonságosan léphessen kapcsolatba a központi rendszer útján az elektronikus ügyintézést, illetve elektronikus szolgáltatást nyújtó szervekkel.

KERESKEDELMI INTERNET

Ma már több mint 200 szolgáltató biztosít internet hozzáférést Magyarországon. Ezek közül számos saját kiépített országos hálózattal rendelkezik.

A különböző hazai internetszolgáltatók nemzetközi irányú kapcsolatainak koordinálását a BIX (Budapest Internet Exchange) szervezet végzi. A BIX alapvető célja, hogy a különböző szolgáltatók közötti magyarországi és regionális internet forgalom ne terhelje az internet szolgáltatók nemzetközi irányú kapcsolatait,[16] valamint, hogy platformot biztosítson a szolgáltatói hálózatok IP alapú összekapcsolásához.

A BIX egy földrajzilag is elosztott hálózati rendszer, amely BIX szolgáltatási pontokból és az azokat összekötő adatátviteli kapcsolatokból áll. A BIX szolgáltatók üzemeltetik a BIX szolgáltatási pontokat és fenntartják az azok közötti adatátviteli kapcsolatokat. A BIX szolgáltatási pontokon csatlakozhatnak saját hálózatukkal a BIX felhasználói, a BIX tagok. BIX szolgáltatási pont csak az lehet, amely legalább egy 1 Gb/s (full duplex) sebességű elsődleges és egy legalább 1Gb/s (full duplex) kapacitású tartalék közvetlen 2. szintű kapcsolattal rendelkezik a budapesti BIX szolgáltatási ponthoz, illetve a tartalék kapcsolat esetében tetszőleges másik BIX szolgáltatási ponthoz. [41]

A legtöbb hazai internet szolgáltató tagja az Internet Szolgáltatók Tanácsának (ITSZ). Az ITSZ magyarországi internet szolgáltatók szakmai koordinációs és érdekvédelmi képviselete, amely külön figyelmet fordít a .hu TLD adminisztráció szabályozására. Ennek keretében – az

[16] Nemzetközi irányú egy kapcsolat, ha azon Magyarországról az internet valamely root name szervere elérhető

egyesületi formában működő szervezet – alapvetően koordinációs és tájékoztatási, valamint tudományos-technikai célokat szolgál belföldön és külföldön egyaránt. [42]

Magyarországon jelenleg több mint 4,5 millió internet előfizetés van. Ezek közül az elmúlt években szembetűnő a mobilinternetes előfizetések számának növekedése.

| Az időszak végén | | Kapcsolt vonalon (modem segítségével, dial-up) + ISDN | xDSL | Kábel-tv | Vezeték nélküli[a] | ebből: mobilinternet | Egyéb pl. LAN, bérelt vonal[b] | Összesen |
|---|---|---|---|---|---|---|---|---|
| 2008. | J–M | 31 209 | 788 282 | 635 934 | 500 041 | 399 550 | 46 674 | 2 002 140 |
| | Á–Jú | 28 000 | 799 057 | 663 380 | 543 901 | 439 577 | 52 583 | 2 086 921 |
| | Jl–Sz | 25 534 | 805 768 | 692 663 | 604 318 | 497 660 | 54 273 | 2 182 556 |
| | O–D | 24 742 | 806 569 | 718 060 | 678 123 | 570 835 | 83 420 | 2 310 914 |
| 2009. | J–M | 24 290 | 806 986 | 738 152 | 644 746 | 541 866[c] | 101 192 | 2 315 366 |
| | Á–Jú | 23 098 | 805 327 | 746 598 | 738 039 | 635 950 | 117 851 | 2 430 913 |
| | Jl–Sz | 22 749 | 801 486 | 765 358 | 871 602 | 767 056 | 137 655 | 2 598 850 |
| | O–D | 22 403 | 800 013 | 782 430 | 1 036 898 | 933 000 | 161 799 | 2 803 543 |
| 2010. | J–M | 17 809 | 793 152 | 819 672 | 1 072 353 | 968 940 | 188 601 | 2 891 587 |
| | Á–Jú | 17 151 | 789 817 | 825 442 | 1 137 879 | 1 036 748 | 205 976 | 2 976 265 |
| | Jl–Sz | 15 300 | 781 892 | 866 580 | 1 274 961 | 1 174 976 | 211 392 | 3 150 125 |
| | O–D | 15 137 | 789 657 | 893 177 | 1 407 039 | 1 306 912 | 236 454 | 3 341 464 |
| 2011. | J–M | 14 667 | 783 676 | 913 977 | 1 495 333 | 1 394 262 | 251 887 | 3 459 540 |
| | Á–Jú | 13 919 | 799 045 | 929 948 | 1 665 090 | 1 561 332 | 260 577 | 3 668 579 |
| | Jl–Sz | 13 786 | 798 160 | 948 591 | 1 970 874 | 1 872 178 | 272 558 | 4 003 969 |
| | O–D | 13 527 | 801 165 | 970 499 | 2 254 948 | 2 154 842 | 292 386 | 4 332 525 |
| 2012. | J–M | 12 888 | 798 092 | 989 705 | 2 443 846 | 2 342 018 | 307 821 | 4 552 352 |
| | Á–Jú | | | | | | | |

10. ábra. A hazai internet előfizetések számának alakulása 2008-tól. [43]

# III. fejezet
# KRITIKUS INFRASTRUKTÚRÁK ÉS A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK ELLENI FENYEGETETTSÉGEK, TÁMADÁSOK

Az információs társadalom kritikus információs infrastruktúráit napjainkban számtalan veszély fenyegeti. Amennyiben szeretnénk ezeket kategorizálni, vagy egyáltalán csak felvázolni és csoportosítani, akkor általánosságban a következő olyan veszélytípusokat tudjuk megkülönböztetni, amelyek közvetlenül vagy közvetve fenyegetést jelenthetnek a kritikus információs infrastruktúra egészére vagy annak egyes elemeire:

- természeti katasztrófák:
    - vízkárok (közművek sérülése, árvíz, belvíz);
    - geológiai katasztrófák (földrengés, talajsüllyedés);
    - meteorológiai jellegű károk (rendkívüli erejű vihar, villámcsapás).
- civilizációs, ipari katasztrófák:
    - nukleáris balesetek (erőművi balesetek);
    - veszélyes anyagok kikerülése (gyárak, üzemek, raktárak szállítójárművek sérülése, robbanások);
    - közlekedési balesetek (közúti, vasúti jármű, repülőgép véletlen vagy szándékos becsapódása).
- fegyveres konfliktusok:
    - háborúk;
    - fegyveres csoportok támadása;
    - belső fegyveres konfliktusok, polgárháborúk, sztrájk.

- terrorizmus:
    - robbantások, támadások (állami intézmények, távvezetékek, hírközpontok, adók, légiforgalmi létesítmények, Internet szolgáltatók stb. ellen);
    - a fenti rendszereket üzemeltető kulcsfontosságú személyek kiiktatása;
    - bűnözés (adatok erőszakkal való megsemmisítése, megszerzése, irányítórendszerek befolyásolása, megbénítása).
- információ alapú támadások. [2]

Mint látható, a kritikus információs infrastruktúrák elleni támadások igen szerteágazóak lehetnek. E tanulmány keretei között nem foglakozunk a különböző természeti eredetű veszélyekkel, ipari katasztrófákkal, stb. A kutatás témájából adódóan vizsgálatunk tárgya elsősorban az információs jellegű, információalapú fenyegetések köré csoportosul.

## *3.1. Az információs társadalom infrastruktúrái működésének korlátozása*

Az előző fejezetben kifejtettük, hogy az információs társadalom kiépítését alapvetően a megfelelő színvonalú információs technológia teszi lehetővé. Korszerű információtechnológiára épülő információs infrastruktúrák nélkül az információs társadalom működésképtelen. De abban az esetben is működésképtelen, illetve működési zavarokkal küszködhet, ha e rendszereket valamilyen ártó szándékú behatás éri. Ezért amellett, hogy e rendszereket működtetjük, szavatolni kell megbízható működésüket is.

Az információs társadalom nagyon fejlett, nagyon hatékony társadalom, ugyanakkor meglehetősen sebezhető is. Sebezhetőségének alapját az adja, hogy működése szorosan kapcsolódik a globális, nemzeti, regionális és lokális információs környezethez. Ennek következtében igen erősen függ az információs környezet fejlett, ám erősen korlátozható, vagy sebezhető

integrált információs infrastruktúráitól, mint pl. a távközlési hálózatoktól és a számítógép-hálózatoktól.

Az információs társadalom hatalmas teljesítményekre képes a tudomány, a termelés, az információcsere és a távolból intézhető ügyek területén. Ugyanakkor ennek a jelentős teljesítménynek vannak árnyoldalai is, amelyek üzemzavarból, szándékos rongálásból, károkozásból vagy pusztításból eredhetnek.

Az infokommunikációs hálózatok célpontjai is és egyben eszközei is mind a nemzetközi terrorizmusnak, mind az elektronikus bűnözésnek. Az információs infrastruktúrák elleni **komplex információs támadások**, mint az információs hadviselés, információs műveletek a katonai, gazdasági, politikai célú érdekérvényesítés új, komplex formájává váltak. Az információs társadalom ezen árnyoldalát már számos fejlett országban felismerték, és komolyan elemezték, vizsgálták, hogy mi történik abban az esetben, ha valamilyen ártó szándékú szervezet fizikai, vagy információs csapást mér a társadalom működtetéséért felelős kritikus információs infrastruktúrákra. Több szimulációs gyakorlaton különböző fajtájú információs és fizikai támadásokat intéztek az integrált infokommunikációs rendszerek ellen, és azt vizsgálták, hogy a támadás következtében azok milyen károkat szenvedhetnek el. Szinte mindegyik gyakorlat végső konklúziója az volt, hogy ilyen típusú támadásokkal egy hálózatilag fejlett ország társadalmi, politikai, gazdasági és védelmi rendszere erősen befolyásolható, korlátozható. A komplex információs támadások következtében az ország vezetése, tőzsdei és bankrendszere, pénzügyi élete, földi, légi, tengeri közlekedése, energiahordozó- és ellátó rendszerei, élelmiszerellátása stb. megbénulnak vagy erősen akadoznak. Az egészségügyi ellátás leáll, a közbiztonság felbomlik, az addigi szervezett rend káosszá változik. [3]

Egy ország információs infrastruktúráin keresztüli sebezhetőségét a katonai vezetők is felismerték. Az első és második Öböl-háború illetve a boszniai és afganisztáni harci tapasztalatok azt bizonyítják, hogy az információs műveleteken belüli komplex információs támadásokkal jelentős mértékben tudták támogatni a harcoló erőket. Az ellenség információs rend-

szereinek és ellátó infrastruktúráinak információs támadásával jelentős mértékben csökkent az ellenség vezetésének hatékonysága és eredményessége.

Az információs infrastruktúrák, infokommunikációs rendszerek elleni támadások a hatásalapú műveletek keretében zajlottak. A katonai műveletekben alkalmazott hatásalapú megközelítés elve szerint a műveleti területen egymással hálózatba kapcsolt objektumok, központok találhatók, amelyek egymással alá- és fölérendeltségi viszonyban állnak. Ez lehetőséget nyújt arra, hogy egy kiválasztott központ és a benne található nagyfontosságú célpontok elleni támadás különböző hatásokat eredményezzen a többi, hozzájuk kapcsolódó központ, objektum működésében is. Mindez igaz a polgári létesítményekre, infrastruktúrákra is, amelyek – az információs társadalom alapelvéből fakadóan – az infokommunikációs hálózatokon keresztül szintén szoros kapcsolatban állnak egymással. Tehát bármely fontos, kritikus információs infrastruktúra illetve annak eleme elleni információs vagy fizikai támadás további működésbeli korlátokat idézhet elő a többi, hozzá kapcsolódó infrastruktúrában, rendszerben is.

A leírtak alapján tehát megállapítható, hogy 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. [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 világgazdasági-, 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 hálózatok-

kal átszőtt világában a World Trade Center összeomlása a teljes globális gazdasági rendszert sokkolta.

Az új típusú társadalom számos pozitív tulajdonságai mellett tehát újfajta kihívásokat, veszélyforrásokat is tartogat számunkra, melyeket folyamatosan szem előtt kell tartanunk. E veszélyeztetés azonban nem csupán az informatikai rendszerekben jelentkezik. 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 az információs fenyegetést, illetve fenyegetettséget vizsgáljuk, 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, vállalatok, 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.

Gondoljunk bele, hogy mi történne, ha valamilyen ártó szándékú csoport, esetleg terrorszervezet fizikai, vagy elektronikai támadást (esetleg támadás sorozatot) intézne az információs társadalom egy vagy több kritikus (információs) 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 modern katonai elméletek hatásalapú megközelítési elve 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 infokommunikációs hálózatok közötti interdependencia következtében 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). Ez azt is jelenti, hogy pl. a távközlési rendszer lehallgatását, zavarását vagy egy szenzorhálózat működésének korlátozását ugyanolyan komolyan kell venni, mint a számítógép-hálózatokban megjelenő különböző támadásokat.

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.

Az információs társadalomban fokozott erőfeszítések zajlanak az információ megszerzéséért, birtoklásáért, illetve a minél hatékonyabb felhasználásáért. Ebben a kérdésben sokan odáig merészkednek, hogy adott esetben illegális információszerző vagy információs támadási módszereket sem tartanak elképzelhetetlennek alkalmazni, annak érdekében, hogy a saját rendszerük működése még hatékonyabb legyen. A legegyszerűbb példa erre, az ipari kémkedés, amikor olyan kutatás-fejlesztési és gyártási adatokhoz, információkhoz jutnak, amelyet felhasználva korábban tudnak különböző termékeket piacra dobni, és ez által jelentős előnyre és profitra szert tenni a versenytársakkal szemben. Ez a fajta tevékenység, az információs technológia megjelenésével és annak a fokozott alkalmazásával jelentős mértékben kibővül.

A nagy integráltságú infokommunikációs rendszerek fejlettségével és globális hozzáférhetőségével párhuzamosan és azzal egyenes arányban növekszik e rendszerek fenyegetettsége és ez által a sebezhetősége is. 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 infokommunikációs rendszerek elleni fenyegetések formái és szintjei, a konfliktus helyzetek, a technikai lehetőségek, és a motivációk szerint változhatnak.

A „jól megválasztott” támadás, amely egy infokommunikációs rendszer ellen irányul akár az egész ország, vagy akár egy szubregionális térség információs infrastruktúráinak sérüléséhez, vagy akár teljes leálláshoz vezethet. Mivel a gazdasági élet szereplőinek – a termelő vállalatok, a kereskedelem, a tőzsde, stb. – a napi működéséhez sok esetben elengedhetetlenek

egyes infokommunikációs rendszerek, ezért ezek támadásával, időszakos bénításával, működésképtelenné tételével, vagy akár végleges kiiktatásával igen nagy anyagi károk is előidézhetők. [4]

Az információs fenyegetések származhatnak:

- egyes személyektől;
- jogosulatlan felhasználóktól;
- terroristáktól;
- különböző nemzeti szervezetektől;
- külföldi hírszerző szolgálatoktól, vagy akár
- katonai szervezetektől is.

Az infokommunikációs rendszer elleni tevékenység eredetét nehéz azonosítani, mivel e csoportok között a határok elmosódnak, pl. egy illetéktelen felhasználói behatolásnak látszó tevékenység valójában származhat egy külföldi hírszerző szolgálattól is. [1] A támadók körét vizsgálva megállapíthatjuk, hogy pl. a jogosulatlan felhasználók a támadó eszközök széles skálájából csak egynéhányat vesznek igénybe, és azok is a kevésbé agresszív támadási módszerek közé tartoznak. Nem így a terroristák, akik a legpuhább támadó módszerektől kezdve a pusztításig bármilyen információs támadást alkalmazhatnak. Ezért napjainkra igen nagy veszélyt jelent az infokommunikációs rendszerek terroristák általi elérésének lehetősége, és az ún. cyber hadviselési módszerek alkalmazása.

A konfliktusok szintje általában kifejezi az infokommunikációs rendszer elleni ellenséges tevékenység érdeklődési körét és mértékét. Békeidőben a számítógép-hálózatokba való illetéktelen behatolás és a különböző passzív eszközökkel végzett elektronikai felderítés a leggyakoribb információs tevékenység, mert ez által képesek kipróbálni az infokommunikációs rendszer gyenge pontjait, felmérni a sebezhetőségét. Amint a válság a nyilvánvaló konfliktushelyzet vagy háború irányába mozdul el, az infokommunikációs rendszerek ellen több közvetlen támadással lehet számolni. Az intenzív katonai cselekmények kibontakozását és a katonai

műveletek megkezdését rendszerint összehangolt információs támadások előzik meg, illetve vezetik be. [1]

A komplex információs támadások egymás után vagy egymással párhuzamosan, egyszerre több színtéren, dimenzióban realizálódhatnak. A komplex információs támadás – és ebből adódóan a komplex védelem is – céljai elérése érdekében az alábbi dimenziókban fejti ki hatásait:

- fizikai dimenzió;
- információs dimenzió és
- tudati – vagyis az emberi felfogóképesség és megértés – dimenzió.

**A fizikai dimenzióban** alkalmazott információs támadási formák a különböző információs infrastruktúrák, infokommunikációs rendszerek elemei elleni ún. „kemény típusú" („Hard Kill") támadásokat jelentik.

**Az információs dimenzióban** jelentkező információs fenyegetések a különböző információs folyamatok, adatszerzés, adatfeldolgozás, kommunikáció, stb. többnyire elektronikus úton való „lágy típusú" („Soft Kill") támadását jelenti annak érdekében, hogy a célpontokra való közvetlen pusztító, romboló fizikai ráhatás nélkül közvetlenül befolyásoljuk azokat.

**A tudati dimenzióban** megvalósuló információs tevékenységek közvetlenül az emberi gondolkodást – észlelést, érzékelést, értelmezést, véleményt, vélekedést – veszik célba valós, csúsztatott vagy hamis üzenetekkel, amelyeket többnyire elektronikus és nyomtatott médián keresztül vagy közvetlen beszéd formájában továbbítanak. [1]

A tudati dimenzióban tehát 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, mint a már korábban felsorolt: természeti és ipari katasztrófák illetve műszaki zavarokból adódó veszélyek, amelyek szintén jelentősen befolyásolhatják

a rendszerek és infrastruktúrák működését, és ez által kihatnak az össztársadalmi folyamatokra is.

Az információs társadalom működését korlátozó 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 megkülönböztethetünk belső és külső forrásból származó veszélyeket, strukturáltságuk alapján, pedig magas szinten szervezett és alacsonyan szervezett fenyegetéseket.

**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. [1]

**Magasan szervezett fenyegetéseket** az előzőekben felsoroltak közül olyan szervezett csoportok, terrorszervezetek, 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.

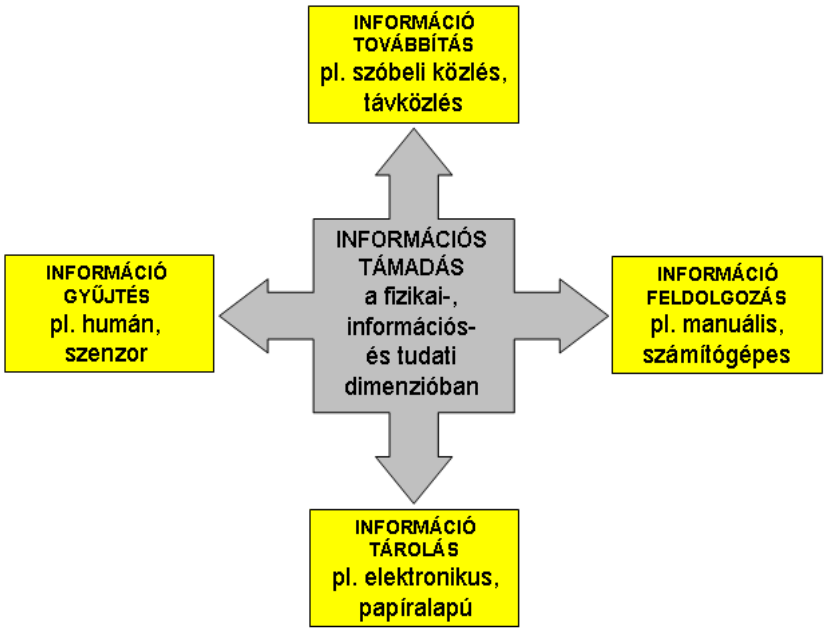
Ezzel szemben az **alacsony szervezettségű támadásokat** azon egyének, jogosulatlan felhasználók (hackerek, crackerek stb.) hajtják végre, akiket elsősorban anyagi haszonszerzés vagy a saját képességeik megmutatása motivál. Ebből adódóan látható, hogy a magasan szer-

vezett 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. [5]

A továbbiakban – egy másik megközelítésben – vizsgáljuk meg egy infokommunikációs rendszer támadhatóságát a funkcionális területeken keresztül. Egy infokommunikációs rendszer alapvetően az alábbi négy funkcionális területen folytat információs tevékenységet:

- információgyűjtés (humán vagy szenzor alapú);
- információtovábbítás (szóbeli közlés vagy távközlés);
- információfeldolgozás (manuális vagy számítógépes);
- információtárolás (papíralapú vagy elektronikus). (1. ábra)




1. ábra. Információs támadási felületek [6]

Ha e négy funkcionális területet a támadhatóság szempontjából elemezzük, akkor szintén megállapíthatjuk, hogy a támadó félnek jó lehetőségei vannak beavatkozni a folyamatokba mind három dimenzióban, mind a négy területen. Támadás érhet:

- egy szenzorhálózatot (pl. elektronikai zavarás útján), amellyel a döntéshez szükséges fontos információk megszerzését lehet akadályozni;
- a távközlési hálózatot (felderítés vagy zavarás útján) amivel az információ továbbítását lehet akadályozni vagy a továbbított információhoz lehet hozzáférni;
- a számítógép-hálózatot, ahol különböző rosszindulatú programokkal szintén adatokhoz lehet hozzáférni vagy korlátozni lehet a feldolgozási folyamatot;
- az adattároló rendszert – mely napjainkban már számítógépes adattárolókat jelent – ahol szintén különböző programokkal hamis adatokat lehet bevinni vagy módosítani, illetve tönkre tenni a tárolt adatbázist.

Mindehhez pedig még társul, hogy a fenti rendszereket, hálózatokat emberek üzemeltetik, kezelik, az adat- illetve információfeldolgozást még számítógépes adatfeldolgozó rendszerek esetén is értékelő-, elemző személyzet végzi, és végül, de nem utolsó sorban a döntéseket is emberek, a vezetők hozzák meg. Ebből következően – mint ahogy azt már korábban is írtuk – a támadások irányulhatnak a humán erőforrás ellen is a tudati dimenzióban (pl. a pszichológiai hadviselés vagy a social engineering).

A leírtak alapján látható, hogy a támadó a céljait nem csak és kimondottan az informatikai rendszer támadásával tudja elérni. Különböző részcélok elérhetők csak egy-egy dimenzióban megvalósuló és csak egy-egy funkcionális terület ellen irányuló támadással is. De amennyiben a támadó az kritikus információs infrastruktúrákat kívánja támadni annak érdekében, hogy jelentős zavarokat idézzen elő a társadalom működési folyamataiban, akkor a megoldás a komplex támadási formák alkalmazásában rejlik. Ezért – mint ahogy azt a későbbiekben tárgyaljuk – nem elégedhetünk meg az információbiztonság leszűkített értelmezésével, vagyis csak az informatikai rendszerre való értelmezésével. [6]

Napjaink egyik korszerű információalapú támadó és védelmi elmélete az **információs hadviselés** (és annak katonai formája az **információs műveletek**) is a komplex, összehangolt, mindhárom dimenzióban végrehajtott információs támadás (és védelem) elvét követi. Az információs hadviselésnek és az információs műveleteknek napjainkra teljes mértékben kialakult az elmélete, többnyire letisztult az eszköz- és eljárásrendszere, amelyet a következő alfejezetben mutatunk be röviden.

## *3.2. Információs hadviselés*

### 3.2.1. Az információs hadviselés kialakulása

Az emberek életük folyamán állandóan információt cserélnek, információs tevékenységet folytatnak, vagyis aktívan kommunikálnak egymással. A megismerkedés, barátság, szövetség, veszekedés, viszály, ellenségeskedés, megbékélés, fennmaradás, túlélés, együttélés, együttműködés, mint fogalmak és humán tevékenységek minden esetben intenzív információcserét, ún. interaktív kommunikációt igényelnek.

A társadalmi élet dinamikus egyensúlyának változásai következtében ezt az igen kényes egyensúlyt számos külső és belső hatás, változás éri. A globális, regionális és nemzeti politikai, gazdasági, társadalmi egyensúly (dinamikus stabilitás) súlyos vagy tartós elvesztése válságokat, tartós válsághelyzeteket idézhet elő.

Békében, válsághelyzetekben és háborúk idején az egyes országok mindig folytattak szándékos és tudatos célzatú információs tevékenységet. Ez alatt a régebbi korokban elsősorban a hírszerzést (kémkedést), félrevezetést, propaganda- és nyilatkozatháborút és egyéb hasonló elnevezésekkel említett információs/kommunikációs tevékenységeket értettek. Mindezek bármilyen tudatosak is voltak, nem képeztek egy olyan egységes, célzott és határozott struktúrába foglalt információs tevékenységi rendszert, mint amit ma az információs társadalomban gyűjtőfogalommal információs hadviselésnek nevezünk.

Békeidőszakban, feszültség- vagy válsághelyzetben a nemzetgazdaság, illetve az alapvető polgári információs infrastruktúrák ellen végrehajtott nagyméretű, korlátozó vagy pusztító hatású információs támadások adott esetben egy háború bevezető szakaszát is jelenthetik! Ezért az információs rendszerek és infrastruktúrák védelme alapvetően fontos biztonságpolitikai tényezővé vált. Az említett támadások (kezdetben csupán jelentős üzemzavarnak értékelhető változások) észlelésekor a legfelsőbb szintű helyzetelemző- és válságtörzsnek igen ko-

molyan mérlegelni kell nemcsak a károk nagyságát, hanem azok okait és a várható újabb eseményeket is.

Az információs hadviselés új fajtájú hadviselési forma, amely a 21. század első évtizedeiben bontakozik ki teljes terjedelmében, amikor az iparilag fejlett országok fokozatosan átlépnek az információs korszakba és az országok életében a távközlési és információtechnikai eszközök, rendszerek és hálózatok meghatározó szerepet fognak betölteni. Az információs társadalmak sebezhetőssége éppen az információtechnika és az információs infrastruktúra révén rendkívüli mértékben megnövekszik. Viszonylag kis költségráfordítással olyan információs hadviselési támadó fegyvereket és fegyverrendszereket lehet előállítani, amelyek különböző mértékű, hatású és időtartamú pusztításokat vagy korlátozásokat képesek előidézni. Ezeknek a veszélyeknek felismerése és a megfelelő ellenrendszabályok kialakítása, minden ország jól felfogott, saját érdeke. [3]

A különböző verseny- és konfliktushelyzetekben mindig is törekvés volt arra, hogy az egymással szembenálló felek több és pontosabb információra tegyenek szert a másik féllel szemben, azokat gyorsabban és hatékonyabban tudják felhasználni. Ez azt jelenti, hogy a másik féllel szembeni információs fölényre való törekvés már akkor is folyamatosan jelen volt. Ezek a tevékenységek azonban korábban nem képeztek olyan egységes rendszert, mint amit ma információs hadviselésnek nevezünk.

Mindezen tényezők arra ösztönözték a katonai teoretikusokat, hogy választ keressenek arra, hogy hogyan lehet a különféle információalapú tevékenységeket összehangolni, egységes mederbe terelni az információs fölény megszerzése és megtartása érdekében. Erre vonatkozóan már viszonylag korán történtek kísérletek: az információs hadviselés, mint összehangolt információs tevékenységek első definícióját az USA védelmi minisztériumának magyar származású kutatója, Thomas P. Rona alkotta meg, egy a Boeing vállalat számára 1976-ban készített kutatási jelentésében. [7] Ebben az információs eszközök és módszerek olyan mindenidejű (békeállapottól, békeállapotig tartó) és minden szintű (stratégiai, hadműveleti és harcászati) alkalmazását értelmezi, amely lehetővé teszi a kitűzött célok elérését.

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

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

Az információs hadviselés teljes körű kialakulásához a végső lökést az információtechnológia rohamos fejlődése adta meg. Napjainkra az információ szerepe, jelentősége úgy a társadalmi- gazdasági-, politikai életben, mind a katonai műveletek vonatkozásában alapvető fontosságúvá vált. Amennyiben nincs megfelelő mennyiségű, pontosságú és a valós helyzetet tükröző információ, akkor nem lehet megalapozott döntéseket hozni. Ez a felismerés ösztönözte a szakembereket, hogy megpróbálják ezt az egészet összehangolni. Az információs hadviselés kezdeti jegyei az első Öböl-háborúban voltak megfigyelhetők, a '91-es „Sivatagi Vihar" műveletek során, ahol első ízben lehetett felismerni azokat a jellegzetességeket, amelyek az információs hadviselés sajátosságait viselték magukon, Mindehhez pedig még hozzájárult a „CNN jelenségként" ismert média tevékenység is, amely az emberek otthonaiba vitte be a háborút. [8]

Igen gyakran előfordul, hogy az információs hadviselést gyakran és helytelenül informatikai hadviselésnek nevezik. Ez utóbbi az információs hadviselésnek csupán egy jól körülhatá-

rolható része, alrendszere, és nem azonos az egésszel. Az információs hadviselés az informatikai hadviselésnél tartalmában jóval kiterjedtebb tevékenység.

### 3.2.2. Információs fölény, vezetési fölény

A fölény szó fogalma – a Magyar Értelmező Szótár szerint – „*azt a realitást jelenti, hogy valaki, valami bizonyos szempontból különb, erősebb, fejlettebb, jobb a másiknál, a hatékonyság terén eredményesebb, valamilyen vonatkozásba, n előnyben van a másikkal szemben*."

Mindenfajta társadalmi formációban a társadalom tagjai, csoportjai, mint piaci szereplők, versenyző felek, ellenfelek, esetenként ellenségek vannak jelen. A versenytársak különböző fajtájú, típusú előnyök és fölények megszerzésére törekszenek. A másik féllel szembeni fölény több területen is jelentkezhet, mint pl. politikai-, pénzügyi-, gazdasági-, jogi-, tudományos-, kutatási-, ipari-, technikai-, gyártástechnológiai-, szállítási-, közbiztonsági-, erkölcsi-, tudásbeli-, vezetési-, információs (informatikai és távközlési) fölény, stb.

Az információs társadalomban az információszerzés sok forrásból történik, amelyek rétegesen át- és lefedik egymást. A többszörösen ellenőrzött és az automatikus adatfúziós és korrelációs információs technológiával szinkronba hozott, minőségileg új és tömörített információk a társadalom, vagy annak egyes rétegei, szervezetei számára ún. **információs fölényt**, huzamosabb megléte **információs uralmat** végső soron **vezetési fölényt** biztosítanak a másik fél felett.

Az **információs fölény** birtokosának lehetővé teszi, hogy infokommunikációs rendszereit és azok képességeit kihasználva a társadalmi élet különböző területein előnyre tegyen szert, vagy a kialakult helyzetet folyamatosan úgy irányítsa, hogy emellett a másik felet megfossza e képességeitől.

Az információs fölény megléte a birtoklója számára a következőket jelenti:

- többet tud a másik félről, mint amit ő tud a saját képességeiről;

- eredményesen tudja korlátozni a másik fél vezetési- és információs rendszereit, döntési folyamatait, miközben ilyen behatásoktól képes megóvni a saját rendszereit;
- a sajátoldali döntési ciklus tudományra támaszkodó, alaposabb, gyorsabb és ennek következményeként hatékonyabb, mint az ellenfél hasonló vezetési folyamata;
- az információtechnológia és más csúcstechnológiai eredmények terén egy lépéssel a másik fél előtt jár, a technológiai fölény megtartására, megóvására és növelésére törekszik.

Az információs fölény megszerzésének és megtartásának három azonos fontosságú oldala van, úgymint:

- információt szerezni a döntést befolyásoló tényezőkről;
- kihasználni és megvédeni a saját információs képességeinket és
- gyengíteni, lerontani az ellenfél információs lehetőségeit.

Mindenek előtt az információs fölény alapját az adja, hogy elegendő, pontos és valós idejű információval kell rendelkezünk a döntést befolyásoló tényezőkről, amelyek három terület köré csoportosíthatók, úgymint: az ellenfél helyzete, a saját helyzetünk valamint a környezeti tényezők. E három területről kell információval rendelkezni a hírszerzés, felderítés és a saját jelentések alapján.

Másodsorban ki kell építeni a saját infokommunikációs rendszereinket, amelyeket hatékonyan kell működtetni annak ellenére is, hogy a másik fél komoly erőfeszítéseket tesz annak érdekében, hogy vagy magát az információ tartalmat vagy az infokommunikációs rendszereket illetve a döntéshozó(ka)t megpróbálja korlátozni, összezavarni, és ez által egy számára kedvező helyezet előidézni. Ez tehát azt jelenti, hogy megfelelő védelmi megoldásokat kell alkalmazni a saját információk, és információs rendszerek megóvása érdekében.

Harmadrészt rendelkeznünk kell mindazon képességekkel, amelyekkel befolyásolni tudjuk a másik fél információit, infokommunikációs rendszereit és folyamatait valamint döntéshozóit. Ennek hatására kevesebb és pontatlanabb információ áll a másik fél rendelkezésére a dön-

tést befolyásoló tényezőkről, aminek következtében a vezető (parancsnok) nem lesz képes objektív, valós idejű döntés meghozatalára. [8]

**Az információs uralom** birtoklása már többet jelent, mint az információs fölény kivívása, megszerzése. Az információs uralom az információs fölény megszilárdulását és időben viszonylag tartóssá válását jelenti az információszerzés, információtovábbítás, információfeldolgozás, információhasznosítás, információvédelem, döntéshozatal és irányítás valamennyi kulcsfontosságú területén. Az információs uralom valamennyi kulcsfontosságú vezetési területre kiterjed és időben tartós jellegű.

Az információs fölény e fokozatai összhatásukban elvezetnek az ellenfél feletti tartós és szilárd **vezetési fölény** kialakulásához, amely a siker egyik fontos záloga. A vezetési fölény egyrészről a szembenálló felek vezetési folyamatai közötti olyan minőségi különbséget jelent, amikor az egyik fél tevékenységét meghatározó intézkedések, utasítások tartalma és időbelisége lényegesen jobban tükrözi a kialakult helyzetet és az ahhoz alkalmazkodó célszerű cselekvésmodellt, mint a másiké. Másrészről azt az állapotot fejezi ki, amikor ugyanezen fél végrehajtó állományának eltökéltsége, hajlandósága az utasítások teljesítésére azonos vagy nagyobb, mint a másik fél tagjaié.

A vezetési fölény kivívása a saját információszerző-, feldolgozó és kommunikációs rendszer hatékony alkalmazására, az információk célirányos és szakszerű felhasználására, a teljes vezetési rendszer optimális működtetésére irányul, amely összességében két fő tényező függvénye, úgymint:

- az információs fölény és uralom kivívása, és
- a saját vezetési és információs rendszer által biztosított képességek hatékony kihasználása, a döntési ciklus lerövidítése, a döntések minőségének fokozása, valamint a kapcsolódó intézkedések hatékony kidolgozása és továbbítása érdekében.

Az információs fölény a többi vezetési fölényelemekben: döntési fölényben, irányítási fölényben, a végrehajtási fölényben folyamatosan jelen van és segíti azok optimális érvényesü-

lését. Az információs fölény elsődleges operatív funkciója, hogy kedvező információs (tudás) helyzetet teremtsen a döntési fölény kialakításához.

Az információs fölény következtében a saját vezetési folyamatunk időben a másik fél vezetési tevékenységén belülre kerül: gyorsabbak vagyunk, gyorsabban észlelünk, döntünk és intézkedünk, mint az ellenfél.

Mivel a tökéletes és hosszantartó információs fölény kialakítása nem lehetséges, ezért keresni kell a lehetőséget, hogy az információs fölényt a számunkra legjobb helyen, legjobb időben és legjobb körülmények között érjük el. Az információs fölény megléte esetén képesek vagyunk befolyásolni a másik félnek a helyzetről alkotott képét, megteremteni a feltételeket a kezdeményezés megragadására. [1]

### 3.2.3. Az információs hadviselés tudományelméleti alapjai

Az információs hadviselés elméleti és tudományos alapját – többek között – a kommunikációelmélet (a rendszerek közötti kapcsolatok elmélete), a káosz-elmélet (a rendszerek életét befolyásoló tényezők elmélete), a komplexitás-elmélet (a struktúrák hierarchiája és függőségi viszonyának elmélete), valamint a kognitív tudomány (megismerés-tudomány), az információelmélet és hálózatelmélet vonatkozó tételei, pl. a kognitív hierarchia hipotézis képezik.

A kommunikációelmélet szerint az anyag, az energia és az információ alapvetően kétféle kapcsolati csatornán áramlik:

- anyag- és energiaszállító csatornákon: közlekedési, szállítási, energiaellátási, logisztikai csatornák igénybevételével;
- információtovábbító csatornákon: távközlési hálózatokban és számítógép-hálózatokban.

Ezek a létfontosságú szállító csatornák biztosítják a szervezetek szilárd belső kohézióját, a szervezet integritását és a szervezetek közötti megbízható kapcsolatokat.

A kognitív hierarchia elve szerint a vezető a megismerési piramis csúcsán áll, fokozatosan ismeri meg és fel a kialakult helyzetet, a felmerülő veszélyeket, melynek alapján képes saját

erőforrásait és azok hatását az ellenfél leggyengébb pontjára összpontosítani és irányítani. Ezáltal adott helyen és időben olyan helyi erőfölényt képes előidézni, amelynek birtokában jogosan számíthat a sikerre.

A komplexitás elmélet egyik tétele szerint a rendszerek anyagi ellátás és információ nélkül többé már nem életképesek. Az anyag- és energiaszállító, valamint az információtovábbító csatornák elvágásával bekövetkezik a rendszerek önzáródása, a belső erőforrások és készletek felemésztését eredményező, ún. belső rendszerösszeomlás effektusa. Amennyiben egy érintett rendszer csak saját magára, saját információs erőforrásaira, saját készleteire képes támaszkodni, hosszú távon életképtelenné válik. A saját erőforrások és készletek ugyanis korlátozott mértékben állnak rendelkezésre, előbb vagy utóbb kimerülnek, elfogynak. Külső segítség nélkül egyetlen szervezet sem képes hosszabb ideig fennmaradni.

A saját erőforrások intenzív belső felhasználásának törvényszerű eredménye: az érintett rendszerben, alrendszerben érvényesül a „káosztörvény”; a szervezett rendből, az irányíthatóságból, vezethetőségből öntörvényűen kialakul a szervezetlenség, rendetlenség, irányíthatatlanság állapota és helyzete. Az információáramlás képességétől megfosztott szervezeteknél érvényesülnek ezek a hatások, bekövetkezik a szervezet és a rendszer összeomlása. A támadó információs hadviseléssel pontosan ilyen állapot előidézése a kívánatos és elérendő cél az ellenfél oldalán. [3]

Az információs hadviselés elmélete szerint, egy társadalomban első- és másodfokú társadalmi-technikai civilizációs fejlettségi rend működhet. A fejlett társadalmi rendszerek jogi és erkölcsi törvényekkel, szabályzókkal, szabványokkal irányítottan léteznek és működnek. Ezek a társadalmak – a magas fokú szervezettség révén – erősen szabályozott társadalmi rendhez tartoznak, amelyet második fokozatú fejlettségi szintnek nevezünk. Amennyiben ez a magas fokú szervezettségi rend valamilyen külső vagy belső negatív társadalmi vagy természeti oknál fogva megszűnik, vagyis a fejlett törvények és szabályzók már nem képesek működni és hatni, akkor az érintett szervezeteknél és technikai rendszereknél bekövetkezik a dereguláció, azaz társadalmi, technológiai visszaesés az első fokozatú civilizációs szervezettségi szintre,

ahol a természet törvényei objektív módon, a káosz törvénye szerint hatnak. Az információs hadviselés során a társadalom alapvető érdeke saját oldalon a második fokozatú civilizációs rend fenntartása és az ellenfélnél az első fokozatú civilizációs rend ideiglenes kialakítása, vagyis irányíthatatlan helyzet, sajátos káoszrend előidézése.

Az információs hadviselés céljai között szerepel a másik fél rendszereinek, hálózatainak, szervezeteinek megfosztása attól a lehetőségtől és képességtől, hogy külső anyagi utánpótlást, energiát vagy vezetési információt kapjanak. További célok közé tartozik annak megakadályozása, hogy az ellenfél védelmi rendszerei egymás között ilyen típusú éltető erőforrásokat, anyagot, energiát, információt és a túlélést biztosító logisztikai szállítmányokat cserélhessenek. Ez történhet az anyagi, energiai és információs folyamatok teljes megszakításával, működésük tartós korlátozásával, vagy ideiglenes kikapcsolásával, zavarásával.

A célpontok többszintű rétegződése és mátrix jellegű hálózatos kapcsolódása következtében az információs hadviselés keretében zajló támadások többnyire nem egyes célpontok ellen irányulnak. Ehelyett inkább az egész rendszert érintő és káros hatást kifejtő, úgynevezett degradáló, deregulációs hatás elérését célzó eredményre törekszik a hatásalapú megközelítés elvének megfelelően.

Saját vonatkozásban, az információs hadviselés célkitűzéseinek másik oldala, védeni saját információs rendszereket, összeköttetéseket, távközlési és logisztikai vonalakat, kritikus infrastruktúrákat. Más megközelítéssel e téren az információs hadviselés célja, hogy a második fokozatú civilizációs rendet minél tovább és minél teljesebb mértékben fenntartsuk, és megakadályozzuk a másik felet abban, hogy társadalmunkat az alacsonyabb fejlettségű, első fokozatú, káosz felé tartó civilizációs rendre visszavesse, visszakényszerítse. [1]

A leírtakból objektíven következik, hogy információs hadviselést rendkívül alacsony műszaki fejlettségű információs környezetben – ahol nem-, vagy csak elenyésző mértékben beszélhetünk információs infrastruktúrákról – nem lehet eredményesen alkalmazni. Fejletlen információs környezetben az információs hadviselés során alkalmazott komplex információs támadás nem fog eredménnyel járni, mivel nem lesznek infokommunikációs célpontok. [3].

### 3.2.4. Az információs hadviselés tartalma

Az információs hadviselés – illetve annak a NATO és a tagországok katonai doktrínáiban elfogadott formája az **információs műveletek** – mindazon összehangolt, koordinált információs tevékenységeket jelentik, amelyek arra irányulnak, hogy a másik 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 hadviselés célja az információs fölény, információs uralom és végső soron a vezetési fölény kivívása, a saját oldali vezetési ciklus számára időcsökkentés, a másik fél vezetési időciklusa tekintetében pedig időnövelés elérése érdekében. Megszerzésének és megtartásának két azonos fontosságú oldala van, úgymint: kihasználni és megvédeni a saját információs képességeket, illetve gyengíteni a másik fél információs lehetőségeit.

Az információs hadviselés nem más, mint különböző elkülönülten is létező, a fizikai-, az információs- és a tudati dimenzióban zajló komplex információs tevékenységek közötti integráló és koordináló tevékenység, melynek szükségességét és létjogosultságát az összehangolt információs tevékenységek nagyságrendekkel növelhető hatékonysága adja.

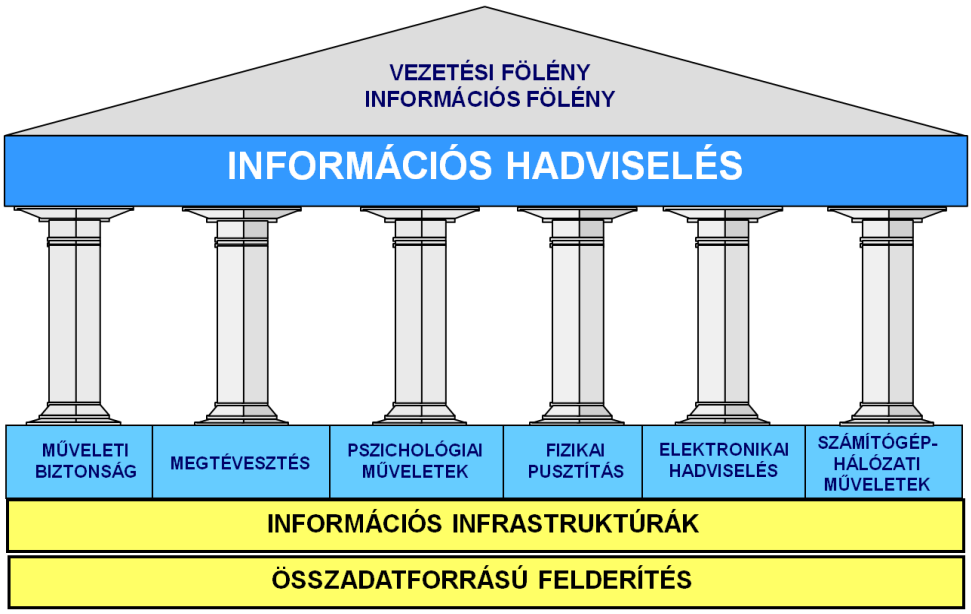
Az információs hadviselés a saját erőknél erősokszorozó, a másik félnél erőcsökkentő, erőmegosztó szerepet tölt be. Ugyanakkor a vezetési időciklust közvetlenül befolyásoló, sajátoldali időtömörítő és ellenoldali időnövelő képességekkel rendelkezik, amelynek eredményeként vezetési időfölényre tehetünk szert. [1].

Az információs hadviselés elemei közé az alábbiak sorolhatók:

- műveleti (működési) biztonság;
- megtévesztés;
- pszichológiai műveletek;
- fizikai pusztítás;

- elektronikai hadviselés;
- számítógép- hálózati műveletek. [1]

Az információs hadviselés sikeres folytatásához a fenti elemeken kívül fontos szerep hárul a jól és hatékonyan működő információs infrastruktúrákra, azok elemeire (infokommunikációs rendszerekre) és az azok működéséhez nélkülözhetetlen adatok megszerzésére, melyek az információs hadviselés támogató elemeit és egyben hatékony végrehajtásának biztosítékát is jelentik. Az adatszerzés és feldolgozás biztosítja az ellenfél vezetési információs rendszereinek elemzését, a célok (célpontok) meghatározását, információs hadviselési képességeinek meghatározását, valamint visszajelzést nyújtanak a saját végrehajtott feladatok eredményességéről. (2. ábra)




2. ábra. Az információs hadviselés elemei [1]

Az információs hadviselés minden eleme egyaránt fontos szerepet játszik az információs fölény kivívásában, megtartásában és vezetési fölénnyé való konvertálásában. Az információs hadviselés erősokszorozó szerepe éppen abban áll, hogy az elemek együttesen, koordináltan, egymással együttműködve, egymás hatásait kihasználva (szinergikusan) kerülnek alkalmazás-

ra. Ez jóval nagyobb hatásfokot eredményez, mintha azok elemei önállóan, koordinálatlanul lennének végrehajtva.

Az információs hadviselés elemei között szoros kapcsolatok és összefüggések állnak fenn. Az egyes elemek a végrehajtás szintjén egymásba átnyúlnak, átfedik egymást. A különböző elemeken belül végzett résztevékenységek az információs hadviselés egy vagy több elemére is hatással vannak, ugyanakkor nem veszítik el önállóságukat.

Az információs hadviselést támogató felderítés egyrészt adatszerzést, másrészt a megszerzett adatok feldolgozását és a szembenálló fél információs rendszereinek kiértékelését jelenti.

Az információs hadviselés **támadó és védelmi jellegű** lehet, amelyeket politikai, gazdasági és kulturális téren, valamint a katonai tevékenységek minden szintjén folytatnak.

**A támadó információs hadviselés** arra irányul, hogy speciális célok érdekében vagy speciális fenyegetésekre válaszul, hatást gyakoroljanak a másik fél információira, információalapú folyamataira, információs rendszereire békeidőben, válság vagy konfliktus idején egyaránt. Az információs hadviselés támadó jellegű alkalmazása képes lelassítani, és megzavarni a másik fél feladatai tervszerű végrehajtásának ütemét valamint befolyásolni a kialakult helyzet értékelését.

A támadó információs hadviselésnek kettős funkciója van: egyrészt minden lehetséges eszközzel elfogni, felfedni, másrészt befolyásolni, tönkretenni a másik fél információit. E kettős funkciót – a támadó jellegű információs hadviselés nagyfokú hatékonysága érdekében – a fizikai-, információs- és a tudati dimenzióban egyaránt, egymással összehangoltan kell érvényre juttatni.

Az információs támadás közvetlen és közvetett formában valósulhat meg. A **közvetlen információs támadás** során a támadó fél egyrészt a különböző információbiztonsági rendszabályokat kikerülve bejut a kommunikációs rendszerekbe és számítógép-hálózatokba, hozzáfér különböző adatbázisokhoz stb. és ez által számára hasznosítható információkhoz jut. Másrészt zavaró jelekkel, megtévesztő információkkal, rosszindulatú szoftverek bejuttatásával tönkreteszi, módosítja, törli stb. a szembenálló fél számára fontos információkat. A **közvetett in-**

**formációs 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. [35]

Természetesen a közvetlen és közvetett támadást megfelelően összehangolva célszerű alkalmazni, ezáltal is erősítve egymás hatékonyságát. Egy közvetett információs támadással el lehet terelni az adatszerző rendszerek figyelmét, így a közvetlen támadás sikeresebben végrehajtható a megcélzott rendszerrel szemben. Ugyanakkor egy közvetlen módon végrehajtott információs támadás arra kényszerítheti a vezetési rendszert, hogy pl. a döntési alternatívák kialakításakor, az összadatforrású felderítő rendszer helyett csak egy forrásból származó információkra, pl. csak az optikai felderítésre támaszkodjon. Ez az egyforrású felderítő rendszer pedig a már említett közvetett támadással hatékonyan félrevezethető. A felsorolt támadási funkciókat, formákat és konkrét tevékenységeket azok hatása és támadási szintjei szerint az 1. táblázat szemlélteti.

**A védelmi információs hadviselés** arra irányul, hogy egyrészt fenntartsa a hozzáférhetőséget az információkhoz, információalapú folyamatokhoz, és biztosítsa az információs rendszerek hatékony használatát, másrészt, hogy megvédje a saját kritikus információinkat. A vezetési információs rendszerek védelme biztosítja a saját vezetési képességeink fenntartását azáltal, hogy kihasználja a saját rendszerekben rejlő lehetőségeket, illetve lehetetlenné teszi, hogy a másik fél beavatkozzon információs rendszereinkbe. Minimálisra csökkenti a saját vezetési és információs rendszereink sebezhetőségét és a közöttük fellépő kölcsönös zavarokat.

A hatékony védelmi információs hadviselés során figyelembe kell venni:

- az információs infrastruktúrák hardver és szoftver elemeit, azok funkcióit, jellemzőit és sajátosságait;
- a működési folyamatokat, hálózati hozzáférési módokat;
- a vezetési sajátosságokat;

- a rendszerek fizikai struktúráját, kapcsolódási viszonyait valamint
- az elfogadható szintű kockázat elérésének és kezelésének módját.

1. táblázat: Az információs támadás hatása és támadási dimenziói [9]

| Funkció: | **ELFOGÁS, FELFEDÉS** | | **BEFOLYÁSOLÁS, TÖNKRETÉTEL** | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Biztonsági jellemző:** | **Bizalmasság** sérül | | Adatok **sérülékenysége** nő<br>Szolgáltatások **elérhetősége** csökken | | | | | |
| **Forma:** | **Közvetett** | **Követlen** | **Közvetett** | | | **Közvetlen** | | |
| **Támadó tevékenység:**<br>**Támadási szint:** | **Információ források felderítése** | | **Megtévesztés** | **Zavarás** | **Pusztítás** | **Megtévesztés** | **Zavarás** | **Pusztítás** |
| **Tudati dimenzió** | Viselkedési formák, befolyásolhatóság figyelésével következtetés a döntési folyamatokra | Párbeszédek, döntési folyamatok figyelése HUMINT módszerekkel | Döntéshozatal, megértési folyamat befolyásolása PSYOPS tevékenységekkel (szórólapok, média, Internet alkalmazása) | | | Titkos műveletekkel beszivárgás a célközönség közé és ott a megértési folyamatot befolyásoló témák terjesztése | | |
| **Információs dimenzió** | Monitorok kisugárzásának felfedése (Van Eck módszer)<br>Hálózati topológia feltérképezése<br>Titkosítás megfejtés, dekódolás | Elektronikai felderítő szenzorok alkalmazása<br>Számítógép hálózatok adataihoz való rejtett hozzáférés, (pl.Trójai )<br>Jelszólopók telepítése | Megtévesztő e–mail üzenet továbbítása<br>Megtévesztő hálózati tevékenység folytatása | Hálózatok adatokkal való mesterséges túlterhelése (Flood Attack),<br>Nyílt forrású információkkal a figyelem elterelése | | Trójai programok bejuttatása megtévesztő tevékenység útján<br>Működő programokkal adatok módosítása | Rosszindulatú szoftverekkel, programokkal (férgek, vírusok stb.) hálózati szolgáltatásokhoz való hozzáférés megakadályozása (DDoS), adatok, adatbázisok tönkretétele | |
| **Fizikai dimenzió** | Vezetékes vonalak induktív módon való lehallgatása<br>Papírhulladék kutatása | Információs eszközök, titkosító kulcsok, fizikai kulcsok, adattároló hordozók ellopása | Social Engineering | Bomlasztó tevékenységek előidézése a felhasználók félrevezetésével | | Fizikai biztonságot feltörve, titkos adatokhoz való hozzáférés | Információs infrastruktúrák fizikai rombolása<br>Infokommunikációs eszközök elektronikai pusztítása (E-bomba) | |

A védelmi információs hadviselés szoros összefüggésben áll a komplex információbiztonság kérdésével, amely többek között magában foglalja az elektronikus információbiztonság hagyományos funkcióit.

Természetesen védelmi információs hadviselést folytathatunk úgy is, hogy megakadályozzuk a másik felet abban, hogy ellenünk alkalmazni tudja információs támadó eszközeit. E megközelítés alapján a saját információs rendszereink védelme lehet támadó és védelmi jellegű. A támadó jellegű védelem az információs hadviselés minden elemét felhasználja, hogy csökkentse a másik fél lehetőségeit a saját információs rendszerek támadására. Így pl. egy rádiózavaró eszköz felderítésével, megsemmisítésével vagy rongálásával meg tudjuk akadályozni, hogy az a saját távközlési rendszereink ellen alkalmazható legyen. Ezzel szemben a védelmi jellegű tevékenység a saját rendszerek sebezhetőségét csökkenti, felhasználva a fent említett tevékenységek, és rendszabályok lehetőségeit.

A hatékony védelmi információs hadviselés összehangolt alkalmazása lehetővé teszi, hogy megvédjük saját kritikus információs infrastruktúráinkat és rendszereinket a szolgáltatásokhoz való hozzáférés megakadályozásától, a jogosulatlan hozzáféréstől, valamint a rongálástól, rombolástól és módosítástól.

Az információs hadviselés elemei mind a támadó-, mind a védelmi információs hadviselés keretén belül alkalmazásra kerülnek. Éles határok nem húzhatók közöttük a tekintetben, hogy mely elemek alkalmazhatók a támadó- és melyek a védelmi információs tevékenységben.

### 3.2.5. Cyberhadviselés

Civil terminológia szerint a cybertér az elektronikus kommunikációs eszközök és rendszerek (számítógép-hálózatok, telefonvonalak, műholdas rendszerek stb.) és a rajtuk található szolgáltatások, információk alkotta virtuális tér vagy világ összefoglaló neve. A cybertér kifejezést – csakúgy, mint a virtuális valóság sok más szakkifejezését is – William Gibson alkotta

meg a „Neuromancer” című novellájában, amelyben a globális internet társadalmát vetíti előre. E kifejezést igen gyakran alkalmazzák a virtuális valóság világára is.

A cybertér katonai értelmezése ettől eltérő, jóval tágabb. Az USA Nemzeti Katonai Stratégia a Cybertéri Műveletekhez (National Military Strategy for Cyberspace Operations) c. dokumentuma szerint a cybertér egy olyan tartomány, ahol hálózatos rendszerekben működő elektronikai eszközöket és az elektromágneses spektrumot használják fel az adatok tárolására, cseréjére és módosítására. [10] Meg kell azonban jegyezni, hogy egy hálózatban lévő különböző elektronikai eszközök, különböző vezetékes kapcsolaton keresztül is csatlakozhatnak egymáshoz. Így pl. az állandó hely rendszerek elterjedt hálózati összeköttetési formája a vezetékes kapcsolat, azon belül is a leginkább elterjedőben lévő optikai kábeles csatlakozás. Ennek megfelelően a fenti értelmezést ki kell terjeszteni azon hálózatokra is, melyek elemei nem rádiócsatornán, hanem vezetéken vannak egymáshoz kapcsolva. Mindezeken túl az elektromágneses spektrum azért is szűkítése a cybertérnek, mivel azt a frekvencia spektrum más tartományaira is ki kell terjeszteni, ami pl. a mechanikus rezgések és a részecskesugárzások fizikai tartományát is tartalmazza. A szeizmikus és akusztikus rezgések, valamint a részecskesugárzások felderítésére eszközök sokasága szolgál (szonárok, hangérzékelők, tüzérségi bemérő eszközök, speciális mikrofonok, sugárzásmérők, stb.), az ellenük vívott harcban pedig elektronikai hadviselési eszközöket kell alkalmazni. [11] Az irányított energiájú fegyverek, amelyek jelentős része (pl.: az infrahangfegyverek, a hallható tartományú lökéshullám generátorok, a nagy energiájú részecske sugárzók, stb.) szintén a fizikai tartományokban működnek Ennek megfelelően helyesebb az elektromágneses spektrum helyett a teljes frekvencia tartományt értelmezni.

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

A cybertér meghatározásával kapcsolatban – civil értelmezés szerint – általánosan elterjedt nézet, hogy az a számítógép-hálózatokkal és az internettel van összefüggésben. A cybertér katonai értelmezése azonban kiterjeszti ezt a dimenziót, és nemcsak a számítógép-hálózatok működési környezetét érti alatta. Napjainkban a harctéren elektronikai eszközökből (pl. rádiók, radarok, navigációs eszközök, harctéri azonosító berendezések stb.) és számítógépekből olyan hálózatokat hoznak létre, ahol igen nehéz különválasztani egymástól a rendszert alkotó komponenseket. Amennyiben ezek elleni tevékenységről és a saját oldalon ezek védelméről beszélünk, akkor mindenképpen egy komplex rendszerként kell azokat értelmezni, melyeknek közös működési környezetük van. A harctéren ezek a hálózatos rendszerek (többnyire mobil rendszerekként) az elektromágneses energiát használják fel az adatok, információk megszerzésére, tárolására, továbbítására. Amennyiben ezek a rendszerek a teljes frekvencia spektrumot használják, akkor azon keresztül lehet hozzájuk férni is, vagyis felderíteni és támadni azokat. [12]

Az internet sebezhetősége manapság nagyon sokak számára ismert. Az információs társadalom működése alapvetően függ attól, hogy igen sok információs rendszer, köztük számos kritikus információs infrastruktúra használja az internetet. Ezért az internetnek – mint önmagában is kritikus infrastruktúrának – a biztonsága nemzetbiztonsági szempontból rendkívül fontos kérdés, melyet a kritikus információs infrastruktúrák védelmének megszervezése során figyelembe kell venni.

Ugyanakkor egy országban számos hálózatba szervezett rendszer is működik, melyek nem csatlakoznak az internethez. A kritikus információs infrastruktúrák döntő többsége elszigetelt, vezetékes vagy vezeték nélküli zárt hálózatokként működnek, közvetlenül nem kapcsolódnak a világhálóhoz. Ha csökkenteni akarjuk ezen infrastruktúrák működőképességét, akkor ezeket a hálózatokat a cybertérben elektronikai úton a teljes frekvencia tartományban kell elérni. [13]

A cybertérben folyó műveletek során a hálózatos képességek saját oldalon való kialakítása, fenntartása, illetve a másik fél oldalán való gyengítése, lerontása döntő fontosságú. A cybertérben folyó tevékenységek során a cél a cyberfölény megszerzése és megtartása. A

cyberfölény az információs fölény azon részét képezi, melyet a különböző hálózatba kötött elektronikai eszközökkel, rendszerekkel és számítógépekkel tudunk elérni, és amelynek következtében a saját cselekvési szabadságunk jelentős mértékben megnő. A cyberfölény kivívásának és megtartásának három egyenrangú és egymással szoros kapcsolatban lévő eleme különböztethető meg:

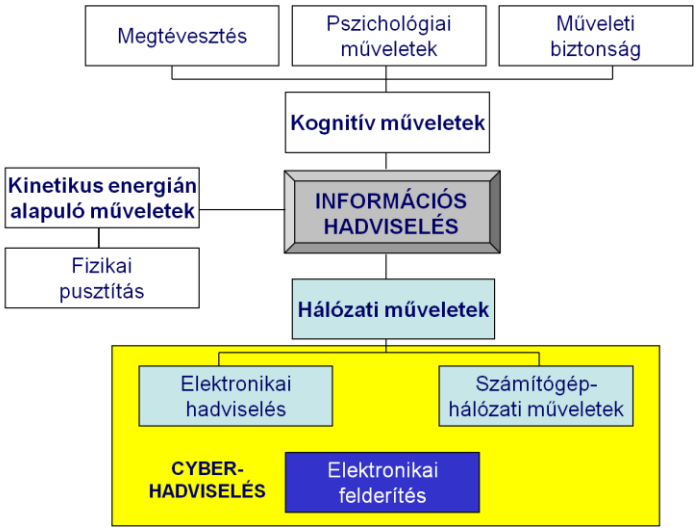
1. A különböző hálózatba kapcsolt elektronikai rendszerekkel az információ biztosítása a döntést befolyásoló helyzetről. Ez egyrészt jelenti a másik fél elektronikai rendszereinek (rádiótávközlő rendszerek, számítógép-hálózatok stb.) felderítését, másrészt a saját helyzetről szóló információk elektronikus feldolgozását, tárolását és továbbítását, harmadrészt pedig a környezetről szóló adatok elektronikai rendszerekkel, eszközökkel való megszerzését, feldolgozását, továbbítását (pl. meteorológiai lokátorokkal adatok megszerzése, digitális térképi információk feldolgozása térinformatikai módszerekkel stb.).
2. A másik fél elektronikus információs rendszerei működésének korlátozása, akadályozása. Ez alatt egyrészt az elektronikai hadviselés keretében végrehajtott ellentevékenységi módszereket értjük, mint pl. elektronikai zavaró eszközökkel a rádiórendszerek, radarrendszerek zavarása, különböző elektronikai megtévesztő tevékenységek folytatása vagy nagyenergiájú impulzus fegyverekkel (e-bomba) az elektronikai eszközök, számítógépek tönkretétele. Másrészt a számítógép-hálózati műveletek keretében a másik fél számítógép-hálózataiba való behatolást és ennek következtében pl. adatbázisok tönkretételét, módosítását, programfutási hibák előidézését jelenti.
3. A saját információs képességek kihasználása és megóvása a másik fél elektronikus úton végrehajtott különböző támadásaival szemben. Ez magába foglalja a saját hálózatos információs rendszereinkben rejlő lehetőségek maximális kihasználását, vagyis a hálózat nyújtotta képességek kialakítását és fenntartását, illetve ezen rendszereink elektronikai- és számítógép-hálózati védelmét.

A cyberfölény fentiek szerinti értelmezése az információs fölényhez kapcsolódik, annak azon részét képezi, amely az információs dimenzióban realizálódik, és amelynek elérését a hálózatba kötött elektronikai rendszerek kihasználása, sajátoldali védelme és a másik fél oldali támadása biztosítja. Cyberfölény nélkül a teljes információs fölény nem vívható ki és nem tartható meg. [12]

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

- kinetikus energián alapuló hadviselés, amely a fizikai dimenzióban kerül végrehajtásra és az információs infrastruktúrák, infokommunikációs rendszerek elemeinek fizikai úton való pusztítását, rongálását, tönkretételét jelenti;
- kognitív hadviselés, amely alapvetően a tudati, értelmi dimenzióban érvényesül, és a katonai megtévesztést, műveleti biztonságot illetve a pszichológiai műveleteket foglalja magába;
- hálózati hadviselés, amely az információs dimenzióban realizálódik, és az elektronikai hadviselést valamint a számítógép-hálózati hadviselést tartalmazza. [14]

Az információs dimenzióban megvalósuló hálózati hadviselés a fenti értelmezés – illetve a cybertér hálózatos rendszerekre való értelmezése – alapján nem más, mint a cybertérben megvalósuló műveletek összessége, vagyis más szóval a cyberhadviselés. Mint ahogy az információs hadviselés alapját képezik az információs infrastruktúrák, illetve az összadatforrású felderítés, úgy a cyberhadviselés alapját is a hálózatokra épülő elektronikus információs rendszerek, és a különböző szenzorhálózatokra épülő elektronikai felderítés adja. (3. ábra)




3. ábra. Cyberhadviselés és az információs hadviselés kapcsolata [12]

A cyberhadviselés célja a cyberfölény kivívása és fenntartása egyfelől a saját oldali elektronikus, hálózatalapú információszerző, információtovábbító-, feldolgozó rendszerek védelmével, másfelől a másik fél hasonló rendszerei működésének zavarásával, korlátozásával, lefogásával, vagy akár elektronikus úton történő megsemmisítésével.

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

A cyberhadviselés módszerei közé sorolhatjuk pl. a távközlési hálózatok lehallgatását, zavarását, a navigációs rendszerek elleni elektronikai ellentevékenység különböző formáit, a számítógép-hálózatok feltérképezését, azokba való bejutást és az adatbázisok tönkretételét, a szerverek túlterhelését. A felsorolt néhány cybertéri tevékenység csak kiragadott példa arról a széles palettáról melyek támadó céllal alkalmazhatók a másik fél elektronikai rendszerei és számítógép-hálózatai ellen, illetve védelmi jelleggel a saját hasonló rendszereink megóvása érdekében.

A cyberhadviselés összetevői:

- az elektronikai felderítés;
- az elektronikai hadviselés és
- a számítógép-hálózati hadviselés.

**Az elektronikai felderítés,** mint információszerző tevékenység általában kettős céllal kerülhet végrehajtásra. Egyrészt az infokommunikációs rendszerekben tárolt és továbbított adatokhoz való hozzáférés és azok felhasználása céljából, másrészt a hatékony támadás kivitelezéséhez szükséges célinformációk megszerzése céljából. A kritikus információs infrastruktúrák elleni támadások hatékonysága nagymértékben függ attól, hogy a támadást elkövető tudja-e, hogy az adott objektum, rendszer fizikailag hol helyezkedik el, milyen a strukturális összetétele, milyen hardver és szoftver elemekből áll, milyen célú és mennyiségű adatforgalom zajlik rajta keresztül, vannak-e gyenge pontjai, és ha igen hol, illetve kik az adott információs rendszer vagy hálózat üzemeltetői, és felhasználói. [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. [11]

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

Az elektronikai támogató tevékenység – hasonlóan az elektronikai felderítéshez – az elektromágneses és más tartományú kisugárzások jeleinek érzékelésével, azonosításával és azok felhasználásával kapcsolatos tevékenység. Ezek alapján képes különböző fenyegetések jelzésére, meghatározására, illetve elektronikai ellentevékenység hatékony végrehajtása érdekében célmegjelölésre.

Az elektronikai ellentevékenység az elektronikai hadviselés támadó képessége (több esetben elektronikai támadásnak is nevezik), ami abban nyilvánul meg, hogy minden olyan technikát, módszert és eszközt felhasznál, ami az elektromágneses és más irányított energiák felhasználásával képes működésképtelenné tenni a szembenálló fél elektronikai eszközeit. Az elektronikai ellentevékenységet elektronikai zavarással, elektronikai pusztítással és elektronikai megtévesztéssel lehet megvalósítani.

Az elektronikai védelem az elektronikai hadviselés azon területe, amely biztosítja az elektromágneses, és egyéb fizikai tartományok saját részről történő hatékony használatát a másik fél elektronikai támogató és ellentevékenysége, valamint a saját nem szándékos elektromágneses interferenciák ellenére. [15]

**A számítógép-hálózati műveletek** egyrészt a másik fél hálózatba kötött informatikai rendszerei működésének befolyásolására, lerontására, lehetetlenné tételére irányulnak, másrészt viszont a saját hasonló rendszerek működésének fenntartására törekszenek. Látható tehát, hogy e tevékenység során itt is támadó és védelmi típusú műveletekről beszélhetünk.

A számítógép-hálózati műveletek magukba foglalják:

- 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 műveletek körébe tartozik a számítógép-hálózati felderítés, a számítógép-hálózati támadás és a számítógép-hálózati védelem.

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.

A **számítógép-hálózati védelem** a saját számítógép-hálózat megóvását jelenti a jogosulatlan hozzáféréssel és behatolással szemben, amelyet abból a célból hajtanak végre, hogy megszerezzék az adatbázisokban tárolt adatokat és információkat, illetve, hogy szándékosan lerontsák, működésképtelenné tegyék információs rendszerünket. [16]

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

## *3.3. Cyberbűnözés, cyberterrorizmus*

2001. szeptember 11-ét követően a terrorizmus ismét a figyelem középpontjába került. Az ezt követő elemzések a hagyományos terrorizmust[17], mint a 21. század elejének legfőbb kihívását elemzik és vizsgálják. A hagyományos terrorizmus mellett azonban napjainkban egyre gyak-

[17] A hagyományos terrorizmus alatt az olyan eszközöket, eljárásokat és akciókat, illetve az ezek mögött álló embereket vagy csoportokat értjük, amelyek a már „megszokott" módon– ember-rablásokkal, robbantásokkal, öngyilkos merényletekkel, illetve az ezekhez hasonlatos módszerekkel – kívánják céljaikat elérni.

rabban esik szó a cybertérből leselkedő hasonló veszélyről. Az elmúlt években a terrorizmussal foglalkozó szakemberek jelentős része még nagyon gyakran egy kézlegyintéssel elintézte ezt a fajta veszélyt, mondván rendkívül kicsi a valószínűsége egy a cybertérből érkező terroristatámadásnak. Azonban ahogy nő az információtechnológia dominanciája a mindennapokban, úgy erősödnek azok a szakértői figyelmeztetések, amelyek e veszélyek fokozódására próbálják meg felhívni a figyelmet.

Ennek oka elsősorban az, hogy amilyen rohamosan fejlődik az információtechnológia, ahogy nő az infokommunikációs eszközök és rendszerek száma úgy nő annak a veszélye, hogy rendszereinket, eszközeinket megtámadják, illetve a megtámadott eszközöket – akár azok tulajdonosainak tudta nélkül[18] – további támadásokra felhasználják.

Infokommunikációs eszközök és hálózatok természetesen nem csak otthonainkban vannak. Azokat az infrastruktúrákat, amelyek a mindennapi életünket kiszolgálják, segítik, vagy támogatják szintén ilyen rendszerek, szenzorok, távközlő hálózatok, számítógépek, számítógéphálózatok, stb. működtetik és irányítják.

Mindezeknek megfelelően meg kell vizsgálni, hogy melyek azok az akár hagyományos, akár információtechnológiai eszközök és lehetőségek, amelyekkel számítógépeink, hálózataink, illetve az információs infrastruktúráink támadhatók.

### 3.3.1. Hagyományos terrorizmus [17]

Ahhoz, hogy az információs dimenzióból érkező esetleges terrortámadásokat – információs terrortámadásokat – meg tudjuk vizsgálni, célszerű néhány olyan tényező felvillantása, amelyek a hagyományos terrorizmussal, mint rokon fogalommal kapcsolatosak. Ilyen főbb tényezők lehetnek a terrorizmussal kapcsolatos főbb fogalmak, szereplők és mozgatórugók áttekintése, mivel számos azonosság tételezhető fel a hagyományos és az információs terrorizmus különbö-

[18] Az ilyen számítógépeket zombi-nak nevezik. A felhasználó tudta nélkül különböző rosszindulatú, pl. trójai programok telepítődnek a gépre, amelyek azután részlegesen vagy teljes egészében átveszik az irányítást a gép felett, és onnan különböző támadásokat és egyéb tevékenységeket végeznek. Részletesebben a Malware-k (rosszindulatú szoftverek) című alfejezetben kerül ismertetésre ez, illetve az ehhez kapcsolódó egyéb támadási formák.

ző formái között. Mindezeken túl, amennyiben sikerül felvázolni néhány jelentős tényezőt a hagyományos terrorizmus kapcsán, akkor talán sikerül az információs terrorizmus néhány hasonló jellemzőjét – az erre a tevékenységre, illetve az ebben szereplők esetében – megvizsgálni. Jellemzők lehetnek:

- az okok;
- a szereplők;
- a célok és
- a végrehajtás módszerei.

Természetesen ezt a rövid bemutatást az is indokolttá teszi, hogy első megközelítésben is látszik az a tény, hogy a hagyományos terrorizmus és a cybertérből érkező terrorizmus egymásra találása, párhuzamosan elkövetett, egymást mintegy kiegészítő akcióik hatványozottan nagyobb károkat okozhatnak, mint a külön-külön elkövetett hagyományos-, illetőleg cyberterrortámadások.

A mai értelemben vett hagyományos terrorizmus az 1970-es években történt számos terrorakció kapcsán került ismét a figyelem középpontjába. Talán még sokak emlékezetében élénken él az olyan terrorcsoportok neve, mint például a Fekete Szeptember[19], IRA[20], Baader–Meinhof Csoport[21] vagy a Vörös Brigádok[22], amelyek abban az időben a napi hírek meghatározói voltak a különböző akcióikkal.

[19] 1972. augusztus 26. és szeptember 11. között Münchenben rendezték meg a XX. nyári olimpiát. Szeptember 5-én a Fekete Szeptember nevű terrorista csoport nyolc tagja az olimpiai faluban behatolt az izraeli csapat szálláshelyére, ahol két izraeli sportolót megöltek és kilencet túszul ejtettek. Miután az izraeli kormány megtagadta a követelt 200 palesztin fogoly szabadon bocsátását, a terroristák a német kormánytól repülőgépet követeltek a túszok elszállítására. A terroristákat és a kilenc túszt két helikopteren átszállították a fürstenfeldbrucki katonai repülőtérre, ahol egy Boeing repülőgép már várakozott, hogy elszállítsa őket valamelyik arab országba. A repülőtéren a német rendőrség túszmentési akciót kezdeményezett, amely olyan szerencsétlenül végződött, hogy a terroristák megölték túszaikat, illetve a tűzharcban öt terrorista és egy rendőr is meghalt. A három további terroristát elfogták. [18]

[20] 1972. január 30-án – amit azóta „véres vasárnapként” emlegetnek – a brit katonák az internálás ellen tüntető tömegbe lőttek, és 13 embert megöltek. Egyes vélemények szerint ez az esemény járult a leginkább hozzá ahhoz, hogy az IRA terrorista szervezetté váljon. Az IRA 1972 februárjában kezdte meg terrorhadjáratát a protestáns és a brit célpontok ellen. Az erőszak megfékezésére a brit kormány felfüggesztette az észak-ír parlamentet és átvette az országrész irányítását, ahol már tizenötezer brit katona állomásozott. Az IRA bomba-merényletekkel és gyilkosságokkal válaszolt erre a lépésre. [19]

[21] Andreas Baader és Ulrike Meinhof vezette csoport nevéhez számos — az 1970-es évek elején elkövetett — merénylet és gyilkosság fűződik. Csoportjukat később átnevezték a RAF–Rote Armee Fraktion, azaz a Vörös Hadsereg Frakció névre.

2001. szeptember 11-e azonban újra a mindennapok részéve tette a terrorizmust. A Pentagon és a Világkereskedelmi Központ elleni merényletek rádöbbentették a világot arra, hogy a hidegháború elmúltával már nem a nagyhatalmi szembenállás a legfőbb veszélyforrás, hanem a terrorizmus, illetve ennek egyik legveszélyesebb formája: a nemzetközi terrorizmus. September 11-ét követően írások, elemzések és szakértői magyarázatok tucatjai születtek a terrorizmust, mint a 21. század új és egyik meghatározó veszélyforrását elemezve. Ezek közül számosat tanulmányozva választ kaphatunk a következő kérdésekre, amelyek további tanulmányozása, illetve az azokból levont következtetések segíthetik a cyberterrorizmus megértését. Ilyen megvizsgálandó kérdések lehetnek:

- a háború és a terrorizmus fogalmi és tartalmi elkülönítése;
- az állami terror és a nem állami terrorista csoportok vizsgálata;
- a terrorizmus mozgatórugójának, motivációinak vizsgálata.

Mielőtt ezeket nagyon röviden megvizsgálnánk, szükségessé válik a terrorizmus fogalmának meghatározása. Ez azonban meglehetősen nehéz feladat, hiszen egyrészt nem létezik egységesen elfogadott definíció, másrészt pedig akárhány megfogalmazást is nézzük, azok számos ponton eltérnek egymástól. Ennek oka elsősorban talán abban keresendő, hogy a fogalom megalkotói más és más szemszögből vizsgálják a kérdést, és így természetszerűleg más és más álláspontot is képviselnek. Mindezek ellenére – vagy talán éppen az előbb említett okok miatt –, álljon itt egyetlen megfogalmazás a terrorizmus leírására, amelyet a Magyar Hadtudományi Társaság határozott meg a Hadtudományi lexikonban: „*Terror, megkülönböztetés*

[22] Vörös Brigádok — *Brigate Rosse*, olasz terroristacsoport, amely a 60-as évek végén Renato Curcio vezetésével szerveződött a Trentói Egyetem szélsőbaloldali köreiben. Tagjai lelkesedtek a forradalom eszméjéért, a parlamentáris demokráciát csak álarcnak tartották, amely mögött zavartalanul folyik a kizsákmányolás és az elnyomás. Céljuk az állam meggyengítése és a proletárforradalom kirobbantása volt. Ezt gyújtogatások, robbantások, emberrablások, gyilkosságok útján akarták elérni. Aldo Moro, volt olasz miniszterelnök, a baloldallal történelmi kiegyezést kereső kereszténydemokrata politikus 1978. március 16-i elrablásával, majd megölésével politikai válságot idéztek elő. Ők a felelősek a bolognai pályaudvar felrobbantásáért is. Bár a csoport tagjait már a 70-es évek közepétől kezdték letartóztatni és elítélni, aktivitásuk a 80-as évek végéig tartott. A megszűntnek hitt szervezet 2003 őszén ismét hallatott magáról. Az olasz rendőrség ekkor tartóztatott le hat embert, akit Massimo D'Antona kormányzati tisztviselő négy évvel azelőtti, és Marco Biagi tanácsadó 2002-es megölésével vádoltak. [20]

*nélküli támadás: minden olyan erőszakos cselekmény, vagy azzal való fenyegetés, amelynek elsődleges célja, hogy rettegést keltsen a polgári lakosság körében."* [21]

Amióta az emberiség „feltalálta" a háborúskodást és háborúkat vív egymással, azóta minden háború természetszerűleg erőszakos cselekményeket tartalmaz és félelmet kelt az emberekben. Amiben a háború mégis különbözik a terrorizmustól az az, hogy itt nem elsődleges cél a terrorizálás, a félelemkeltés, hanem az csak egy járulékos tény, hiszen Clausewitz-el élve a háború nem más, mint a politika folytatása erőszakos eszközökkel; két élő erő nyílt összeütközése. Egy másik meghatározó különbség a háború és a terrorizmus között az lehet, hogy a háborúkat alapvetően államok vívják, míg a terrorizmust az állammal (vagy több állammal) szembenálló, nem állami csoportok, szervezetek jelenítik meg. Ehhez még az a jellemző is hozzájárul, hogy *„a terrorizmus lényege egyértelműen a nyílt ütközet tagadása."* [22]

Természetesen a történelemben nagyon sok példát láthatunk arra, hogy az állam, vagy az állami hatalmat gyakorlók lépnek fel a terror eszközeivel, az ország állampolgáraival szemben. Ez a fajta terror azonban inkább elnyomó, sokszor brutálisan totális befolyása miatt érdemli ki ezt a jelzőt, ellentétben az általunk tárgyalt hagyományos terrorizmus figyelemfelkeltő, demonstráló jellegével.

Későbbi vizsgálataink előtt – amelyek a cybertérben potenciálisan meglévő terrorizmusra irányulnak –, fontos tisztázni, hogy mi, vagy mik azok a motivációk és mozgatórugók, amelyek a hagyományos terrorizmus esetében tapasztalhatók. Fontos ennek kiderítése, illetve feltérképezése, hiszen amennyiben ebben az esetben találunk egyértelmű és kézzelfogható indítékot, akkor ennek analógiáján megkereshető a cyberterror esetében az a kiinduló ok, amely az ottani akciókat mozgathatja és motiválhatja.

Megvizsgálva számos terrorakciót közös tényként értékelhető, hogy minden terrorakció egyik kulcseleme a **nyilvánosság.** Ez az egyik, nagyon sok esetben – eltekintve a hasonló kivitelezési módoktól –, az egyetlen közös a különböző terrorakciók között. Függetlenül az indítéktól, minden terrorszervezet számára létfontosságú a nyilvánosság különböző fokú biztosítása, hiszen csak ezen keresztül lehetséges, hogy a társadalom szélesebb rétegei is kapja-

nak információt magáról az akcióról, illetve a szervezet céljairól. A terrorszervezet csak így tudja biztosítani, hogy az erőszakos eszközökkel elkövetett akciók a megfélemlítésen, a bizonytalanságon keresztül befolyásolják a közvéleményt, illetve a kormányzatot. Így tehát a terrorakciók a nyilvánosság számára és a nyilvánosság befolyásolására születnek. Ennek hiányában a terrorizmus értelmetlen és céltalan!

### 3.3.2. Terrorizmus és információtechnológia [17]

A 20. század végének és a 21. század elejének társadalmában az információtechnológia és az erre épülő technika rohamos térhódítása már-már mindennapos ténynek számít.

Természetesen a különböző terrorista szervezetek és csoportok is ugyanúgy – hacsak nem jobban! – használják, és kihasználják a csúcstechnika nyújtotta lehetőségeket, mint a hétköznapok többi szereplője. A következőkben néhány olyan tevékenység felsorolása és rövid elemzése történik, amelyek során a hagyományos terrorszervezetek az információtechnológiával kapcsolatba kerülhetnek.

**Tervezés**

Természetesen a hagyományos terrorista szervezetek tagjai is használják az információtechnológia nyújtotta lehetőségeket, hiszen őket sem hagyja érintetlenül a 21. század. Az internet segítségével kommunikálhatnak, szervezhetik akcióikat. Az internetről letölthető és viszonylag könnyen kezelhető titkosító programok segítségével még annak a veszélye is igen kicsi, hogy kommunikációs, kapcsolattartó tevékenységüket „lehallgassák”.[23] A titkos üzenetváltás egy másik módszere lehet az úgynevezett szteganográfia[24]. Ez azt jelenti, hogy látszólag érdektelen és ártalmatlan hordozókba építenek be a kívülállók számára láthatatlan módon információkat.

[23] Meg kell azonban jegyezni, hogy gyakran hangoztatott szakértői vélemények szerint a kódolt adatcsomagok megfejtése, és ezáltal az információtartalom visszanyerése az esetek jelentős részében az elektronikus felderítésre szakosodott NSA-nek (National Security Agency) nem jelent különösebb gondot.

[24] A szteganográfia nem a 21. század találmánya. Már az ókorban is használtak olyan eszközöket és eljárásokat, amelyek segítségével titkos üzeneteket lehetett küldeni valamely nyílt üzenetbe rejtve. Ilyen volt például a „láthatatlan” tinta, amely alkalmazásával az üzenet csak akkor vált láthatóvá, ha megfelelő hőmérsékletűre melegítették. Napjainkban a szteganográfia a digitális technika alkalmazásával újra fénykorát éli.

Ilyenek hordózók lehetnek például különböző formátumú képek, ahol a kép digitális jelei közé vannak elrejtve az információk, vagy ilyen lehet akár egy hang fájl is, amely esetében a háttérzaj tartalmazhatja az információt. Mivel ezekben az esetekben nincs semmi, ami a titkos információtovábbításra utalna ezért legtöbbször nem is kerülnek a „felderítők" látókörébe.

**Toborzás, propaganda, pénzügyi támogatás**

Új tagok verbuválása, toborzása terén szintén hatalmas lehetőségeket nyújt az internet a hagyományos terrorista szervezetek számára. A különböző terrorista szervezetek által fenntartott weboldalakon nyíltan is történik új tagok toborzása. Ezeken az oldalakon a potenciális új tagok meggyőzésére számos megoldás kínálkozik. A webes technikának köszönhetően egy weboldalon lehetőség van felhívni az érdeklődők figyelmét az „ügyre" különböző írásokkal, publikációkkal, a szervezet történetének és vezetőinek bemutatásával, az eddigi akciókról készített videók, pedig sokszor le is tölthetők. Lehetőség van továbbá pénzbeli adományok[25] gyűjtésére is e lapok segítségével.

A toborzás terén olyannyira követik a trendeket, hogy a hagyományos propagandafilmek helyett, amelyek hosszúak, unalmasak, nehezen követhetőek voltak, olyan új médiumokat láthatunk, mint például a rövid, színes mozgalmas flash animációk, vagy a gyerekeknek szánt vicces képek. Ezek sokkal jobban megragadják a figyelmet, mint a már említett hagyományos, egy kamerával rögzített, a vezető (pl. Oszama Bin Laden) beszédeit több tíz percen keresztül mutató videók. Az új médiumtípusokkal elsősorban a fiatalokat célozzák meg.

**Adat- és információszerzés**

Gyakran ismételgetett, és már-már szállóigévé vált meghatározás az internettel kapcsolatban: „ami nincs az interneten, az nincs is". Ez a kissé vicces kijelentés arra utal, hogy ma már gyakorlatilag nincs az életnek olyan területe, amelyről ne találnánk legalább egy kicsinyke információmorzsát az interneten.

[25] Ezt a fajta tevékenységet donation–nak nevezik, amely közvetett pénzügyi támogatást jelent. A szervezetet támogatni szándékozónak nincs más dolga, mint egy meglehetősen egyszerű elektronikus űrlapot kitölteni, megadni az adatait, bankkártyája számát, a kívánt összeget, és már kész is.

A terrorista szervezetek számára is adott hát a lehetőség, hogy a számukra szükséges információkat megkeressék, és ami ennél sokkal rosszabb – meg is találják. A „házkészítésű bomba” (homemade bomb) szavakat begépelve az egyik legismertebb internetes keresőbe 0,29 másodperc alatt kb. 2,7 millió találatot kapunk. Ezeknek a találatoknak a jelentős része természetesen a terroristák esetében irreleváns. De a találatok között van olyan, amely kész recepttel szolgál az otthon, akár a kereskedelemben szabadon megvásárolható alapanyagokból való bombák előállításához („konyhakész bomba”). A találatok között nagyon sokáig keresnünk sem kell, hogy akár kész video-filmeket is találjunk a témában.

A nyugati társadalmak információszabadsága a különböző terrorszervezetek számára tehát nagyon hasznos, hiszen az internet révén olyan adatokhoz és információhoz is hozzáférhetnek, amelyek megszerzése szinte elképzelhetetlen lett volna 15-20 évvel ezelőtt, nem beszélve arról, hogy maga az információszerzés is hallatlan kockázattal járt volna.

A nyílt csatornákon történő információszerzésre az egyik legjobb példa, hogy 2003 januárjában Donald Rumsfeld, akkori amerikai védelmi miniszter, kiadott egy utasítást, mely szerint azonnal radikálisan csökkenteni kell a DoD és egyéb USA intézmények olyan weboldalainak a számát, illetve tartalmát, amelyeken keresztül különböző terrorszervezetek szenzitív információkra tehetnek szert, vagy a különböző honlapokon külön-külön meglévő adatok felhasználásával juthatnak értékes, az USA számára pedig hihetetlenül veszélyes következtetésekre. Ennek az utasításnak az apropója az az Afganisztánban talált terrorista kézikönyv volt, amelyben a felhasznált információk több mint 80%-a nyílt DoD weboldalakról származott. [23]

### 3.3.3. Támadók a cybertérben [17]

Mielőtt megvizsgálnánk, hogy kik is azok, akik potenciálisan szóba jöhetnek, mint cyberterroristák, meg kell vizsgálnunk, hogy kik is azok, akik a cybertérben olyan tevékenységeket folytatnak, amelyek adott esetben akár terrorista – esetünkben cyberterrorista – akciók

végrehajtására is alkalmasak lehetnek. A vizsgálatot természetesen a cybertér szereplőivel kell kezdenünk:

- Hackerek: A hacker olyan személy, aki internet segítségével hozzá tud férni védett adatokhoz a számítógépeken. Kezdetben külön fogalmat alkottak a hackerek, akik azért törtek fel rendszereket, weboldalakat, illetve programokat, hogy bizonyítsák azok gyenge pontjait, azonban ezeket a hiányosságokat a rendszergazdák tudomására hozták, azaz általában jóindulatúan jártak el. Ők voltak az úgynevezett fehérkalaposok, azaz a „white hat" csoport tagjai. Az ellentábort azok a fekete kalaposok, „black hat" alkották, akik sokszor rosszindulatból, vagy valamilyen haszonszerzés reményében hatoltak be egy–egy rendszerbe. Ma már általában gyűjtőnévként csak a hackert használják, függetlenül a behatolás okától. Korábban igen elterjedtek voltak az úgynevezett phreak-ek, akik csoportjai telefonvonalat lopva jutottak anyagi előnyökhöz. A phreak-ek a telefonközpontok vezérlő számítógépeinek, a távközlési vonalak ingyenes igénybevételének és általában a telekommunikációnak a szakértői voltak. Rendelkeztek azzal a tudással, ami a központok átprogramozásához szükséges. Emellett a mobil telefonhálózat forgalmának, belső adatainak lehallgatásához is voltak (vannak) megfelelő eszközeik.
- **Hacktivisták (Hactivists):** A hackerek és az aktivisták tulajdonságait, illetve céljait közösen vallók társasága. Rendszerint valamilyen politikai motivációval rendelkeznek. Számos olyan akciót hajthatnak végre, amelyek során valamilyen – számunkra fontos – ügy érdekében internetes oldalakat törnek fel, átalakítják azok kinézetét, adatokat lopnak el onnan, illetve akadályozhatják az oldal működését pl. virtuális ülősztrájkkal (flood vagy DoS támadással.) Számos esetben támogatnak olyan terrorista szervezeteket, amelyek céljai vagy akciói partikulárisan egybeesnek az övékével. Az egyik ilyen hactivista megmozdulás 1999-ben volt, amikor az Egyesült Államok, illetve a NATO csapatok Szerbiát bombázták, és találat érte a belgrádi kínai nagykövetséget, amely után kínai hackerek tucatjával intéztek támadásokat amerikai szerverek ellen. Napjainkban e

téren az Anonymous csoport hallatja hangját és hajt végre támadásokat különböző szervezetek, de akár országok, kormányok ellen is.

- **Számítógépes bűnözők:** Azok a gyakran igen magas szintű hálózati és számítógépes ismeretekkel rendelkező elkövetők, akik elsődleges célja a pénzszerzés. A később tárgyalt rosszindulatú szoftverek, illetve eljárások alkalmazásával – pl. phishing – hajtják végre akcióikat. Az elmúlt években a számítógépes bűnözők által elkövetett bűncselekmények, illetve az ezekkel okozott károk nagysága nagyságrendekkel nőtt.
- Trendként értékelhető az elmúlt években, hogy míg korábban a jó képességű és sikeres betöréseket végrehajtó hackerek közzétették tapasztalataikat, pl. egy adott rendszerben hol található gyenge, vagy behatolásra alkalmas pont, addig ma már ezt megtartják maguknak, illetve megpróbálnak ezekből az információkból pénzt kinyerni. Azaz felajánlják az általuk feltört rendszerek tulajdonosainak vagy üzemeltetőinek mintegy megvételre ezeket a kulcsfontosságú adatokat. Más esetekben pedig megbízásból, anyagi ellenszolgáltatás fejében – pl.: a behatoláshoz, vagy információszerzéshez tudással, eszközökkel és módszerekkel nem rendelkező hagyományos bűnözői körök számára –, adatokat, információkat szereznek, törölnek vagy módosítanak. Mindazonáltal a hagyományos bűnözésre szakosodott, sok esetben szervezett bűnözői körök is felismerték a pénzszerzés új módszereit ezen a téren. Más esetekben nem a közvetlen pénzszerzés a cél, hanem a más módszerekkel megszerzett illegális jövedelmek nyomainak eltüntetése, vagy e jövedelmek tisztára mosása jelenik meg elsődleges motivációként.
- **Ipari kémek:** Természetesen az iparban elkövetett illegális információszerzés nem napjaink találmánya, hiszen amióta elkezdődött az iparosodás, azóta ez a jelenség állandóan jelen van. Ami mégis új dolog, az a módszerekben és a kivitelben keresendő. A számítógépes tervezés, irányítás és rendszerfelügyelet magában hordozza azt a lehetőséget, hogy a számítógépeken tárolt, vagy a hálózatokon áramoltatott adatokat és információkat illetéktelenek – ebben az esetben ipari kémek: konkurens cégek alkalma-

zottai, vagy éppen az előbb említett számítógépes bűnözők, akik a megszerzett adatok piacra dobásával üzletelnek – szerzik meg. Megjelent tehát egy új, elektronikus csatorna az illegális adatszerzők kezében, amelyen keresztül hatalmas mennyiségű adatot képesek szerezni, amely ráadásul nemcsak polgári cégek adataiban merülhet ki, hanem katonai technológiák adatainak a megszerzésére is irányulhatnak, amelyek esetenként sokkal több pénzt is érnek bizonyos piacokon.

- **Belső szakértők és külső szerződők:** Egy adott vállalat életében óriási szerepet játszanak a szakértők, akik sok esetben számos helyen, akár több telephelyen is végzik munkájukat. A szakértők munkájuk elvégzése érdekében általában magas szintű hálózati hozzáféréssel rendelkeznek. Ebből következően adott esetben – pl.: munkahelyi konfliktusok, zsarolás, stb. – igen értékes adatokat tudnak eltulajdonítani, illetve akár különböző rosszindulatú programok bevitelére is lehetőségük van, hiszen a hálózathoz belülről férnek hozzá.
- A külső szerződők szintén kaphatnak hozzáférési jogokat a hálózathoz, és természetesen szintén számos, igen értékes adathoz férhetnek hozzá, amelyekkel később visszaéléseket követhetnek el.
- **Terroristák:** A terroristák attól függően, hogy milyen célból használják az információtechnológiát, két csoportra oszthatóak. Az első csoportba, azok a terrorista szervezetek tartoznak, amelyek a már említett célokra – propaganda, toborzás, adatszerzés – használják e rendszereket. A másik – sokkal veszélyesebb – csoportba azok a terroristák tartoznak, akik nem csak ilyen, úgynevezett „soft” tevékenységre kívánják használni a rendszereket, hanem azt, illetve azon keresztül rombolni vagy egyéb erőszakos, „hard” cselekményeket is végre akarnak hajtani.

### 3.3.4. Kapcsolat a hagyományos- és a cyberterrorizmus között [17]

Napjainkig mindezidáig egyetlen cyberterrorista, vagy annak nevezhető akció került napvilágra, amely az LTTE (Tamil Eelam Felszabadító Tigrisei) nevéhez fűződik. A szervezet aktivistái 1997-ben spamekkel árasztották el a világ különböző országaiban működő Srí Lanka-i követségek e-mail postaládáit. Az akció nagy kárt nem okozott, de felhívta a figyelmet az információs rendszerek sebezhetőségére. [24]

Az LTTE akciójából azonban látszik, hogy ez nem az a „valódi" cyberterrorista akció, inkább egy hagyományos terrorszervezet új dimenzióban, azaz a cybertérben elkövetett akciója.

Mindazonáltal annak a veszélye, hogy komoly, nagy károkat okozó, az internetet kihasználó, vagy éppen azt, illetve az egyéb hálózatokat támadó valódi cyberterrorista események bekövetkezhetnek igencsak reális. Bizonyítja ezt az is, hogy az FBI (Federal Bureau of Investigation) már konkrét definícióval is rendelkezik, amely elég világosan meghatározza a cyberterrorizmus fogalmát. E szerint: „a cyberterrorizmus olyan bűncselekmény, amelyeket számítógépekkel és telekommunikációs lehetőségekkel úgy hajtanak végre, hogy azok rombolják és/vagy megzavarják a szolgáltatások működését, zavart és bizonytalanságot keltve ezzel a lakosságban. Ezen akciók célja a kormányzat vagy a lakosság erőszakos befolyásolása a szervezet egyéni politikai, társadalmi vagy ideológiai céljai érdekében." [25]

2007 tavaszán azonban bekövetkezett egy olyan esemény, amelyről bizonyos, hogy még sokáig fogunk vitatkozni: cybertámadás vagy háború volt-e.

2007 májusában Észtország internetes hálózata szinte teljesen megbénult. Tallinn felszabadítóinak szovjet emlékműve áthelyezése miatt rendszeres internetes támadásokat szerveztek főként Észtországon kívülről az észt államigazgatás hivatalos kommunikációs vonalainak és weboldalainak blokkolására irányuló kísérletek keretében. E mellett az interneten és mobiltelefon-üzeneteken keresztül folytatódtak az intenzív propaganda-támadások, amelyek fegyveres ellenállásra és további erőszakra szólítottak fel.

Az okokat minden elemző szerint külső terhelések kényszerítették ki. Az első forgalombénító DDoS-támadások május elején kezdődtek, célpontjaik a parlament, a kormányhivatalok, sőt a bankok és az észt média számítógépes központjai voltak. Az észt hálózaton az adatforgalom sokszor órákon át a normális ezerszerese volt. Az ország internetes forgalmát irányító központok napjában többször leálltak, az állami szervek hálózatait le kellett választani az internetről. A banki rendszerek megbénultak, a pénzügyi megbízások rendszeresen akadoztak. A támadások azért is érintették érzékenyen a balti államot, mert kiugróan fejlett az internetes kultúrája.

Május közepén tetőzött a támadási hullám, de utána kisebb intenzitással folyt a terhelés, számos hálózati rendszer még hetekig csökkentett üzemmódban volt csak képes dolgozni. Május 15-én például az ország második bankja, a SEB Eesti Ühisbank a tömeges internetes támadások miatt kénytelen volt felfüggeszteni azt a szolgáltatását, hogy külföldről is be lehet lépni a pénzintézet egyes rendszereibe. Egy észt bank, a Hansabank nyilvánosságra hozta a támadások miatti veszteségét, a jelentés szerint május 10-én több mint egymillió dolláros forgalomkiesést szenvedtek el.

Az elemzők szerint az akciók túlságosan jók és összehangoltak voltak ahhoz, hogy mindössze néhány rosszindulatú programozó indította volna őket. Néhány támadást sikerült orosz szerverekig visszanyomozni, sőt az Európai Parlament állásfoglalásában leszögezte, hogy e támadások az orosz közigazgatás IP címeiről érkeztek, de az alkalmazott technika miatt rendkívül nehéz a forrásokat pontosan meghatározni.

Az Európai Parlament 2007. május 24-én állásfoglalást adott ki ez ügyben. A NATO május közepén szakértőt küldött Észtországba, hogy kivizsgálja a történteket, és segítsen kivédeni a további támadásokat.

Az online beavatkozást sem az észtek, sem az EU, sem a NATO nem minősítette katonai akciónak. A NATO nyilvánosan nem foglalt állást abban a kérdésben, hogy kik volt a támadók, kinek az irányításával történt, támadásnak minősíti-e az eseményeket. A NATO hivatalo-

san bejelentette, hogy a szövetség vizsgálja, milyen hatásai lehetnek ezeknek az akcióknak, s folyamatos kapcsolatban áll az észt szervekkel. [2]

Bár nem tartozik a cyberterrorizmus kategóriájába, de a 2008. augusztus 7-én kirobbant orosz-grúz háború szintén fontos mérföldköve a cyberhadviselés történetének. Az ötnapos háború során elsőként alkalmaztak a fizikai térben zajló katonai műveletekkel összhangban kifinomult cybertámadásokat. Az elsődleges célpontok a grúz kormányzati weboldalak, a kritikus infrastruktúrák és a bankrendszer volt. A támadók a legfontosabb hírportálokat túlterhelték vagy pedig deface-elték[26], kihelyezve rájuk a saját propagandájukat. Magyarán, egyidőben blokkolták a grúz lakosság informálást, illetve terjesztették a saját üzeneteiket. Mindezek mellett igyekeztek minden fontosabb katonai kommunikációs csatornát zavarni, illetve blokkolni.

Az orosz fél tagadta, hogy bármi köze lenne a támadásokhoz, annak ellenére, hogy számos alkalommal visszavezették a behatolásokat Oroszországig, továbbá külön orosz internetes fórumok működtek a háború alatt, ahol megjelölték a grúz célpontokat. [26]

Az orosz-grúz konfliktus egyértelműen megmutatta a modernkori háborúk új jellegét, ahol a katonai műveletek nem csupán a földön, vízen, levegőben, hanem a cybertérben egyaránt folynak.

A különböző helyi vagy nemzetközi konfliktusok idején gyakran tapasztalható, hogy az adott felek szimpatizánsai az interneten is kifejezik véleményüket különböző támadásokkal, amelyek nagyban hasonlítnak a hacktivisták akcióihoz. Így történt ez az izraeli csapatok Gázába történő újbóli 2006 nyarán történt benyomulása esetén is, amikor palesztinokat támogató hackerek 750 izraeli honlapot törtek fel, és megtámadták Izrael legnagyobb bankját is. [27]

Bár nem kapcsolható közvetlenül terrorista szervezetekhez az *Electronic Intifada* (EI) – Elektronikus Intifáda[27] weboldal, amely ars poeticája szerint az izraeli-palesztin konfliktust

[26] A módszer célja, hogy a támadó megváltoztassa az adott weboldal tartalmát, pontosabban elhelyezze rajta a saját üzenetét.

[27] Az intifáda az izraeli megszállás elleni palesztin népfelkelés. Az ún. első intifáda 1987 decemberében kezdődött, miután egy izraeli katonai teherautó a Gáza-övezetben–valószínűleg véletlenül – palesztinok közé hajtva négy embert halálra gázolt. A zavargások 6 éven át tartottak a Gáza-övezetben és Ciszjordániában. A felkelés, ill. ellenállás sajátos formájaként palesztin fiatalok rendszeresen kövekkel dobálták az izraeli katonákat, de sor került sztrájkokra és tüntetésekre is. Az izrae-

próbálja meg bemutatni egy másik – ebben az esetben palesztin – szemszögből. Izraelnek erről biztosan más a véleménye, hiszen láthattuk a terrorista kontra szabadságharcos, illetve az azokat támogatók besorolása igencsak nézőpont kérdése.


1. kép**.** Az EI bemutatkozása [28]

Az világosan látszik az eddig elmondottakból, hogy az igazi, és ki kell mondani: a reális veszélyt az jelenti, amennyiben a hagyományos terrorizmus találkozik a cyberterrorizmussal.

Bár nehéz meghúzni a határt a cybertérben elkövetett bűnözés, amely mint láttuk, bár sokszor rendkívül nagy szakértelmet igényel, mégsem különbözik sokban a köztörvényes bűnözéstől (leszámítva természetesen azt a tényt, hogy ez nem a hagyományos dimenzióban, hanem a cybertérben végzi tevékenységét), valamit a cyberterrorizmus között. A cyberterrorizmust azok a tényezők különböztetik meg a cyberbűnözéstől, amelyeket a hagyo-

li katonák válaszul fegyvert is használtak és több száz embert bebörtönöztek. A válaszlépések közé tartozott a gazdasági szankciók életbe léptetése is, valamint további telepek létesítése a megszállt területeken. Az összetűzéseknek 2000 palesztin és 200 izraeli esett áldozatul. Az első intifádának az 1993-as oslói béke-megállapodás vetett véget. A második intifáda, amelyik még jelenleg is tart, 2000. szeptember 29.-én kezdődött. Ennek kiváltó oka az volt, hogy Ariel Sharon, akkori ellenzéki Likud-pártvezető megjelent Jeruzsálemben a Templomhegyen, és miután ott található az Al-Aksza Nagymecset, a palesztinok provokációnak vették a látogatást. Ugyanakkor vannak olyan vélemények is, hogy mindez csak ürügy volt egy már korábban tervbe vett felkelésre. Az előző intifádához képest jelentős változás, hogy az izraeli katonasággal történő nyílt összecsapás helyett a palesztinok kis fegyveres csoportok, ill. egyéni öngyilkos merénylők bevetésével veszik fel a harcot. [29]

mányos terrorizmusnál is feltérképeztünk, azaz a motiváció – ideológiai, vallási, vagy politikai –, és természetesen a célok, hiszen a cyberterrorizmusnak nemcsak az anyagi haszonszerzés a célja, hanem a kitűzött politikai célok elérése is terrorista eszközökkel: megfélemlítéssel, terrorral.

Mégis azt kell mondanunk, hogy mindezidáig nem láttunk példákat, amelyek igazi cyberterrorista támadásokra utaltak volna. Nem voltak olyan – a cybertérből érkező – támadások, amelyek egyértelmű célpontjai a kritikus információs infrastruktúrák lettek volna. Ez persze nem jelenti azt, hogy nem is lehetnek ilyen támadások. Sajnálatos módon infrastruktúráink jelentős része igen komoly mértékben sebezhető és támadható, akár azokkal az eszközökkel és módszereket, amelyeket ehelyütt is tárgyaltunk. Az is nyilvánvaló és az eddig elmondottakból szintén következik, hogy a hagyományos terrorizmus, illetve a potenciálisan meglévő cyberterrorizmus közös, esetenként egymást kiegészítő, párhuzamos támadásai a legsebezhetőbb, ráadásul a mindennapi élethez nélkülözhetetlen információs infrastruktúráink ellen, beláthatatlan anyagi és humán károkat okoznának.

Abban az esetben, amennyiben egy ilyen közös támadás, vagy az azzal való fenyegetés megjelenik, és azok valóban az információs rendszereinket célozzák, beszélhetünk **információs terrorizmusról**.

Az információs terrorizmus tehát: a cybertámadásokat és a hagyományos terrortámadásokat egyszerre alkalmazó olyan terrortevékenység, amely az információs infrastruktúrákat felhasználva, a kritikus információs infrastruktúra elleni támadásokkal próbálja meg célját elérni.

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 táma-

dási módszereket és eszközöket, és az információs hadviselés teljes repertoárját alkalmazni fogja. [5]

## *3.4. 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 információ-technológiai eszközök konvergenciájából fakad.

Egy másik csoportosítási elv szerint a fenyegetés módszerei szerinti célszerű kategorizálni az információs támadásokat. Eszerint az alábbi támadási módszereket különböztethetjük meg:

- számítógép-hálózati támadás;
- elektronikai felderítés;
- elektronikai támadás.[5]

### 3.4.1. Számítógép-hálózati támadás

**A számítógép-hálózati támadás fajtái**

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 **hálózati 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. [5]

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 (mint ahogy azt korábban a támadó információs hadviselésnél említettük). A közvetlen támadás során a támadó fél egyrészt a különböző információbiztonsági rendszabályokat kikerülve bejut a számítógép-hálózatokba, hozzáfér különböző adatbázisokhoz, és ez által 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 ez által félrevezeti és befolyásolja a helyzetértékelést, illetve hamis adatokkal túlterheli a rendszert, aminek következtében a hálózati hozzáférést akadályozza (lásd 1. táblázat). [9]

**A számítógép-hálózati támadás eszközei és módszerei**

**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 igen nehéz. Alapvetően két nagy kategóriájukat lehet megkülönböztetni:

- a program típusú malware-eket és
- a szöveg típusú malware-eket.

Program típusú malware-ek közé többek között az alábbiakat sorolhatjuk: [17]

- **számítógépvírusok**: a vírusok technikai értelemben olyan rosszindulatú programok, amelyek saját programkódjukat egy másik programhoz hozzáfűzik, és így szaporodnak. A kapcsolódás módjai különbözőek lehetnek, például a vírus saját programkódját beleírja a gazdaprogram kódjába, azaz módosítja azt. Az egyik rendkívül veszélyes fajtája a vírusoknak a makrovírusok. Ezek célpontjai a dokumentumfájlok, amelyek ezeken keresztül is érkeznek, illetve szaporodnak.
- **programférgek (worms):** a programférgek olyan önállóan futó, gazdaprogramot nem igénylő programok, amelyek képesek saját maguk megsokszorosítására. Másolataikat

részben a megtámadott számítógép merevlemezén készítik el, részint pedig a hálózaton keresztül juttatják el.

- **vírusfejlesztő kitek:** a vírusfejlesztő kitek olyan szoftverek, amelyek vírus program megírását és fejlesztését szolgálják. Ezek segítségével komolyabb szoftverfejlesztői vagy programozói tudás nélkül is lehetőség van vírusok megírására és előállítására.
- **trójai programok:** a trójai programok látszólag, vagy akár valóságosan is hasznos funkciókat látnak el, de emellett olyan nem kívánt műveleteket is végrehajtanak, amelyek adatvesztéssel járnak. Például adatokat módosítanak, könyvtárakat, adatállományokat törölnek, stb.
- **backdoor programok:** a backdoor programok eredetileg a rendszeradminisztrátorok, vagy rendszer felügyeleti jogokkal rendelkező személyek részére nyitottak olyan lehetőségeket, hogy a kívánt számítógépet távolról is elérjék, és azon különböző javításokat, illetve beállításokat végezzenek. A rosszindulatú backdoor programok azonban jogosulatlanul próbálnak meg „hátsó ajtókat” nyitni a rendszerhez. Többségük e-mail mellékletként, vagy egyéb letöltés „mellékleteként” érkezik. Az igazi veszélye a backdoor programoknak az, hogy ezek remek megoldásokat nyújtanak a rendszeradminisztrációs jogok megszerzésére.
- **dropperek**: a dropperek a trójai programok speciális fajtájának tekinthetőek, mivel hasonló elven kerülnek a számítógépbe. Ott azonban legyártanak kettő vagy több, az operációs rendszer által futtatható vírust, majd elindítják azokat. Mivel nem saját magát másolja a program, hanem új programot állít elő, ezért ezeket nem lehet a klasszikus vírus kategóriába sorolni.
- **kémprogramok**: a kémprogramok a rendszerbe juttatva, ott elrejtőzve, a háttérből figyelik a rendszer eseményeit és ezekről jelentéseket, illetve adatokat küldenek.

- **keyloggerek**: a keyloggerek a háttérben települve a billentyűleütéseket – így akár a jelszavakat, bankkártya-számokat, azonosítókat is – rögzítik és juttatják ki ezeket az információkat a hálózaton keresztül.
- **egyéb kártékony programok.**

Vannak azonban olyan malwarek, amely nem programként tipizálhatóak, hiszen ezek nem konkrét szoftverek, hanem valamilyen szövegként jelentkeznek, és így jelentenek veszélyt. A szöveg típusú malware-ek néhány fajtái az alábbiak lehetnek: [17]

- **spam**: a spam kéretlen leveleket jelent, amelyek igen változatos témában, ráadásul időnként rendkívül nagy számban érkeznek egy-egy számítógépre. A nagy szám miatt sávszélességet és tárhelyet foglalnak, illetve kiválogatásuk a többi – várt és számunkra hasznos – elektronikus levél közül idő- és energiaigényes.
- **hoax**: a spam egyik speciális csoportja, amelyekben vagy valamilyen veszélyre (vírus, spam, csatolt file) figyelmeztetnek, vagy valamilyen nyereményt (szerencsét) helyeznek kilátásba, ha x helyre továbbítjuk őket. Több veszélyt rejt magában, hiszen amennyiben x helyre továbbítjuk ezeket, akkor sávszélességet és tárhelyet foglalunk le, ugyanakkor lehetnek ezek önmagukban például trójait tartalmazó melléklettel ellátottak is.
- **holland és spanyol lottónyeremény levelek, nigériai csalások:** az emberek naivitására és gyanútlanságára építő e-mail alapú malwer-ek. Vagy valamilyen lottónyereményt ígérnek, amely átvételéhez csak be kell fizetnünk néhány tíz dollárt, vagy valamilyen nigériai (olaj) üzletember zárolt bankszámlájának a feloldásához kérnek tőlünk segítséget, természetesen részesedés fejében, amelyhez szintén csak át kell utalnunk néhány száz dollárt.
- **phishing**: az utóbbi idők egyik legelterjedtebb csalásra, illetve az emberek hiszékenységére és megtévesztésére épülő eljárása. A phising, azaz az „adathalászat” eljárása roppant egyszerű. Látszólag a bankunktól érkezik egy e-mail, amelyben arra szólítanak fel, hogy valamilyen banki átalakítás után legyünk kedvesek adatot egyeztetni. Ehhez

előzékenyen meg is adnak egy linket, amely látszólag a bank oldalára mutat. Rákattintva erre a hivatkozásra a bankéval látszólag tökéletesen megegyező honlapra kerülünk, ahol kérik a login nevünket, jelszavunkat és elektronikus azonosítónkat is. A honlap azonban csak látszólag a banké. A csalók az eredeti banki oldalhoz a megtévesztésig hasonló oldalra navigálták így a felhasználókat, akik közül sokan bedőlnek, és meg is adják adataikat. Ezeket az adatokat azután a csalók elektronikus vásárláshoz, vagy pénzátutaláshoz használják a saját céljaikra. A bankok és a média tömeges és látványos, a veszélyre figyelmeztető felhívásokat tesznek közre időről-időre, de ennek ellenére még mindig euró milliárdokra tehető a phishing-el okozott veszteség Európában.

- **pharming**: szofisztikáltabb megoldás az adathalászatra, amely a számítógépen található hosts fájlba írja bele a meghamisított banki oldalak címét. Ennek megfelelően a megtámadott számítógépen a felhasználó hiába írja be böngésző címsorába bankja URL címét, a címfeloldás nem a megszokott DNS-szerveren történik, hanem helyben, az átírt hosts fájl segítségével, és az ügyfél a hamis banki oldalon találja magát, ahol gyanútlanul megadja adatait.
- **egyéb, szöveges típusú kártékony tartalmak.**

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;
- vezérlés-átvétel, 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;
- denial of service;
- distributed denial of service;
- spamming, viral ~ (pl.: love-letter);
- man-in-the-middle attack;

- SMTP backdoor command attack;
- IP address Spoofing attack;
- IP fragmentation attack;
- TCP Session High jacking;
- information leakage attack;
- JavaScript,- applet attack;
- cross site scripting (XSS), és még sok más.

E tanulmány keretében 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 Carnivore 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. [36]

A **Denial of Service (DoS)** támadások – ami magyarul szolgáltatás-megtagadással járó támadást vagy túlterheléses 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. [30]

A DoS támadásoknak két nagy típusa ismeretes: a protokolltámadások és az ún. 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 támadás irányulhat a célpont hálózati kapcsolatának, vagy pedig a célpont valamely – szolgáltatást nyújtó – alkalmazásának túlterhelésére. Ennek megfelelően szokás a támadásokat hálózati vagy alkalmazási rétegben végrehajtott típusokra osztani, az OSI[28] modell két rétegére utalva. [31]

A DoS támadások többnyire ún. **elosztott támadások (Distributed DoS – DDoS),** ahol több támadó, egy időben több végpontról, együttesen kívánja előidézni a rendszer összeomlását. A DDos támadásoknál igen gyakran olyan gépeket vesznek igénybe, amelyek nem is tudnak arról, hogy egy ilyen típusú támadás aktív részesei. Ehhez természetesen ellenőrzést kell szerezni a támadásra szolgáló számítógépek felett. 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 gé-

[28] Open Systems Interconnection (OSI) Reference Model, magyarul, a Nyílt Rendszerek Összekapcsolása referencia modell. Az OSI modellje a hálózatok kommunikációjához a különböző protokollok által nyújtott funkciókat egymásra épülő rétegekbe sorolja. Minden réteg csak és kizárólag az alsóbb rétegek által nyújtott funkciókra támaszkodhat, és az általa megvalósított funkciókat pedig csak felette lévő réteg számára nyújthatja.

pet „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. Az ilyen – zombinak nevezett – számítógépek hálózatba szervezhetők, amelyekkel veszélyes támadások indíthatók. Ezeket a hálózatokat botneteknek nevezik. Ugyanúgy, mint a hagyományos DoS támadásokat, a DDoS akciókat is lehetséges a hálózati rétegben vagy az alkalmazási rétegben kivitelezni.

A DDoS támadási módszerek továbbfejlesztését jelentik a **reflektív DDos** támadások, amelyeknek során más, "ártatlan" végpontokat használnak fel támadóként (vagy inkább fegyverként). Ezeket a végpontokat nem szükséges uralni, elegendő az Internet sajátosságait megfelelő módon kihasználni. A reflektív támadás során a támadó gondosan megválasztott adatforgalom segítségével arra készteti a támadásban részt vevő ártatlan végpontokat, hogy a célpont számára kárt okozó adatforgalmat generáljanak, ezért a tényleges támadó kiszűrése szinte lehetetlen. A DDoS támadásokhoz hasonlóan a reflektív DDos támadások is kivitelezhetők a hálózati és az alkalmazási rétegben egyaránt. [31]

Napjainkban számos DDoS támadással találkozhatunk. Szinte naponta kapjuk a híreket, hogy különböző ismert és nagy forgalmú weboldalak DDoS támadás áldozatává váltak. Az egyik legnagyobb nyilvánosságot kapott ilyen támadás volt a korábban ismertetett orosz – észt cyber – háborúnak kikiáltott eset.

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.

A számítógépek, hálózatok és egyéb elektronikai eszközök elleni fenyegetési módszerek között találhatók hardver eszközökre alapuló eljárások is. Ilyen hardveres támadás például a **chipek manipulálása (Chipping)**. Ma a nagy integráltságú áramkörökbe, processzorokba több millió tranzisztort integrálnak egyetlen lapkára. A chipek dokumentációja üzleti okokból sem tehető publikussá, különösen nem akkor, amikor még a piacon van. A megjelenő rend-

szervázlatok igen nagy vonalakban képesek a belső felépítést bemutatni, és egyébként is ki garantálja, hogy csak az van a lapkán, ami a katalóguslapon megjelenik.

A chipping alkalmazása az elektronikai, informatikai eszközök elleni támadási lehetőségek széles tárházát kínálja. A piacon milliós tételben eladott áramkörök belsejében olyan funkcionális egységek is elhelyezkedhetnek, amelyeket szigorú titokban, és feladattal terveztettek bele. Adott politikai, gazdasági, vagy katonai szituációban a gyártó ország (amely általában nem a legszegényebb elmaradott országok közül kerül ki) úgy dönt, hogy a feszültség fokozódásának egy bizonyos pontján pl. egy műholdról adott jeleket sugározni az arra tervezett áramkörök számára, vagy a hálózatokon át megfelelő programot elindítani a világhálón lévő számítógépek millióira. A parancs a chipbe jutva tetszés szerinti működést válthat ki, leállhat, időlegesen, vagy véglegesen tönkremehet. Mivel ez ellen védekezni mindaddig nehéz, sőt lehetetlen, amíg saját mikroelektronikai gyártási technológiával és termékekkel nem rendelkezik egy ország, addig nem zárható ki a chipping lehetősége. [11]

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.

### 3.4.2. Elektronikai felderítés

**Az elektronikai felderítés alapjai**

Az információs társadalom technológiai fejlettségéből adódóan fokozottan jelen vannak, sőt meg is sokszorozódott a számuk, azoknak az elektronikai eszközöknek, rendszereknek, amelyek potenciális adat-, vagy információforrást jelentenek. Ugyanakkor, köszönhetően éppen az új technikákban és technológiákban rejlő információvédelmi lehetőségeknek, rendkívüli módon megnehezült ezekből a potenciális forrásokból a közvetlenül felhasználható információ kinyerése.

Az elektronikai felderítés, mint információszerző tevékenység általában kettős céllal kerülhet végrehajtásra:

- az infokommunikációs rendszerekben tárolt és továbbított adatokhoz való hozzáférés és azok felhasználása céljából, illetve
- 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. [11]

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.

A felderítés fajtáit tekintve számos felosztással, kategorizálással találkozhatunk. A jelenleg még érvényben lévő Magyar Honvédség Összhaderőnemi doktrínáját alapul véve a felderítés fajtái az alábbiak:

- emberi erővel folytatott felderítés (Human Intelligence – HUMINT): bármely, emberi adatforrástól, illetve bármilyen adatszolgáltatótól szerez felderítési adatot;
- képfelderítés (Imagery Intelligence – IMINT): a fotografikus, radar, elektrooptikai, infravörös, hő, illetve multispektrális érzékelők által vett jelekből képzett képanyagból állít elő adatot;
- rádióelektronikai felderítés (Signals Intelligence – SIGINT): rádiófelderítésre (Communications Intelligence – COMINT) illetve rádiótechnikai felderítésre (Electronic Intelligence – ELINT) osztható. A COMINT a szembenálló fél kommunikációs rendszereinek lehallgatásával szerez információt, az ELINT pedig a kisugárzott nem kommunikációs elektromágneses jelek (pl. radarok) elemzéséből szolgáltat adatot;
- hangfelderítés (Acoustic Intelligence – ACINT): akusztikai tartományból származó adatokat állít elő;
- kisugárzás és jelfelderítés (Measurement and Signature Intelligence – MASINT): a különböző tartományokban műszeres mérésekkel állít elő adatot;
- radarfelderítés (Radar Intelligence – RADINT): rádiólokációs technikával végzett felderítéssel szerez adatokat;
- technológiai felderítés (Technical Intelligence – TECHINT): az eszközök technikai paramétereit felderítve állít elő adatot;

- nyílt források felhasználásával folytatott felderítés (Open-source Intelligence – OSINT): a széles körben hozzáférhető nyílt adatforrások, például rádió-, televízióadás, újság, könyv felhasználásával szerez adatot. [32] [33]

Áttekintve a felsorolt felderítési fajtákat látható, hogy természetesen nem mindegyik épül az elektronikai eszközökkel végzett adatszerzésre, de mindegyikben megtalálhatók adatszerzési vagy adattovábbítási és feldolgozási szinteken az elektronikus eszközök.

Az elektronikai felderítés alatt az elektronikai eszközökkel végzett **adatszerzést** és ezen **adatok feldolgozását** értjük.

Az **adatszerzésnek** az elektronikai felderítés területén az alábbi speciális módszerei léteznek:

- felfedés;
- figyelés;
- lehallgatás;
- iránymérés;
- helymeghatározás.

A **felfedés** olyan szervezett tevékenység, amely arra irányul, hogy a másik fél rádiólokációs, navigációs, távvezérlő és távközlő rendszereiben alkalmazott elektronikai eszközöket érzékelve feltárja, és a felderítő ismérvek alapján meghatározza felderítési értéküket. A felfedés célja az új elektronikai eszközök, ezen keresztül a másik fél elektronikai rendszerei működésének feltérképezése.

A **figyelés** alapvető módszere az ellenőrzés. Az ellenőrzést az objektum fontossági fokának megfelelően, a korábban szerzett adatokkal összevetve, a változások regisztrálásával és azoknak a kiértékelőkhöz való továbbításával végzik. A figyelés folyamán ellenőrzik a korábbi iránymérési adatokat, melyek alapján jelezhető az objektum mozgása. A figyelés folyamán a felfedéskor rögzített adatok esetleges változásait értékelik, ezért az adatrögzítés, dokumentálás, a felfedéssel megegyező eszközökkel és módszerekkel történik. A különbség, hogy míg a

felfedés gyakorlatilag nulla adatokkal indul, addig itt a nagymennyiségű, korábban szerzett felfedési, figyelési adathalmazt is kezelni kell. Az adatbázis tartalmazza az objektum típusát, az észlelési időt, a vivőfrekvenciát, a modulációt, az üzemmódokat, az antenna típusát, a sugárzási irányt és egyéb paramétereket, illetve korszerű felderítő eszközök alkalmazása esetén a jel analizátorok által szolgáltatott „elektronikus ujjlenyomatok" adatait.

A **lehallgatás** alapvetően a rádióelektronikai felderítés (SIGINT) módszere, amely az átviendő információ tartalmának, a telemetriai folyamatok eredményeinek megszerzésére irányuló tevékenység. A lehallgatás az adatforrás folyamatos, megszakítás nélküli figyelését, ellenőrzését igényli. A hagyományos értelemben vett lehallgatás célpontjai a kommunikációs célú, nyílt, beszédátviteli csatornák voltak, de ezek a digitális technika megjelenésével egyre inkább kiszorulóban vannak a modern kommunikációból. Ezek az átviteli módok, illetve maga a moduláció digitalizálással titkosítható, ami a lehallgató számára csak rendkívül nagy nehézségek árán, általában hosszú időt, erős számítástechnikai hátteret igényelve fejthető csak meg. Ennek megfelelően tehát a korszerű lehallgatás nem az információtartalmat, hanem az egyéb, a felhasználóra és a működési szokásaira jellemző paramétereket keresi, amelyek alapján az aktuális, vagy várható tevékenység előre jelezhető.

Az **iránymérés** a célobjektumok által kisugárzott elektromágneses energiának a vétel pontjába való beérkezési irányát – a mágneses, vagy a földrajzi északhoz viszonyított oldalszögét, a vízszintessel bezárt helyszögét – határozza meg.

A **helymeghatározás** során a célobjektum helyének pontos meghatározása a cél, amelyhez egy vagy több iránymérő eszköz alkalmazása szükséges. [32]

Az **adatfeldolgozás** alapvetően a megszerzett adatok felderítési információvá illetve célinformációvá való alakítását jelenti. A digitális technika alkalmazása, illetve a megváltozott körülmények miatt a különböző adatforrások információinak nemcsak megszerzése, de felderítési adattá való átalakítása is jelentős kihívás elé állítja az adatfeldolgozást. A rendelkezésre álló nagyszámú, különböző rendeltetésű és fajtájú felderítőeszköz által megszerzett adatokat

adott szinteken, egy helyen kell összegezni, kiértékelni, egyeztetni és a felhasználók számára hozzáférhetővé tenni. Ezt az igényt elégíti ki összadatforrású felderítés.

Az összadatforrású felderítés **adatfúziós technológiája** biztosítja a különböző érzékelési tartományú szenzorok által szerzett adatok összegyűjtését, feldolgozását, összegzését és az eredmények szétosztását. Ezáltal a felderítési információk hitelesebbé válnak, és pl. a megtévesztés, félrevezetés hatékonysága jelentősen csökkenthető, mivel a korábbi egy forrású felderítés helyett egy adott célobjektumról több forrásból (pl.: radar felderítéssel, képi felderítéssel, rádiófelderítéssel stb.) szerezhetők adatok.

**Az elektronikai felderítés korszerű eszközei [32]**

Szinte mindenfajta fizikai tevékenység egyik igen jellemző tulajdonsága, hogy azok valamilyen zajjal járnak. A hang, mint a mechanikai rezgések tartományába tartozó fizikai tényező, felderítése **akusztikai felderítő** eszközökkel lehetséges. Ezek olyan elektronikus eszközök, amelyek a hangot – azaz az ebbe a tartományba eső mechanikai rezgéseket alakítják át – elektromos jellé. A legismertebb ilyen eszköz a mikrofon. Ezek kivitele, érzékenysége és gyakorlati megvalósítása ma már lehetővé teszi olyan iránykarakterisztikák kialakítását, amelyek rendkívül éles szögben képesek a hang felderítésére, és ez által nem csak az információ közvetítésére, hanem az irány, illetve több mikrofon alkalmazása esetén a hely megjelölésére. Érzékelőként elhelyezve – a kis méret, a kis energia felvétel, és a nagy irányítottság miatt – kiválóan alkalmasak például egy adott terület folyamatos megfigyelésére, monitorozására.

A víz alatti, illetve a közvetlen vízfelszíni ún. **hidroakusztikai** felderítés speciális elektronikai eszközöket – úgynevezett szonárokat – igényel. Ezek lehetnek aktívak, amelyek hangimpulzusokat bocsátanak ki, majd a visszaverődő hanghullámokat érzékelik, illetve lehetnek passzívak, amelyek egyszerűen a víz alatt terjedő hangokat veszik és elemzik.

A mechanikai rezgések tartományába tartoznak a **szeizmikus** rezgések is, amelyek a föld mozgását jelzik, és ennek köszönhetően az adott területen mozgó tárgy (pl. jármű) mozgását lehet detektálni. Ebben az esetben is a felderítő eszköz az érzékelt és vett mechanikai rezgést

elektromos jellé alakítja. Az eljárás alapja az, hogy mérik az akusztikus jelnek a céltárgyig majd az érzékelőhöz való visszatéréséig szükséges időt. Ha a hang vízben való terjedési sebessége ismert, kiszámítható a céltárgy távolsága.

A szeizmikus szenzorok a megfigyelt, illetve felderíteni kívánt területen történő mozgást, illetve a mozgás által keltett szeizmikus rezgéseket képesek érzékelni. 10-15 évvel ezelőtt a harckocsik, illetve az általuk keltett szeizmikus rezgések felderítésére használták, de ma már érzékenységüknek köszönhetően képesek a viszonylag nagy távolságban lévő embert, illetve az általa keltett szeizmikus rezgést érzékelni.

A látható fény tartományában működő **hagyományos kamerákat és fényképezőgépeket** máig eredményesen használják a felderítésben, mivel a hagyományos filmre rögzített kép minősége, azaz felbontóképessége nagyon jó. A speciálisan a felderítésre készült kameráknak és filmeknek a legkülönbözőbb követelményeknek kellett, és kell még napjainkban is megfelelniük. Ezek például a felbontóképesség, a lencse optikai teljesítménye, fókusztávolsága, a használt film emulziós rétegének kontrasztvisszaadó képessége, vagy akár a film mérettartó képessége. Egy óriási hátránya azonban van a hagyományos kamerával végzett felderítésnek, nevezetesen, hogy a filmet elő kell hívni ahhoz, hogy arról információkat lehessen kinyerni. Abban az esetben, ha nagyon rövid időn belül, vagy akár azonnal szükség van a felderítő kamera által szolgáltatott információra, akkor nincs idő az előhívásra. A megoldást az elektrooptikai eszközök használata jelenti.

A CCD (Charge Coupled Device), azaz töltéscsatolt eszközök megjelenésével lehetővé vált az optika által látott kép digitalizálása. A **digitális fényképezőgépek** CCD chipet használnak a fény elektromos jellé történő átalakítására. Ezeknek a fényképezőgépeknek az egyik fő előnye, hogy azonnal láthatjuk az elkészült képet, nincs filmelőhívási procedúra, ráadásul a „nyersanyag" digitális formában áll a rendelkezésünkre, azaz azt elektronikus úton azonnal továbbítani lehet, vagy elektronikus eszközökkel azonnal fel lehet dolgozni. A ma elérhető digitális fényképezőgépekben már 12-15 millió pixeles – képpontos – CCD chipek is találhatók. Ez azonban óriási nagyságú digitális jelet eredményez, ezért annak valamilyen módszer-

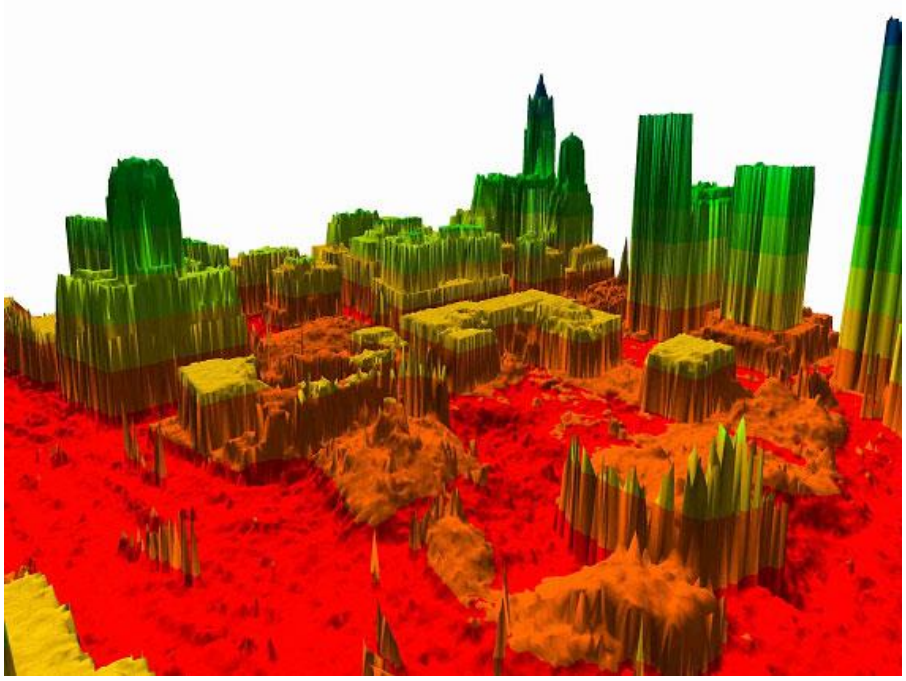
rel történő tömörítése szükséges, ahhoz hogy a továbbítás, feldolgozás, vagy a tárolás könnyebb legyen. A tömörítés többféle algoritmus szerint végezhető, amelyek nemzetközi szabványokban is megjelentek – például tif, gif, jpg – és amelyek között a végeredményt illetően nemcsak méretbeli különbségek, de a tömörítés eredményeképpen megjelenő eltérő veszteségek (minőségromlás) is vannak. A digitális fényképezőgépek esetében nemcsak a felbontás, de hasonlóan a hagyományos gépekhez a zársebesség, a fókuszálás, az objektív is mind-mind jellemző paraméterek lehetnek. A digitális fényképezőgépek (hasonlóan a hagyományos fényképezőgépekhez) azonban nem alkalmasak éjszaka, sötétben való használatra, illetve rossz látási viszonyok között az alkalmazhatóságuk erősen korlátozott.

A digitális fényképezőgép által készített állóképek sorozata – amely állóképek átvitele nem igényel akkora nagyságrendű átviteli sebességet, mint a folyamatos kép átvitele – nagyon jó információforrásnak bizonyul.

A mozgóképek rögzítésére alkalmas **digitális videokamerák** a jelet digitális szalagon, vagy akár merevlemezen rögzítik. Az egyszerűbb kamerákban egy, az újabb kamerákban 3 CCD chip látja el a digitális kép előállítását. A színérzékelés RGB szűrőkkel történik. A CCD chipekről 100 Mbit/s sebességgel történik a képek rögzítése.

Napjaink egyik leginnovatívabb fejlesztése **a LIDAR (Light Detection and Ranging),** azaz a **lézer radar,**[29] amely nem más, mint egy optikai elven működő sebesség és távolságmérő eszköz. A LIDAR egyaránt működhet a látható fény, az ultraviola, vagy az infravörös hullámtartományában. A LIDAR működési elve hasonló a hagyományos radaréhoz, azaz a kisugárzott jel céltárgyról való visszaverődéséből kapunk adatokat. A LIDAR nem rádióhullámokat bocsát ki, hanem koherens fénysugarakat – azaz ez az eszköz lézer fényforrást alkalmaz. Mivel a fény nagyon kis hullámhosszal rendelkezik, ezért nagyon kis elmozdulás is mérhető a segítségével. Az adatfeldolgozás elektronikusan történik, amely kimenetén nagy felbontású digitális formában rendelkezésre álló képet kapunk (2. kép).

[29] Bár a megnevezése radar, a működési hullámtartománya mégis a látható-, illetve a közeli látható fény tartománya.



2. kép**.** LIDAR-ral készült kép New York-ról, 2001. szeptember 17-én [34]

A LIDAR előtt perspektivikus lehetőségek vannak számtalan területen, így az elektronikai felderítésben is. Óriási előnye, hogy nagyon jó – közel fénykép – minőségű radar képet tud biztosítani digitális formátumban, amely továbbítása, feldolgozása, és értékelése így gyorsabb és egyszerűbb.

Amint azt a hagyományos és digitális fényképezőgépek, illetve kamerák esetén láthattuk, azok nem képesek éjszaka – sötétben – felderítést folytatni. Ehhez olyan eszközökre van szükség, amelyek korlátozott fényviszonyok, vagy teljes sötétség esetén is képesek képet rögzíteni, és ezáltal információt közvetítetni.

Minden tárgy és élőlény sugároz magából energiát az elektromágneses spektrumban (feltéve, ha az adott tárgy vagy „élőlény”az abszolút 0 foknál, azaz - 273 °C-nál[30] magasabb hőmérsékletű). Ez a hősugárzás a molekuláris mozgás eredménye, és amelynek a spektrális el-

[30] Egész pontosan -273,15 °C-nál magasabb hőmérsékletű, ami pontosan 1 K-nek (kelvin) felel meg.

oszlása a test hőjével jellemezhető. Abban az esetben, ha ezt a hőt meg tudjuk különböztetni a környezettől, akkor látható fény nélkül is lehet képet készíteni az adott tárgyról, vagy térrészletről.

Az **infravörös kamerák** a céltárgy által kisugárzott hőt érzékelik, így azok éjszaka illetve kevés fény mellett is tudnak működni. Az infrakamerával végzett felderítéssel detektálni lehet pl. egy – a vizuális felderítés ellen jól álcázott – tárgy vagy személy hőképét, megállapítható, hogy a gépjárművek működtek-e az elmúlt percekben (3. kép), sőt még az úton – igaz csak rövid ideig – megmaradó „hőlenyomatuk" alapján azok mozgására is következtetni lehet.


3. kép. Infrakamerával készült kép [35]

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. Ugyanakkor a digitális technika elterjedésével párhuzamosan a SIGINT-nek számos technológiai kihívással kell szembenéznie. Megjelentek és terjednek a kis valószínűséggel felderíthető (Low Probability of Interception – LPI) technológiák, mint pl.: a kiterjesztett spektrumú rendszerek. Ezek elterjedése, illetve az elektronikus kriptográfia fejlődése rendkívül nehézzé teszi a titkosított elektronikus adások információtartalmának megfejtését.

Ezek a kihívások azt eredményezik, hogy a SIGINT – és azon belül különösen a rádiófelderítés – korábban alkalmazott hagyományos módszerei egyre kevésbé használhatók. Napjaink korszerű felderítő eszközei alapvetően csak ezen digitális adások jeleinek detektálására, illetve a kisugárzások helyének meghatározására képesek ami az esetleges fizikai vagy elektronikai támadás végrehajtásához szükséges.

A nagysebességű (paramétereit gyorsan változtató) adások vételére napjainkban olyan vevőket alkalmaznak, amelyek egy időben dolgozzák fel a teljes spektrumot. Ilyenek a gyors szintézeres vevők, a digitális szűrőbank vevők és a Bragg cellás vevők.

A **gyors szintézeres vevő** működése azon alapul, hogy a vevő az adott teljes frekvenciasávot annyi idő alatt söpri végig, amennyi időt a frekvenciaugratásos adó egy frekvencián tartózkodik. Így lehetőség van, hogy a vevőn megjelenítsük a vett jel frekvencia periódusait. Ez a frekvencia utólagos nyomon követésére alkalmas, de a moduláló algoritmus ismeretének hiányában nincs lehetőség az információtartalom megfejtésére. Így a vett jelnek csak frekvenciaspektruma elemezhető. Ugyanakkor ez is eredmény, mivel a felderített jelsorozat alakjának („ujjlenyomatának"), a használt frekvenciasávnak, a rendszer térbeli elhelyezkedésének vagy az adások időbeliségének elemzésével hasznos információhoz lehet jutni.

A **digitális szűrőbank vevő** olyan egymás mellé hangolt vevők sorozatát jelenti, amelyek összességében átfogják a kívánt frekvencia spektrum egészét. A vevők egymással párhuzamosan veszik a saját frekvenciatartományukba eső kisugárzott jeleket, és azokat egy jelfeldolgozó egységre juttatják. A jelfeldolgozó egység gyors Fourier transzformációt használ, és a jelanalízis végeredménye folyamatos jel lesz.

A **Bragg cellás vevők** is keresés nélküli felderítési módszert alkalmaznak, de itt szűrőbank helyett úgynevezett Bragg cellákat használnak a jelek detektálására és átalakítására. A vett bemenő jelek előerősítés és alacsonyabb frekvenciára történő átalakítás után piezoelektromos átalakítóra kerülnek. A piezoelektromos átalakítás után keletkezett ultrahang egy lézerfényforrás által megvilágított kristályban, a rezgéseknek megfelelő fénytörést idéz elő. A koherens fény elhajlási szöge ennek megfelelően összefüggésben van a beérkezett jel frekvenciájával.

A fényt CCD chipre vezetve ábrázolható és megmérhető a beérkezett jel frekvenciája. Ezzel a módszerrel lehetőség van az adott jel frekvenciaugrásainak, illetve egy adott frekvencián eltöltött idejének megfigyelésére. Ez a megoldás sem alkalmas azonban az információtartalom visszafejtésére.

A korszerű SIGINT rendszerekben általában egy központi számítógépes egység végzi a beérkező jelek valós idejű adatfeldolgozását, amely az iránymérésre, a demodulálásra, valamint a rögzítésre vonatkozik. A rendszer szoftveresen képes vezérelni az egész folyamatot, kezdve az iránymérő és vevő antennák kiválasztásától egészen az adatok feldolgozásáig.

A rendszer részét képezi a szélessávú iránymérő, a hozzátartozó analóg/digitális átalakítóval, valamint a keskenysávú vevők, amelyek szintén analóg/digitális átalakítón keresztül juttatják el a vett jeleket a számítógépre. Ezt követően nemcsak a valós idejű jelfeldolgozás történik meg, hanem egyrészt ezzel párhuzamosan, ha szükség van a jelstruktúra megjelenítésére, akkor a monitorozás, másrészt a vett jel struktúrájának összevetése történik az adatbázisokban meglévőkkel. Ennek érdekében minden jel rögzíthető az adatbázisban, amelyek akár automatikusan is frissíthetőek. Az utóbbi években a frekvenciaugratásos adások megfigyelése céljából fejlesztették ki a vízesés típusú displayt, amely frekvencia-idő tartományban mutatja a vett jeleket.

Mint ahogy láthatjuk, a korszerű adásmódok felderítésekor a fentiekben említett eszközök és eljárások egyike sem alkalmas (vagy csak nagyon kis valószínűséggel) a rádióforgalom és az információ tartalom elemzésére, megfejtésére. Ez a dekódolási feladat speciális apparátust, a legmodernebb technológiát és óriási számítási kapacitást igényel.

Ebből következően a rádiófelderítés számára sem az információtartalom, hanem az adók által hagyott „elektromágneses ujjlenyomat” lesz az elsődleges azonosító jellemző. Ez azt is jelenti, hogy a COMINT, mint tevékenységi forma ELINT típusúvá válik, vagyis csak a vett jelek paramétereit és a kisugárzás helyét képes meghatározni. Mivel az információtartalom megfejtésére nincs lehetőség, ezért a rádióforgalom további lehallgatása is értelmetlenné vá-

lik. Ehelyett az így felderített rádiórendszereket elektronikai támadással (pl. elektronikai zavarással) kell működésképtelenné tenni.

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** (Unattended Ground Sensors – UGS). 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. (4. kép) A különböző állapotváltozásokat detektáló szenzorokból általában szenzorrendszert alakítanak ki, amely lehetővé teszi egy objektum vagy céltárgy észlelését a különböző tartományokban.

4. kép. Infra és szeizmikus érzékelő [36]

A felügyelet nélküli szenzorok számos előnyös tulajdonsággal rendelkeznek, 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, akár 30-40 napig is képesek működni. A szenzorok nem napi 24 órás folyamatos üzemben működnek, mivel csak abban az esetben kapcsolnak be, ha aktivitást észlelnek, majd a vett, illetve érzékelt tevékenységekről szóló adatokat kódolt formában, meghatározott időközönként nagyon kevés ideig tartó kisugárzással – például csomagkapcsolt adásokban – juttatják el a vevő és adatfeldolgozó központjaikba. Az objektumok őrzésvédelmi rendszereit leszámítva a harctéri szenzorok döntő többségükben rádiós kapcsolaton keresztül kapcsolódnak össze az adatgyűjtő és kiértékelő központtal. A kis fizikai méretek korlátozott hatótávolságot tesznek csak lehetővé, ezért a szenzorokat kommunikációs átjátszók, adatgyűjtő és továbbító készülékek támogathatják.

A modern szenzorrendszerek lényege már nem a szenzorokban van, hanem a hozzájuk kapcsolódó adatátviteli és harcvezetési berendezésekben. A mérési értékeket, különböző spektrális és egyéb jellegzetességek alapján kategorizálni kell, meg kell határozni a pontos állapotváltozást, és ezt az ún. előfeldolgozott adatokat kell továbbítani. A felderítőközpontokban lehetőség van a terepen, vagy az adott célterületen elhelyezett érzékelők adatainak megjelenítésére, amely például egy digitális térképi felületre téve kitűnően alkalmas a terület, illetve az ott folyó mozgás és tevékenységek monitorozására, megfigyelésére. [11]

Az információs technikai és technológiai forradalom a szenzorok területén is óriási változást hozott. Az elmúlt években kerültek kifejlesztésre az olyan intelligens szenzorok, amelyek már egy chipben, a chip egyes rétegeiben tartalmazzák magát az érzékelőt, az adatfeldolgozó egységet, az operációs rendszert, és a hozzá tartozó „hardver” elemeket. Így tehát már miniatürizált érzékelő-számítógépekről beszélhetünk, amelyek egymással, illetve az őket irányító központi számítógépekkel vezeték nélküli ad-hoc hálózatba szerveződött kommunikációs rendszerben tartják a kapcsolatot.

Az elektronikai felderítés céljára felhasználható eszközök jelentős része kereskedelemi forgalomban szabadon hozzáférhető és megvásárolható. Így e tevékenység nem pusztán a

különböző hírszerző szolgálatok privilégiuma. Ezekkel az eszközökkel más illetéktelen személyek, csoportok esetleg terroristák is hozzáférhetnek a számukra szükséges adatokhoz.

A felsorolt elektronikai felderítés eszközeinek többsége nem csak mint a fenyegetés, hanem mint a védelem fontos eszközei is lehetnek. Ilyenek pl. a különböző biztonságtechnikai szenzorok, behatolás jelzők (infra-, szeizmikus-, mágneses érzékelők, stb). Így ezeket az eszközöket a komplex információbiztonság tervezése és a megvalósítása során is figyelembe kell venni.

### 3.4.3. 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 az elektronikai hadviselés azon területe, amely magába foglalja az elektromágneses és irányított energiák kisugárzását abból a célból, hogy megakadályozza

vagy csökkentse az elektromágneses spektrum másik fél által való hatékony használatát. Az elektronikai támadás tehát minden olyan technikát, módszert és eszközt felhasznál, ami az elektromágneses és más irányított energiák felhasználásával képes lerontani a másik fél 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.

**Elektronikai zavarás**

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 megnehezítik, vagy kizárják az elektronikai eszközök útján továbbított hasznos jelek vételét és az információk kiválasztását. A berendezések vevőegységére hatva az elektronikai zavarok 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 zavarok lehetnek:

- természetes elektronikai zavarok vagy
- mesterséges elektronikai zavarok.

A **természetes elektronikai zavarok** a természeti folyamatok által létrehozott elektromágneses és akusztikus zavarok, amelyek atmoszférikus, kozmikus, illetve a Föld körüli térség elektromágneses sugárzásából származhatnak. A **mesterséges elektronikai zavarok** az elektromágneses hullámok energiáját tükröző visszaverők, illetve az elektromágneses rezgéseket kisugárzó berendezések által keltett zavarok, melyek akadályozzák egy meghatározott műszaki jellemzőkkel rendeltetésszerűen működő elektronikai eszköz normális üzemét. Az információs fenyegetések szempontjából mindkét zavartípus korlátozhatja egy-egy infokommunikációs rendszer működését, azonban e rendszerek elleni szándékos tevékenység szempontjából a mesterséges zavarok a lényegesek.

Az elektronikai zavarás célobjektumait elsősorban az információs rendszerekben működő érzékelő, adatátviteli, és hírközlő berendezések képezik, illetve maguk az alkalmazók válhatnak azzá. Az elektronikai zavarással megbontható a rádióhíradás, a műholdas hírközlés és navigáció, a mobil telefonhálózat, a műsorszórás, a mikrohullámú rendszerek működése, a rádiólokáció, vagy akusztikus hullámtartományú jelekkel akár az emberi munkavégző képesség is befolyásolható.

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]

A **rádiózavaró berendezések** rendeltetésüknek megfelelően a rádióforgalmazás lefogására, akadályozására, vagy megtévesztésére szolgálnak. A fejlődés során elsősorban a frekvenciatartomány szerinti típuscsoportok jöttek létre. Ennek megfelelően vannak rövidhullámú, ultrarövid hullámú, rádiórelé és mikrohullámú rádióösszeköttetések lefogására alkalmas berendezések. E berendezések többnyire földön telepített eszközök, amelyek kisugárzott telje-

sítménye a frekvenciatartomány és a rendeltetés függvényében általában 500W és 5 kW között változhat.

A földi telepítésű eszközök mellet a rádióhálózatokhoz való jobb **elektronikai hozzáférés** céljából a rádiózavaró berendezéseket repülőeszközök, elsősorban helikopterek fedélzetén is elhelyezik. Az egyenes láthatóság határa ilyenkor megnövekszik, a szabadtéri terjedést nem akadályozza a domborzat és a tereptárgyak reflexiós hatása, azonban a fedélzeten nem lehet kW-os nagyságrendű folyamatos zavarteljesítményt előállítani, ami pedig hátrányosan érintheti a zavarhatékonyságot.

Napjainkban a direkt szekvenciális, frekvenciaugratásos, időugratásos szórt spektrumú rendszerek, a gyorsadók, a kódolt, titkosított digitális rádió berendezések megjelenése és széleskörű elterjedése jókora lépéselőnyhöz juttatták a távközlést a felderítéssel, lehallgatással és zavarással szemben. Ezek ellen a hagyományosnak nevezhető harmadik generációs felderítő-iránymérő-zavaró komplexumok már nem vagy csak korlátozottan használhatók. Olyan új berendezésekre van szükség, amelyek kiváltják a zavarjelekkel való kézi manőverezést, tehát számítógép vezérlésű, gyors áthangolású berendezéseket kell alkalmazni. szükségesek. A több kW-os teljesítményű eszközök helyett inkább a kisteljesítményű, de a zavarandó berendezések közelébe kijuttatható intelligens zavaróadók eredményesebben alkalmazhatók ezen adásmódok ellen. A zavarandó eszközök közelébe való kijuttatás pilóta nélküli repülőgépekkel, robotokkal, vagy különleges csoportokkal történhet.

A legújabb elgondolások alapján[31] a zavarandó eszközökhöz közeli alkalmazással az elektronikai kisugárzó eszközök felderítése egyszerűbb elektromágneses környezetben történik, kisebb érzékenységű eszközökkel is megvalósítható. A kisebb érzékenység miatt a távoli adók jeleit már nem veszik, ezért azokra nem is fejthetnek ki amúgy hatástalan zavaró tevékenységet. A rendszer működési alapgondolata**,** hogy az szembenálló fél területén minden elektronikai eszköz zavarása hasznos lehet, ezért a tömeges alkalmazással kritikus elektronikai zavar-

[31] Lásd az USA WolfPack rendszer elgondolását: http://www.darpa.mil/STO/strategic/wolfpack.html

helyzet hozható létre a másik fél számára anélkül, hogy a saját elektronikai eszközök számára káros interferenciát okoznánk. Az elgondolás szerint a kicsi, viszonylag olcsó, nagy tömegben alkalmazható, intelligens felderítő-zavaró eszközökből álló rendszert hálózatba kell szervezni. Ez lehetővé teszi, hogy a rendszer felismerje és kategorizálja a vett elektronikai kisugárzásokat, amelyek származhatnak rádió, vagy rádiólokációs eszközöktől. A rendszervezérlő több szenzor adatának korrelációja által meghatározza a felderített sugárforrás koordinátáit, majd kijelöli az optimális zavaró eszközt, amelynek a zavarási feladatot végre kell hajtani. [11]

A **mobil cellarádiós (GSM) rendszerek zavarása** teljesen új terület. A 900, 1800 és 1900 MHz-es sávban üzemelő mobil hírközlő eszközök (nem csak telefonok, hanem kommunikációs modullal ellátott számítógépek) néhány év alatt sok százmillió példányban terjedtek el a világon. Mivel mindennapjaink kommunikációja döntő mértékben már a GSM hálózaton zajlik, ezért egy komplex információs támadás során a támadó számára kiemelt fontosságú ezen rendszerek elektronikai lefogása.

Ennek keretében a fő feladat a működő eszközök, bázisállomások felkutatása, zavarása akár szelektív módon, az adott frekvenciakészlet lefogásával, akár csoportosan, a bázisállomásokat vezérlő mikrohullámú rendszerek megbontásával.

A világpiacon kész GSM zavaró berendezések kaphatók, (5. kép) amelyek akár egy cigarettás dobozban is elférnek. Ezeket a kis hatótávolságú (általában 10 m alatt) eszközöket egyrészt a kritikus infrastruktúrák (kórházak, számítóközpontok, repülőgépek) védelmében, másrészt az emberek nyugalmának érdekében (színházak, éttermek, stb.) lehet alkalmazni.[32] Az ilyen típusú GSM zavarók alkalmazásakor a felhasználó úgy érzékeli, mintha egy, a mobilhálózattal teljesen lefedetlen területen járna valaki, vagyis nincs térerősség. GSM zavarási feladatra is alkalmazhatók a kis-, vagy akár mikroméretű pilóta nélküli repülőgépek, mivel segítségükkel egy adott térségben üzemelő készülékcsoportot anélkül lehetne lefogni, hogy a rendszer többi elemében kárt tennénk, vagy a lefogás tényét egyértelműen felfednénk.

[32] Magyarországon – mint több más országban – az elektronikus hírközlési törvény rendelkezik arról, hogy más szolgáltatását zavaró eszközt nem szabad használni, ami alól még a templomok, színházak sem kivételek.

5. kép. Kereskedelmi forgalomban kapható GSM zavaró eszközök [37]

Hasonló a helyzet a **műholdas navigációs rendszerek zavarásával** is. A NAVSTAR GPS[33] műholdas navigációs rendszer már nemcsak a repülők és hajók navigációját biztosítja, hanem a polgári felhasználók körében is rendkívüli mértékben elterjedtek. A GPS navigációs rendszer szolgáltatásait egyre több civil felhasználás veszi igénybe (pl. közlekedés, szállítás, földmérés, környezetvédelem, stb.) Így ennek a rendszernek a megzavarása is jelentős hatással lehet az információs társadalom működési folyamataira.

A GPS műholdak által sugárzott rádiójelek rendkívül kis teljesítményűek, a Föld felszínén mérhető GPS jelteljesítmény 1018-szor kisebb, mint egy 100 W-os izzóé! A GPS vevők csak azért képesek a háttérzajból kiszűrni a GPS jeleket, mert azoknak nagyon speciális a struktúrájuk. A kis teljesítmény miatt a GPS jeleket nagyon könnyen lehet zavarni egy ugyanabban a mikrohullámú sávban üzemelő nagyobb teljesítményű rádióadóval. Már léteznek olyan zavaró berendezések, amelyek elegendően „nagy" energiájú és megfelelő karakterisztikájú zavaró jelet bocsátanak ki a GPS frekvenciákon, amely interferenciát okoz.

[33] NAVigation System using Time And Ranging, Global Positioning System. Az amerikai haderő által üzemeltetett műholdas navigációs rendszer.

A zavaró jel típusa lehet:

- keskenysávú folyamatos zavar (CW) a GPS sávban;
- szélessávú folyamatos zavar sáv átfedéssel;
- szórt spektrumú GPS jelhez hasonló zavar.

A GPS vevők zavarására létezik egy másik módszer is, amit GPS Spoofing-nak neveznek. Ez a GPS felhasználó megtévesztésére szolgáló hamis C/A jelek kisugárzását jelenti, aminek következtében a vevő által számított pozíció távolodik a valódi helyzettől.

A GPS vevők zavarására léteznek nagyteljesítményű (kW-MW) katonai felhasználású zavaró berendezések, amelyek többféle karakterisztikájú zavaró jelet tudnak kibocsátani. Ezek azonban igen drágák és könnyen bemérhetők majd megsemmisíthetők. Elektronikai boltokban kapható alkatrészekből házilag is megépíthetőek kisteljesítményű, egyszerű felépítésű zavaróeszközök, amelyek a tömeggyárthatóságból adódóan igazi veszélyt jelentenek. (6. kép) [38]

6. kép. Kisteljesítményű GPS zavaró [39]

A **műsorszóró rádiók és TV rendszerek** – mint a tömegtájékoztatás eszközei – ellen az elektronikai támadás eszközei szintén jól alkalmazhatók: elektronikai zavarással akadályozhatjuk, hogy a vevőkészülékek venni tudják a sugárzott műsort. Ez történhet földről stabil,

vagy mobil eszközökkel, illetve repülőgépen elhelyezett zavaró berendezések segítségével. Békeidőben, a szocialista országokban politikai okokból zavarták például a Szabad Európa rádió adásait, de az utóbbi évek regionális konfliktusaiban, Panamában, a Perzsa Öbölben, Haitin, és a jugoszláviai háború során is fontos szerephez jutottak a speciálisan erre a célra kifejlesztett berendezések. [40]

**Elektronikai megtévesztés**

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 az elektronikai kisugárzások manipulálásával, torzításával vagy meghamisításával éri el, hogy a másik fél saját érdekeivel ellentétesen tevékenykedjen.

Az elektronikai megtévesztés fő módszerei a következők:

- szimulációs elektronikai megtévesztés;
- manipulációs elektronikai megtévesztés;
- imitációs elektronikai megtévesztés.

A **szimulációs elektronikai megtévesztés** célja, hogy a saját elektronikai eszközök tudatosan hamis elhelyezkedésben és munkarendben való üzemeltetése útján az ellenfél téves következtetésre jusson. Ennek a megvalósítása arra épül, hogy a szimulációs elektronikai megtévesztést alkalmazó számít a másik fél elektronikai felderítő tevékenységére, amely a megtévesztés céljából működtetett objektumokat valós objektumokként észleli és az azoktól szár-

mazó információk feldolgozása, valamint a helymeghatározás alapján téves következtetésekre jut. A megtévesztés ennek megfelelően vagy egy fiktív tevékenység, vagy egy komplex fiktív elhelyezkedés és tevékenység szimulálására irányulhat.

A **manipulációs elektronikai megtévesztés** rendeltetése, hogy a saját elektronikai eszközök tudatosan megváltoztatott működési eljárásai és üzemeltetési jellemzői útján a szembenálló fél elektronikai felderítését téves következtetések levonására késztessék. A manipulációs elektronikai megtévesztés alapvető módszerei a rendszeresség kiküszöbölése az eszközök rendeltetésszerű üzemeltetéséből, a megszokott eljárásmódok megváltoztatása a döntő időszakokban, az eszközök megszokott üzemeltetési paramétereinek a megváltoztatása.

Az **imitációs elektronikai megtévesztés** során, a saját elektronikai eszközök igénybevételével oly módon juttatunk elektromágneses jeleket a másik fél működő elektronikai eszközeinek bemenetére, mintha azok saját rendszereiktől származnának. Az imitáló jelek egyrészt megzavarhatják az eszközök megszokott működési rendjét, másrészt félrevezethetik az eszközök felhasználóit. Az imitációs megtévesztés egy lehetséges módszere lehet pl. az ellenfél távközlési rendszereibe való belépés és azokba hamis közlemények, megtévesztő információk bejuttatása. [15]

A szakszerű és hihető megtévesztéshez sokkal kifinomultabb módszerek és eszközök szükségesek, mint az elektronikai zavaráshoz, mivel alapvető követelmény, hogy a megtévesztés során alkalmazott módszereknek nem szabad kompromittálódni. 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.

**Elektronikai pusztítás**

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. Elegendően nagy feszültség esetén természetesen más alkatrészekben, illetve alkatrészek között is létrejöhet átütés, ami szintén roncsolja az adott alkatrészt, működésképtelenné téve így a berendezést.

Az elektromágneses impulzus (EMP) kisugárzása 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. A működésben hozott nagyenergiájú eszközök rendkívül hatékonyan használhatók fel minden olyan infokommunikációs rendszer működésének részleges vagy teljes bénítására, amely mikroprocesszorokat, illetve mikroelektronikai áramköröket használ. [4] Az elektromágneses impulzushatás, bár időben nagyon rövid lefolyású, néhány-

szor 10 ns, azonban amplitúdóját tekintve óriási elektromágneses teret kelt, amely elérheti a több ezer KV-ot is. [41] Gyakorlatilag a jelenség egy óriási mű villámcsapáshoz hasonlítható.

Az elektromágneses impulzus kisugárzása elvén működő eszközök alkalmazhatók:

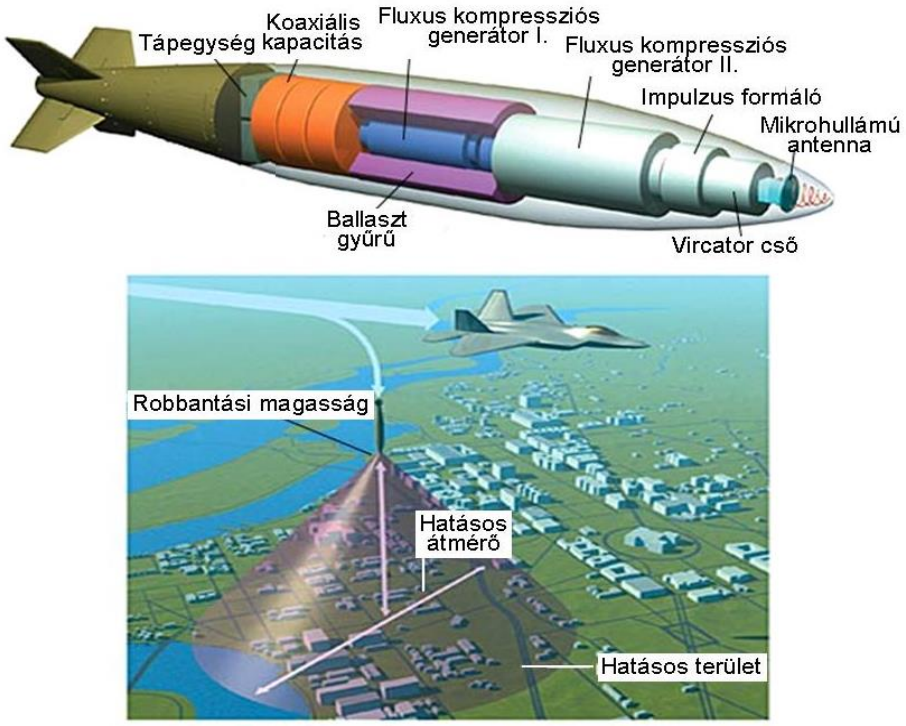
- nagy energiájú rádiófrekvenciás sugárforrásként illetve
- bombaként (E-bomba).

A **nagy energiájú rádiófrekvenciás sugárforrások,** mint az elektronikai eszközök támadásának lehetséges eszközei már régóta ismertek. A nagyteljesítményű adástechnika területén folyó eszközfejlesztések során olyan speciális vákuumtechnikai eszközöket (magnetronokat, klisztronokat, stb.) fejlesztettek ki, amelyek mérete lehetővé tette, hogy koncentrált energianyalábot lőjenek ki vele. Az így kisugárzott rádiófrekvenciás energia a vevőantennán átjutva a bemeneti áramkörre kerül, amely a nagy túlterheléstől tönkremegy. Ilyen eszköz a nagy energiájú rádiófrekvenciás fegyver (High Eneregy Radiofrequency Weapon – HERF), amelynek előnye a többszöri felhasználhatóság. A fejlesztések jelenleg abban az irányban folynak, hogy olyan méretbe állítsák elő ezeket az eszközöket, hogy azokat pl. pilóta nélküli repülőgépek fedélzetére helyezve ki lehessen juttatni az elektronikai célpontok közvetlen közelébe. A közeli térből már jóval kisebb energiaszükséglet mellett is hatékony elektronikai csapást lehet mérni anélkül, hogy emberi, vagy fizikai pusztítást okoznánk.

Az **impulzusbombák** szintén az elektronikai berendezések megrongálására, működésképtelenné tételére szolgálnak. A fizikai működési mechanizmusukban abban különböznek a nagy energiájú rádiófrekvenciás sugárforrásoktól, hogy csak egy hatalmas teljesítményű elektromágneses impulzust állítanak elő, majd ők is fizikailag megsemmisülnek, illetve véglegesen megrongálódnak. Működési alapelvük szerint többféleképpen állíthatják elő a rezgéskeltéshez szükséges energiát. Egy módja lehet például az, hogy vegyi robbanóanyag robbanási energiáját alakítják elektromos energiává, majd ezt egy üregrezonátorra sütik rá, amely a saját frekvenciáján létrehozott rezgést egy tölcsérsugárzón, vagy helixes kicsatoláson egy pa-

rabolatükörre sugározza. A hatás annál nagyobb, minél rövidebb impulzust sikerül előállítani ugyanakkora átlagteljesítmény esetén.

Alkalmazásukat tekintve az impulzus bombák bevetését a hagyományos bombavetéshez hasonló módon hajtják végre. A célobjektum fölött kioldva, a bomba közel függőleges helyzetben közeledik a föld felé. Amikor eléri a meghatározott pusztítási sugár nagyságához tartozó magasságot, létrehozza az elektromágneses impulzust, ami közel kör alakú területen pusztítja, rongálja az elektronikai eszközöket. [40] Az E-bomba felépítését és alkalmazásának hatásosságát szemlélteti a 4. ábra.



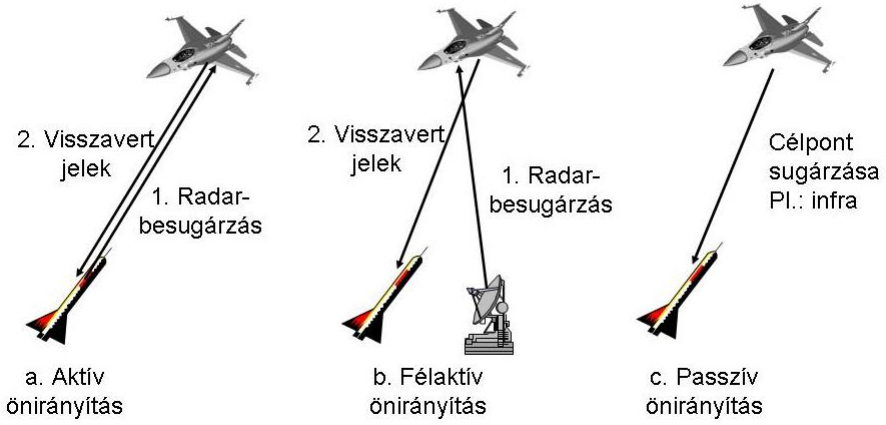

4. ábra. E-bomba felépítés és alkalmazása [42]

Napjainkban a nagy veszély abban áll, hogy az elektromágneses impulzus hatás elvén működő eszköz könnyen hozzáférhető elemekből alig 1000 dollárért, házilag is összebarkácsol-

ható. 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.

Az elektronikai pusztító eszközök csoportjába szokás besorolni az **önirányítású rakétafegyvereket** is, mivel a célravezetéshez szükséges vezérlő jelek kialakítása a rakéta fedélzetén automatikusan történik. Az irányításhoz szükséges információt (irányító jeleket) maga a cél szolgáltatja. A rakéta fedélzetén elhelyezett érzékelő elemek (önrávezető fej) követik a célt, és ahhoz viszonyítva meghatározzák a találkozáshoz szükséges röppályát. Az önirányítási rendszerek több változata ismert. Attól függően, hogy az alapjelek meghatározásához szükséges energiaforrás (információforrás) honnan és hogyan származik, megkülönböztetünk:

- aktív önirányítási rendszert;
- félaktív önirányítási rendszert;
- passzív önirányítási rendszert. (5. ábra)




5. ábra. Önirányítási módszerek

Az aktív önirányítás esetén, a rakéta fedélzetén elhelyezett rádiólokátor "megvilágítja" a célt, és az arról visszavert jelek alapján kidolgozza az irányításhoz szükséges parancsokat. Az aktív önirányítás független a külső (rakétán kívüli) energiaforrástól.

A félaktív önirányítás esetén a cél besugárzásához szükséges energiát (pl. lézer) egy külső forrás, pl. egy repülőgép fedélzetén elhelyezett berendezés állítja elő. A rakéta önrávezető feje a célról visszavert jelet érzékeli, a fedélzeti berendezése pedig irányító parancsokat dolgoz ki a céllal való találkozáshoz.

A passzív önirányítás esetén az irányításhoz szükséges energiát maga a cél generálja. Ezek lehetnek: fény, hang, hő illetve elektromágneses hullámok. A rakéta önrávezető feje a cél által kibocsátott energiát (pl. infrafejes rakéta esetén a cél hőkisugárzását) veszi és azokból olyan jeleket dolgoz ki, amelynek hatására a rakéta az energiaforrás irányába halad.

Az **akusztikus zaklatás eszközei** bár hatásukat tekintve a pszichológiai hadviseléshez tartoznak, azonban a hatást elektronikai eszközökkel érik el, ezért célszerű itt, az elektronikai támadás keretében szót ejteni róluk.

Már régen ismert, hogy az emberi szervezet bizonyos akusztikai hullámtartományban kisugárzott rezgésekre érzékenyen reagál. A 10 Hz alatti rezgések pánikérzetet, menekülési kényszerképzetet okoznak, a kb. 7,5 Hz-es rezgés pedig a szívvel lép interferenciába, ami kritikus esetben halált is okozhat.

Akusztikus zaklatás céljára egyfajta megoldás szerint egymástól kis távolságra elhelyezett két nagyteljesítményű piezo sugárzórendszert alkalmaznak. Egy közös központból vezérelve az egyik sugárzóra például 200 kHz, a másikra pedig 200,01 kHz frekvenciájú jelet kapcsolnak, amelyeket a piezo sugárzók akusztikus hullámok formájában sugároznak le. Abban a zónában, ahol mind a két sugárzó jele észlelhető, ott egy nemlineáris elemen, mint például az emberi fül, kikeveredik az összeg és a különbségi jel is. A 400,01 kHz-es összegjelet nem érzékeli az ember, ellenben a 0,01 kHz-es azaz 10 Hz-es különbségi infrahangra már a fent leírt módon reagál. A rendszer hangolható, az alkalmazókra nézve teljesen veszélytelen, mivel a sugárzás jól irányítható és hátrafelé keverésre alkalmas zóna a leírások szerint nem alakul

ki. A sugárzókat telepítő személyzetre ható közeli kb. 200 kHz-es rezgés semmilyen hatást nem gyakorol.

Egy másik eljárás szerint speciális jellel modulált rádiófrekvenciás jeleket sugároznak az ember tartózkodási helyére. A bekapcsolás után az embereken idegesség lesz úrrá, képtelenek uralkodni magukon és a felfokozott stresszhelyzetben az emberek munkavégzésre alkalmatlanná válnak.

Az ilyen eszközök diverziós csoportokkal, pilóta nélküli repülőeszközökkel és még sok más módon kijuttathatók a célterületre, a működtetésük lehet programozott vagy távvezérelt. [44] Mivel a kritikus információs infrastruktúrákat a humán erőforrás, vagyis az ember üzemelteti, működteti, felügyeli, stb. így ki van téve e támadó eszközök hatásainak. Ezért ezen hatások figyelembe vétele is fontos szempont a kritikus információs infrastruktúrák védelme során.

# IV. FEJEZET
# KRITIKUS INFRASTRUKTÚRA ÉS KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA VÉDELME

## *4.1. Védelem különböző országokban, az Európai Unióban és a NATO-ban*

### 4.1.1. Amerikai Egyesült Államok [1]

Az Amerikai Egyesült Államokban már 1997-ben, a Clinton elnök által felkért bizottság jelentésében a következő szektorokat emelték ki, mint olyan kulcsfontosságú rendszerek, amelyek kritikusak lehetnek az ország szempontjából [2]:

- energiaellátó rendszerek;
- banki és pénzügyi rendszerek;
- közlekedés és szállítás;
- egészségügyi rendszer;
- telekommunikációs rendszerek.

A 2001. szeptember 11-i terrortámadások után elfogadott USA Patriot Act[34] törvény újból meghatározta a kritikus infrastruktúrákat, azaz kritikus infrastruktúrának „*azokat a fizikai és virtuális rendszereket, eszközöket tekinti, amelyek olyannyira létfontosságúak az Egyesül Államok számára, hogy e rendszerek és eszközök működésképtelensége vagy megsemmisülése gyengítené a védelmet, a nemzeti gazdaság biztonságát, a nemzeti közegészséget és biztonságot vagy mindezek kombinációját.”* [3]

[34] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

2003 év elején került kiadásra a *Nemzeti stratégia a kritikus infrastruktúrák fizikai védelmére*[35], amely a következő szektorokra osztotta a kritikus infrastruktúrákat [4]:

- mezőgazdaság és élelmiszer;
- vízellátás;
- közegészségügyi rendszer;
- vészhelyzeti (készenléti) szolgálatok;
- védelmi ipar;
- telekommunikáció;
- energia;
- közlekedés;
- bank és pénzügyi szektor;
- vegyipar és veszélyes anyagok;
- postai szolgáltatások.

Ezt a listát kiegészítették olyan elemekkel, amelyek a kulcsfontosságú vagyontárgyakat, emlékhelyeket és műemlékeket tartalmazza. Ezek a stratégia megfogalmazása szerint azért kerültek a kritikus infrastruktúrák közé, mert ezek *„megsemmisítése ugyan nem veszélyeztetne létfontosságú, országos rendszereket, azonban helyi katasztrófát okoznának, vagy nagymértékben rongálnák a nemzeti morált és a nemzetbe vetett bizalmat”.* [4]

Ezek a kulcsfontosságú vagyontárgyak a következők [4]:

- nemzeti műemlékek és emlékhelyek;
- atomerőművek;
- gátak;
- kormányzati épületek;
- kulcsfontosságú kereskedelmi rendszerek.

[35] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

2003 decemberében a George Bush elnök által kiadott *Elnöki nemzetbiztonsági direktíva*[36] már nem csak felsorolja, hanem meg is határozta a különböző szervezetek és ügynökségek számára a felelősségi köröket a kritikus infrastruktúrák azonosítására, priorizálására és védelmére. Ez a direktíva előírta a Belbiztonsági Minisztérium (Department of Homeland Security – DHS) és más szövetségi ügynökségek együttműködését a magánszektor szereplőivel az információcsere és a kritikus infrastruktúrák védelme érdekében.

A rendelet nem csak átvette azokat a kritikus infrastruktúra kategóriákat, amelyeket a már említett *Nemzeti stratégia a kritikus infrastruktúrák fizikai védelmére* című határozat használt, hanem felülvizsgálta azt és némileg módosított besorolást határozott meg. Ez a lista szintén azokat a szektorokat sorolja fel, amelyek kulcsfontosságúak a nemzet biztonsága és gazdaságának működése szempontjából. A direktíva minden szektorhoz hozzárendelte a felelős minisztériumot, vagy szövetségi ügynökséget. A lista a következő:

- információtechnológia (felelős: Belbiztonsági Minisztérium[37]);
- telekommunikáció (felelős: Belbiztonsági Minisztérium);
- kémiai anyagok (felelős: Belbiztonsági Minisztérium);
- közlekedési rendszerek (tömegközlekedés, repülés, hajózás, vasút) (felelős: Belbiztonsági Minisztérium);
- vészhelyzeti mentő szervezetek (felelős: Belbiztonsági Minisztérium);
- postaszolgáltatás (felelős: Belbiztonsági Minisztérium);
- mezőgazdaság és élelmiszeripar (hús, baromfi, tojástermékek) (felelős: Mezőgazdasági Minisztérium[38]);
- közegészségügy és élelmiszer (egyéb hús, baromfi és tojástermékek) (felelős: Egészségügyi Minisztérium[39]);

[36] Homeland Security Presidential Directive 7/HSPD-7, Washington, December 17, 2003.
[37] Department of Homeland Security
[38] Department of Agriculture
[39] Department of Health and Human Services

- ivóvíz- és csatornarendszer (felelős: Környezetvédelmi Ügynökség[40]);
- energia, olajfinomítók, gáz- és olajtároló valamint szállító rendszerek, villamos energia (felelős: Energetikai Minisztérium[41]);
- bank és pénzügy (felelős: Pénzügyminisztérium[42]);
- nemzeti emlékművek és szimbólumok (felelős: Belügyminisztérium[43]);
- védelmi ipari bázis (felelős: Védelmi Minisztérium[44]).

Szintén 2003 februárjában adták ki a *Nemzeti Stratégia a Cybertér Biztonságára* (National Strategy to Secure Cyberspace) című dokumentumot, amely fő célja az Egyesült Államok állampolgárai – a cybertérrel vagy a cybertérben való – bármilyen tevékenységének biztonságossá tétele.

Ezt követte a *Belbiztonsági Nemzeti Stratégia*. Ez a stratégia hat területet jelölt ki, mint a legfontosabb biztonsággal összefüggő területek. Ezek közül az egyik a kritikus infrastruktúrák és kulcsfontosságú létesítmények védelme. A dokumentum megállapítja, hogy amennyiben a terroristák egy vagy több elemét támadják a nemzeti kritikus infrastruktúrának, akkor az egész rendszer összeomolhat, amely komoly károkat okozna az egész nemzet számára.

Ezért különösen fontos az olyan elemek védelme, amelyek a különálló rendszereket összekötik. E cél elérése érdekében egy nyolc feladatból álló tervet dolgoztak ki:

1. A Belbiztonsági Minisztérium által legsürgősebben megteendő feladatokat meghatározni;
2. Felépíteni egy teljes védelmi rendszert az Egyesült Államok kritikus infrastruktúrái számára;
3. Megteremteni az együttműködés lehetőségeit a helyi kormányzati szervek és a magánszektor különböző szereplői között;

[40] Environmental Protection Agency
[41] Department of Energy
[42] Department of Treasury
[43] Department of the Interior.
[44] Department of Defence

4. Kidolgozni egy nemzeti infrastruktúra védelmi tervet;
5. Megvédeni a cyberteret;
6. Kidolgozni a legjobb elemző és modellező eszközök felhasználásával hatékony védelmi megoldásokat;
7. A belső veszélyforrásokra is fel kell készíteni a védelmet;
8. Nemzetközi együttműködés megteremtése a nemzetközi kritikus infrastruktúra védelme érdekében.

Ezek után került kiadásra a *Nemzeti Stratégia Cybertér Biztonságára,* amely hangsúlyozza, hogy a cybertér biztonságának megteremtése hatalmas kihívást jelent a kormányzat és az egész társadalom egészére nézve. Ezért a stratégiát még terv formájában a lehető legszélesebb körben vitára bocsátották. A stratégia a cyberteret mint az információs infrastruktúrák egymással összefüggő hálózatainak összességét határozza meg.

A stratégia fő célkitűzései:

- a nemzeti infrastruktúra védelme a cybertámadásoktól;
- csökkenteni a nemzeti sebezhetőséget a cybertámadásokkal szemben;
- minimalizálni a veszteségeket vagy a helyreállítás idejét egy cybertámadást követően.

Mindezek után került kiadásra a *Nemzeti Stratégia a Kritikus Infrastruktúrák és Kulcsfontosságú Létesítmények Fizikai Védelmére* című dokumentum. A stratégia megállapítja, hogy egy a nemzeti kritikus infrastruktúrákat ért támadás nemcsak súlyos anyagi és humán károkat okozna, hanem a nemzet presztízsét, morálját és magabiztosságát is komolyan befolyásolná.

A stratégia fő célkitűzései:

- meghatározni és megvédeni mindazokat az infrastruktúrákat és létesítményeket, amelyek nemzeti szinten számítanak a legfontosabb rendszereknek. Ilyenek, pl. a közegészségügy, a kormányzati rendszer, gazdaság, vagy a nemzetbiztonság;
- megfelelő figyelmeztető rendszer biztosítása, amely képes időben jelezni a veszélyeket, vagy támadásokat;

- biztosítani az olyan egyéb infrastruktúrák és létesítmények védelmét, amelyek kedvelt terrorista célpontok.

*2006-ban jelent meg a* Belbiztonsági Minisztérium által elkészített *Nemzeti Infrastruktúra Védelmi Terv (National Infrastructure Protection Plan – NIPP).* A terv már nemcsak a különböző kormányzati szervekhez, minisztériumokhoz, valamint ügynökségekhez rendeli hozzá a meghatározott kritikus infrastruktúrákat, hanem minden szervezet számára konkrét feladatot is szab a védelem megteremtése érdekében. A tervet szintén széles nyílt társadalmi vita előzte meg, amely után 2006-ban megjelenhetett a végleges változat.

2009 májusában Obama elnök elfogadta a cyberbiztonság áttekintése után tett javaslatokat, amelyben egy olyan cyberbiztonsági vezető is szerepet kap, aki közvetlenül az elnöknek van alárendelve. Az *Átfogó Nemzeti Cyberbiztonsági Kezdeményezés (The Comprehensive National Cybersecurity Initiative – CNCI)* fő célja kiépíteni és erősíteni egy olyan cybervédelmet, amely a teljes cyberteret és az onnan érkező veszélyeket és kihívásokat lefedi. [5]

### 4.1.2. Egyesült Királyság [1]

Az Egyesült Királyságban kritikus nemzeti infrastruktúrának (Critical National Infrastructure – CNI) tekintik mindazokat a rendszereket, amelyek „*folyamatos működése annyira fontos a nemzet számára, hogy kiesésük, jelentős üzemzavaruk, vagy a szolgáltatások szintjének csökkenése életeket veszélyeztetne, súlyos gazdasági vagy komoly társadalmi következményekkel járnának.*” [1]

Az Egyesült Királyságban is számos kritikusnak minősülő szolgáltatás épül információtechnológiára. Ezeket működtetésében nem csak állami, hanem magán szolgáltatók is részt vesznek. Ebből a tényből következően az előzőekben ismertetett kritikus nemzeti infrastruktúra meghatározásban szereplő nemzeti jelző azokat az infrastruktúrákat jelzi, amelyek az egész Egyesült Királyság nemzeti érdekei szempontjából számítanak kritikusnak.

A kormány 10 szektorra és 39 alszektorra osztotta a kritikus infrastruktúrákat. A felosztás során mind a fizikai, mind az elektronikus támadások által okozható károkat figyelembe vették. A kritikus nemzeti infrastruktúra besorolás a következő [1]:

- kommunikáció (adat kommunikáció, vezetékes hang kommunikáció, levelezés, tömegtájékoztatás, mobil kommunikáció);
- veszélyhelyzeti szervezetek (mentők, tűzoltók, tengeri mentők, rendőrség);
- energiaellátás (villamosenergia-szolgáltatás, földgáz, kőolaj);
- pénzügyek (bankok, takarékpénztárak, tőzsde);
- élelmiszer ellátás (gyártás, import, feldolgozás, szállítás, tárolás);
- kormányzati- és közszolgáltatások (központi kormányzat, regionális kormányzat, helyi kormányzat, parlament és képviselők, igazságszolgáltatás, nemzetbiztonság);
- közbiztonság (kémiai, biológiai, radiológiai és nukleáris terrorizmus, tömegrendezvények);
- egészségügy (egészségügyi ellátás, közegészségügy);
- szállítás (légi, tengeri, vasúti és közúti);
- vízellátás (víz és csatorna).

Az Egyesült Királyságban 1998-ban jelent meg a Kereskedelmi és Ipari Minisztérium[45] versenyképességi fehér könyve (Competitiveness White Paper), amely megállapította, hogy az információtechnológiai ipar az egyik kulcsszereplő a gazdasági növekedésben. Ez volt az információs társadalom első fontos mérföldköve Angliában.

1999-ben megjelent egy tanulmány – *e-commerce@its.best.uk* címmel –, amely felsorolta azokat a feladatokat, amelyeket a jövőben, mint stratégia kell végrehajtani a fejlődéshez. Ez a stratégia az *UK Online* címet kapta. A stratégia végrehajtását az úgynevezett e-miniszter és e-nagykövet felügyeli.

[45] Department of Trade and Industry

A kritikus infrastruktúra védelme érdekében az angol kormányzat kétféle veszéllyel számol: terroristatámadásokkal a különböző épületek, berendezések ellen, és elektronikus támadásokkal számítógépes és kommunikációs rendszerek ellen.

A kormány 2005-ben új stratégiát dolgozott ki az információbiztonság megteremtése és fenntartása érdekében. A stratégia terrorellenes tevékenységek főbb területeit és feladatait, a nemzetbiztonság főbb kérdéseit, és a high-tech bűnözés elleni tevékenység főbb feladatait is magába foglalta.

A stratégia egyik legfontosabb megállapítása, hogy az egymással szoros és kölcsönös kapcsolatban lévő információs infrastruktúrák védelme érdekében komoly kormányzati szerepvállalás szükséges.

Az Egyesült Királyságban a kritikus információs infrastruktúrák védelméért elsősorban a Belügyminiszter (Home Secretary) felel. Természetesen számos egyéb minisztérium is részt vesz ebben a munkában.

Az állami és magánszektor közötti koordinációt az 1999-ben alakult Nemzeti Infrastruktúra Biztonsági Koordinációs Központ (National Infrastructure Security Coordination Centre – NISCC) végzi. A NISCC összefogja azoknak a szervezeteknek a munkáját, amelyek valamilyen téren érintettek a védelem kérdéseiben. Ilyen szervezetek (a feladataikkal együtt):

- a kritikus infrastruktúra és kritikus információs infrastruktúra fizikai védelmét a Titkosszolgálat (Security Service) és a rendőrség végzi;
- a hálózati biztonság kérdéseiért az Információbiztonsági Központ (Central Sponsor for Information Assurance) felel;
- a kormányzat és az állami feladatok koordinálását a védelem területén a Miniszterelnöki Hivatal (Civil Contingencies Secretariat within the Cabinet Office) végzi.

A NISCC konkrét koordinációs feladatai a következők:

- olyan párbeszéd kialakítása a kritikus infrastruktúrákat tulajdonló vállalatokkal, amelyek során azonosítani lehet a legkritikusabb rendszereket;

- figyelmeztetések kiadása támadások esetén;
- segítségnyújtás a támadásokra adandó válaszok és reakciók terén;
- összegyűjteni és elemezni a potenciális veszélyeket, fenyegetéseket, valamint az elemzések eredményeit a felhasználókhoz eljuttatni;
- a sebezhetőség felmérése;
- védelmi szakemberek és szakértők biztosítása.

A NISCC-el szoros együttműködésben léteznek további szervezetek, amelyek a védelem megteremtéséért tevékenykednek:

- Unified Incident Reporting and Alert Scheme – UNIRAS:
- Az UNIRAS szervezet gyakorlatilag az Egyesült Királyságban a CERT szerepét tölti be. Fő feladatai:
    - az elektronikus és egyéb nagy, az információbiztonságot veszélyeztető támadások kezelése;
    - az információbiztonsági és sebezhetőségi figyelmeztetések kiadása;
    - információgyűjtés az informatikai incidensekről.
- National High Tech Crime Unit – NHTCU:

  A rendőrség high-tech bűnözés felderítésére szakosodott szervezete, amely szorosan együttműködik a NISCC-el. Fő feladata az ilyen bűncselekmények felfedése, valamint a nyomozás hatósági feladatainak ellátása.
- Security Service's National Security Advice Centre – NSAC:

  A titkosszolgálat nemzetbiztonsági tanácsadó központja kormányzati szinten az egyik meghatározó testület a kritikus infrastruktúrák védelme terén. Olyan területek tartoznak hozzá, mint például a szállítás, energiaellátás, ivóvízhálózat, illetve ezek terrortámadásokkal szembeni sebezhetőségének felmérése, csökkentése és védelme. Nagy szerepe van a fizikai és a személybiztonság megteremtése területén az említett szektorokban.

- Ministry of Defence Computer Emergency Response Team –MODCERT:

  A Védelmi Minisztérium CERT-je. A MODCERT központi koordinációs központból, számos monitoring és jelentő központból, figyelmeztető, tanácsadó és jelentő pontokból áll. Szorosan együttműködik a kormányzati CERT-ekkel, és az UNIRAS-al.

Érdemes megemlíteni még két olyan kezdeményezést, amelyek ugyan nem vesznek részt közvetlenül a kritikus infrastruktúrák védelmében, ugyanakkor munkájuk az emberek tájékoztatásában illetve felkészítésében fontos szerepet kap:

- ITsafe – IT Security Awareness for Everyone: Ez egy internetes honlapot jelent, amelyet 2005 februárjától üzemeltetnek. A NISCC-től kapott publikus információkat teszik itt közzé. Alapvetően az egyéni felhasználókat és a kisvállalkozásokat célozza meg, azzal, hogy olyan tanácsokat ad, amelyek a számítógépeik, hálózataik vagy mobiltelefonjaik védelmére irányulnak. A honlap számos szolgáltatást üzemeltet a technikai kifejezések gyűjteményének elérésétől kezdődően, az ingyenes e-mail-ben vagy sms-ben történő vírusriasztásig. Havonta megjelenő hírlevele összefoglalja a megjelent vírusokat, támadási módszereket, valamint tanácsokat ad a védelemre.
- GetSafeOnline: Az információbiztonság oktatását és terjesztését vállalta fel ez a kezdeményezés a kormány támogatásával. 2005 októbere óta érhető el a weblapja, amely szintén az egyéni felhasználóknak és a kivállalkozásoknak ad tanácsot a biztonságos internethasználatra. Az oktatás és ismeretterjesztéssel a cél az adatlopások, vírustámadások, spamek, és egyéb veszélyek radikális csökkentése.

2010-ben jelent meg az Egyesült Királyság új Nemzetbiztonsági Stratégiája, amely nagyon világosan megfogalmazza a cybertérből érkező veszélyeket. [6]

### 4.1.3. Németország [7] [1]

Németországban is korán felismerték, hogy a kritikus infrastruktúrák meghatározása, illetve védelme mind a kormány, mind a társadalom érdeke, hiszen nagymértékű függőség alakult ki ezek biztonságos működésével szemben.

Az infrastruktúrának minden olyan eleme, amely meghibásodása kiesést jelentene a működésben, illetve a lakosság nagy részét érintené, kritikusnak minősül Németországban. A német alkotmány szerint az állam feladata garantálni a biztonságot, illetve biztosítani a lakosság alapvető ellátását. Ebből következően a mindenkori kormány feladata biztosítani a kritikus infrastruktúrák védelmét. Németországban a következő szektorokat határozták meg, mint kritikus infrastruktúrák [1]:

- szállítás és közlekedés (repülés, tengeri közlekedés, vasúti közlekedés, helyi közlekedés, belföldi vízi szállítás, úthálózat, posta hálózat);
- energia (villamos energia, ásványolaj, gáz, atomerőművek);
- veszélyes anyagok (kémiai és biológiai alapanyagok, veszélyes áruk szállítása, védelmi ipar);
- telekommunikációs és információtechnológia;
- pénzügy és biztosítás (bank, pénzügy, pénzügyi szolgáltatók, tőzsde piacok);
- közszolgáltatások (egészségügy, polgári védelem, élelmiszer és ivóvíz-szolgáltatás, hulladékkezelés);
- közigazgatás és igazságszolgáltatás (kormányzat, kormányzati ügynökségek, közigazgatás, vám, szövetségi fegyveres erők);
- egyéb (média, főbb kutató intézetek, műemlékek, kulturális létesítmények).

Németországban, 1999-ben, a Szövetségi Belügyminisztériumban (BMI) megalakult az AG KRITIS (German Arbeitsgruppe Kritischer Infrastructuren – Német Kritikus Infrastruktúra Munkacsoport) a kritikus infrastruktúrák védelmére.

A munkacsoportban az IS 5 (fizika védelem), a PII 1 (fenyegetettség megelőzés) és az IT 3 (IT és IT függőség) szakértői vesznek részt. Emellett a Szövetségi Bűnügyi Rendőrség Hivatala (BKA) és a Szövetségi Katasztrófavédelem és Polgári Védelem Hivatala (BBK) és a Szövetségi Informatikai Biztonság Hivatala (BSI) szakértői is rendszeresen bekapcsolódnak a munkába.

Az AG KRITIS fő feladatai a következők voltak:

- felvázolni a lehetséges veszélyeket;
- végigvinni egy teljes sebezhetőségi elemzést a német kritikus szektorokról;
- javaslatot tenni a lehetséges válaszlépésekre;
- felvázolni egy korai figyelmeztető rendszert.

1998 első felében az AG KRITIS a teljes német közigazgatást átvilágította, vizsgálva és elemezve az információtechnológiától való függőséget, a lehetséges támadási pontokat a kritikus infrastruktúra szektorok vonatkozásában. Néhány eredmény e vizsgálatból:

- az információs fenyegetésekre való figyelmeztetés mikéntje és színvonala teljesen eltérő a különböző szervezeteknél;
- számos helyen nagy ellenállásba ütközött a felmérés, amely az infrastruktúra sebezhetőségét vizsgálta volna;
- általánosságban az adatokhoz való jogosulatlan hozzáférést és az illetéktelen behatolást tekintették a legnagyobb veszélyforrásnak a szervezetek tagjai.

Az AG KRITIS és az általa elvégzett munka kiváló alapot jelentett a további kutatásokhoz. Ilyen további kutatást folytat, pl. a már említett BSI.

A BSI a BMI égisze alatt rendkívül fontos szerepet játszik a kritikus infrastruktúrák védelmi programjában. A BSI kezeli szinte valamennyi, az információs társadalom biztonságához kapcsolódó területet, megelőző lépéseket tesz infokommunikációs gyengeségek elemzése és védelmi eljárások kidolgozása formájában, ideértve a következő területeket:

- internet biztonság: elemzések, koncepciók, tanácsadás;

- vírusközpont és CERT menedzselése;
- hálózatbiztonság és kriptográfia, nyilvános kulcsú infrastruktúra (public key infrastructure – PKI) és biometria;
- kritikus infrastruktúrák.

Németországban a kormányzat és a civil szervezetek, vagy cégek közötti együttműködése (PPP[46]) jelentősnek tekinthető. E jelenség kiindulópontja az, hogy a kritikus infrastruktúrák hatékony védelme csak a köz- és magánszektor szoros együttműködésével valósulhat meg. Így számos ilyen kezdeményezés játszik szerepet a német kritikus infrastruktúrák védelmében.

Ezek közül példaként említhető a D21 Kezdeményezés, mely non-profit szervezetként több mint 300 céget tömörít magába a különböző ágazatokból. A kezdeményezés célja, hogy a kormányzati és közigazgatással együttműködve felgyorsítsák Németország átmenetét az ipari társadalomból az információs társadalomba.

Megemlítendő még az AKSIS[47] kormányzati és polgári infrastruktúra védelmi munkacsoport is, melynek célja a kritikus infrastruktúrák összekapcsolódásának elemzése volt, hangsúlyozva azok függőségét az információs technológiáktól. További céljuk megelőzés, válaszadás érdekében eljárások, és meg-felelő biztonsági menedzsment kialakítása volt.

A BSI keretében 2001-ben hozták létre a német közigazgatás CERT-jét, CERT-Bund néven. A CERT-Bund fő feladata a szövetségi adminisztráció számára biztosítani a megfelelően biztonságos hálózatokat. E munka érdekében a szervezet figyelmeztetéseket ad ki az incidensekről, a várható veszélyekről, tanácsokat ad az információtechnológia döntéshozóinak és együttműködik más CERT-ekkel.

A német CERT-eket az úgynevezett CERT-Verbund (CERT Network – CERT hálózat) fogja össze. A CERT-Verbund szövetség közös bázist teremt a különböző CERT-ek munkái-

[46] A PPP (Public Private Partnership) a közfeladatok ellátásának az a módja, amikor az állam a szükséges létesítmények és/vagy intézmények létrehozásába, fenntartásába és üzemeltetésébe (versenyeztetés útján) bevonja a magánszektort.
[47] German Arbeitkreis Schultz Kritischer Infrastructuren (1997–2000)

nak koordinálására, valamint megteremti a lehetőségét, annak hogy egy komolyabb támadás esetén a válaszlépéseket és a szükséges intézkedéseket szervezetten lehessen megtenni, azaz a CERT-ek között megfelelő munkamegosztás legyen egy ilyen – az egész szövetségi államot érintő – esemény bekövetkezése esetén is.

A CERT-eken kívül a védelem területén az egyik komoly előrelépés lehet Németországban az IT Crisis Response Center (IT krízisreagáló központ) felállítása. Ez a központ szintén a BSI keretében működne, fő feladata, pedig a nemzeti kritikus infrastruktúrákat ért támadások kezelése lenne. Az eredeti tervek szerint a központ nem állandó jelleggel, hanem csak támadások idején, illetve konkrét veszélyhelyzetekben funkcionált volna.

2005-ben jelent meg a Nemzeti Terv az Információs Infastruktúrák Védelmére 2009 (National Plan For Information Infrastructure Protection) stratégia, valamint 2011-ben a Németország Cyberbiztonsági Stratégiája, amelyekben nagyon erősen megjelenik a kritikus információs infrastruktúrák fontossága. Jelenleg Németországban az úgynevezett Cyber-Abwehrzentrum végzi ezen infrastruktúrák koordinált védelmét.

### 4.1.4. Franciaország [1]

Franciaországban kritikus infrastruktúráknak azokat tekintik, amelyek elengedhetetlenül szükségesek a főbb szociális és gazdasági folyamatokhoz. Ezek a következők [1]:

- banki és pénzügyi szolgáltatások;
- vegyi és biotechnológiai gyárak;
- energia és villamos energia;
- atomerőművek;
- közegészségügy;
- közbiztonság;
- telekommunikáció;
- szállító rendszerek;
- vízszolgáltatás.

Franciaországban 1997-ben döntöttek stratégiai szinten az információs társadalom építéséről. A cél olyan információs társadalom kiépítése, amely a digitális szakadékok legyőzésével segít a francia gazdaságnak a versenyképesség megőrzésében, illetve a fejlődésben.

Az igen fejlett infrastruktúra védelméért alapvetően a Nemzetvédelmi Miniszter (Secretary-General of National Defense – SGDN) felelős. A Nemzetvédelmi Minisztérium Központi Információs Rendszerek Biztonsági Részlege (Central Information Systems Security Division – DCSSI), az Információs Rendszerek Tárcaközi Bizottsága (Inter-Ministerial Commission for the Security of Information Systems – CISSI) és a Belügyminisztérium Hi-Tech Bűnözés Elleni Központi Irodája (Central Office for the Fight Against Hi-Tech Crime of Ministry of the Interior) szorosan együttműködik a kritikus infrastruktúrák védelme érdekében.

Franciaországban három különböző CERT működik. Ezek a következők:

- CERT-RENATER: 1993-ban alapították, tudományos kutatási feladatokkal;
- CERTA: 2000 óta a DCSSI ad helyet ennek a szervezetnek, amely fő feladata a közigazgatás számára tanácsadás, védelmi megoldások kidolgozása, a közigazgatási információs rendszereket ért incidensek kezelése;
- CERT-IST (CERT-Industry, Services, and Tertiary) 1999-ben alapította számos francia nagyvállalat (pl.. Alcatel, CNES, France Telecom, TotalFinaElf). Fő feladata a versenyszféra számára biztosítani az információs rendszereket ért támadások esetén az incidenskezelést, a figyelmeztetést és előrejelzést. E munkában természetesen együttműködik az SGDN-el és a DCSSI-vel, valamint a másik két CERT-el.

### 4.1.5. Oroszország [1]

Az elmúlt néhány évben Oroszország hatalmas lépéseket tett az infrastruktúra fejlesztése területén. Az orosz dokumentumok megállapítják, hogy az ország védelmi és gazdasági biztonsága az információbiztonság magas szintjén múlik. Ez a függőség azonban – a jövőben várható

technológiai fejlesztések miatt – nőni fog. Az *Orosz Föderáció információbiztonsági doktrínája* a következő veszélyeket sorolja fel, amelyek az egyes szektorokat kritikussá teszik [1]:

- hazai ipar, különösen a nemzeti információs ipar;
- az Orosz Föderáció információs támogatása;
- információs és telekommunikációs rendszerek, média;
- pénzügyi rendszer;
- szállító infrastruktúra (különösen a vasút és a hajózás);
- energia (gáz, olaj, villamos energia);
- katonai infrastruktúra (különösen az űr- és rakéta védelem).

Oroszországban 2000 szeptemberében jelent meg az Orosz Föderáció Információbiztonsági Doktrínája. A doktrína célja az volt, hogy technikai és szervezeti megoldásokat nyújtson Oroszország információbiztonságának növelése érdekében. Elemezte és felmérte azokat a veszélyeket, amelyek információs téren az orosz állampolgárokat, a társadalmat és az államot fenyegetik. A dokumentum négy fő fejezetet tartalmazott:

- Információbiztonság: meghatározza Oroszország nemzeti érdekeit az információs szektorban, elemzi az információs technológia gazdaságban betöltött szerepét;
- Az információbiztonság kialakításának módszerei: ebben a fejezetben gazdasági, szervezeti, valamint technikai megoldásokat elemez a kritikus információs infrastruktúrák vonatkozásában;
- Főbb állami feladatok az információbiztonság kialakításában és fenntartásában: a kormányzat főbb feladatait elemzi a dokumentum e fejezete;
- Az információbiztonság szervezeti alapjai: az információbiztonság rendszerének főbb feladatait elemzik ehelyütt. Meghatározzák az elnök, az állami tanács, a Duma, a kormány valamint az orosz biztonsági tanács főbb feladatait ezen a téren.

2001-ben egy rendkívül érdekes stratégia jelent meg, amelyet a Gazdaságfejlesztési és Kereskedelmi Minisztérium adott ki. A stratégia az Elektronikus Oroszország címet kapta. A

terv 8–10 évre előre meghatározza az információs technológia fejlesztését, mint a jövő gazdasági versenyképességének fő alapját és motorját. A terv négy alapvető területre koncentrál:

- szabályzó környezet és intézményi keretek;
- e-kormányzás;
- e-oktatás;
- internet infrastruktúra.

A stratégia által meghatározott főbb feladatok:

- a hatékony információtechnológiára épülő kormányzás törvényi alapjainak kidolgozása;
- a fejlett információtechnológiai eszközök és rendszerek használatával megteremteni a nyílt kommunikációt az állami szervek és a magánszektor szereplői között;
- az információtechnológia minél hatékonyabb felhasználásának megteremtése a gazdaságban és a szociális szférában;
- rendszeres informatikai továbbképzések tartása szakemberek számára;
- az információs infrastruktúra fejlesztése, beleértve a telekommunikációs hálózatokat, számítógép-hálózatokat, elektronikus könyvtárakat, tudományos és technikai adatbázisokat, oktatási intézményeket.

Az orosz CERT-et, amely neve RU-CERT, azaz Russian Computer Emergency Response Team, 1998-ban hozták létre. A szervezetet az Orosz Nyilvános Hálózatok Intézete (Russian Institute of Public Network – RIPN) tartja fenn. A RU-CERT része az úgynevezett Orosz Gerinchálózatnak (Russian Back-bone Networks – RBNet). Az RBNet-et alapvetően a tudományos intézmények és a középiskolák számára internetes szolgáltatások biztosítására hozták létre.

A RU-CERT számítógépes incidensekre való figyelmeztetéseket, illetve ezek kezelését, mint szolgáltatást biztosítja az RBNet felhasználóinak. A RU-CERT feladata az első időkben a főleg Moszkvában és a környékén lévő hackerek elleni tevékenység volt. Ezek a hackerek főleg úgynevezett *script kiddik*, azaz olyan fiatalok voltak, akik tudásukat fitogtatva kisebb számítógépes behatolásokat és egyéb bűncselekményeket úgy követtek el, hogy lopott betár-

cázós jelszavakkal jelentékeny anyagi károkat okoztak. Ugyanakkor gyorsan világossá vált, hogy a szolgáltatók sokkal jobban szeretik maguk elintézni az ilyen ügyeket, és elrejteni a károkat. Ennek megváltoztatása lehet az egyik fő feladata a jövőben a RU-CERT-nek.

### 4.1.6. Ausztria [1]

Az osztrák dokumentumok napjainkban az államra, a társadalomra és az egyénre vonatkozó veszélyforrásokat a politikából, a gazdaságból, a hadügyből, magából a társadalomból, a környezetből, a kultúrából és a vallásból, valamint az információtechnológiából eredeztetik. Megállapítják, hogy az információtechnológia új biztonsági dimenzióként jelent meg az elmúlt időben, amely saját területet igényel a biztonság általános kérdéskörén belül, mivel számos kapcsolata – adott esetben komoly hatása – van a biztonság egyéb aspektusaival.

Mindezidáig Ausztriának nincs egységes és elfogadott definíciója a kritikus infrastruktúrákra. Abban azonban egyetértés van, hogy egy olyan kis ország, mint Ausztria különösen sebezhető az információs infrastruktúráin keresztül. Ez a sebezhetőség igaz a polgári és a katonai rendszerekre, valamint egyre növekvő mértékben az üzleti és ipari életre.

A közeljövőre nézve az a legvalószínűbb, hogy az ország, mint az Európai Unió tagállama, átveszi az EU kritikus infrastruktúra meghatározását. Mint ahogy később látni fogjuk, az EU szerint a kritikus infrastruktúrák a következők [8]:

- energia (olaj és gáztermékek, finomítók, tárolás a csőhálózattal, villamosenergia-előállítás, és továbbítás);
- információs és kommunikációs technológiák (információs rendszerek és hálózatok védelme, műszerautomatizálás és irányító rendszerek, internet, vezetékes telekommunikáció biztosítása, mobil telekommunikáció biztosítása, rádió kommunikáció és navigáció, műholdas kommunikáció, műsorszórás);
- víz (ivóvízellátás biztosítása, vízminőség ellenőrzése, vízmennyiség biztosítása és szinten tartása);
- élelmiszer (élelmiszer ellátás biztosítása, élelmiszer biztonság felügyelete);

- egészségügy (járóbeteg és kórházi ellátás, gyógyszer és oltóanyag ellátás, laboratóriumok);
- pénzügyek (nem állami pénzügyi rendszer és szolgáltatások, kormányzati pénzügyi feladatok);
- közbiztonság (közbiztonság fenntartása, biztonság, igazságügyi rendszer)
- polgári adminisztráció (kormányzati funkciók; fegyveres erők; polgári adminisztráció szolgáltatásai; készenléti szervek; postaszolgáltatások);
- szállítás (közúti, vasúti, légi közlekedés, belföldi vízi szállítás, tengeri hajózás);
- vegyi és nukleáris ipar (vegyi és nukleáris anyagok, összetevők gyártása, feldolgozása, tárolása, veszélyes anyagok szállító csővezetékei);
- űr és kutatás.

Ausztriában, a 2001-ben kiadott Biztonsági és Védelmi Doktrína jelenti az alapját minden területen a védelemnek. A doktrína elemezte mindazokat a kihívásokat és veszélyeket, amelyekkel az olyan kis országoknak szembe kell nézniük, mint amilyen Ausztria is.

2000-ben jelent meg az e-kormányzás (e-government) program, amely az elektronikus kormányzás megteremtését irányozta elő. A program több lépcsőben kívánja megvalósítani a teljes elektronikus kormányzást, amelyben többek között az állampolgárok minden hivatalos ügyüket elektronikusan intézhetik.

Ausztriában nincs külön önálló központi szervezet, amely a kritikus infrastruktúrák védelmével foglalkozna. Ugyanakkor a Kancellári Hivatal feladata a koordináció a különálló és a védelmi kérdésekben valamilyen szinten érintett szervezetek között. A kritikus infrastruktúrák védelme elsősorban a Belügyminisztérium, a Védelmi Minisztérium, valamint a Közlekedési, Innovációs és Technológiai Minisztérium hatáskörébe tartozik.

Ausztria rendelkezik egy korai előrejelző rendszerrel, amely fő feladata a nukleáris, ipari és természeti katasztrófák jelzése. Ugyanakkor nincs a kritikus infrastruktúrák, illetve a kritikus információs infrastruktúrák támadásaira figyelmeztető központi rendszer.

Az informatikai támadásokat a Computer Incident Response Coordination Austria (CIRCA) kezeli. A CIRCA egy olyan koordinációs szerv, amely összeköti az állami és a magánszektort ezen a téren. Szerepet kap a munkájában a Kancellári Hivatal, az osztrák internetszolgáltatók szövetsége (Federation of the Austrian Internet Service Providers – ISPA), és az osztrák információtechnológiai biztonsági központ (Center for Secure Information Technology Austria – A-SIT). Természetesen a szervezetben képviseltetik magukat a gazdasági élet különböző szereplői, illetve a kritikus infrastruktúra rendszerek tulajdonosai is.

Az ISPA olyan biztonságos elektronikus hálózatot hozott létre, amelyben a különböző szervezetek online módon tudják munkájukat végezni, illetve a Kancellári Hivatal ezen keresztül tudja a koordinációt elvégezni. E hálózatnak elsődlegesen a koordinált információáramláson kívül az a feladata, hogy egy korai figyelmeztető rendszer szerepét betöltse. Azaz ezen keresztül lehet a különböző vírusokra, támadási eszközökre és módszerekre irányuló védelmi figyelmeztetéseket eljuttatni a felhasználókhoz.

### 4.1.7. Európai Unió [1]

Az Európai Unióban a kritikus infrastruktúrák problematikája szintén új és sajátos kérdésként merül fel. Szemben az uniós jogi és intézményi rendszer legtöbb elemével, itt nem lehet tagállami gyakorlatokra és tapasztalatokra alapozni az európai lépéseket, és a kezdeti döntéseket úgy kell meghozni, hogy sem az alapszerződésekben, sem a másodlagos szabályokban egyelőre nincs jogalapjuk. [9]

A 2004. június 18–19-i brüsszeli Európai Tanácson a tagállamok állam- és kormányfői felkérték az Európai Unió Bizottságát és Tanácsát, hogy készítsen átfogó stratégiát a létfontosságú infrastruktúrák védelmére. [10]

A Bizottság 2004. október 20-án közleményt fogadott el *A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben*[48] címmel, amelyben javaslatokat tett arra vonatkozóan, hogyan lehetne az európai megelőzést, felkészültséget és a válaszadást javítani a létfontosságú infrastruktúrákat érintő terrortámadások tekintetében. Ebben a közleményben a Bizottság meghatározást ad a kritikus infrastruktúra fogalmára: „*A kritikus infrastruktúrák magukba foglalják mindazon fizikai és információs technológiai létesítményeket, hálózatokat, szolgáltatásokat és eszközöket, amelyek megzavarása vagy pusztítása komoly hatással lenne az állampolgárok egészségére, biztonságára, gazdasági jólétére, vagy közvetlen hatással lenne a tagállamok kormányzati működésére."* [11]

A dokumentum megállapítja, hogy a kritikus infrastruktúrák számos szektorban, a gazdasági élet minden területén, beleértve a banki és pénzügyi, a szállítás és elosztás, az energiaellátás, a közművek, az egészségügy, az élelmiszerellátás, a kommunikáció, vagy akár a kormányzat legfontosabb feladatainak területein, egymással szoros összeköttetésben működnek. Természetesen ezeknek a szektoroknak néhány kritikus eleme önmagában nem infrastruktúra, de mégis az infrastruktúra egészének működéséhez elengedhetetlenül szükségesek. A kritikus infrastruktúrákat a következőkben határozta meg [11]:

- az energiaellátás berendezései és hálózata (pl.: villamos energia-, olaj- és földgáztermelő, tároló, finomító, szállító és elosztó létesítmények);
- kommunikáció- és információtechnológia (pl.: telekommunikációs-, műsorszóró rendszerek, szoftverek, hardverek és hálózat, beleértve az internetet is);
- pénzügyi szektor (pl.: bankok, befektetési intézmények);
- egészségügy (pl.: kórházak, rendelőintézetek, vérellátó rendszer, laboratóriumok, gyógyszer gyártók, kutatás és mentés, készenléti szervek);
- élelmiszer (pl.: biztonságos élelmiszergyártás és elosztás);

[48] Commission of the European Communities: 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 http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf

- víz (pl.: gátak, tárolás, kezelés és hálózatok);
- szállítás (repülőterek, kikötők, raktárak, vasúti és tömegközlekedési hálózatok, közlekedésirányító rendszerek);
- veszélyes anyagok gyártása, tárolása, szállítása (pl.: vegyi, biológiai, radiológiai és nukleáris anyagok);
- kormányzat (pl.: kritikus szolgáltatások, létesítmények, információs hálózatok, nemzeti műemlékek).

A Miniszterek Tanácsa ezek után két dokumentumot fogadott el: Egyrészt *A terrortámadások megelőzése, felkészültség és válaszadás* című konklúziókat, másrészt a *terrorfenyegetések- és támadások következményeivel kapcsolatos EU szolidaritási programot*, amelyek alapján a 2004. december 16–17-i brüsszeli állam- és kormányfői csúcstalálkozó felszólította az Európai Bizottságot, hogy dolgozzon ki javaslatot egy *Kritikus Infrastruktúra Védelmi Európai Programra*. [12]

A 2004-es madridi, majd a 2005-ös londoni terrortámadások rávilágítottak arra a tényre, hogy az Uniónak szintén nagyon komolyan kell vennie az infrastruktúrák irányában is megnövekedett terrorfenyegetéseket. Uniós szinten nyilvánvalóvá vált, hogy a komplex infrastruktúra rendszerek miatt, azok egy elemének időleges vagy teljes kiesése más infrastruktúrákra, illetve közvetett módon a gazdaságra is komoly negatív hatással lehet. [1]

Az Európai Bizottság 2005 novemberében közzétette az úgynevezett *Zöld Könyvét.*[49] A dokumentum 11 szektorra, és 37 termékre/szolgáltatásra osztotta az *európai kritikus infrastruktúrákat (European Crical Infrastructures – ECI)*. (2. táblázat).

A Zöld Könyv nyomán lefolytatott konzultáció alapján 2006. december 12-én irányelvjavaslatot terjesztettek a Miniszterek Tanácsa elé *az európai létfontosságú infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről.*[50]

[49] Európai Bizottság, *Zöld Könyv egy Kritikus Infrastruktúra Védelmi Európai Programról* , COM(2005) 576, 2005. november 17. (Commission of the European Communities: Green Paper on a European Programme for Critical Infrastructure Protection, Brussels, 17.11.2005 COM(2005) 576 final)

Ezt követően rendszeressé és fokozottá vált ez EU kritikus infrastruktúrákat érintő irányelveinek és cselekvési terveinek kiadás. Ezek közül a fontosabbak:

- Az Európai Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről
- Az Európai Bizottság Közleménye a kritikus információs infrastruktúrák védelméről: „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása" címmel (COM(2009) 149 final), 2009. március 30.
- Az Európai Tanács Állásfoglalása (2009. december 18.) a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről (2009/C 321/01);
- Digitális Menetrend 2010 (Európa 2020 Stratégia része);
- Közlemény az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) megerősítésére és modernizálására vonatkozóan 2010;
- Az Európai Bizottság Közleménye a kritikus informatikai infrastruktúrák védelméről: „Eredmények és következő lépések: a globális kiberbiztonság felé" címmel (COM(2011) 163 final), 2011. március 31.

### 4.1.8. NATO [1]

A NATO Polgári Vészhelyzeti Tervezés (NATO Civil Emergency Planning – CEP) 2005-2006 számára kiadott miniszteri irányelvek már számos utalást adtak a kritikus infrastruktúra védelmére. A Polgári Vészhelyzeti Tervező Bizottság (Senior Civil Emergency Planning Committee – SCEPC) egyetértett abban, hogy folytatni kell a tagállamok felkészülését a kritikus infrastruktúrákat ért esetleges terrortámadások ellen. Az SCEPC nyolc tervező csoportot és bizottságot (Planning Boards and Committees – PB&Cs) hozott létre, hogy funkcionális

[50] Az Európai Közösségek Bizottsága: A TANÁCS IRÁNYELVE az európai létfontosságú infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. Brüsszel, 12.12.2006 COM(2006) 787 végleges

szempontból vizsgálják a kritikus infrastruktúrák védelmét, amely során egységes szakértelemmel támogassák minden területen a bizottságokat.

A NATO 2010-es új stratégiai koncepciója, amely az *Aktív Szerepvállalás, Modern Védelem Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságáról címet* viseli, már kiemelt szerepet kap a cybervédelem.

*„A kibertámadások egyre gyakoribbá, szervezettebbé és a kormányok, vállalkozások, gazdaságok és potenciálisan a közlekedési és ellátási hálózatok valamint más kritikus infrastruktúrák számára is egyre nagyobb károkat okozóvá válnak. Elérhetik azt a küszöböt, ami már a nemzeti és euro-atlanti prosperitást, biztonságot és stabilitást veszélyezteti. Külföldi haderők és titkosszolgálatok, szervezett bűnözők, terrorista és/vagy szélsőséges csoportok egyaránt lehetnek egy ilyen támadás végrehajtói.* „ [13]

Ezzel összhangban a 2012-es chicagói csúcs után kiadott *Chicago Summit Declaration* a következőképpen fogalmaz:

*„Számítógépes támadások továbbra is jelentősen növekedni fognak mind azok számát, mind azok kifinomultság és a komplexitását tekintve. Megerősítjük a lisszaboni csúcstalálkozón tett számítógépes védelmi kötelezettségvállalásainkat. Lisszabon után tavaly a NATO elfogadta a Cyber Védelmi Koncepció című politikát és cselekvési tervet, amely most kerül végrehajtásra. Építve a NATO meglévő képességeire, a NATO Számítógép Vészhelyzeti Incidenskezelő Képesség (NATO Computer Incident Response Capability -NCIRC) Teljes Műveleti Képessége (Full Operational Capability - FOC), beleértve a legtöbb helyszínt és a felhasználót, kialakításra kerül 2012 végéig. Vállaljuk, hogy biztosítjuk a forrásokat és véghezvisszük a szükséges reformokat ahhoz, hogy minden NATO alá tartozó szerv központosított számítógépes védelemben részesüljön, annak érdekében, hogy a fokozott számítógépes védelmi képességekkel megvédjük a kollektív NATO értékeket.*

*Tovább integráljuk a számítógépes védelmi intézkedéseket a Szövetség struktúrájában és folyamataiban, valamint minden egyes tagországában, és továbbra is elkötelezettek vagyunk mindazon nemzeti cybervédelmi képességek ügyében, amelyek erősítik az együttműködést és a*

*kölcsönös átjárhatóságot a Szövetségen belül, többek között a NATO védelmi tervezési folyamatokban. Továbbra is fejleszteni fogjuk azokat a képességeinket, amelyekkel képesek vagyunk a megelőzésére, a felderítésére, a védelemre, és a számítógépes támadások következményeinek felszámolására. Arra törekszünk, hogy párbeszédet folytassunk a partner nemzetekkel, a nemzetközi szervezetekkel, többek között az EU-val, az Európa Tanáccsal, az ENSZ-el és az EBESZ-el, abból a célból, hogy a számítógépes biztonsági fenyegetésekkel kapcsolatban javítani lehessen a közös biztonságot és a konkrét együttműködést. Teljes mértékben kihasználjuk az észtországi Cybervédelmi Kiválósági Központ (Cooperative Cyber Defence Centre of Excellence – CCDCOE) által kínált szakértelmet."* [14]

Ugyanezen csúcsértekezlet után került kiadásra a Védelmi Képességek: A NATO Erők 2020-ban (Summit Declaration on Defence Capabilities: Toward NATO Forces 2020) dokumentum, amely a cyberbiztonságot szintén előtérbe helyezi. [15]

## *4.2. Kritikus információs infrastruktúra védelmére létrehozott nemzetközi szervezetek [7]*

A kritikus információs infrastruktúrák védelmére szakosodott nemzetközi szervezeteket mutatjuk be röviden a következőkben.

### International Watch and Warning Network (IWWN)

Tagja a 14 legfejlettebb gazdasággal rendelkező állam (pl. USA, Japán, Német-ország, Hollandia, stb.), valamint Magyarország. A szervezet célja, hogy minden tagországból közös fórumot biztosítson a nemzetgazdaságot érintő kockázatok kezelésben a jogszabályalkotóknak (Policy Makers), a kormányzati CERT szervezeteknek (governmental CERTs), valamint a bűnüldözési szervezeteknek (Law Enforcement).

### TF-CSIRT

A TF-CSIRT az Európában működő CERT szervezetek közös szervezete, aminek célja a CERT szervezetek közötti információcsere hatékony biztosítása, valamint a globális fenyegetésekkel szembeni közös fellépés elősegítése.

### Forum of Incident Response Teams (FIRST)

A FIRST a CERT szervezetek világszervezete, aminek célja a CERT szervezetek együttműködésének elősegítése globális szinten, valamint a globális fenyegetésekkel szembeni közös fellépés elősegítése.

### European Governmental CERTs (EGC)

Az EGC szervezet a vezető európai uniós államok kormányzati CERT szervezeteinek szoros együttműködését tűzte ki célul, és jelenleg hét tagja van (pl. Németország, Franciaország, Finnország, Hollandia).

## *4.3. KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA VÉDELME MAGYARORSZÁGON*

### 4.3.1. Hazai jogszabályi környezet a védelem megteremtése érdekében

Felsorolás jelleggel megadjuk azokat a jogszabályokat, amelyek utalásokat tartalmaznak kritikus infrastruktúra, illetve a kritikus információs infrastruktúra védelmére.

- 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről;
- A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény;
- Az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény (Ekszt.);

- A nemzeti adatvagyon körébe tartozó állami nyilvántartások védelméről szóló 2010. évi CLVII. törvény;
- 2080/2008. (VI.30.) Korm. határozat A Kritikus Infrastruktúra Védelem Nemzeti Programról;
- A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról;
- 1249/2010. (XI. 19.) kormányhatározat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról;
- Digitális Megújulás Cselekvési Terv 2010-2014., Nemzeti Fejlesztési Minisztérium, Budapest, 2010;
- 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról.

### 4.3.2. A hazai védelem szervezeti keretei

Természetesen Európa többi országához hasonlóan hazánkban is megvannak szervezeti keretei a kritikus infrastruktúra és a kritikus információs infrastruktúra védelemének.

Ugyanakkor el kell mondani, hogy ma Magyarországon nincs meg a koordinált védelem központi szervezete. Ez az előző alfejezetből, ahol felsorolásra kerültek a törvényi és jogszabályi keretek, talán ki is derült, hiszen hiányzik a felsorolásból a kritikus infrastruktúrák védelméről szóló törvény, vagy az információbiztonsági törvény, amely némi alapot szolgáltathatna a kritikus információs infrastruktúrák védelméhez.

Ugyanakkor nyilvánvalóan minden kritikus infrastruktúra és a kritikus információs infrastruktúra tulajdonos vagy üzemeltető a maga szintjén védi ezeket a rendszereket.

Jelen tanulmányban a védelem szervezeti kereti bemutatásakor elsősorban a kritikus információs infrastruktúrák, illetve azok egyes elemeinek védelmére létrehozott szervezetet mutatunk ba.

Hazánkban főleg az internet felől érkező veszélyek és incidensek kezelése érdekében szakmailag felkészült támogató csoportok – CERT-ek illetve CSIRT – jöttek létre az elmúlt években. [7]

Az egyik ilyen szervezet, a 2010. január 1-től Nemzeti Hálózatbiztonsági Központ néven, a Puskás Tivadar Közalapítvány keretein belül működő CERT (korábbi nevén CERT-Hungary).

A CERT-Hungary, illetve Nemzeti Hálózatbiztonsági Központ nemzetközi téren is aktívan közreműködik a kormányzati hálózatbiztonsági központok munkájában: 2007. február 2. hatállyal a Központot felvették az Európai Kormányzati CERT-ek Csoportjába (EGC), továbbá teljes jogú tagja a 14 legfejlettebb állam kormányzati szerveit tömörítő International Watch and Warning szervezetnek. A CERT Hungary Központ nemzetközi elismertségét jelzi, hogy megkapta a hálózatbiztonsági központok világszervezetének (Forum of Inciden Response Teams) és európai szervezetének (TF-CSIRT) akkreditációját (Trusted Introducer) is. [7]

A CERT-Hungary Központ nemzeti koordinációs pontként is működik, amely tevékenység keretét a hálózatbiztonság terén működő vagy ahhoz kapcsolódó civil, kormányzati és üzleti szervezetekkel kötött együttműködési megállapodások szabják meg. Ilyen szerződések kerültek aláírásra a következő felekkel: [7]

- Nemzeti Nyomozóiroda;
- BME CrySys Lab;
- eSec.hu konzorcium;
- MTA SZTAKI51;
- HUN-CERT;
- ISACA52;

[51] Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutató Intézet

- Magyar Bankszövetség;
- Magyar Nemzeti Bank;
- Magyar Tartalomipari Szövetség;
- Infomediátor.

## *4.4. A komplex információs támadásokkal szembeni védelem eszközei és módszerei*

### 4.4.1. A komplex információbiztonság értelmezése

A védelem – a magyar nyelvben – tevékenység, illetve tevékenységek sorozata, amely arra irányul, hogy megteremtse, fejlessze, vagy szinten tartsa azt az állapot, amit biztonságnak nevezünk. Tehát a védelem tevékenység, amíg a biztonság egy állapot.

A biztonság, mint egy kedvező állapottal szemben elvárható, hogy a fenyegetések bekövetkezésének lehetősége, valamint az esetlegesen bekövetkező fenyegetés által okozott kár a lehető legkisebb legyen. Ahhoz azonban, hogy teljes legyen ez a biztonság az szükséges, hogy minden fajta valós fenyegetésre valamilyen védelmet nyújtson, minden támadható ponton biztosítson valamilyen akadályt a támadó számára. Mindezek mellett elvárható, hogy folyamatosan fenntartható legyen. [16]

*„A védelem a biztonság megteremtésére, szinten tartására, fejlesztésére irányuló tevékenység.*

*A biztonság a védelmi rendszer olyan – az érintett számára kielégítő mértékű – állapota, amely zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet valósít meg. Ahol a zárt védelem az összes releváns fenyegetést figyelembe vevő védelmet, a teljes körű védelem pedig a rendszer valamennyi elemére kiterjedő védelmi intézkedések összességét jelenti. A folytonos védelem az időben változó körülmények és viszonyok ellenére is megszakítás nélkül valósul meg. A kockázattal arányos védelem esetén egy kellően nagy időintervallumban a*

[52] Information System Audit and Control Association — Információrendszer Ellenőrök egyesülete

*védelem költségei arányosak a potenciális kárértékkel, azaz a védelemre akkora összeget és olymódon fordítanak, hogy ezzel a kockázat az érintett számára még elviselhető, vagy annál kisebb."* [16]

Az információ a szervezetek számára a legfőbb erőforrások egyike, a megfelelő és megbízható működés alapja. Kiemelt erőforrásként még nagyobb hangsúlyt kap a gazdálkodó szervezetek életében, ezért minden esetben gondoskodni kell megbízhatóságáról és biztonságáról, hiszen ez alapvetően befolyásolhatja egy szervezet működését, szolgáltatásainak, termékeinek minőségét.

Annak érdekében, hogy az információk megfelelően védettek legyenek, az alábbiakat kell biztosítani:

- bizalmasság;
- rendelkezésre állás;
- sértetlenség;
- hitelesség;
- letagadhatatlanság.

**A bizalmasság** olyan biztonsági tulajdonság, amely lehetővé teszi, hogy az információ jogosulatlan egyedek (emberek, folyamatok) számára ne legyen elérhető, vagy ne kerüljön nyilvánosságra. A bizalmasság elvesztése az információ illetéktelenek általi hozzáférését, megismerését jelenti.

**A rendelkezésre állás** a biztonság azon szempontja, amely lehetővé teszi, hogy a feljogosított szubjektum (humán közreműködő vagy gépi folyamat) által támasztott igény alapján az adott objektum elérhető és használható legyen. A rendelkezésre állás elvesztése azt jelenti, hogy az információhoz vagy az informatikai rendszerhez való hozzáférés vagy annak használata akadályokba ütközik, vagy adott időtartamra vagy teljes mértékben megszűnik.

**A sértetlenség** olyan biztonsági tulajdonság, amely azt jelenti, hogy az adatot, információt vagy programot csak az arra jogosultak változtathatják meg és azok észrevétlenül nem módo-

sulhatnak és nem törölhetők, semmisíthetők meg. A sértetlenség elvesztése az információ jogosulatlan módosítását vagy megsemmisítését jelenti. A sértetlenség fogalmába beleértendő az információk hitelessége és letagadhatatlansága is.

**A hitelesség** az entitás olyan biztonsági tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más entitás számára bizonyíthatóvá tesz. Egy információ akkor tekinthető hitelesnek, ha mind tartalmának, mind létrehozójának (küldőjének) sértetlensége garantálható.

**A letagadhatatlanság** olyan biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az infokommunikációs rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően. [17]

Az adatminősítés jelenlegi rendjét figyelembe véve, a komplex információbiztonság szempontjából – a tárolt adatok minősítésétől függően – a vállalatoknál, intézményeknél, kormányzati és védelmi célú szervezeteknél is a következő biztonsági osztályokat kell kialakítani:

- információvédelmi alapbiztonsági osztály;
- információvédelmi fokozott biztonsági osztály;
- információvédelmi kiemelt biztonsági osztály.

Az **információvédelmi alapbiztonsági osztály** a személyes adatok, üzleti titkok, pénzügyi adatok, illetve a szervezet belső szabályozásában hozzáférés–korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszerek biztonsági osztálya.

Az **információvédelmi fokozott biztonsági osztály** a szolgálati titok, valamint a nem minősített adatok közül a különleges személyes adatok, nagy tömegű személyes adatok, banktitkok, közepes értékű üzleti titkok feldolgozására, tárolására is alkalmas rendszerek biztonsági osztálya.

Az **információvédelmi kiemelt biztonsági osztály** az államtitok, a katonai szolgálati titok, valamint a nem minősített adatok közül a nagy tömegű különleges személyes adatok és nagy értékű üzleti titkok feldolgozására, tárolására alkalmas rendszerek biztonsági osztálya. [18]

Ha az információs társdalom működésének korlátozása vagy akadályozása a cél, akkor az a komplex kritikus információs infrastruktúrák (számítógép-hálózatok, távközlő hálózatok, műsorszóró hálózatok, távirányító rendszerek, légi irányító rendszerek, navigációs rendszerek, stb.) elleni összehangolt támadássorozattal valósulhat meg a már említett három – a fizikai, az információs, és a tudati – dimenzióban. Látható tehát, hogy e tevékenységek nem csupán az információs infrastruktúra egy szegmense ellen irányulnak, pl. csak a számítógép-hálózatok ellen. Így ez azt is jelenti, hogy a védelem megtervezése, megszervezése és kivitelezése is e három dimenzióban kell, hogy megvalósuljon. Vagyis az egyirányú, egy területre (pl. az informatikai rendszerek védelmére) fókuszáló információbiztonság helyett csakis a komplex információbiztonság megvalósítása vezethet eredményre.

Komplex és integrált védelmet kell megvalósítani, ami azt jelenti, hogy azokat a kritikus információkat[53] kell megvédeni, amihez a másik fél a fizikai-, az információs- és a tudati dimenzióban – megfelelő védelem hiányában – hozzáférhet, azt felhasználhatja a saját döntési folyamataiban, vagy esetleg tönkreteheti, és ezáltal a saját döntési folyamatainkat akadályozhatja. A megoldás, ha ezeket a kritikus információkat elrejtjük a másik fél elől, vagy megakadályozzuk, hogy hozzájuk férjenek. Erre alkalmasak a komplex információbiztonsági rendszabályok, megoldások. A komplex információbiztonság területén tehát olyan megoldásokat kell keresni, amelyek az információs infrastruktúrák és az infokommunikációs rendszerek teljes spektrumát lefedik a biztonság oldaláról.

A különböző információs támadások minden esetben a társadalom funkcionális és támogató információs infrastruktúrái ellen irányulnak, amelyek sok esetben egybe esnek a kritikus információs infrastruktúrákkal. Az infrastruktúrákon belül lévő különböző infokommunikáci-

[53] A kritikus információk azok a saját szándékokra, képességekre, tevékenységekre vonatkozó fontos információk, amelyek a másik fél számára feltétlenül szükségesek saját tevékenységük hatékony tervezéséhez és végrehajtásához.

ós rendszereket vagy rendszerelemeket próbálják meg támadni, hiszen azok a leginkább hozzáférhető pontok, azokon keresztül lehet behatolni egy rendszerbe. De természetesen nem ezek az információs támadás végső célpontjai, hanem a politika, a gazdaság, a kultúra, a védelmi szféra, stb. és az itt lévő döntéshozók, akik egy adott terület vonatkozásában megfelelő döntéseket kívánnak hozni. A támadó ezt akarja megakadályozni.

Ha tehát a támadás végső célja különböző stratégiai fontosságú döntéshozatal megakadályozása, akkor az mindenképpen fontos nemzetbiztonsági kihívás, nemzetbiztonsági feladat, mind össztársadalmi szinten, mind pedig a mikrorendszerek szintjén. Hiszen lehetnek olyan vállalatok, cégek, intézmények, amelyeknek a támadása az infrastruktúrák közti interdependencia következtében igen komoly lavinát indíthat el akár gazdasági vagy politikai színtéren vagy egyéb más területeken, ami egy ország teljes biztonságát veszélyeztetheti.

A kritikus információs infrastruktúrák komplex információbiztonságát biztosító védelmi eszközöket és módszereket terjedelmi korlátok miatt a szándékos és kizárólag az információs dimenzióban jelentkező támadási módszerek (számítógép-hálózat elleni támadás, elektronikai felderítés és az elektronikai támadás) szerint mutatjuk be. A védelem módszereinél nem foglalkozunk a különböző nem szándékos eredetű károkozások (természeti katasztrófák, üzemzavarok, stb.), és a humán eredetű fenyegetések elleni védelem kérdéseivel.

Ez alapján a védelem területei igazodnak 3.4 alfejezetben ismertetett információs támadás eszközeihez és módszereihez így ezek az alábbiak:

- számítógép-hálózatok védelme;
- elektronikai felderítés elleni védelem;
- elektronikai támadással szembeni védelem.

### 4.4.2. A számítógép-hálózatok védelme

A számítógép-hálózatok védelme a saját számítógép-hálózat megóvását jelenti a jogosulatlan hozzáféréssel és behatolással szemben, amelyet abból a célból hajtanak végre, hogy megsze-

rezzék az adatbázisokban tárolt adatokat és információkat, illetve, hogy szándékosan lerontsák, működésképtelenné tegyék információs rendszerünket. [19]

Alapvető számítógép-hálózati biztonsági alapelveknek kell tekinteni, hogy:

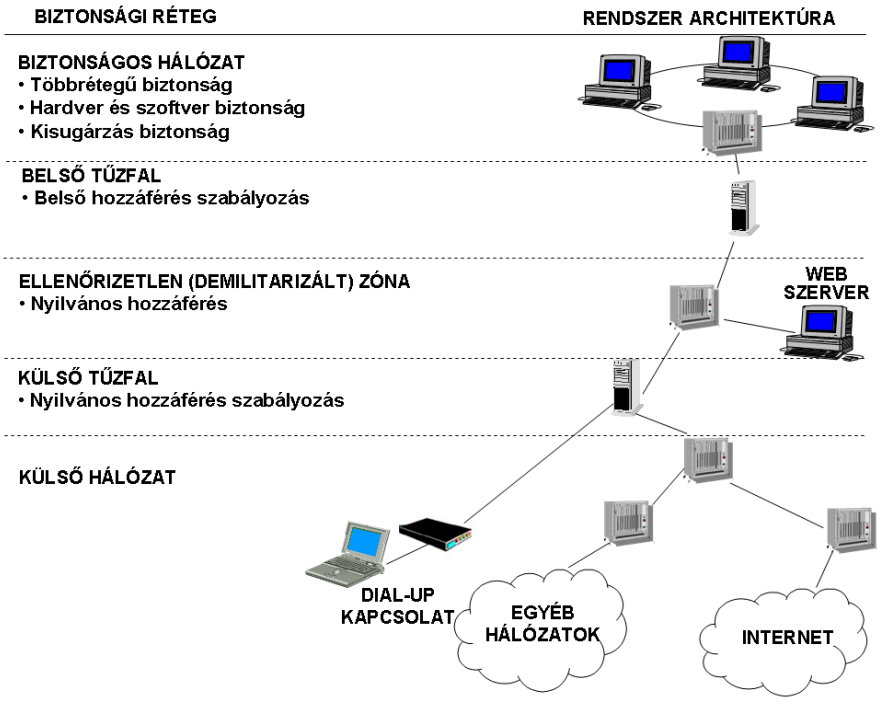
- a védelem ne kerüljön többe, mint a védendő információ, illetve, hogy
- a védelemnek olyannak kell lennie, hogy ellenálljon a feltörési, eltulajdonítási kísérleteknek addig, amíg a védendő információ értékes.

Az információbiztonság kérdése általában csak azoknál a szervezeteknél hatékony, ahol egyenlő súllyal kezelik a nem informatikai tárolókon lévő, keletkező, valamint az informatikai eszközökön fellelhető információkat. [20]

A korábban ismertetett információbiztonsági osztályokat (alap- fokozott-, kiemelt információbiztonság) a számítógép-hálózatok védelmének kialakításakor is messzemenően figyelembe kell venni. Egy számítógép–hálózatban minél magasabb információbiztonsági osztályba tartozó adatok tárolását, feldolgozását végzik, annál magasabb szintű védelmi rendszabályokat kell érvényesíteni és megvalósítani.

A megbízható számítógép-hálózatoknak[54] rendelkezniük kell a már korában ismertetett 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 1. ábra. [19]

[54] Trusted Networks




1. ábra. Többrétegű hálózat biztonsági felépítése [19]

A számítógép-hálózatok védelmének megvalósítása lehet passzív és aktív.

A passzív védelmi módszerek és eszközök az alábbiak:

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

Az aktív védelem módszerei közé sorolhatók:

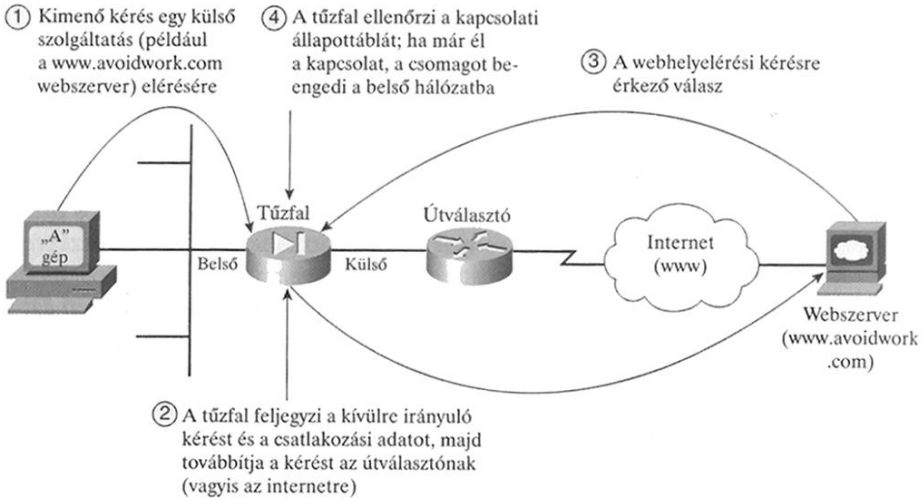
- a megelőző támadások (Pre-emptive Attacks);
- az ellentámadások (Counterattacks) és
- az aktív megtévesztés (Active Deception). [21]

Az aktív védelmi módszereket az esetek többségében csak háborús konfliktusokban, katonai műveletekhez kapcsolódóan alkalmazzák, emiatt a továbbiakban ezt nem tárgyaljuk.

### Tűzfalak

A számítógép-hálózat más hálózatoktól (pl. Internet) való elválasztásának az egyik elterjedt módja a tűzfal,[55] 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 szűrése. 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 működését szemlélteti a 2. ábra. Az „A” gép mögött ülő személy a böngészőjében meg szeretné jeleníteni a www.avoidwork.com weboldalt.




2. ábra. A tűzfal működési elve [22]

[55] A "tűzfal" nevet is onnan kapták, hogy szerepük hasonló, mint régen a fából készült házsorokba beépített téglafalaké, amelyek megakadályozták a tűz továbbterjedését.

A kívülre irányuló kérést a tűzfal megjegyzi (beírja az úgynevezett munkamenet állapot-nyilvántartó táblába), és továbbítja azt az útválasztónak. A kérés eljut a külső szolgáltató webszerveréhez, amely fogadja a kérést és válaszol rá. A választ először a tűzfal kapja meg, és ha a kapcsolat már él, akkor beengedi a belső hálózatba, így a kért webtartalom megjelenik az internetező böngészőjében. [22]

A korábban bemutatott többrétegű megbízható hálózatban (1. ábra) egy külső tűzfal 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. Ha lehetséges, akkor csak egy ponton kell csatlakozni a nyilvános hálózathoz, s ezt a csatlakozó számítógépet látják el tűzfal funkciókkal, ez a külső tűzfal. Ez a védelem azonban nem elegendő, gondoskodni kell arról is, hogy ha azon átjutott a behatoló, akkor se férhessen hozzá adatainkhoz. A tűzfalak működése ezért azon alapul, hogy a rendszergazda beállíthatja, melyik IP-forgalmat engedje át, és melyiket tiltsa le. Ha az üzenetek szűrése nincs körültekintően beállítva, a védelem hatékonysága máris csökken. [19]

A tűzfalak alábbi három típusát különböztethetjük meg:

- személyi tűzfal (Personal firewall);
- multifunkcionális tűzfal (All-in-one firewall);
- hardveres tűzfal.

A **személyi tűzfalak** valamilyen operációs rendszerre települő, különleges szoftverek, amelyek tűzfalfunkciókat látnak el. Általában a szélessávú kapcsolathoz csatlakozó számítógépeket védjük velük, ami manapság szinte elengedhetetlen. Az operációs rendszerek gyártói úgy reagáltak a kihívásokra, hogy beépített IP-alapú tűzfalakat fejlesztettek ki a termékeikhez. A nem beépülő, külön telepíthető tűzfalak általában kijavítják, illetve helyesen beállítják az operációs rendszer felfedezett hibáit, illetve helytelen beállításait, és letiltják az internetkapcsolatot. A felhasználónak, illetve rendszergazdának úgynevezett szabályokat kell létrehozni, hogy egy adott program (pl. böngésző) el tudja érni a webes szolgáltatásokat (ilyenkor meg

kell adni a program nevét, hogy mely portokat használja, ill. a kommunikáció irányát). Minden más program és tevékenysége számára a hozzáférés tiltva van.

A **multifunkcionális tűzfal** (pl. egy router[56]) kereskedelmi forgalomban is kapható, a mindennapi igényekhez mért tűzfaltípus. A nevét onnan kapta, hogy az eszköz tartalmaz egy útválasztót, egy Ethernet-kapcsolót és egy vezeték nélküli elérési pontot (Access point), illetve beépített tűzfalfunkciókkal is rendelkezik (pl. IP packet forwarding[57]). Majdnem az összes típus böngészőn keresztül menedzselhető, általában egy weboldalhoz hasonló, könnyen kezelhető felületet biztosít a felhasználó számára. [22]

**A hardveres tűzfalak** abban az esetben alkalmazhatók, ha több száz, esetleg több ezer felhasználós hálózatot kívánunk üzemeltetni. Ebben az esetben a kisebb hálózatra szánt tűzfalak egyrészt lassúak lehetnek a kisebb teljesítményük miatt, másrészt az egyszerű szoftveres kivitelezés miatt nagyon nehézkessé is válhat az üzemeltetés. A hardveres tűzfalak, kibővített memóriával és extra interfészekkel rendelkeznek, továbbá analóg eszközökkel is leválasztják a belső hálózatot az internetről. Természetesen ez a fajta tűzfal is saját operációs rendszerrel rendelkezik. [53; 64]

A tűzfallal való hálózatvédelem jellemzői az alábbiak:

- 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;

[56] A router (útválasztó) a számítógép-hálózatokban egy forgalomirányítást végző eszköz, amelynek a feladata a különböző - például egy otthoni vagy irodai hálózat és az internet vagy vállalaton belüli hálózatok összekapcsolása, azok közötti adatforgalom irányítása.
[57] Magyarul IP-csomag továbbítás, a tűzfalak egyik speciális funkciója

- 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 titkosítva áramlanak. [23]

Meg kell jegyezni, hogy a tűzfalak beépítése sem ad százszázalékos védelmet, mert a tűzfalak 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 a védelem feltörhető.

### Vírusirtók

A különböző rosszindulatú programok elleni küzdelem leghatékonyabb eszközei a különböző antivírus szoftverek, amelyek elsősorban a vírusazonosító adatbázisaik alapján, illetve heurisztikus vagy egyéb módszerek segítségével ismerik fel a rosszindulatú programokat. A vírusirtók működésének hatékonyságát nagymértékben befolyásolja vírusazonosító adatbázisuk frissessége. Ezért a vírusirtó szoftverek adatbázisaikat automatikusan, naponta többször is frissítik.

A víruskeresőkkel szemben támasztott legfőbb követelmények:

- legyen megbízható;
- legyen alkalmas minél többféle kártevő azonosítására;
- legyen alkalmas a kártevő eltávolítására;
- álljon rendelkezésre rendszeres frissítés;
- legyen képes folyamatos ellenőrzésre;

- legyen elfogadható a futási sebessége;
- használata legyen kényelmes.

A víruskereső programok lehetnek:

- háttérben futó, vírusazonosító mintákat használó keresőprogramok;
- alkalmi vírusellenőrző és memóriarezidens programok;
- heurisztikus keresést alkalmazó programok.

**A háttérben futó víruskeresők** jellemzője, hogy a számítógép indításával egyidőben – a beállított paramétereknek megfelelően – azok is elindulnak, és 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 vírusazonosító mintákkal megegyeznek. E szoftverek alkalmasak a Malware-ek eltávolítására, törlésére, esetleg karanténba helyezésére, ahol már nem okozhatnak kárt. Természetesen alkalmasak arra is, hogy eseti módon ellenőrizzék a számítógép összes lemezét vagy csak egyes meghatározott lemezeket, objektumokat.

Hálózatba kötött gépek esetében a központi szervereken telepített vírusellenőrzés is igen hatékony védelmet biztosít, amennyiben a munkaállomások adatállományaikat hálózati meghajtókon hozzák létre és tárolják. Ilyen rendszereken viszonylag csekély a vírustámadások kockázata. Ebben az esetben a munkaállomásokon elegendő 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.

A **heurisztikus víruskeresők** 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 rosszindulatú programokban fordulnak elő. Ilyen gyanús művelet lehet például, a végrehajtható állományokba való írás. A heurisztikus víruskeresők segítségével még fel nem fedezett vírusok is felismerhetők. [19]

Napjaink vírusirtó szoftvereinek szinte mindegyike alkalmas mindhárom ismertetett módban való működésre.

### Hozzáférés szabályozás

A hozzáférés szabályozás két leginkább alkalmazott módszere a jelszavak alkalmazása és a hitelesítés.

Egy adott számítógéphez való hozzáférés a legtöbb esetben **jelszóhoz** kötött. 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.

Biztonságosan védett számítógép–hálózatokban gyakran többszintű jelszavas védelmet alkalmaznak, azaz a rendszer egymás után, különböző szinteken több jelszót kér. A jelszavas védelem más módszerekkel is kombinálható pl. PIN kártyával, ujjlenyomat ellenőrzéssel, írisz letapogatással stb.

**A hitelesítés** (Authentication) 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. Mindazonáltal a hitelesség nehezen igazolható csak ilyen módon, különösen, ha többen is (esetleg illetéktelenül is) rendelkeznek az adott hozzáférési joggal.

Az operációs rendszerek, adatbázis–kezelők, levelező rendszerek jegyezhetik, hogy ki, mit, mikor tett, de egyrészt ezeket sokszor be lehet csapni, másrészt nem mindig könnyű a visszaellenőrzés. A dokumentumok, üzenetek formája is árulkodhat azok hitelességéről. [24]

A hitelesítésnek az előbbinél hatásosabb módszere a **titkosítás (kriptográfia)**. A titkosítás olyan matematikai eljárás, melynek során egy üzenetet úgy változtatunk meg felismerhetetlenül, hogy abból az eredeti üzenet csak valamilyen, kizárólag a küldő és a címzett által ismert eljárás segítségével fejthető vissza. A titkosítással a legtöbb esetben biztosítható a tartalom rejtettsége, érintetlensége, letagadhatatlansága és a forrás igazolhatósága.

A titkosítás két legismertebb fajtája a szimmetrikus- és az aszimmetrikus titkosítás.

A **szimmetrikus kulcsú titkosítás** azon a feltevésen alapul, hogy a kódoló (küldő) és a dekódoló (fogadó) egyaránt birtokában van olyan információnak, amelyet mások előtt titokban tartanak. Ez tartalmazza a titkosításhoz szükséges titkos kulcsot és a kulcsot felhasználni képes eljárást (algoritmust). A küldő az ismert algoritmus és a titkos kulcs segítségével kódolja a nyílt üzenetet, majd a fogadó ugyanazon titkos kulcs és az algoritmus segítségével dekódolja azt. Harmadik fél a titkos információ hiányában sem megérteni nem tudja a rejtjelezett üzenetet, sem pedig rejtjelezni nem tud hamis üzenetet. A titkos kulcsok általában különböző bit hosszúságú kódok.

A szimmetrikus kulcsú titkosításban a leggyakrabban a DES-sel (Data Encryption Standard) találkozhatunk. Ez egy 56 bit-es kulcsot használó ún. blokk-rejtjelezés, ami a mai technikával már könnyen feltörhető. Ezen eljárás fejlettebb és biztonságosabb változata a 3DES (Tripla DES), amely a DES algoritmusát használja háromszor egymást követően különböző kulcsokkal (általában: titkosít - visszafejt - titkosít). A napjainkban ismert egyik legjobb algoritmus az IDEA (International Data Encryption Algorithm), amely 128 bit-es titkos kulcsot használ. [25]

Az **aszimmetrikus kulcsú titkosítás** vagy más néven nyilvános kulcsú titkosítás előnye, hogy a küldő és a fogadó félnek nem kell semmilyen titkos jelszót vagy kulcsot cserélnie egymással. Ehelyett minden egyes felhasználó rendelkezik egy kulcspárral, mellyel a bizton-

ságos kommunikáció létrejöhet. Az egyik kulcsot magánkulcsnak (privát kulcsnak), a másikat nyilvános kulcsnak (publikus kulcsnak) nevezzük. A két kulcs ugyanazon kulcsgenerálási eljárásból származik, teljesen összetartoznak, de egyik a másikból nem következtethető ki. A magánkulcsot minden felhasználónak titkosan kell kezelnie, míg a nyilvános kulcsot mindenkivel ismertetni kell, akivel kommunikálni szeretnénk. Az aszimmetrikus kulcsú titkosítás esetén a feleknek nincs szükségük megbízható csatornára vagy személyes találkozásra, csak a kulcs hitelességét, tulajdonosához való tarozását kell bizonyítani.

A titkosítás során a titkosítás (kódolás) a fogadó oldal titkosító tanúsítványához tartozó nyilvános kulccsal történik, míg a visszafejtés (dekódolás) a fogadó oldalon, a titkosításhoz használt nyilvános kulcshoz tartozó magánkulccsal lehetséges csak. Ebből kifolyólag a titkosított adatot csak és kizárólag az a személy tudja értelmezni/olvasni, aki rendelkezik a nyilvános kulcshoz tartozó magánkulccsal. Ennek megfelelően titkosított adatot csak az a személy fogadhat, aki rendelkezik megbízható hitelesítés-szolgáltató által kibocsátott érvényes titkosító tanúsítvánnyal. Az aszimmetrikus kulcsú titkosítási eljárás legelterjedtebb változata az RSA, amelynek elnevezése az algoritmus megalkotói vezetéknevének kezdőbetűből képzett mozaikszóból ered.[58] [26]

A hitelesítés további módszer a **digitális aláírás**, amely a nyilvános kulcsú rendszerek sajátosságaira épít. Azon a feltételezésen alapszik, hogy a titkos kulcs kizárólag annak tulajdonosa számára hozzáférhető, és ezt az információt máshonnan (például a nyilvános kulcsból) nem is lehet kikövetkeztetni, illetve a titkos kulcs ismerete nélkül nem lehet olyan kódolást készíteni, ami a titkos kulcs párját alkotó nyilvános kulccsal fejthető vissza. Így tehát egy titkos kulcs használata kétséget kizáróan és letagadhatatlanul az adott személyhez köthető. A digitális aláírásnál a titkos kulcs használatával létrehozott adatsort használják ezen túl az eredeti üzenet sértetlenségének igazolására is. [27] A digitális aláírás gyakorlatilag az egyetlen jól bevált mód, mellyel egy teljes dokumentumról igazolni lehet nem csak annak hiteles alá-

[58] Rives, Shamir, Aldeman

írását, 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.

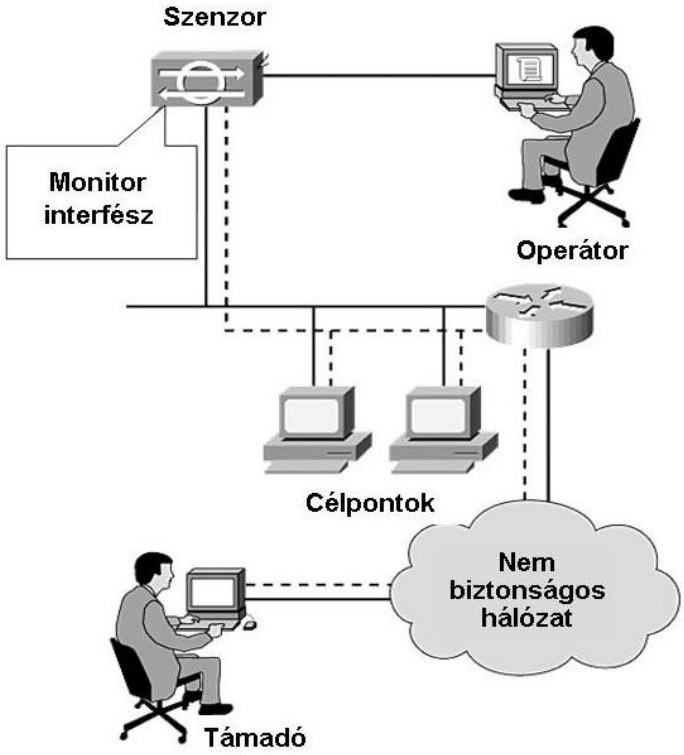
### Behatolás detektálás és adaptív válaszlépések

A behatolás detektálás és adaptív válaszlépések az informatikai 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 külső behatolási kísérletek általában a szervereket és munkaállomásokat veszik célba, de nem ritka a hálózati elemek "piszkálása" sem. A behatolás detektáló 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. (3. ábra) [20]

A behatolás detektáló rendszerek – annak alapján, hogy milyen módszerrel érzékelik a betöréseket – alapvetően két csoportba sorolhatók:

- mintaalapú behatolás detektáló eszközök (Signature-based IDS);
- viselkedést vizsgáló behatolás detektáló eszközök (Behavior-based IDS).

A **mintaalapú behatolás detektáló eszközök** manapság talán a leghatékonyabb és ezért legelterjedtebb eszközök a hálózatba való betörés megakadályozásában. A módszer lényege az, hogy a rendszer tartalmaz egy úgynevezett támadási adatbázist, amely tárolja a lehetséges támadási mintákat, jellemzőket. A beérkező információt, illetve aktivitást a rendszer összehasonlítja az adatbázisban tárolt mintákkal, és megpróbálja eldönteni, hogy ez az aktivitás támadásnak minősül-e.




3. ábra. Behatolás detektálás

Ha igen, akkor képes a megfelelő személyeket (általában rendszergazdákat) riasztani, illetve meg is tagadhatja a kérést. A rendszer a hatékonysága ellenére számos hátránnyal küszködik.

Minél nagyobb biztonságot szeretnénk elérni, annál több mintát kell eltárolnunk, így annál nagyobb lesz az adatbázisunk. Emiatt az egyes kérések vizsgálata tovább tart, és ha a hardverkörnyezet nem megfelelő teljesítményű, a szolgáltatás lassúsága bosszantó lehet. Két lehetőség kínálkozik tehát: az egyik a lehető legnagyobb teljesítményű szerver üzemeltetése, a másik a minták számának ésszerű csökkentése.

A másik problémát éppen a rendszer működési elve adja. Csak azokat a támadási fajtákat képes érzékelni, amelyekről a minta-adatbázisban tárol. Ha olyan támadást intéznek a rend-

szer ellen, amelyről nincs információ, akkor a riasztás, illetve a kérésmegtagadás elmarad, az ártó tevékenység pedig folytatódik. Éppen ezért nagyon fontos a frissítések naprakészsége arra az esetre, hogy ha a szoftver fejlesztői hibát észlelnek, akkor a rendszer a lehető legrövidebb időn belül aktualizálja az adatbázisát.

A mintaalapú behatolás detektáló eszközök a detektálás helyének függvényében az alábbiak lehetnek:

- hálózati behatolás detektáló eszközök (Network-based IDS);
- hosztalapú behatolás detektáló eszközök (Host-based IDS);
- hibrid behatolás detektáló eszközök (Hybrid IDS).

A **hálózati behatolás detektáló rendszer** a hozzákapcsolt hálózati szegmens csomagjait különböző módokon vizsgálja meg. Létezik olyan típus, amely az „ujjlenyomatmintákat" vizsgálja meg az adatbázis alapján. Más típusok a szokatlan mennyiségű csomagok alapján következtetnek arra, hogy támadás van vagy lehet folyamatban. A hálózati IDS-ek nagy előnye, hogy a telepítés után a hálózatban szinte észrevétlenül tudnak működni. Célszerű kettőt alkalmazni: egyet a külső, egyet pedig a belső hálózati forgalom figyelésére, így a mindkét irányból kezdeményezett támadásokat is ki lehet védeni. [22]

A **hoszt- vagy gépalapú behatolás detektáló eszköz** feladata az, hogy azt a hosztot, vagyis kiszolgálót védje, amelyre telepítették. A rendszer indításakor meghatározzák azoknak a detektálni kívánt eseményeknek a körét, amelyeket naplózni (logolni) fog. Az eszköz ezeket fogja figyelni, és ha rendellenes eseményt észlel, akkor beírja a log fájlba, és figyelmezteti a rendszergazdát. Értelemszerűen lehetőség van arra is, hogy a naplózási konfiguráció megváltoztatásakor is legyen értesítés, ha esetleg a támadó ezzel kívánja indítani a tevékenységét.

A hosztalapú betörés-detektáló eszközök nagy előnye az alacsony beszerzési költség és az egyszerűség. Hátránya viszont, hogy a védeni kívánt gépre kerül feltelepítésre, ezért annak erőforrásait használja a működéséhez. Mivel a riasztás az összehasonlítás után történik, ezért a betörés részben már meg is történt. Ráadásul, ha a támadás ténye nem jelenik meg a log

fájlban, akkor az eszköz számára is észrevétlen marad a támadás ténye, így arra reagálni sem fog.

A **hibrid behatolás detektáló eszköz** onnan kapta a nevét, hogy egyesíti a gépalapú és a hálózati IDS-ek előnyeit. Egy hibrid IDS teljes egészében megvalósít egy hosztalapú rendszert, valamint hálózati betörés-detektáló rendszerként is funkcionál. A kiszolgálóra telepített úgynevezett IDS agent program képes több szinten is a hálózati forgalom figyelésére, sőt a titkosított forgalmat is láthatja amellett, hogy a dekódolt információkhoz is hozzáférhet.

A hibrid IDS-ek optimális megoldást jelenthetnek a behatolások detektálására, azonban hátrányos tulajdonságaik is vannak. Az egyik, hogy mivel a védendő gépre telepítik, ezért annak erőforrásait használják, így gyengébb hardveren ez gondot jelenthet. A másik hátrány és fontos kitétel egyben, hogy az IDS agentet csak olyan operációs rendszeren lehet futtatni, amilyenre a fejlesztő programozók megírták.

A **viselkedést vizsgáló behatolás detektáló eszközök** a mintalapú betörés-detektáló eszközök kiegészítésére, a zárt adatbázisból származó korlátok feloldására alkalmasak. Ezek lényege abban rejlik, hogy a mesterséges intelligenciát felhasználva egy aktivitásról meg lehessen állapítani, hogy az a szokásostól eltérő-e vagy sem. [18]

### 4.4.3. Elektronikai felderítés elleni védelem

Az elektronikai felderítés elleni védelem alapjai [28]

Az elektronikai felderítés elleni védelem célja észlelni, megbecsülni és megakadályozni a felderítési adatok gyűjtését, továbbítását, feldolgozását és szétosztását. E tevékenység tartalmazza a másik fél teljes felderítő adatgyűjtő rendszerének feltárását, a saját sebezhető pontok megállapítását, valamint a biztonsági rendszabályokat és azok értékelését.

Az elektronikai felderítéssel szembeni védelem alapvető módszerei a következők:

- a felderítő eszközök és azok hordozói, valamint az információgyűjtő és felderítő központok megsemmisítése, elfoglalása, megrongálása;

- a felderítő berendezések és az adatokat továbbító kommunikációs eszközök elektronikai zavarása;
- elektronikai eszközök sugárzásainak korlátozása;
- a felderítés ellen védendő objektumok, eszközök és tevékenységekre utaló áruló jelek megszüntetése, elektronikai álcázása;
- a felderítés hatékonyságának technikai módszerekkel való csökkentése.

**A felderítő eszközök és azok hordozói, valamint az információgyűjtő és felderítő központok megsemmisítésének, elfoglalásának, megrongálásának** alapját az eszközök felderítése és alkalmazási helyük meghatározása képezi. A felderítő eszközök és azok hordozóinak helymeghatározása – mivel ezek elsősorban passzív eszközöket (vevőberendezéseket) tartalmaznak – csak komplex felderítési tevékenység eredményeképpen lehetséges. A felderítő központokban üzemelhetnek aktív kisugárzással működő eszközök is, amelyek speciális felderítő eszközökkel érzékelhetők és ezek alapján a helymeghatározás végrehajtható. Ennek ismeretében lehetővé válik az objektumok megsemmisítése, illetve speciális erőkkel való elfoglalása. E tevékenység kimondottan háborús konfliktus során alkalmazható.

**A felderítő berendezések és az adatokat továbbító kommunikációs eszközök elektronikai zavarása** szintén a háborús helyzetekben alkalmazható tevékenységi forma. A felderítő rádiólokátorokkal, rádió- és rádiótechnikai felderítő vevőkkel, felderítést irányító, adattovábbító rendszerek, infravörös- és hidroakusztikai felderítő berendezések vevőivel szemben az elektronikai zavarás alkalmazható.

Az aktív rádiólokációs, elektrooptikai felderítő rendszerek folyamatos vagy válaszimpulzus zavarokkal, a passzív felderítő eszközök általában célzott, vagy szélessávú zavarokkal foghatók le. Meg kell azonban jegyezni, hogy pl. egy passzív rádiófelderítő vevő megzavarása a visszájára is fordulhat, hiszen a vevő ebben az esetben képes detektálni a zavarjelet, ezáltal a kezelők konstatálhatják a zavarás tényét. Egy ilyen helyzetben a zavarjel kisugárzásának iránya illetve helye meghatározható, ami a zavaró eszköz megsemmisítésének alapja lehet.

**Az elektromágneses kisugárzás korlátozása** (Emission Control – EMCON), mint végső megoldás alkalmazása az eszközök rendeltetésszerű működését korlátozza. A korlátozás történhet időben, frekvenciában, teljesítményben esetleg üzemmódban stb. Leginkább az időbeni korlátozást alkalmazzák, ami azt jelenti, hogy az adóberendezéseket csak a feladat végrehajtásához szükséges időtartamig szabad bekapcsolni, mivel a túl hosszú kisugárzási idő alatt a másik fél könnyebben felderítheti, analizálhatja rendszereinket és megkeresheti azokat a kisugárzásokat, amelyekből használható információt nyerhet.

**Az elektronikai álcázás** az elektronikai objektumok (eszközök), és a csapatok tevékenységének lényeges, csak rájuk jellemző „áruló" tulajdonságaik kiküszöbölésével, meghamisításával, illetve a másik fél számára hozzáférhetetlenné tételével érhető el. Az elektronikai álcázás magába foglalja:

- az elektronikai rejtést és
- az elektronikai megtévesztést.

Az **elektronikai megtévesztés** az elektronikai támadás egyik fajtája, amely a felderítő rendszerek félrevezetésével, hamis információk továbbításával az elektronikai védelem érdekében is végrehajtásra kerülhet.

Az **elektronikai rejtés** aktív és passzív tevékenységek és rendszabályok összességét jelenti. Az aktív elektronikai rejtő tevékenységek közé a következők tartoznak:

- rádiózavarás;
- rádiólokációs zavarás;
- infra zavarás.

A felsorolt aktív rejtő tevékenységek álcázó zavarokkal elfedik a védendő elektronikai kisugárzásainkat, így azokat a másik fél felderítő rendszerei a zavarok miatt nem képesek felfedni.

A passzív elektronikai rejtő tevékenységek közé az alábbiak sorolhatók:

- az elektronikai eszközök áruló jeleinek megszüntetése;
- a rádiólokátorok passzív zavarása (szögvisszaverőkkel, tükrökkel, dipólusokkal, lencsékkel);
- elektro-optikai felderítés elleni álcázás (füstökkel, ködökkel, festékkel és egyéb anyagokkal);
- akusztikai álcázás (zajcsökkentő megoldásokkal);
- elektromágneses kisugárzások árnyékolása (árnyékoló eszközök alkalmazásával).

**A felderítés hatékonyságának technikai eszközökkel való csökkentése** többek között az új modulációs eljárásokat, korszerű adásmódokat (pl. szórt spektrumú adásmódok), teljesítménnyel való manőverezést, információtömörítési eljárásokat, irányított kisugárzások alkalmazását stb. jelenti.

### A rádió-, rádiótechnikai és a rádiólokációs felderítés elleni védelem módszerei [28]

A **rádiólokációs felderítés elleni rejtés** megnehezíti, hogy a másik fél radarjai a felderítendő objektum helyéről, mozgási irányáról, kiterjedéséről stb. értékelhető információkat szerezzenek. A rádiólokációs felderítés hatékonysága attól függ, hogy az objektumoknak vagy technikai eszközöknek milyen az elektromágneses hullámokat visszaverő képessége a környezethez viszonyítva. Ez függ az objektum anyagától, formájától, méretétől.

A tárgyak terepen való rádiólokációs felderítésének elve azon alapul, hogy a háttér és az objektum közötti kontraszt pontosan kirajzolódik a radar vevőkészülékének indikátorán. Az objektum rejtése érdekében ezt a kontrasztot kell csökkenteni úgy, hogy az ne emelkedjen ki a környezetéből. Speciális eszközökkel hamis célok is megjeleníthetők, vagy elektronikai zavarokkal lefoghatók a másik fél felderítő rádiólokátor berendezései.

Rádiólokációs felderítés elleni rejtés megvalósítható:

- a terep és tereptárgyak árnyékoló tulajdonságának kihasználásával;
- a rádióhullámokat elnyelő bevonatok alkalmazásával;
- aktív rádiózavarokkal;
- objektumok szögvisszaverőkkel való imitálásával.

Az álcázó anyagok hatékonysága nagymértékben függ nedvességtartalmuktól. Jelenleg a rádióhullámok visszaverődésének csökkentésére elnyelő anyagokat alkalmaznak. Az elnyelő réteg csökkenti az elektromágneses hullámok visszaverődését, és a beérkező elektromágneses energiát hővé alakítja át. Sokrétegű elnyelő anyag felhasználásával nő az elnyelés frekvenciasávja.

Természetesen épületeket is lehet rejteni a rádiólokációs felderítés ellen. A falakat több rétegben beton és grafit keverékével vonják be. Az ilyen bevonat elnyeli (abszorbeálja) a hullámokat az üregeiben.

A **rádió- és rádiótechnikai felderítés elleni tevékenység** főbb módszerei a következők:

- minimális kisugárzás, amely elérhető:
    - csak a szükséges kisugárzás biztosításával (teljesítmény, idő);
    - a kisugárzás előtt az üzenet megtervezésével (felesleges kisugárzási idő csökkentése);
    - kisugárzás gyors és pontos végrehajtásával (érthető beszéd, megfelelő modulációs mód, helyes rádióforgalom);
    - olyan eszköz alkalmazásával, amely képes az adatok szétdarabolt továbbítására;
    - a lehetőségek függvényében alternatív eszközök alkalmazásával (kábel, futár).
- a felderítéstől védett adások alkalmazása, amely elérhető:
    - alacsony teljesítmény alkalmazásával;
    - irányított antennák alkalmazásával (a kimenő teljesítménynek megfelelő nagyságú és iránykarakterisztikájú antenna);

- a felderítéstől védett hely kiválasztásával, amely árnyékolja az adó jelét;
- mobil antennák alkalmazásával (gyors áttelepíthetőségi lehetőség);
- megtévesztő antennák alkalmazásával (a vizuális felderítés megtévesztése érdekében);
- titkosítással, rejtjelzéssel;

- a helyes kezelői fogások begyakorlása, amelyekbe beletartozik:
  - a kezelői sajátosságok csökkentésének begyakorlása (frekvencia, hívónév változtatásával);
  - a rendszertelen rádióforgalom alkalmazása (rendszertelen jelentési idők bevezetése, rendszeres jelentések más kommunikációs eszközön történő továbbítása);
  - azonosítás (hitelesítés) nem titkosított eszköz alkalmazásakor (azonosítás kérése, azonosító jellemzők rendszertelen megváltoztatása);
  - kommunikációs biztonsági eszközök alkalmazása;
  - rövidítések, kulcsszavak alkalmazása.

### Kis valószínűséggel felderíthető adásmódok alkalmazása [28]

A rádiófrekvenciás tartományban a rádió-, rádiótechnikai és a rádiólokációs felderítés elleni védelem egyik igen hatásos technikai megoldása a különböző kis valószínűséggel felderíthető eszközök (Low Probability of Interception – LPI) alkalmazása.

A kis valószínűséggel felderíthető adásmódok alkalmazása igen nehéz helyzetbe hozzák a rádiófelderítés és zavarás szervezőit és végrehajtóit. A korábbi hagyományos eszközökkel és módszerekkel az adások nem deríthetők fel, nem hallgathatók le, nem mérhető meg a földrajzi elhelyezkedésük és zavarásuk igen komoly nehézségekbe ütközik.

A **szórt spektrumú átviteli rendszerek** alaptulajdonsága, hogy azonos alapsávi forgalom esetén a bennük alkalmazott speciális csatornakódolási (modulációs) eljárások következtében a csatornákban felhasznált teljes sávszélesség esetleg nagyságrendekkel nagyobb, mint a hagyományos modulációs rendszerekkel létrehozott jelek sávszélessége. A szórt spektrumú átvi-

teli rendszerek másik fontos tulajdonsága az álvéletlen (Pseudo Random) jelleg, ami annyit jelent, hogy az átviteli csatornákon folyó kommunikáció egy rendszeren kívüli megfigyelő számára nagy sávszélességű, zaj jellegű véletlen jelnek tűnik, a rendszeren belüli partnerek viszont – ismerve a csatornakódolás szabályait – dekódolni tudják a jeleket és kinyerik az információt.

A szórt spektrumú jel:

- nagy sávszélességű;
- nehezen deríthető fel;
- nehezen fejthető meg és
- egyes esetekben automatikusan védelmet nyújt a fading hatások ellen.

A szórt spektrumú kommunikációs rendszereket a rövidhullámú sávtól egészen a mikrohullámú tartományokig a vezeték nélküli átvitelre használják, de előfordulnak vezetékes alkalmazások is (pl. energiahálózati adatátvitel). A pont-pont közötti összeköttetéseken kívül elterjedőben vannak a kommunikációs szórt spektrumú hálók, emellett a csomagkommunikációs rendszerekben és a digitális celluláris mobil telefonrendszerekben történő alkalmazások.

A csomagkommunikációs rendszerekben a szórt spektrumú hírközlés többféle előnyös tulajdonsága használható ki:

- csomagbefogadási képesség (Capture) növelése, amely azt jelenti, hogy egy vevő különböző adóktól érkező, hozzá címzett, ütköző csomagok közül képes hibátlanul venni legalább egy csomagot;
- kódosztásos többszörös hozzáférés (Code Division Multiple Access – CDMA) lehetősége, vagyis különböző szórt spektrumú kódokkal rendelkező információk ütközése során még akkor is hibátlanul vehető legyen az ütközésben résztvevő információk közül a vevő kódjával megegyező, ha azok teljes szinkronban vannak, s azonos vételi szinttel rendelkeznek;

- több utas terjedésből származó interferencia elleni védelem, amelyek a kommunikációs csatorna erős terjedési veszteségei (elnyelődés), valamint a több utas hullámterjedés okozta diszperziós és fading problémák miatt alakulnak ki;
- külső zavarjelek elnyomásának képessége, amely a szándékos zavarok elleni védelem növekedését, illetve az ipari zajos környezetben a zavarelnyomás-képesség kihasználását is jelenti;
- kis teljesítménnyel történő adás, illetve alacsony teljesítménysűrűségű alkalmazás esetén, például a vezeték nélküli helyi hálózatok szórt spektrumú megvalósításánál lehetővé válik, hogy a hálózat szűk területén kívülre lényegében ne sugározzon teljesítményt, így minimalizáljuk a jel detektálhatóságát a rendszeren kívüli személy számára.

A szórt spektrumú modulációnak elméletileg a következő változatai lehetnek:

- közvetlen zajmodulációs eljárás (Direct Sequence – DS);
- frekvenciaugratásos eljárás (Frequency Hopping – FH);
- impulzus frekvenciamoduláció vagy chirp eljárás (Pulse Frequency Modulation – PFM);
- időugratásos eljárás (Time Hopping – TH);
- hibrid rendszerek.

Mivel az elméletileg lehetséges megoldások közül alapvetően a közvetlen zajmodulációt és a frekvenciaugratásos eljárást alkalmazzák, ezért a továbbiakban részletesebben ezeket a módszereket mutatjuk be.

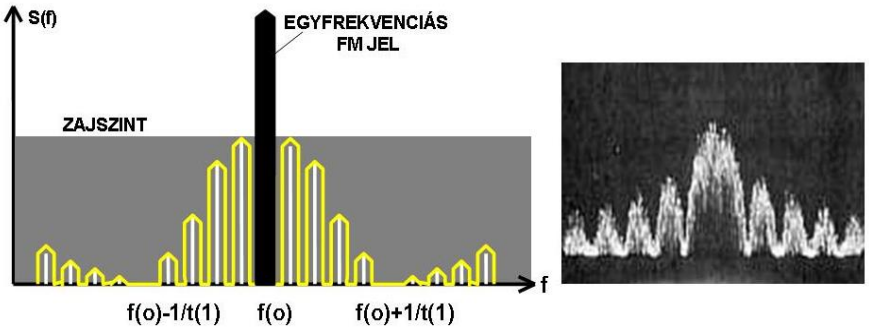
A szórt spektrumú modulációhoz a megfelelő jelet úgy állíthatjuk elő, hogy az információt hordozó jelet megszorozzuk a spektrumot kiterjesztő álvéletlen jelsorozattal, amelyre két lehetőség van:

- az információs jelet ténylegesen megszorozzuk egy (gyors) álvéletlen jelsorozattal;
- a vivőfrekvenciát véletlenszerűen (álvéletlenszerűen) széles tartományban változtatjuk.

Az előbbit közvetlen zajmodulációs eljárásnak, az utóbbit frekvenciaugratásos rendszernek nevezik.

**A közvetlen zajmodulációs jelet előállító adóberendezés** kettős modulációval dolgozik:

- az első a szokásos módon keskenysávú moduláció, a moduláló jel lehet analóg vagy digitális jellegű;
- a második moduláció a teljesítményerősítő előtt történik, ahol a vezéroszcillátor jelét (mint vivőt) a fázismodulátorban digitális zajjal billentyűzik, majd erősítés után ez kerül kisugárzásra (4. ábra).




4. ábra. Közvetlen zajmodulációs rendszer spektrumképe

A **kódolás** folyamán az adó oldalon, ha az üzenet bit értéke egy, akkor a kiterjesztett jelekben egy álvéletlen, vagy kvázizaj (Pseudo Noise – PN) kódsorozat kerül a helyébe, ha a bit értéke nulla, akkor a kódsorozat chirp-jei invertálva kerülnek a kimenetre. Ennek eredményeként a hasznos jel nem emelkedik ki a zajból, így felfedése csak speciális berendezésekkel lehetséges.

A **dekódolásnál** a vevő oldalon a kívánt jel visszaállításakor a kiterjesztett jelet megszorozzuk az álvéletlen (PN) kóddal és a keresett jel visszakerül az eredeti alacsony sebességű, kis sávszélességű állapotba. A vevőben a helyi oszcillátor jelét (melynek frekvenciája a középfrekvenciával tér el a vételi csatornáétól) digitális zajjal billentyűzik, így a keverő után már a szokásos középfrekvenciás jel áll rendelkezésre.

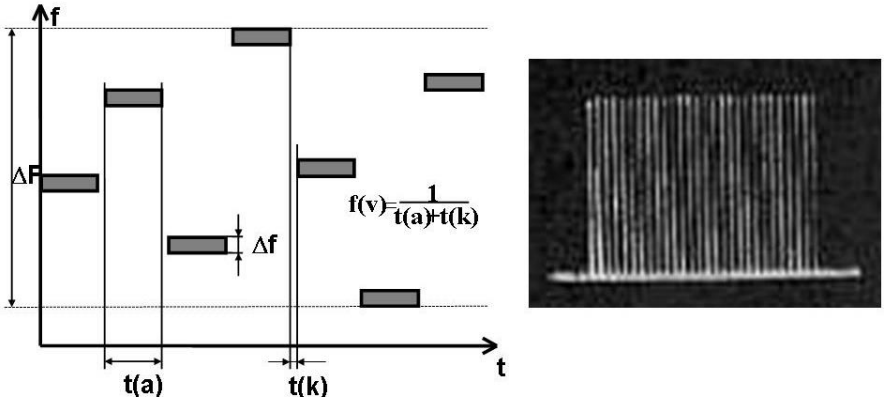
A legsúlyosabb problémát a vevőoldali kódgenerátor szinkronizálása jelenti az adó oldalihoz képest.

A szinkronizálásra alapvetően három eljárást dolgoztak ki:

- az információval együtt a frekvenciakód kisugárzása;
- frekvencia- és fázisszinkronizáció egy harmadik jel, például etalon frekvenciájú állomások segítségével;
- a szórt spektrumú jel egyedi kiértékelésével történő szinkronizáció.

A **frekvenciaugratásos adókban** a vivőfrekvencia pillanatnyi értékét változtatjuk úgy, hogy egy frekvenciakészleten belül az egyes diszkrét frekvenciák felhasználási sorrendjét egy álvéletlen generátorral programozzuk. Már ismertek olyan rendszerek, amelyek a frekvencián tartózkodás idejét is folyamatosan változtatják, ezzel tovább növelve a felderíthetőség és zavarás elleni védettségüket.

A frekvenciaváltás sebességét (f(v)) a frekvencián tartózkodás ideje (t(a)) és az átkapcsoláshoz szükséges idő (t(k)) határozza meg, ami a korszerű nagyfrekvenciás kapcsolóelemeknek köszönhetően csupán néhány ms (5. ábra).




5. ábra. A frekvenciaugratásos rendszer frekvencia kiosztása és spektrumképe

A fokozottan zavarvédett rádiók fejlesztési programjaiban általában előírták a frekvenciaváltások sebességét is. Ez a korábbi kutatások eredményeként három csoportba sorolható:

- lassú frekvenciaugratásos rendszer (Slow Frequency Hopping – SFH), mp-ként néhányszor tíz frekvenciaváltás;
- közepes sebességű frekvenciaugratásos rendszer, mp-ként néhány száz frekvenciaváltás;
- gyors frekvenciaugratásos rendszer (Fast Frequency Hopping – FFH), mp-ként több ezer frekvenciaváltás.

A lehallgatás és zavarás ellen a minél gyorsabb frekvenciaátkapcsolás jelentené a nagyobb védelmet, viszont a sebességgel együtt nő, (mégpedig nemlineárisan) a berendezések bonyolultsága, ára, romlik az összeköttetések stabilitása és növekednek az elektromágneses kompatibilitási problémák.

A frekvenciaugratásos rádiózás tulajdonképpen a szinkronizálási nehézségek miatt alakulhatott ki ilyen „későn”, mert a nagysebességű, adó és vevőoldali szinkron frekvenciaváltásoknak nem voltak meg a technikai feltételei. A szinkronizálás egyik korai módszere volt, hogy kisugározták az új frekvencia kódját is. A hasznos információt digitalizálták, majd nagyobb sebességgel továbbítva, a szabaddá váló időben továbbították az új frekvencia kódját. Ez a módszer a rádiórendszereket fokozottan érzékennyé tette a zavarással szemben. Elég volt csupán a kód átjutását megakadályozni, az összeköttetés máris szétesett.

A másik, az úgynevezett etalonidőhöz szinkronizálás módszernél az adott időpillanathoz tartozó frekvenciát előre tudják a berendezések, (valamilyen módon eljuttatták egymáshoz), de még nem biztos, hogy az óráik ugyanolyan nagy pontossággal, és főleg szinkronban járnak.

A helyhez kötött, vagy mozgásuk közben a nagy, globális hálózatok elérésére alkalmas rendszereknél alkalmazható eljárás lényege, hogy a rádiórendszerben résztvevők mindegyike hozzájut az igen nagy pontosságú atomórákkal szinkronizált központi időalaphoz és ezután

már csak a kódgenerátorukat kell ezzel szinkronban üzemeltetni, amelyben a frekvenciakód általában 24 órára előre megtalálható. A navigációs műholdak alkalmazásának széleskörűvé válásával az etalonidőhöz jutás mind több felhasználó számára lehetővé válik. Ez azonban azt is feltételezi, hogy az állomás rendelkezik egy műholdvevő készülékkel is.

A kis valószínűséggel felderíthető adásmódok a leírtak alapján igen nehezen felderíthetők. A korszerű digitális felderítő vevők (pl. digitális szűrőbank vevők, Bragg cellás vevők) is csak a vett jel detektálására, esetleg a kisugárzás irányának meghatározására alkalmasak.

### Kompromittáló elektromágneses kisugárzás elleni védelem [28]

Az elektronikus berendezések kompromittáló kisugárzásának lehallgatása napjaink egyik fontos problémája. A hardver elemek elleni felderítésnek ezt a módját TEMPEST[59] támadásnak szokták nevezni.

A kompromittáló kisugárzás elleni védelem olyan intézkedések és eszközök alkalmazását jelenti, amelyek célja az áthaladó információ illetéktelen megjelenítésének és az elektromos berendezések kompromittáló kisugárzása analizálásának megakadályozása. Az átviteli utak és végberendezések által keltett kisugárzások illetéktelen detektálása és rögzítése azért veszélyes, mert nem érzékelhető az információk kompromittálódása vagy olyan rendszerinformációk megszerzése, amely további támadásokhoz szolgálhat támpontként. A védelmi rendszabályok irányulhatnak eszközökre és működési környezetre.

Működése során minden elektronikus eszköz létrehoz olyan elektromágneses erőteret, amelynek érzékelésével a működésre vagy a kezelt (továbbított) adatokra vonatkozó információk szerezhetők be, akár illetéktelen személyek által is. [29]

Az információkhoz való illetéktélen hozzáférés egy különleges módja a Van Eck–Phreaking[60], ami szintén ezt a jelenséget használja ki. Az elektromágneses eszközök, pl. a számítógép képernyője, kábelei, hardver elemei bizonyos mennyiségű és intenzitású elektro-

[59] Transient ElectroMagnetic Pulse Emanations Standard
[60] Wim Van Eck holland kutatóról elnevezett lehallgatási technika

mágneses sugárzásai megfelelően érzékeny vevőkkel detektálhatók, értékelhetők és belőlük az információk helyreállíthatók. Van Eck a katódsugárcsöves (CRT[61]) monitorokat vizsgálta. Az ilyen monitorok képét a képernyő belső felületére felvitt foszfor felvillanásai adják, amelyeket egy elektronsugár gerjeszt. Az elektronsugár, amelyet elektromágneses tekercsek térítenek el a megfelelő irányba, másodpercenként néhány tucatszor végigpásztázza a képernyőt. A tekercseket vezérlő nagyfeszültségű jel – amely a képernyőn megjelenő összes információt tartalmazza – a tévéadáshoz hasonló elektromos kisugárzást gerjeszt. A jelet nagyfrekvenciás antennákkal fogva és szinkronizálva akár nagy távolságról is kiolvasható belőle az eredeti kép.

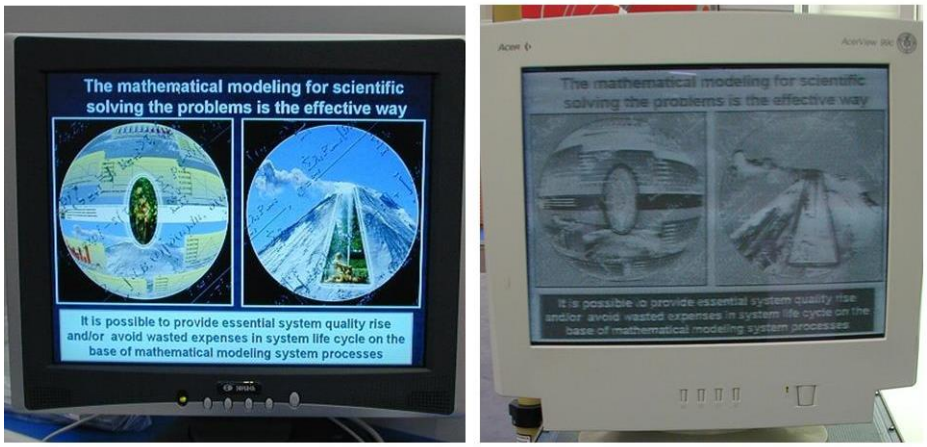
Később kifejlesztettek hasonló elven működő lehallgatási módszereket LCD[62] képernyőkre is. Mind a CRT, mind az LCD monitorokat lehallgató eszközök viszonylag olcsó, könnyen beszerezhető alkatrészekből összeállíthatók. [30] Egy ilyen lehallgatási tesztet mutat a 6. kép, amelyen egy 25 m távolságban elhelyezett lehallgató eszköz monitorán tisztán olvasható az eredeti Power Point prezentáció szövege, és a képi információ is felismerhető.

A kompromittáló kisugárzások lehallgatásának megakadályozás érdekében az eszközöket olyan aktív és passzív védelmi elemekkel kell kiegészíteni, amelyek ezeket a nem szándékosan kisugárzott jeleket árnyékolják, vagy más módon semlegesítik. Védendő eszközök alatt nemcsak a végberendezéseket kell érteni, hanem ide kell sorolni az összes olyan eszközt (kapcsolók, szerverek stb.), amelyek az összetett átviteli út során biztosítják az adatok továbbítását. [29]

A helyiségek kompromittáló kisugárzás elleni védelmének lényeges területe a helyiségekből kivezető csövek (víz, gáz, fűtés) megfelelő szigetelése – beleértve a hanghullámok továterjedésének vizsgálatát és megakadályozását is –, a vezetékek (erős- és gyengeáramú kábelek) szűrése és a megfelelő földelési rendszer kialakítása. Azokat a helységeket, ahol nagy mennyiségű elektronikai- és számítástechnikai eszköz van elhelyezve egy, ún. Faraday-

[61] Cathode Ray Tube – Katódsugárcsöves monitor
[62] Liquid Crystal Display – Folyadékkristályos monitor

hálóval, azaz a helység mind a hat falába beépített földelt fémhálóval szokták védeni. Elektromágneses kisugárzás ellen védeni kell a helyi hálózatokat is. Ehhez árnyékolt kábeleket célszerű használni. Előfordulhat, hogy az elektronikus eszközökből a táphálózatra jutnak ki jelek, amelyek a tápáramra szuperponálódnak. Ezeket megfelelő eszközökkel a támadó távolabbról is kiszűrheti, ezért az elektromos hálózat szűrésére, leválasztására is szükség van.




6. ábra. Monitor kisugárzás lehallgatása [31]

Az infokommunikációs rendszerek védelménél az árnyékolástechnika alkalmazható:

- teljes szobaárnyékolásnál, amely védelmet nyújt az elektronikus lehallgatás és a kívülről jövő elektromágneses zavarok ellen is;
- infokommunikációs hálózatok védelménél speciális szűrőkkel, zavarvédett kábelekkel és kábelkötegekkel az elektronikus lehallgatás és a külső zavarokkal szemben;
- biztonsági kábelek kettős árnyékolásánál, amely kis- és nagyfrekvenciás zavarokkal szemben is védelmet nyújt;
- biztonsági táskáknál mágneses adattárolóknál, ahol a mechanikai sérülés és elektroszmog ellen is biztonságos védelmet nyújt;

- elektronikai berendezéseknél, hálózatok utólagos szigetelésénél, zavarvédelem kialakításánál nagyfrekvenciás tömítőanyagok és szigetelőanyagok felhasználásával;
- zavarvédett műszerdobozok nagyérzékenységű, illetve kiemelt fontosságú elektronikák (biztonsági- és életmentő berendezések, fedélzeti computer) zavarvédelménél.

Nagyfrekvenciás árnyékolási célokra célszerű fémezett szöveteket alkalmazni. Az elektronikából ismert, hogy a nagyfrekvenciájú áramok túlnyomó részben a vezető felületén, illetve egy vékony felületi rétegben haladnak[63]. Ahhoz, hogy ezt kiküszöbölhessük, minél nagyobb effektív vezetőfelülettel rendelkező árnyékoló anyagokat használunk. A fémszövetek effektív felülete többszöröse egy vele azonos méretű fémlemeznek, így a nagyfrekvenciás árnyékoló hatása is nagyobb. A fémezett szövetek kialakítása során a poliamid hordozószövetet vékony rétegben rézzel vagy ezüsttel vonják be, majd az így vezetővé tett szövetre hagyományos galváneljárással tetszőleges fémréteg (réz, ezüst, nikkel, arany stb.) vihető fel.

A fémezett szövetek előnyei:

- a mechanikai igénybevételt jól bírják, nagy a kopásállóságuk, nehezen szakadnak;
- a felületi vezetésben részt vevő nagy mennyiségű fémezett szál rendkívüli nagyfrekvenciás árnyékoló hatást biztosít;
- a fémezett szövet könnyű, rugalmas, légáteresztő, korrózióálló;
- mind a hordozószövet struktúrája, mind a felvitt fémréteg összetétele (Cu, Ag, Au, Ni, Sn) és vastagsága tág határok között variálható;
- a fémezett szövetek alkalmazásával kialakíthatóak olyan gépjármű felépítmények, katonai sátrak, álcahálók, amelyek a rádiófrekvenciás tartományban árnyékoló hatásuk következtében tökéletes rejtettséget, elektronikai védelmet biztosítanak az elektronikai felderítéssel szemben. A fent említett árnyékolástechnikai megoldás lehetőséget nyújt a különböző termek, konténerek, adatátviteli vonalak utólagos árnyékolására. [32]

[63] Skin-effektus, Maxwell 1873

### 4.4.4. Elektronikai támadás elleni védelem

Az elektronikai támadás elleni védelem jelentősen kötődik az elektronikai felderítés elleni védelem módszereihez, rendszabályaihoz és eszközeihez. Amennyiben az elektronikai felderítés ellen hatékonyan tudunk védekezni, akkor jelentős lépést teszünk az elektronikai támadás elleni védelem irányába is. Megfelelő információk (pl. frekvencia, üzemmód, elhelyezkedés stb.) hiányában ugyanis a támadó nem képes célirányos, hatékony, az adott infokommunikációs rendszernek megfelelő elektronikai támadást (pl. elektronikai zavarást) megvalósítani. Ezért az előzőekben ismertetett elektronikai felderítés különböző módszerei elleni védelmi megoldások többnyire eredményesen alkalmazhatók a támadás kivédésére is, így az elektronikai támadás elleni védelmet az elektronikai felderítéssel összhangban kell megvalósítani.

Az elektronikai eszközök elektronikai támadással (zavarással, megtévesztéssel, pusztítással) szembeni védelemnek, ha nem is elektronikai, de mindenképpen a leghatásosabb módszere a támadó eszközök, zavarforrások (zavaró állomások) megsemmisítése, rongálása. Ehhez pontos információk szükségesek pl. a zavaró eszköz elhelyezkedésére vonatkozóan. Ezen információk birtokában a zavaró eszközök különböző módon pusztíthatók vagy rövidebb, hosszabb időre működésképtelenné tehetők. Természetesen ez a fajta ún. megelőző védelmi tevékenység kizárólag egy háborús konfliktus időszakában alkalmazható.

Természetesen ezeken kívül számos más megoldás is létezik az elektronikai támadások elhárítására. A továbbiakban röviden áttekintjük az elektronikai pusztítás és az elektronikai zavarás elleni védelem elektronikai módszereit és eszközeit.

#### Elektronikai pusztítás elleni védelem [33]

Az elektromágneses impulzusok elleni védelem alapvető problémája, hogy nem ismert az elektromágneses impulzus nagysága a védett eszköznél. Így nehéz megállapítani, hogy milyen nagyságú elektromágneses impulzust kell lecsökkenteni olyan mértékre, amelyet még károsodás nélkül elviselnek az érzékeny elektronikai eszközök. A szükséges érték ismeretében

ben lehetőség lenne meghatározni azt az optimálisan szükséges védelmi módszert és eszközt, így nem kellene minden esetben a maximális védelmi értéket biztosító eljárást vagy eszközt alkalmazni.

Két alapvető módszer létezik az elektromágneses impulzusok elleni védelemre. Az egyik, hogy olyan elektronikai áramköröket építenek az eszközökbe, amelyek ellenállnak az elektromágneses impulzus hatásainak, a másik pedig, hogy árnyékolással megakadályozzák, hogy az elektromágneses impulzus bejusson a védett térbe. Természetesen az a legjobb, ha mindkét módszert egyszerre alkalmazzuk, mivel ez adja a legnagyobb védelmet.

Az elektromágneses impulzusok elleni védelem eszközeinek széles választéka létezik. Ezek a teljesség igénye nélkül az alábbiak lehetnek:

- szikraközös villámhárító eszközök;
- hálózati szűrők;
- fémoxid varistorok;
- elektrooptikai eszközök;
- nagy sebességű zener diódák;
- árnyékoló és elnyelő anyagok.

A **szikraközök** alaptípusának felépítése és működése egyszerű. Két elektróda között szigetelőrétegként levegő helyezkedik el. Alaphelyzetben az elektródák között a szigetelőréteg miatt nem folyhat áram, ezért ez az állapot a kapcsoló nyitott helyzetének felel meg. Ha az elektródák közötti feszültséget emeljük, akkor elérjük azt a feszültséget, amelyen bekövetkezik az átütés, és elektromos ív alakul ki. Az ív nagyon kis ellenállású elektromos összekötésnek tekinthető, ezért ez az állapot a kapcsoló zárt helyzetének felel meg. Az átütési feszültséget az elektródák távolsága határozza meg: úgy állítják be, hogy az átütés hamarabb következzen be a szikraközben, mint a védett fogyasztóban. [34]

A **hálózati szűrők** alkalmazásával kiszűrhetők az adathálózaton terjedő zajok, zavarok és túlfeszültségek, amelyek a tápegységek, adatátviteli eszközök korai meghibásodásához vezet-

hetnek. A legegyszerűbb hálózati kiegyenlítő egy nagy lágyacél transzformátor és egy pár kondenzátor, így nincs lehetősége a túláram átjutásának egyik oldalon sem. Bonyolultabb felépítésű a Zero hálózati kiegyenlítő, amelyben passzív elemek hálózatával mérsékelik az áramlökést, majd elvezetik a semleges vonalra, amely szabvány szerint a földre van kötve. Ezek az egységek a földbe vezetik az áramlökést a számítógépnél, amikor az keresztülmegy a soros portokon, hálózati csatlakozókon stb. [35]

Az adatátviteli vonalakon a túlfeszültség elleni védelemre sikeresen alkalmazható dióda, varisztor, gázlevezető is, amiket érdemes kombinálni. A dióda az egyenfeszültséget nem engedi át a berendezés felé, míg a gázlevezető túlfeszültség esetén hirtelen leföldeli a rendszert.

**Elektrooptikai eszközök** alkalmazásával megoldható az adatátviteli kábelek védelme. Elektrooptikai eszközök (pl. optikai kábelek) széleskörűen alkalmazhatók:

- az adat és kommunikációs csatornáknál;
- az energiafigyelő és irányító rendszereknél;
- az ellenőrző irányító rendszereknél;
- az őrzésvédelmi rendszereknél;
- egyéb biztonsági rendszereknél.

A **nagy sebességű zener diódák** működése azon alapszik, hogy belső ellenállását igen gyorsan megváltoztatja (rövidre zár) ha a rákötött feszültség hirtelen megnövekszik, illetve átlépi a meghatározott küszöbszintet. A korszerű zener diódáknál a folyamat sebessége a $10^{-9}$ másodperc, az elméleti határ pedig $10^{-12}$ másodpercet is elérheti. Eltérően a varistoroktól a zener dióda jellemzői többszöri túlterhelés hatására sem változnak.

**Az elektromágneses hullámok elleni árnyékolással** ideális védelem biztosítható az elektromágneses impulzusok ellen. Az elektromágneses hullámok elleni árnyékolás módszerei lehetnek:

- abszorbeáló (elnyelő) árnyékolás és
- reflektáló (visszaverő) árnyékolás.

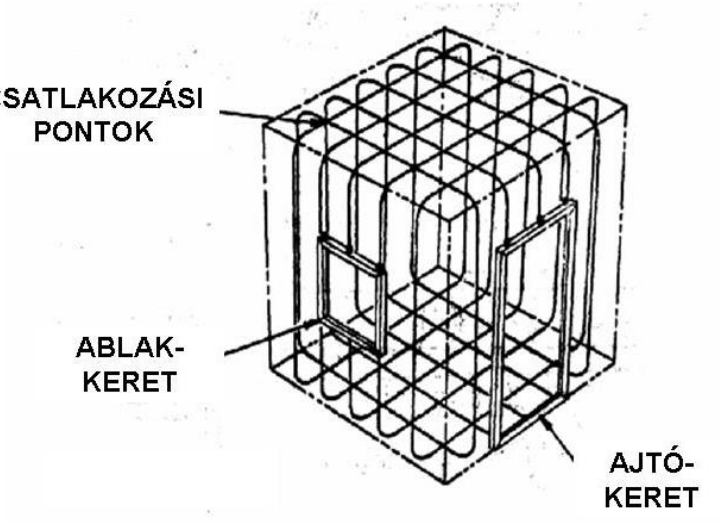
Az abszorbeáló árnyékolási módszernél rádiófrekvenciás energiát elnyelő anyagokat alkalmaznak, ahol az energia elnyelés nagyságától és a frekvenciasávtól függően a vastagság a 60 cm-t is elérheti. Az árnyékolt területen átlátszó, üvegezett felületek nem megengedhetők. Ezt az árnyékolási módszert általában laboratóriumoknál alkalmazzák.

A reflektáló árnyékolási módszernél a védendő teret rádiófrekvenciásan reflektáló anyagokkal vonják be oly módon, hogy a bevonat folyamatos legyen. Az árnyékolás elválasztja a külső teret a védendő belső tértől, a jel a reflektáló rétegen csak erősen csillapítva (50-120 dB) juthat át.

Nagy előnye ennek az eljárásnak, hogy lényegesen olcsóbb, mint az abszorbeáló módszer, sokkal kevesebb a helyigénye, és fényáteresztő üveg felületek is megengedhetők. A reflektáló módszer előnyös tulajdonságai miatt szinte kivétel nélkül ezt a megoldást alkalmazzák a rádiófrekvenciás árnyékolásban.

A számítógéptermek, műszerszobák, fontos elektronikai eszközökkel felszerelt helyiségek védelme esetén a teljes védendő tér körül Faraday-kalitkát kell kialakítani. Ez egy fémből, vagy fémhálóból készült doboz, amelybe belehelyezve az adott elektronikai eszközt, az védve van a külső elektromágneses tér elől. [36] A 7. ábrán egy egyszerű Faraday kalitka felépítése látható, ahol különböző nyílások is megengedhetők.

Faraday kalitka alkalmazásakor a teret határoló teljes falfelületet vezetőanyaggal kell borítani, a vezetőképesség nem szakadhat meg a felületek találkozásánál, sőt a nyílászáróknál sem. A védett térbe belépő vezetéket (erősáram, telefon, beléptető rendszer, biztonságtechnikai és tűzvédelem, számítógépes hálózat stb.) megfelelő szűréssel kell ellátni. Külön gondot kell fordítani a védet térbe vezető klíma- és szellőzőrendszer kialakítására, a megfelelő potenciálra hozására, ellenkező esetben ezek mint szekunder antennák és csatolók továbbítják a sugárzott jelet. Az ekvipotenciális felületek minél ritkábban szakítandók meg ablakokkal és ajtókkal, mivel ezek árnyékolása lényegesen költségesebb, és potenciális hibaforrást is jelenthetnek.




7. ábra. Faraday kalitka [28]

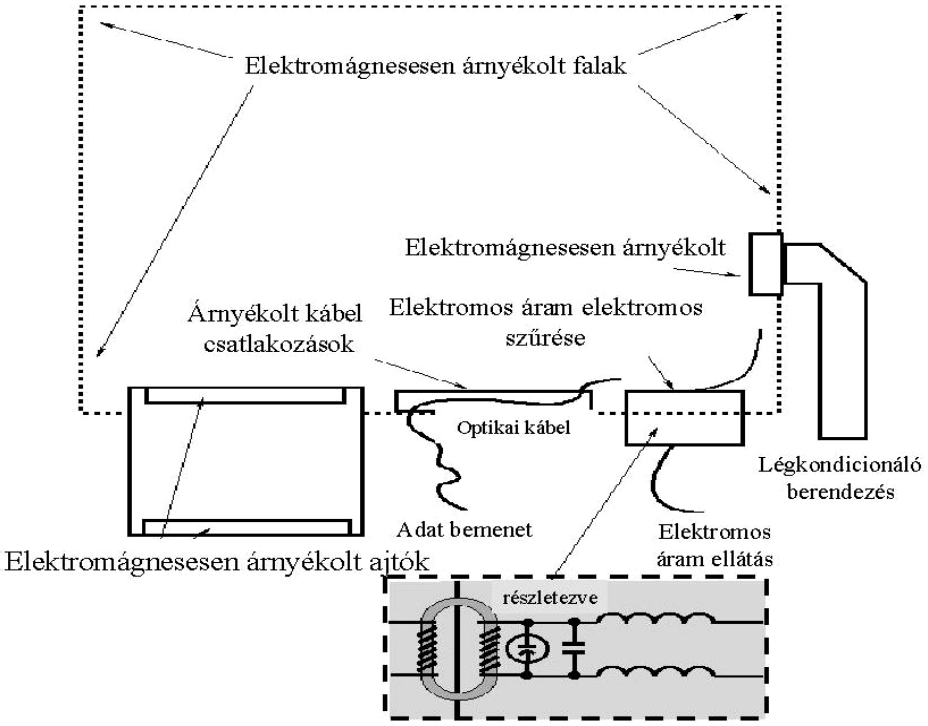
Az elektromágneses hullámok a védett térbe bejuthatnak vezetéken haladva (induktív-, vagy kapacitív csatolással) vagy elektromágneses sugárzással, ezért az árnyékolásnak, mint a vezetett, mint a sugárzott zavarás ellen megfelelő védelmet kell biztosítania.

Az elektromágneses árnyékolás a megvalósítást tekintve lehet pontszerű vagy területi. Pontszerű árnyékolás esetén az árnyékolást egy szűk területre, pl. egy alkatrészre korlátozódik, területi árnyékolás pedig egy bizonyos területen elhelyezett összes elektronikai berendezés árnyékolását biztosítja.

Az árnyékolások kivitelezésére és azok tesztelésére számos szabvány létezik, amelyek betartásával megfelelő védelem biztosítható az elektromágneses impulzus bombák és nagy energiájú rádiófrekvenciás sugárforrások ellen. A 8. ábrán példaként egy számítógépes szoba elektromágneses árnyékolása látható.

Az elektromágneses árnyékolás kialakításának lehetséges módszerei a következők:

- rendszer árnyékolás;
- alrendszer árnyékolás;
- eszköz, alkatrész árnyékolás.




8. ábra. Egy számítógépes szoba lehetséges elektromágneses árnyékolása [37]

Az elektromágneses árnyékolás megvalósításánál az oldalfalakon kívül nagy figyelmet kell fordítani a nyílászárók árnyékolására is, illetve biztosítani kell a védet térbe csatlakozó vezetékek (áramellátás, számítógépes hálózat stb.) elektromágneses szűrését.

Az árnyékolások kivitelezésére és azok tesztelésére számos szabvány létezik, amelyek betartásával megfelelő védelem biztosítható az elektromágneses pusztító eszközök ellen.

Az elektronikai berendezések védelménél az árnyékolástechnika alkalmazható:

- teljes szobaárnyékolásnál, amely védelmet nyújt az elektronikus lehallgatás és a kívülről jövő elektromágneses zavarok ellen is;
- információs hálózatok védelménél speciális szűrőkkel, zavarvédett kábelekkel és kábelkötegekkel az elektronikus lehallgatás és a külső zavarokkal szemben;

- biztonsági kábelek kettős árnyékolásánál, amely kisfrekvenciás és nagyfrekvenciás zavarokkal szemben is védelmet nyújt;
- biztonsági táskáknál, mágneses adattárolóknál, ahol a mechanikai sérülés és elektroszmog ellen is biztonságos védelmet nyújt;
- elektronikai berendezéseknél, hálózatok utólagos szigetelésénél, zavarvédelem kialakításánál nagyfrekvenciás tömítőanyagok és szigetelőanyagok felhasználásával;
- zavarvédett műszerdobozok nagyérzékenységű, illetve kiemelt fontosságú elektronikák (biztonsági- és életmentő berendezések, fedélzeti computer) zavarvédelménél.

### Elektronikai zavarás elleni védelem [28]

Az elektronikai zavarás elleni tevékenységgel kapcsolatban használjuk a zavarstabilitás és zavarvédettség fogalmát.

A **zavarstabilitás** az elektronikai rendszerek azon tulajdonsága és képessége, amely kifejezi, hogy az adott rendszer az elektronikai zavarás viszonyai között képes-e funkcionális feladatainak végrehajtására.

A **zavarvédettség** az elektronikai eszközök azon tulajdonsága, hogy milyen mértékű, intenzitású, típusú zavaró jelekkel szemben védettek. Ez azt jelenti, hogy a rendszeren belül minél zavarvédettebb eszközök vannak, annál nagyobb a rendszer zavarstabilitása.

Az egyes eszközök zavarvédettségét alapvetően a fejlesztés-, tervezés-, kivitelezés során kell biztosítani, és lehetővé tenni, hogy a berendezések minél nagyobb mértékben legyenek képesek kiszűrni a zavarokat.

Az elektronikai eszközöket vizsgálva az elektromágneses zavarást előidéző jel alapvetően két forrásból fakadhat:

- magából a vizsgálat alá vett eszközből, rendszerből, ami belső eredetű zavar;
- eszközön, rendszeren kívülről, ami más berendezés (rendszer) által generált elektromágneses tér által okozott külső eredetű zavar lehet.

A zavar terjedését tekintve vezetett vagy sugárzott zavart különböztethetünk meg.

**Vezetett zavar** az, amely fémes vezetők közvetítésével galvanikusan, kapacitív vagy induktív csatoláson keresztül terjed:

- galvanikus csatolás során a zavaró hatások az áramkörök közös (ohmos) elemein keresztül jönnek létre. A zavaró jellemző az áram;
- kapacitív csatolás esetén a zavaró hatások a váltakozó villamos terek útján kerülnek a zavaró áramkörből a berendezés zavart részébe. A zavaró jellemző a feszültség;
- induktív csatoláskor a zavaró hatások egy zavarforrás váltakozó mágneses tere által indukált feszültségként keletkeznek a zavart elszenvedő vevőben. Okuk a zavarforrás áramának változása.

A vezetett zavart előidéző jelek elsősorban a berendezések tápellátását biztosító kábeleken vagy a földvezetéken keresztül zavarják meg más áramkörök működését.

**Sugárzott zavarás** esetében a zavart olyan szabadon terjedő elektromágneses hullámok okozzák, amelyek becsatolódnak a berendezés egyes részeibe. Sugárzott zavarásról beszélünk abban az esetben, ha a zavarójelet valamilyen közegen keresztül (pl. légkör) az elektromágneses tér terjedése közvetíti.

Az elektromágneses zavar és mértéke három tényező függvénye, úgymint:

- a zavarforrás paraméterei, elsősorban a spektrumsűrűség;
- a zavart közvetítő közeg, vagy vezetési tulajdonságokkal rendelkező anyag átviteli karakterisztikája;
- a zavart elszenvedő berendezés, áramkör, alkatrész érzékenysége.

Az elektromágneses zavarás kialakulásának folyamata bár egyszerűnek tűnik, a valóságban bonyolult folyamatot takar. A bonyolultságot az okozza, hogy a valós közvetítő közegben telepített rendszereket az esetek döntő többségében előre meg nem határozható zavarforrások veszik körül, miközben a rendszerek elemei is létrehozhatnak belső eredetű zavarokat.

Minden üzemelő, elektromágneses energiát kisugárzó adóállomás – a hullámterjedés sajátosságait figyelembe véve – kelt valamekkora elektromágneses térerősséget az üzemelő vevőállomások bemenetén.

Egy, a zavart elszenvedő – adott feltételek között működő – vevőállomás zavarásának mértéke erősen függ:

- a zavarforrás frekvenciájától, üzemelési időpontjától, területi elhelyezkedésétől;
- mindkét berendezés modulációs módjától;
- a hasznos jel és a zavarforrás által keltett jel térerősségének arányától;
- a zavart elszenvedő vevőállomás és a zavarforrás antennájának iránykarakterisztikájától;
- a hasznos jel és a zavarforrás által keltett jel polarizációjának eltérésétől;
- a zavart elszenvedő vevőállomás frekvenciafüggő átviteli és demodulációs jellemzőitől stb.

A zavarforrás zavart okozhat, ha:

- a zavarforrásból származó energia a zavart elszenvedő vevő számára a hasznos jelnél – a zavarállóságot is figyelembe véve – nagyobb;
- a zavarforrásból származó energia frekvenciaspektruma egybeesik a zavart elszenvedő vevő vételi sávjával.

Mint ahogy azt korábban is írtuk, az elektronikai zavarás lehet szándékos és nem szándékos. E tanulmány keretében csak a szándékos zavarás elleni védelemmel foglalkozunk.

**A szándékos zavarás hatékonyságát csökkentő általános módszerek** a következők lehetnek:

- a zavarás és zavarok felismerése;
- a zavar eredetének meghatározása (a zavar külső, ha a zavar az antennán keresztül jut be a vevőbe; a zavar belső, ha a zavar nem az antennán keresztül jut be a vevőbe);

- a zavar hovatartozásának meghatározása (a zavar szándékos, pl. ellenséges zavarás esetén; a zavar nem szándékos, pl. saját eszköz zavarása, atmoszféra zavarok stb. estén);
- a zavarás és a zavarok hatékonyságának csökkentése;
- az üzemelés folytatása (a zavar hatékonyság felmérésének akadályozása céljából);
- a hasznos jel és a zavaró jel arányának javítása;
- a vevőberendezés beszabályozása (helyi oszcillátor, sávszélesség, hangerő stb. beszabályozása);
- az adó kimenő teljesítményének növelése;
- az antenna beszabályozása vagy megváltoztatása (pl. az antenna polarizáció megváltoztatása minden állomáson);
- átjátszó állomás létesítése;
- az antenna helyének a megváltoztatása;
- alternatív átviteli útvonalak alkalmazása;
- frekvencia megváltoztatása;
- műholdas kommunikáció esetén másik műholdra való átállás.

E módszerekkel csak akkor érhetjük el az információk kellő időben történő és értelmezhető továbbítását, ha arra időben felkészülünk és az áttérést kellő szinten begyakoroljuk.

A szándékos zavarok elleni védelem általános módszerei alapján megállapítható, hogy azokat egyrészt szervezési (pl. alternatív híradó útvonalak), másrészt technikai (pl. az adó kimenő teljesítményének növelése) módszerekkel lehet biztosítani.

A továbbiakban különböző elektronikai eszközök közül a rádiólokációs- rádió és rádiórelé berendezések szándékos zavarok elleni védelemének módszereit tekintjük át részletesebben.

**A rádiólokátorok** fejlesztésében az elektronikai zavarás elleni elektronikai védelmi eszközök és tevékenységek mindig arra irányulnak, hogy minimalizálják az elektronikai zavaróeszközök, eljárások hatását, sőt ha lehetséges előnyöket kovácsoljanak az elektronikai zavaró berendezések és zavarási módszerek tökéletlenségéből.

Általános elektronikai védelemi filozófia az, hogy legyőzzék a teljesítményveszteségekből fakadó hátrányokat, minimalizálják a megtévesztő zavarás hatását, vagy rákényszerítsék a szembenálló felet szélessávú zavarójelek előállítására, melynek következtében a zavarás hatékonysága jelentősen csökkenhet. Mivel a szélessávú zavarójeleknek csak a vevő sávszélességébe eső (töredék) része jelenik meg mint zavar, ezért hatékonysága is ennek arányában csökken. Ebben az esetben ugyanis a rádiólokátor vevője által vett zavarójel teljesítménye már kisebb lehet, mint a céltárgyról visszavert hasznos jelé. A rádiólokátor vevőrendszer zavarvédelmi képességeinek növelése (pl. szelektivitás, dinamikatartomány-növelés, antenna oldalnyaláb szintcsökkentés stb.) mind olyan lehetőségek, amelyekkel jelentősen csökkenthető az elektronikai zavarás hatása. Napjainkra már a korszerű MTI/MTD[64] detektortechnikák és útvonalképző algoritmusok, eljárások hatására, ha nem is szüntethetők meg, de jelentősen kompenzálhatók a különböző passzív zavarást alkalmazó eljárások (pl. a dipólok, hamis célok) céltárgy felderítést rontó képessége.

**A rádiólokátor elektronikai ellentevékenység általi sebezhetőségét** több tényező is jelentősen befolyásolja. Ezek:

- a rádiólokátor pontos, vagy hozzávetőleges helyének, pillanatnyilag alkalmazott vivőfrekvenciájának, adójel-struktúrájának és egyéb műszaki paramétereinek ismerete;
- a rádiólokátor és az elektronikai zavaróeszközök relatív pozícióinak helyzete, a rádiólokátor és elektronikai zavaróeszközök műszaki jellemzői;
- a rádiólokátor elektronikai zavarásra való érzékenysége.

Ha a támadó nem ismeri a rádiólokátor pontos, vagy megközelítőleges helyét, pillanatnyilag alkalmazott vivőfrekvenciáját-, adójel-struktúráját, akkor csak a teljes területet-, és frekvenciasávot lefogó zajzavarás („nyers erő”) módszerével próbálkozhat. Ebben az esetben a rendelkezésére álló zavaró adóteljesítményt és/vagy passzív zavaró eszközöket a teljes rádiólokátor által használt frekvenciasávban és a teljes területet lefedve kell alkalmaznia. Ha figye-

[64] MTI – Moving Target Indicator – mozgó céltárgy indikátor
MTD – Moving Target Detector – mozgó céltárgy érzékelő

lembe vesszük a rádiólokátorok által lefedett terület nagyságát és a rádiólokátor üzemi frekvencia sávját, mindkét esetben jelentősen korlátozódnak a zavarás lehetőségei, mivel a rádiólokátor egyenlet, az elektromágneses hullámok terjedési viszonyainak ismerete, az elektronikai zavaróeszközök alkalmazhatóságának és a lehetséges elhelyezési pozíciók ismereteiből meghatározható, hogy a zavaró jelek a rádiólokátor számára milyen hatásokat idézhetnek elő. Ebből a szempontból kiemelt jelentősége van a rádiólokátor zavarásra való érzékenységének, mivel ez által jellemezhetők a különböző elektronikai ellentevékenység eszközök és eljárások által létrehozható rádiólokátor teljesítményrontó tényezők.

A rádiólokátorokban alkalmazott fő elektronikai védelmi eljárásokat az 1. táblázat tartalmazza.

Természetesen napról-napra sokkal kifinomultabb elektronikai zavarási eljárások és eszközök kerülnek kidolgozásra, alkalmazásra, kikényszerítve ezzel az eddig ismert elektronikai védelmi eszközök és eljárások továbbfejlesztését. Ez végső soron az ultra-szélessávú rádiólokátorok és nagyon kis oldalnyaláb szintekkel rendelkező antennák kidolgozásához vezet, melyet sokoldalú különösen fejlett jelfeldolgozás egészít ki. A rádiólokátorokban egyre fejlettebb impulzus-kompressziós eljárások kerülnek alkalmazásra, melyek tovább javítják a zavarállóságot.

**A rádió és rádiórelé eszközöknél** – a rádiólokációs berendezésekhez hasonlóan – a szándékos zavarok elleni védelem (zavarvédettség fokozása) szervezési és technikai módszerekkel biztosítható. A fontosabb szervezési módszerek a következők lehetnek:

- tartalék rádióhálók és irányok szervezése;
- rejtett rádióhálók és irányok szervezése;
- kerülő hírcsatornák, közbeeső állomások szervezése és az átjátszó módszer szerinti forgalmazás;
- tartalék üzemi frekvenciák meghatározása és a hívójelek nélküli összeköttetés felvétele;
- üzemmód váltása;
- közlemények különböző hírcsatornákon való egyidejű adása és vétele.

1. táblázat: A rádiólokátor alrendszerekben alkalmazható elektronikai védelmi eljárások [28]

| **Rádiólokátor alrendszerek** | **Elektronikai védelmi eljárások** |
|---|---|
| Antenna | Nagy irányítottságú antennák<br>Több sugárnyaláb<br>Alacsony oldalnyaláb szint<br>Oldalnyaláb „blankolás”<br>Oldalnyaláb elnyomás<br>Adaptív fázisrács<br>Véletlenszerű letapogatás |
| Adó | Nagy energia-kisugárzás<br>Teljesítményvezérlés időben és térben<br>Frekvenciaváltás és csúsztatás<br>Belső impulzus moduláció<br>Indításváltoztatás, szaggatás, kódolás<br>Automatikus frekvencia kiválasztás<br>Milliméteres hullámtartomány használata |
| Vevő | Kétszeres frekvencia konverzió<br>Nagy dinamika tartomány |
| Jelfeldolgozás | Digitális koherens és adaptív mozgócél kiválasztás<br>Detektálás előtti vaklárma normalizálás<br>Impulzus szélesség és ismétlődési frekvencia diszkriminátor |

A rádió- és rádiórelé állomások szándékos zavarok elleni védelemének fokozását biztosító technikai módszerek hasonlóak a rádiólokátor berendezéseknél már ismertetekhez.

A fontosabb technikai módszerek a következők lehetnek:

- az adó teljesítményének növelése;

- különböző szelektivitást növelő módszerek alkalmazása (térszelekció, amplitúdószelekció, frekvenciaszelekció);
- vételzavar elleni védett hibajavító kódok alkalmazása;
- gyors adók, frekvenciaugratásos rádióberendezések alkalmazása stb.

Az adók teljesítményének növelése ugyan a szándékos zavarás elleni védelem legegyszerűbb módja, de ez a saját nem szándékos zavarok jelentős növekedéséhez vezethet, egyben megkönnyíthetjük a rádiófelderítést is. Ezért a teljesítménynövelést akkor célszerű alkalmazni, amikor már kimerítettük a szándékos zavarok elleni védelem összes többi lehetőségét.

A térszelekció az élesen irányított adó- és vevőantennák alkalmazásával biztosítható, amelynek megvalósítása az ultrarövid-hullámú sávban már nem ütközik nehézségbe. Az antenna sugárzási karakterisztika forgatásával, fáziskompenzációs módszerrel a zavaró jelek elnyomhatók. Nézzük meg közelebbről e technikai módszer lényegét.

A térszelekció alkalmazásakor egymástól néhány üzemi hullámhossz távolságra két vevőantennát telepítünk merőleges iránnyal a hasznos jel sugárzási irányára. A kisugárzott hasznos jeleket két antennával egyidejűleg vesszük, azaz egyenlő fázissal. Ha a hasznos jel frekvenciáján zavarás van, és ha a zavaró jel kisugárzási iránya különbözik a hasznos jel kisugárzási iránytól, akkor a vevőantennák a zavaró jelet bizonyos fáziskülönbséggel veszik.

A zavaró jel elnyomásához meg kell változtatni a hasznos jel és a zavarójel közötti fáziskülönbséget (mivel a két antenna között fellépő fáziskülönbség 180 fok), majd pedig amplitudóit is egyenlővé kell tenni. A fáziskülönbség megváltoztatását fázisfordítóval, az amplitúdók kiegyenlítését pedig az antennákra épített variométerrel és szintautomatikával lehet végrehajtani.

A két ellentétes fázisú és különböző amplitúdójú jel összegzésének eredményeként a vevő bemenetén a hasznos jel a zavarójelhez képest kisebb gyengülést szenved. Időszelekció alkalmazása esetén a vevőberendezések csak a hasznos jel megjelenésének időszakában működnek.

Amplitúdószelekció a vevőfokozatban a különböző zajvágó áramkörökkel hozható létre. Frekvenciaszelekció a vevőberendezésben alkalmazott különböző rezgőköri elemekkel érhető el. (Viszonylagos egyszerűségénél fogva ez a legjobban elterjedt szelektivitást növelő módszer.)

A szándékos zavarok elleni védelem fokozásának egy további módszere a hibajavító kódok alkalmazása.

A fent megvizsgált szándékos zavarok elleni védelmet fokozó módszerek csak a zavarok egy bizonyos csoportjára hatásosak. Ugyanakkor napjainkban az elektronikai eszközök zavarvédettségét fokozó technikai módszerek egyetlen ismert eszköze sem biztosítja az elektronikai zavarás elleni teljes védettséget. A zavarvédettség megoldását a szervezési és technikai módszerek komplex alkalmazásában kell keresni.

# RÖVIDÍTÉSEK JEGYZÉKE

| | | |
|---|---|---|
| ADSL | Asymmetrical Digital Subscriber Line | Aszimmetrikus digitális előfizetői vonal |
| ANS | Advanced Network Services | Fejlett hálózati szolgáltatások |
| ARIB | Association of Radio Industries and Business | Távközlési Ipari és Kereskedelmi Szövetség (Japán) |
| ARPA | Advanced Research Project Agency | Fejlett Kutatások Hivatala |
| ATM | Automated Teller Machine | Pénzkiadó automata |
| AUC | Authentication Centre | Előfizetői azonosító központ |
| BIX | Budapest Internet Exchange | Budapest Internet Csereközpont |
| BS | Base Station | Bázisállomás |
| BSS | Base Station Subsystem | Bázisállomás Alrendszer |
| CDMA | Code Division Multiple Access | Kódosztásos többszörös hozzáférés |
| CEP | NATO Civil Emergency Planning | NATO Polgári Vészhelyzeti Tervezés |
| CERT | Computer Emergency Response Team | Számítógépes Vészhelyzeti Reagáló Csoport |

| | | |
|---|---|---|
| CI2RCO | Critical Information Infrastructure Research Co-ordination | Kritikus Információs Infrastruktúra Kutató Koordináció |
| CIA | Central Intelligence Agency | Központi Hírszerző Ügynökség |
| CIRCA | Computer Incident Response Coordination Austria | Osztrák Számítógépes Incidens Reagáló Koordinációs Csoport |
| CIWG | Critical Infrastructure Working Group | Kritikus Infrastruktúra Munkacsoport |
| CIWIN | Critical Infrastructure Warning Information Network | Kritikus Infrastruktúra Figyelmeztető Információs Rendszer |
| CNI | Critical National Infrastructure | Kritikus nemzeti infrastruktúra |
| COBIT | Control Objectives for Information and Related Technology | Információs és kapcsolódó technológiák ellenőrzésének irányelvei |
| COCOM | Coordinating Committee for Multilateral Export Controls | Többoldalú Exportellenőrzési Koordináló Bizottság |
| CRT | Cathode Ray Tube | Katódsugárcsöves monitor |
| CTCPEC | Canadian Trusted Computer Product Evaluation Criteria | Biztonságos Számítástechnikai Termékek Értékelési Kritériumai Kanadában |
| CSIRT | Computer Security Incident Response Team | Számítógép Biztonság Incidens Kezelő Csoport |
| DARPA | Defense Advanced Research Project Agency | Védelmi Fejlett Kutatások Hivatala |

| | | |
|---|---|---|
| DCA | Defence Communication Agency | Védelmi Kommunikáció Ügynökség |
| DCN | Distributed Computer Network | Elosztott számítógép-hálózat |
| DDoS | Distributed Denial of Service | Elosztott szolgáltatás megtagadási támadás |
| DES | Data Encryption Standard | Kódosztásos többszörös hozzáférés |
| DHS | Department of Homeland Security | Belbiztonsági Minisztérium (USA) |
| DMO | Direct Mode Operation | Közvetlen módú működés |
| DNS | Domain Name System | Névkezelő rendszer |
| DoD | Department of Defense | Védelmi Minisztérium (USA) |
| DoS | Denial of Service | Szolgáltatás megtagadási támadás |
| DS | Direct Sequence | Közvetlen zajmodulációs eljárás |
| DTMF | Dual-Tone Multi-Frequency | Kéthangú többfrekvenciás jelzésátviteli rendszer |
| DWDM | Dense Wavelength Division Multiplexing | Nagysűrűségű hullámhossz multiplexálás |

| | | |
|---|---|---|
| EADS | European Aeronautic Defence and Space Company | Európai Légi és Űr Vállalat |
| ECI | European Critical Infrastructure | Európai kritikus infrastruktúra |
| EDGE | Enhanced Data Rates for Global Evolution | Globális evolúció érdekében megnövelt adatátviteli sebesség |
| EDR | | Egységes Digitális Rádiórendszer |
| EGC | European Governmental CERT | Európai Kormányzati CERT |
| EIR | Equipment Identification Register | Készülék Azonosító Regiszter |
| EKG | | Elektronikus Kormányzati Gerinchálózat |
| EKK | | Elektronikuskormányzatközpont |
| EKOB | | E-Kormányzat Operatív Bizottság |
| EMCON | Emission Control | Kisugárzás korlátozás |
| ENISA | European Network and Information Security Agency | Európai Hálózati és Informatikai Biztonság Ügynökség |
| EPCIP | European Programme for CIP | Európai Program a Kritikus Infrastruktúrák Védelmére |

| | | |
|---|---|---|
| ETSI | European Telecommunications Standards Institute | Európai Távközlési Szabványosítási Intézet |
| EU | | Európai Unió |
| FBI | Federal Bureau of Investigation | Szövetségi Nyomozó Iroda |
| FDMA | Frequency Division Multiple Access | Frekvenciaosztásos többszörös hozzáférés |
| FH | Frequency Hopping | Frekvenciaugratásos eljárás |
| FFH | Fast Frequency Hopping | Frekvenciaugratásos rendszer |
| FIRST | Forum of Incident Response Team | Incidenskezelő Csoportok Fóruma |
| FPLMTS | Future Public Land Mobile Telecommunications System | A Jövő Nyilvános Földi Mozgó Távközlési Rendszere |
| FTP | Foiled Twisted Pair | Fóliázott csavart érpár |
| FTP | File Transfer Protocol | Fájl átviteli protokoll |
| GET | | Földgázellátásról szóló törvény |
| GMPCS | Global Mobile Personal Communications by Satellite | Globális Műholdas Mobil Személyi Kommunikáció |

| | | |
|---|---|---|
| GPRS | General Packet Radio System | Általános Csomagkapcsolt Rádió Rendszer |
| GSM | Global System for Mobil Communication | Globális Mobilkommunikációs Rendszer |
| HLR | Home Location Register | Honos Előfizetői Helyregiszter |
| HSCSD | High Speed Circuit Switched Data | Nagy Sebességű Áramkörkapcsolt Adatok |
| HSPD | Homeland Security Presidential Directive | Belbiztonsági Elnöki Direktíva |
| HTTP | Hyper Text Transfer Protocol | Hyperszöveg Átviteli Protokol |
| IDEA | International Data Encryption Algorithm | Nemzetközi adattitkosító algoritmus |
| IDS | Intrusion Detection System | Behatolás detektáló rendszer |
| IEC | International Electrotechnical Commission | Nemzetközi Elektrotechnikai Bizottság |
| IHL | Internet Header Length | Internet (datagram) fejrész hossz |
| IIF | | Információs Infrastruktúra Fejlesztési (program) |

| | | |
|---|---|---|
| IMP | Interface Message Processor | Interfész üzenet processzor |
| IP | Internet Protocol | Internet protocoll |
| IRA | Irish Republican Army | Ír Köztársasági Hadsereg |
| IrDA | Infrared Data Association | Infravörös Adatátvitel Nemzetközi Szervezete |
| ISDN | Integrated Services Digital Network | Integrált szolgáltatású digitális hálózat |
| ISMS | Information Security Management System | Informatikai Biztonság Menedzsment Rendszer |
| ISO | International Organisation for Standardisation | Nemzetközi Szabványügyi Szervezet |
| ISP | Internet Service Provider | Internetszolgáltató |
| ISPA | Federation of the Austrian Internet Service Providers | Osztrák Internetszolgáltatók Szövetsége |
| ITB | | Informatikai Tárcaközi Bizottság |
| ITIL | IT Infrastructure Library | Informatikai szolgáltatás módszertana |
| ITSZ | | Internet Szolgáltatók Tanácsa |

| | | |
|---|---|---|
| ITU | International Telecommunications Union | Nemzetközi Távközlési Unió |
| IWWN | International Watch and Warning Network | Nemzetközi Figyelő és Figyelmeztető Hálózat |
| KHVM | | Közlekedési, Hírközlési és Vízügyi Minisztérium |
| KIETB | | Kormányzati Informatikai Egyeztető Tárcaközi Bizottság |
| KITKH | | Kormányzati Informatikai és Társadalmi Kapcsolatok Hivatala |
| KSH | | Központi Statisztikai Hivatal |
| LAN | Local Area Network | Helyi hálózat |
| LCD | Liquid Crystal Display | Folyadékkristályos monitor |
| LTTE | Liberation Tigers of Tamil Eelam | Tamil Eelam Felszabadító Tigrisei |
| MAN | Metropolitan Area Network | Városi hálózat |
| MAVIR | | Magyar Villamosenergia-ipari Átviteli Rendszerirányító |
| MIBÉTS | | Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma |

| | | |
|---|---|---|
| MITS | | Magyar Információs Társadalom Stratégia |
| MMS | Multimedia Messaging Service | Multimédiás üzenetküldő szolgáltatás |
| MODCERT | Ministry of Defence Computer Emergency Response Team | Védelmi Minisztérium Számítógépes Vészhelyzeti Reagáló Csoport |
| MS | Mobil Station | Mobil állomás |
| MSC | Mobile Switching Centre | Mobil szolgáltató kapcsolóközpont |
| MTD | Moving Target Detector | Mozgó céltárgy érzékelő |
| MTI | Moving Target Indicator | Mozgó céltárgy indikátor |
| MVM | | Magyar Villamos Művek |
| MVMT | | Magyar Villamos Művek Tröszt |
| NATINADS | NATO Integrated Air Defence System | NATO integrált légvédelmi rendszer |
| NATO | North Atlantic Treaty Organisation | Észak-atlanti Szerződés Szervezete |
| NCP | Network Control Protocol | Hálózat irányító protokoll |

| | | |
|---|---|---|
| NHTCU | National High Tech Crime Unit | Nemzeti Csúcstechnológiás Bűnözés Elleni Egység |
| NIC | Network Interface Card | hálózati kártya |
| NIIF | | Nemzeti Információs Infrastruktúra Fejlesztési (Program) |
| NIPP | National Infrastructure Protection Plan | Nemzeti Infrastruktúra Védelmi Terv |
| NISCC | National Infrastructure Security Coordination Centre | Nemzeti Infrastruktúra Biztonsági Koordinációs Központ |
| NITS | | Nemzeti Információs Társadalom Stratégia |
| NMC | Network Management Centre | Hálózatfelügyeleti központ |
| NNTP | Network News Transfer Protocol | Hálózati hírátviteli protokoll |
| NSAC | National Security Advice Centre | Nemzeti Biztonsági Tanácsadó Központ |
| NSF | National Science Foundation | Nemzeti Tudományos Alapítvány |
| NSS | Network Switching Subsystem | Hálózati és kapcsoló alrendszer |
| OMH | | Országos Mérésügyi Hivatal |

| | | |
|---|---|---|
| OSI | Open System Interconnection | Nyílt rendszer összekapcsolás |
| OSS | Operating Subsystem | Üzemeltetési alrendszer |
| OTKA | | Országos Tudományos Kutatási Alap |
| PB&C | Planning Boards and Committees | Tervező csoport és bizottság |
| PCCIP | Presidential Commission on Critical Infrastructure Protection | Elnöki Bizottság a Kritikus Infrastruktúra Védelmére |
| PDD | Presidential Decision Directives | Elnöki Direktívák |
| PFM | Pulse Frequency Modulation | Impulzus frekvenciamoduláció vagy chirp eljárás |
| PN | Pseudo Noise | Álvéletlen zaj (kódsorozat) |
| POP | Point Of Presence | Gerinchálózati csatlakozási pont |
| PSTN | Public Switched Telephone Network | Nyilvános kapcsolt telefonhálózat |
| PTA | | Puskás Tivadar Alapítvány |
| RAF | Rote Armee Fraktion | Vörös Hadsereg Frakció |

| | | |
|---|---|---|
| RLL | Radio in the Local Loop | Rádió a helyi körben |
| RNC | Radio Network Controller | Rádióhálózat-vezérlő egység |
| SCEPC | Senior Civil Emergency Planning Committee | Polgári Vészhelyzeti Tervező Bizottság (NATO) |
| SDH | Synchron Digital Hierarchy | Szinkron digitális hierarchia |
| SDS | Short Data Service | Rövid adatszolgáltatás |
| SFH | Slow Frequency Hopping | Lassú frekvenciaugratásos rendszer |
| S-FTP | Shielded and Foiled Twisted Pair | Fémharisnyás és fóliázott csavart érpár |
| SMSC | Short Messages Centre | Rövid üzenet szolgálati központ |
| SMTP | Simple Mail Transfer Protocol | Levelező protokoll |
| SRI | Stanford Research Institute | Stanford Kutató Intézet |
| STP | Shielded Twisted Pair | Fémharisnyás csavart érpár |
| SZTAKI | | Számítástechnikai és Automatizálási Kutató Intézet |

| | | |
|---|---|---|
| TAPS | TETRA Advanced Packet Service | TETRA fejlett csomag szolgáltatás |
| TC | Trans Coder | Transzkóder |
| TCP | Transmission Control Protocol | Átvitelt vezérlő protokoll |
| TD-CDMA | Time Divison- Code Division Multiple Access | Kód és időosztásos többszörös hozzáférés |
| TDMA | Time Division Multiple Access | Időosztásos többszörös hozzáférés |
| TEDS | TETRA Enhanced Digital Service | TETRA megnövelt digitális szolgáltatás |
| TETRA | Terrestrial Trunked Radio | Területi trönkölt rádió |
| TF-CSIRT | Task Force Computer Security Incident Response Team | Számítógép Biztonság Incidens Kezelő Csoportok Akciócsoportja |
| TH | Time Hopping | Időugratásos eljárás |
| TIA | Telecommunications Industry Association | Távközlési Ipari Szövetség (USA) |
| TSO | Transmission System Operator | Átviteli rendszerirányító |
| TTA | Telecommunications Technology Association | Távközléstechnológiai Szövetség (Dél-Korea) |

| | | |
|---|---|---|
| TTL | Time to Live | Élettartam |
| UCLA | University California at Los Angeles | Kaliforniai Egyetem Los Angeles |
| UCPTE | Union for the Coordination of Production and Transmission of Electricity | Nyugat-Európai Villamosenergia-Rendszeregyesülés |
| UCTE | Union for the Co-ordination of Transmission of Electricity | Nyugat-Európai Villamosenergia-Rendszeregyesülés |
| UCSB | University California at Santa Barbara | Kaliforniai Egyetem Santa Barbara |
| UDP | User Datagram Protocol | Felhasználói datagram protokoll |
| UMTS | Universal Mobile Telecommunication System | Univerzális mobil telekommunikációs rendszer |
| UNIRAS | Unified Incident Reporting and Alert Scheme | Azonosított incidens jelentő és riasztó séma |
| URAN | UMTS Radio Access Network | UMTS rádióelérésű hálózat |
| URH | | Ultrarövid-hullám |
| UTAH | University of Utah | Utah Egyetem |
| UTP | Unshielded Twisted Pair | Árnyékolatlan csavart érpár |
| UTRAN | UMTS Terrestrial Radio Access Network | UMTS földi rádió-hozzáférési hálózat |

| | | |
|---|---|---|
| VER | | Villamosenergia-rendszer |
| VLR | Visitor Location Register | Látogató előfizetői hely-regiszter |
| VoIP | Voice over IP | Internet protokoll feletti beszédátvitel |
| VSAT | Very Small Aperture Terminal | Kétutas műholdas kom-munikációra alkalmas földi terminál |
| W3C | World Wide Web Consortium | Világháló Konzorcium |
| WAN | Wide Area Network | Nagykiterjedésű hálózat |
| WAP | Wireless Application Protocol | Vezeték nélküli alkalma-zási protokoll |
| W-CDMA | Wideband Code Division Mul-tiple Access | Szélessávú kódosztású többszörös hozzáférés |
| WCIT | World Congress on Infor-mation Technology | Információtechnológiai Világkongresszus |
| WI-FI | Wireless Fidelity | Vezeték nélküli szab-vány |
| Wi-Max | Worldwide Interoperability for Microwave Access | Mikrohullámú vezeték nélküli hozzáférés |
| WLAN | Wireless Local Area Network | Vezeték nélküli helyi hálózat |

| | | |
|---|---|---|
| WLAN | Wireless LAN | Vezeték nélküli helyi hálózat |
| WWW | World Wide Web | Világháló |

# ÖSSZEFOGLALÁS

Jelen tanulmány arra vállalkozott, hogy a *TÁMOP 4.2.2/B-10/1-2010-0001 Tudományos képzés műhelyeinek támogatása – Kockázatok és válaszok a tehetséggondozásban (KOVÁSZ)* projekt támogatásával bemutassa a kritikus infrastruktúrák és a kritikus információs infrastruktúrák területén a volt Zrínyi Miklós Nemzetvédelmi Egyetemen, illetve ennek jogutódján a Nemzeti Közszolgálati Egyetemen a kritikus infrastruktúrák és a kritikus információs infrastruktúrák végzett kutatásokat, azok eredményeit, illetve az azokból levonható következtetéseket.

Tanulmányunk felépítésénél arra törekedtünk, hogy a több mint egy évtizedre visszanyúló egyetemi kutatásokat oylan átfogó módon mutassuk be, amelyek nemcsak egy „egyszerű" kutatási jelentésként értelmezhetőek, hanem magába a témába engednek bepillantást. Természetesen a tanulmány szerkezetének elvi kialakítása után a szerkesztő és a szerzők is azzal a ténnyel kellett, hogy szembesüljenek, amely az egymástól eltérő területek nem egyforma terjedelmű, és nem egyforma mélységű kidolgozottságát jelentette. Így állt elő a tanulmány – nem minden esetben teljesen azonos terjedelmű fejezetekre, illetve alfejezetekre osztott – szerkezete. A fejezetek terjedelme is támpontot nyújt arra, hogy bepillantást nyerjünk egy-egy részterületen folyó kutatás milyen mélységben és milyen eredményekkel folyt az elmúlt években.

Mindezeknek megfelelően tanulmányunk a hazai kritikus infrastruktúra és kritikus információs infrastruktúra osztályozását, csoportosításait, a legfontosabb infrastruktúrákat, ezek felépítését, működését kívánta bemutatni. Mindezek túl azokat a veszélyeket is górcső alá vette, amelyek e rendszereinket fenyegethetik, valamint bemutatta, hogy a feltárt veszélyekre válaszul milyen védelmi megoldások alkalmazása lehetséges.

Fontos hangsúlyozni, hogy jelen tanulmány az eddig elkészült és publikált kutatási eredményekre épít, így minden jelen tanulmányban leírt vagy felhasznált tény ezeken alapul. Így joggal mondhatjuk: jelen tanulmány egy kibővített kutatási jelentés.

Tanulmányunkban igyekeztünk – pontos irodalmi hivatkozásokkal – felhasználni, minden olyan tudományos igényű írást vagy publikációt – legyen annak szerzője doktorandusz, vagy akár a témában évek óta kutató egyetemi oktató –, amely a korábban a Zrínyi Miklós Nemzetvédelmi Egyetemhez, illetve ennek jogutódjához a Nemzeti Közszolgálati Egyetemhez, az ott működő és a témát kutató csoportokhoz köthetőek.

# MELLÉKLET

Bibliográfia a Zrínyi Miklós Nemzetvédelmi Egyetemen, majd a Nemzeti Közszolgálati Egyetemen megjelent, illetve az ott kutatók által megjelentetett kritikus információs infrastruktúrákat érintő publikációkról
A sorrend a megjelenés éve szerint növekvő, majd azon belül a címek alfabetikus rendjét követi, mert a cikkek címét, tartalmát kívánjuk könnyebben áttekinthetővé tenni és nem a /szerzők/ szerinti keresést.

## KÖNYVEK

**Globális terrorizmus és az információs hadviselés** /Várhegyi István/ In: szerk.: Vámosi Zoltán: Az új világrend kihívása: terrorizmus és biztonság. Biztonságpolitikai füzetek (különszám). TIT Hadtudományi és Biztonságpolitikai Egyesület, Budapest, 2001.

**Hadviselés az információs hadszíntéren** /Haig Zsolt, Várhegyi István/ Zrínyi Kiadó, Budapest, 2005. ISBN 963 327 391 9

**Az infokommunikációs rendszerek biztonságának szabályozása a Magyar Köztársaságban különös tekintettel a Magyar Honvédségre** /Kerti András, Pándi Erik/ Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar Híradó Tanszék, Budapest, 2010.

## TUDOMÁNYOS CIKKEK, TANULMÁNYOK

**1996**

**Az információs hadviselés** /Várhegyi István/ Új Honvédségi Szemle, L. évfolyam 7. szám 1996. július.

**2002**

**Az információs társadalom veszélyforrásai: A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban** /Makkay Imre, Seebauer Imre, Haig Zsolt, Vass Sándor, Ványa László, Kovács László/ Tanulmány a Miniszterelnöki Hivatal számára, az SZT-IS-1 Széchenyi Terv Pályázatban, ZMNE, Budapest, 2002.

**Információs színtér, információs környezet, információs infrastruktúra /** Munk Sándor/ Nemzetvédelmi Egyetemi Közlemények, 2002 (VI.) /2. pp. 133-154. ISSN 1417-7323

**2004**

**Információs támadás és védelem, mint nemzetbiztonsági kihívás** /Haig Zsolt/ SZAKMAI SZEMLE (KATONAI BIZTONSÁGI HIVATAL) 3. sz.: pp. 5-25. Budapest, 2004.

**2006**

**Az információbiztonság komplex értelmezése** /Haig Zsolt/ Hadmérnök különszám. Robothadviselés 6. tudományos szakmai konferencia, Budapest, 2006. november 22. ISSN 1788-1919
http://hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.html

**Az információs terrorizmus eszköztára** /Kovács László/ Hadmérnök különszám. Robothadviselés 6. tudományos szakmai konferencia, Budapest, 2006. november 22. ISSN 1788-1919
http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html

**Lehetséges-e terrortámadások végrehajtása az információs rendszereken keresztül?** /Kovács László/ Nemzetvédelmi Egyetemi Közlemények, 10. évfolyam 3. tematikus szám, pp. 237-240. ZMNE Budapest, 2006. ISSN 1417-7323

**2007**

**Az információbiztonság szabályzói és szervezeti keretei** /Haig Zsolt/ Hadmérnök különszám. Robothadviselés 7. tudományos szakmai konferencia, 2007. november 27., Budapest. ISSN 1788-1919
http://hadmernok.hu/kulonszamok/robothadviseles7/haig_rw7.pdf

**Az információs társadalmat fenyegető információalapú veszélyforrások** /Haig Zsolt/ Hadtudomány, XVII. évfolyam 3. szám. Budapest, 2007. szeptember. 37-56 pp. ISSN 1215-4121 http://www.zmne.hu/kulso/mhtt/hadtudomany/2007/3/2007_3_4.html

**DoS támadások veszélyei és az ellenük való védekezés lehetséges módszerei** /Gyányi Sándor/ Hadmérnök különszám. Robothadviselés 7. tudományos szakmai konferencia, Budapest, 2007. november 27. ISSN 1788-1919
http://hadmernok.hu/kulonszamok/robothadviseles7/gyanyi_rw7.html

**Információs műveletek, SIGINT és EW kapcsolatrendszere** /Haig Zsolt/
Felderítő Szemle 6:(Különszám) pp. 27-48. Budapest, 2007. ISSN 1588-242X

**Internet terrorizmus** / Haig Zsolt/ Nemzetvédelmi Egyetemi Közlemények, XI. évf.:(2. sz.) pp. 81-93. ZMNE Budapest, 2007. ISSN 1417-7323

**IT kockázatok, elemzésük, kezelésük** /Póserné Oláh Valéria/ Hadmérnök, II. évfolyam 3. szám 2007. szeptember. ISSN 1788-1919
http://hadmernok.hu/archivum/2007/3/2007_3_poserne.html

**Kritikus információs infrastruktúrák Magyarországon** /Kovács László Hadmérnök különszám. Robothadviselés 7. tudományos szakmai konferencia. Budapest, 2007. nov. 27. ISSN 1788-1919 http://hadmernok.hu/kulonszamok/robothadviseles7/kovacs_rw7.html

**2008**

**A cybertér és a cyberhadviselés értelmezése** /Haig Zsolt, Várhegyi István/ Hadtudomány XVIII. évf.:(Elektronikus szám) pp. 1-12. ISSN 1215-4121
http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf

**A kritikus információs infrastruktúrák értelmezése** /Varga Péter/ Hadmérnök, III. évfolyam 2. szám 2008. június. ISSN 1788-1919
http://hadmernok.hu/archivum/2008/2/2008_2_varga.html

**Az információs társadalom információbiztonsága** /Haig Zsolt/ Bolyai Szemle XVII. évf. 4. szám. pp. 167-180. ISSN: 1416-1443

**Az információs terrorizmus elleni tevékenység kormányzati feladatai** /Kovács László/ Hadmérnök III. évfolyam 2. szám 2008. június. ISSN 1788-1919
http://hadmernok.hu/archivum/2008/2/2008_2_kovacsl.html

**Az internet, mint kritikus információs infrastruktúra támadhatósága** /Előházi János/ Hadmérnök III. évfolyam 4. szám 2008. december. ISSN 1788-1919
http://hadmernok.hu/archivum/2008/4/2008_4_elohazi.html

**Botnetek kialakulása, használatuk, trendjeik** /Illési Zsolt/ Hadmérnök III. évfolyam 2. szám 2008. június. ISSN 1788-1919
http://hadmernok.hu/archivum/2008/2/2008_2_illesi.html

**Cyber-támadások elleni védekezés és a válaszcsapások lehetőségei** /Gyányi Sándor/ Hadmérnök III. évfolyam 2. szám 2008. június. ISSN 1788-1919
http://hadmernok.hu/archivum/2008/2/2008_2_gyanyi.html

**Egy kutatás margójára: a terrorizmus elleni harc nemzetbiztonsági feladatai Magyarország információs társadalmának kiépítése során** /Kovács László/ In: Csontos István (szerk.) In: Bolyai Szemle: A Robothadviselés 8. Konferencia előadásainak szerkesztett változata. Budapest, 2008.11.27. pp. 213-220. ISSN: 1416-1443

**Energiaellátó rendszerek rendszerirányítása** /Haig Zsolt, Kovács László/ In: Szenes Katalin (szerk.) Az informatikai biztonság kézikönyve : Informatikai biztonsági tanácsadó A-Z. 3.7.4. fejezet. Budapest: Verlag Dashöfer Szakkiadó, 2008. pp. 51-75.

**Fenyegetések a cybertérből** /Haig Zsolt, Kovács László/ Nemzet és Biztonság 2008/5. pp. 61-70. HU ISSN 1789-5286
http://www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf

**Internet Magyarországon** /Haig Zsolt, Kovács László/ In: Szenes Katalin (szerk.) Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z. 3.7.5. fejezet. Budapest: Verlag Dashöfer Szakkiadó, 2008. pp. 77-100.

**Kritikus információs infrastruktúrák elleni fenyegetések** /Haig Zsolt, Kovács László/ In: Szenes Katalin (szerk.) Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z. 3.7.7. fejezet. Budapest: Verlag Dashöfer Szakkiadó, 2008. pp. 137-148.

**Kritikus információs infrastruktúrák védelme** /Haig Zsolt, Kovács László/
In: Szenes Katalin (szerk.) Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z. 3.7.8. fejezet. Budapest: Verlag Dashöfer Szakkiadó, 2008. pp. 149-170.

**Kritikus információs infrastruktúrákhoz kapcsolódó, sajátos katonai (védelmi szférabeli) képességeket igénylő feladatok** /Munk Sándor/ III. évfolyam 3. szám 2008. szeptember http://hadmernok.hu/archivum/2008/3/2008_3_munk.html

**Kritikus infrastruktúrák védelme információs támadások ellen /** Munk Sándor/ Hadtudomány, 2008. (XVIII.)/1-2. pp. 95-106. MHTT Budapest, 2008. ISSN 1215-4121 http://www.zmne.hu/kulso/mhtt/hadtudomany/2008/1_2/096-106.pdf

**2009**

**A fenyegetettség egyes aspektusai az információs infrastruktúrák tekintetében** /Papp Zoltán, Pándi Erik, Töreki Ákos/ In.: szerk. Fekete Károly Kommunikáció 2009. ZMNE, Budapest, 2009. pp. 155-163. ISBN 978-963-7060-70-0

**A kritikus információs infrastruktúrák meghatározásának módszertana** /Haig Zsolt, Hajnal Béla, Kovács László, Muha Lajos, Sik Zoltán Nándor/ Tanulmány. © ENO Avisory Kft.,
http://www.cert-hungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf

**A villamosenergia-ellátás biztonságáról** /Bárdos Zoltán/ Bolyai szemle XVIII. évfolyam 1. szám. pp. 77-83. ZMNE, Budapest, 2009. ISSN: 1416-1443
http://portal.zmne.hu/download/bjkmk/bsz/bszemle2009/1/07_bardoszoltan.pdf

**Adatbázisok kritikus infrastruktúrákban** /Munk Sándor, Fleiner Rita/ Hadmérnök IV. évfolyam 1. szám 2009. március . ISSN 1788-1919
http://hadmernok.hu/2009_1_fleiner.php

**Adatbázisok szerepe kritikus infrastruktúrák biztonságában** /Fleiner Rita/ Hadmérnök IV. évfolyam 2. szám 2009. június. ISSN 1788-1919
http://hadmernok.hu/2009_2_fleiner.php

**Az információs társadalom információbiztonsága** /Haig Zsolt/ Egyetemi jegyzet Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2009. 179 p.

**Az információs társadalom infrastruktúrái, azok sebezhetősége** /Mikulás Sándor Szakmai szemle: a Katonai Biztonsági Hivatal Tudományos Tanácsának kiadványa, 2009. 2. szám.

**Az információtechnológiai rendszer veszélyeztetettségi kérdései a rendvédelem területén** /Prisznyák Szabolcs, Pándi Erik, Farkas Tibor/ In.: szerk. Fekete Károly Kommunikáció 2009. ZMNE, Budapest, 2009. pp. 127-135. ISBN 978-963-7060-70-0

**Az információvédelem időtállósága a kritikus infrastruktúrában** /Pölcz Péter, Pándi Erik, Pándi Balázs/ Hírvillám: a Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszék szakmai tudományos kiadványa, I. évfolyam 1. szám, ZMNE Budapest, 2010.

**Classification of information based attacks** /Haig Zsolt/ Hadtudományi Szemle 2. évf.:(3. sz.) pp. 9-14. ZMNE Budapest, 2009.
http://hadtudomanyiszemle.zmne.hu/files/2009/1/2hzs.pdf

**Connection between cyber warfare and information operations** /Haig Zsolt/ AARMS Volume 8:(Issue 2) pp. 329-337. (2009) ZMNDU Budapest, 2009. ISSN 1588-8789

**Infokommunikációs biztonsági stratégia** /Muha Lajos/ Hadmérnök IV. évfolyam 1. szám 2009. március. ISSN 1788-1919
http://hadmernok.hu/2009_1_muha.php

**Információs hadviselés kínai módra** /Kovács László/ Nemzet és biztonság, II. évfolyam 7. szám 2009. szeptember. HU ISSN 1789-5286
http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo-informacios_hadviseles_kinai_modra.pdf

**Kritikus adatbázisokra épülő informatikai rendszerek architektúrái és biztonsági szempontjai** /Fleiner Rita/ Hadmérnök IV. évfolyam 3. szám 2009. szeptember. ISSN 1788-1919
http://hadmernok.hu/2009_3_fleiner.php

**Kritikus információs infrastruktúrák sebezhetősége** /Haig Zsolt/ In: Wireless technológiák – adatátvitel és biztonság IIR szakmai konferencia elektronikus kiadvány (CD). Budapest, 2009.06.09-2009.06.10. pp. 1-39.

**Obama's new cyberspace policy** /László Kovács/ Hadtudományi Szemle, 2009. 2. évfolyam 3. szám ZMNE, Budapest 2009.

**Possible methodology for protection of critical information infrastructures** /László Kovács/ Hadmérnök IV. évfolyam 3. szám 2009. szeptember. ISSN 1788-1919
http://hadmernok.hu/2009_3_kovacsl.php

**The information infrastructures of the information society** /Zsolt Haig/ Bolyai szemle, 2009. XVIII. évfolyam 4. szám. ISSN: 1416-1443
http://portal.zmne.hu/download/bjkmk/bsz/bszemle2009/4/11_haigzsolt.pdf

**The security of Web applications** /Valéria Póserné Oláh/ AARMS: Academic and Applied Research in Military Science Vol. 8, No. 1 2009. 173-178 pp. ZMNDU Budapest, 2009. ISSN 1588-8789

**2010**

**A digital Mohács: a cyber attack scenario against Hungary** /László Kovács, Csaba Krasznay/ Nemzet és Biztonság, III. vol. special issue winter 2010/2011 Budapest, 2011. pp. 49-59. HU ISSN 1789-5286

**A kritikus információs infrastruktúra védelem és a védelmi célú katasztrófavédelmi híradás kapcsolatrendszere** /Sándor Miklós, Kuris Zoltán/ Hadmérnök, V. évfolyam 3. szám 2010. szeptember, ZMNE Budapest, 2010. ISSN 1788-1919
http://hadmernok.hu/2010_3_sandor_kuris.php

**A polgári műsorszórás, mint kritikus információs infrastruktúra elemzése** /Varga Péter/ Hadmérnök V. évfolyam 3. szám 2010. szeptember. ISSN 1788-1919
http://hadmernok.hu/2010_3_varga.php

**A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala** /Kovács László, Sipos Marianna/ Hadmérnök 5:(4) pp. 163-172. (2010). ISSN 1788-1919
http://hadmernok.hu/2010_4_kovacs_sipos.pdf

**Digitális Mohács: egy kibertámadási forgatókönyv Magyarország ellen** /Kovács László, Krasznay Csaba/ Nemzet és Biztonság, III. évfolyam 1. szám 2010. február. HU ISSN 1789-5286
http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf

**Információs hadviselés: nem csak kínai módra** /Rácz Lajos/ Nemzet és Biztonság, III. évfolyam 1. szám 2010. február. HU ISSN 1789-5286
http://www.nemzetesbiztonsag.hu/cikkek/racz_lajos-informacios_hadviseles___nem_csak_kinai_modra.pdf

**Kritikus adatbázisok meghatározásának lehetőségei, módszerei a kormányzati szektorban /**Fleiner Rita/ Bolyai szemle 2010. XIX. évfolyam 1. szám. ZMNE, Budapest, 2010. ISSN: 1416-1443
http://portal.zmne.hu/download/bjkmk/bsz/bszemle2010/1/22_fleinerrita.pdf

**2011**

**A kritikus információs infrastruktúra védelme és a közigazgatás** /Sik Zoltán Nándor/ Vezetéstudomány: a Budapesti Közgazdaságtudományi és Államigazgatási Egyetem Gazdálkodástudományi Kar Budapesti Vezetőképző Központ havi szakfolyóirata (1976-)
XLII. évfolyam 2011. 3. szám .

**A Stuxnet és ami mögötte van II.: célok és teendők** /Kovács László, Sipos Marianna/ Hadmérnök VI. Évfolyam 1. szám - 2011. március, pp.: 222-231. ISSN 1788-1919
http://www.hadmernok.hu/2011_1_kovacs_sipos.php

**Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata** /Haig Zsolt, Kovács László, Ványa László/ Felderítő szemle, X. évfolyam 1-2. szám 2011. március-június. pp. 183-209. MK KFH Budapest, 2011. HU ISSN 1588-242X

**Az információs hadviselés kialakulása, katonai értelmezése** /Haig Zsolt/ Hadtudomány, XXI. évfolyam 1-2. szám, pp. 12-28. MHTT Budapest, 2011. ISSN 1215-4121
http://mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_4.pdf

**Az információs hadviselés második hulláma** /Várhegyi István/ Hadtudomány, XXI. évfolyam 1-2. szám , pp. 49-64. MHTT Budapest, 2011. ISSN 1215-4121
http://mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_7.pdf

**Cyberhadviselés** /Kovács László, Illési Zsolt/ Hadtudomány, XXI. évfolyam 1-2. szám, pp. 29-41. MHTT Budapest, 2011. ISSN 1215-4121
http://mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_5.pdf

**Információs hadviselés korunk alacsony intenzitású konfliktusaiban** /Kis-Benedek József/ Hadtudomány, XXI. évfolyam 1-2. szám, pp. 6-11. MHTT Budapest, 2011. ISSN 1215-4121
http://mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_3.pdf

**Kiberháború?: internetes támadások a Wikileaks ellen és mellett** /Kovács László/ Nemzet és biztonság, IV. évfolyam 1. szám 2011. február. Budapest, 2011. HU ISSN 1789-5286
http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo-kiberhaboru__internetes__tamadasok_a_wikileaks_ellen__es_mellett.pdf

**Kiberterrorizmus: valós veszély?** /Mezey Nándor Lajos/ Belügyi szemle 59. évfolyam 2011/2. pp. 21-48. Belügyminisztérium, Budapest, 2011. ISSN 1789-4689

**2012**

**A nemzeti kritikus információs infrastruktúrák védelmének szabályozási és szervezeti kérdései: helyzetkép az EU irányelv 2012-ben esedékes felülvizsgálata előtt** /Nagyné Takács Veronika/ Hadmérnök VII. évfolyam 1. szám 2012. március. pp. 179-191. ISSN 1788-1919
http://www.hadmernok.hu/2012_1_takacs.pdf

**Úton a kritikus információs infrastruktúrák azonosítása és védelmük kialakítása felé** /Bonnyai Tünde/ Hadmérnök, VII. Évfolyam 2. szám - 2012. június, p.: 90-105. ISSN 1788-1919
http://www.hadmernok.hu/2012_2_bonnyai.pdf

# IRODALOM

## I. Fejezet


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

[2] Információs társadalom. http://hu.wikipedia.org/wiki/Információs_társadalom. (Letöltve: 2012. 07. 23.)

[3] Toffler, Alvin: Harmadik hullám. Typotex Kiadó. Budapest, 2001

[4] Bell, Daniel: The social framework of the information society. In M. Dertouzos & J. Moses (Ed.), The Computer Age: A Twenty-year View pp. 163-211. 1979. MIT Press Cambridge ISBN: 0262540363

[5] Identity and Change in the Network Society. Conversation with Manuel Castells. http://globetrotter.berkeley.edu/people/Castells/castells-con4.html (Letöltve: 2012. 07. 23.)

[6] Magyar Információs Társadalom Stratégia, 2003. http://www.etudasportal.gov.hu/download/attachments/5734444/MITS.pdf (Letöltve: 2012. 08. 02.)

[7] Nemzeti Információs Társadalom Stratégia. 2001.

www.artefaktum.hu/kozgaz/nits_kesz.doc (Letöltve: 2012. 07. 23.)

[8] Lisbon European Council, Presidency Conclusions, 23–24 March 2000. http://www.europarl.europa.eu/summits/lis1_en.htm (Letöltve: 2012. 07. 23.)

[9] Elfogadta a Kormány a Magyar Információs Társadalom Stratégiát. http://www.sg.hu/cikkek/29930/elfogadta_a_kormany_a_magyar_informacios_tarsadalom_strategiat (Letöltve: 2012. 07. 23.)

[10] Papp, László: A XX. század elektronikája és a fejlődés irányai. Természet Világa 2006. I. különszám, 105-111.p. Tudományos Ismeretterjesztő Társulat folyóirata ISSN 0040-3717

[11] Moore-törvény. http://hu.wikipedia.org/wiki/Moore-törvény (Letöltve: 2012. 07. 23.)

[12] Álló, Géza – Bartolits, István: Korlátlan sávszélesség és számítási teljesítmény http://www.nhit-it3.hu/images/stories/tag_and_publish/Files/it3-2-1-1-u.pdf (Letöltve: 2009. 08. 30.)

[13] Sallai, Gyula – Abos, Imre: A távközlés, információ- és médiatechnológia konvergenciá ja. Magyar Tudomány, Infokommunikációs hálózatok. 2007. július. 844-851. p. ISSN 1588-1245

[14] Dömölki, Bálint et al: Információs társadalom technológiai távlatai. Tanulmány. Harmadik kötet. Új tanulmányok. 2007. szeptember. http://www.nhit-it3.hu/images/stories/tag_and_publish/Files/it3-9-1-1-3.pdf (Letöltve: 2009. 08. 30.)

[15] COM (2010) 245 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:LV:PDF (Letöltve: 2012. 07. 23.)

[16] Digitális Megújulás Cselekvési Terv 2010-2014. Nemzeti Fejlesztési Minisztérium, 2010

[17] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny 2012. 19. sz. 1378-1387p.

[18] KSH Gyorstájékoztató. Távközlés, internet 2011. IV. negyedév, 2012. március 7. http://www.ksh.hu/docs/hun/xftp/gyor/tav/tav21112.pdf (Letöltve: 2012. 07. 23.)

[19] Magyar értelmező kéziszótár, MTA, Budapest, 2002.

[20] HAIG ZSOLT–KOVÁCS LÁSZLÓ–MAKKAY IMRE–SEEBAUER IMRE–VASS SÁNDOR–VÁNYA LÁSZLÓ: Az információs társadalom veszélyforrásai. A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban. Tanulmány. MEH Informatikai Kormánybiztosság, 2002.

[21] Critical Foundations Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection, Washington, October, 1997.

[22] VÁRHEGYI ISTVÁN–MAKKAY IMRE: Információs korszak, információs háború, biztonságkultúra. OMIKK, Budapest, 2000.

[23] HAIG ZSOLT: Network-Centric Warfare and Sensor Fusion. AARMS Volume 2, Issue 2. MZNDU, Budapest, 2003.

[24] Térinformatikai fogalomtár:
http://gisfigyelo.geocentrum.hu/kisokos/kisokos_taverzekeles.html (Letöltve: 2012. 07. 23.)

[25] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.
http:// www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf (Letöltve: 2012. 07. 23.)

[26] HAIG ZSOLT: Az információs társadalmat fenyegető információlapú veszélyforrások. Hadtudomány 2007/3. ISSN: 1215-4121

[27] PRÉCSÉNYI ZOLTÁN–SOLYMOSI JÓZSEF: Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé. Hadmérnök, 2007. március.
http://zrinyi.zmne.hu/hadmernok/archivum/2007/1/2007_1_precsenyi.html ISSN 1788-1919 (Letöltve: 2012. 07. 23.)

[28] BUKOVICS ISTVÁN–VAVRIK ANTAL:Infrastruktúrák kockázata és biztonsága: kritikai problémaelemzés. Hadmérnök, 2006. december.
http://zrinyi.zmne.hu/hadmernok/archivum/2006/3/2006_3_bukovics.html ISSN 1788-1919 (Letöltve: 2012. 07. 23.)

[29] MUHA LAJOS: A Magyar Köztársaság információs infrastruktúráinak védelme. Doktori (PhD) értekezés tervezet, ZMNE, Budapest, 2007.

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

[31] MUNK SÁNDOR: Információs színtér, információs környezet, információs infrastruktúra. Nemzetvédelmi Egyetemi Közlemények 2002. 2. sz. ZMNE, Budapest, ISSN 1417-7323]

[32] GERENCSÉR ANDRÁS: Rövid összefoglalás kritikus információs infrasruktúrák védelméről. http://www.isaca.hu/addons/news_1626_CIIP_GerencserAndras.pdf (Letöltve: 2012. 07. 23.)

## II. Fejezet

[1] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny 2012. 19. sz. 1378-1387 p.

[2] 2112/2004. (V. 7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól

[3] Magyarország energiapolitikai tézisei 2006–2030, A Magyar Villamos Művek Közleményei különszám, MVM, XLIII. ÉVFOLYAM 2006. NOVEMBER http://www.mvm.hu

[4] A Magyar Villamos Művek története. http://www.mvm.hu/engine.aspx?page=cegtortenet (Letöltve 2009. 07.10.)

[5] A Paksi Atomerőmű látképe http://www.atomeromu.hu/thumbnail/3542/700x500fit/0017%20copy.jpg (Letöltve: 2012. 07.12.)

[6] A magyar villamosenergia-rendszer (VER) adatai 2006, MAVIR 2006

[7] Magyarországi erőművek listája - szócikk http://hu.wikipedia.org/wiki/Er%C5%91m%C5%B1vek_Magyarorsz%C3%A1gon (Letöltve: 2012. 07. 12.)

[8] WILDE GYÖRGY: Olajipari értelmező szótár. http://www.petroleum.hu/wildeszotar.htm

[9] Adatpublikációs oldal. http://mavir.hu/web/mavir/adatpublikacio (Letöltve: 2012. 07. 12.)

[10] A MAVIR honlapja. http://www.mavir.hu

[11] MOL Földgázszállító Rt. Bemutatkozás http://www.mol.hu/repository/165062.pdf (Letöltve: 2012. 07. 12.)

[12] GET adatforgalmi rendszer tanulmány verzió <1.0> Magyar Energia Hivatal, Scada-Kovex-Me AKKI , 2003 http://www.eh.gov.hu/gcpdocs/200311%5Cgetaf.pdf

[13] A MOL Földgázszállító Rt. Informatikai Platformjának továbbfejlesztése http://e-ker.hu/news.php?id=4417&type=printer (Letöltve: 2012. 07. 12.)

[14] http://www.nabucco-pipeline.com/company/markets-sources-for-nabucco/index.html

[15] http://www.gkm.gov.hu/sajtoszoba/sajtoanyagok/2006_sajtohirek/junius/nabucco.html

[16] Mol: Bizonytalan a Nabucco-projekt
http://index.hu/gazdasag/2012/04/23/mol_bizonytalan_a_nabucco-projekt/ (Letöltve: 2012. 08. 12.)

[17] MTI: Újabb gázvezeték Magyarországon át?
http://hvg.hu/gazdasag/20060619gazvezetek.aspx (Letöltve: 2012. 08. 12.)

[18] Déli Áramlat – szócikk. http://hu.wikipedia.org/wiki/D%C3%A9li_%C3%81ramlat (Letöltve: 2012. 08. 12.)

[19] JOBBÁGY SZABOLCS–SEREGE GÁBOR: Az egységes készenléti digitális trön-költ rádiórendszer TETRA és TETRAPOL jellemző, sajátosságai. Kommunikáció 2003, ZMNE, ISBN 963 86229 9 2

[20] A TETRA rendszer. http://www.tetraforum.hu/tetrarendszer.htm

[21] Sikeres volt az első budapesti TETRA-próbahívás.http://www.radio.hu

[22] Az EADS honlapja. http://www.eads.com

[23] MAROS DÓRA: Távközlési hálózatok működésének nemzetközi és hazai szabályozási kérdései veszély- és katasztrófahelyzetekben. Doktori (PhD) értekezés, Budapest, 2007.

[24] KSH: Vezetékes vonalak és mobil-előfizetések száma az időszak végénhttp://www.ksh.hu/docs/hun/xstadat/xstadat_evkozi/e_onp001.html (Letöltve: 2012. 08.04.)

[25] Bodnár Ádám: MPVI lesz az állami mobilszolgáltató vállalat neve. HWSW 2012. március 22. http://www.hwsw.hu/hirek/48265/mpvi-zrt-magyar-posta-villamos-muvek-mfb-mobilszolgaltato-nmhh-frekvencia-tender.html (Letöltve: 2012. 08.04.)

[26] T-Mobile cégtörténet
http://www.t-mobile.hu/egyeni/rolunk/ceginformaciok/cegtortenet/index.shtml

[27] Pannon GSM cégtörténet
http://www.pannon.hu/pannon/sajtoszoba/ceginformaciok/cegtortenet

[28] Telenor cégtörténet
http://www.telenor.hu/telenor-magyarorszag/ceginformacio/tortenet

[29] A Vodafone Magyarország története
http://www.vodafone.hu/sajtoszoba/a_vodafone_mo_tortenete.html (Régi oldal)

[30] A Vodafone Magyarország története
http://www.vodafone.hu/vodafonerol/a-vodafone-magyarorszag-tortenete (Új oldal) (Letöltve: 2012. 08. 26.)

[31] Az internet. http://www.aldasuai.sulinet.hu/tantargy/sztech/internet.doc

[32] COCOM címszó. http://lazarus.elte.hu/~climbela/cocom.htm (Letöltve: 2012. 08. 26.)

[33] IT3 honlapja. http://www.nhit-it3.hu/ (Letöltve: 2012. 08. 26.)

[34] http://www.iif.hu/index.php?headline=infra&menu=menu-kapcs.html&text=infra1.html

[35] NIIF története. http://www.niif.hu/hu/story (Letöltve: 2012. 08. 26.)

[36] NIIF Bemutatkozás. http://www.niif.hu/hu/intro (Letöltve: 2012. 08. 26.)

[37] EKK Kormányzati Stratégia ismertetése.
http://www.meh.hu/szervezet/hivatalok/ekk/ekormanyzat/stratismerteto.html

[38] EKK Alapdokumentumok.
http://www.meh.hu/szervezet/hivatalok/ekk/ekk/alapdok20070323.html

[39] http://www.iif.hu/index.php?headline=hungarnet&text=hungarnet.html&nomenu=1

[40] http://www.meh.hu/szervezet/hivatalok/ekk/keszr/ekg/ekg20050920.html

[41] http://www.bix.hu/index.php3?lang=hu&page=charter

[42] http://www.iszt.hu/iszt/alapszabaly.html

[43] http://www.ksh.hu/docs/hun/xstadat/xstadat_evkozi/e_oni001.html

## III. Fejezet


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

[2] Muha, Lajos: A Magyar Köztársaság információs infrastruktúráinak védelme. Doktori (PhD) értekezés. ZMNE, Budapest, 2007.

[3] Várhegyi, István – Makkay, Imre: Információs korszak, információs háború, biztonságkultúra. OMIKK, Budapest, 2000.

[4] Haig, Zsolt – Kovács, László – Makkay, Imre – Seebauer, Imre – 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] Haig, Zsolt: Az információs társadalmat fenyegető információlapú veszélyforrások. Hadtudomány 2007/3. ISSN: 1215-4121

[6] Haig Zsolt: Az információbiztonság komplex értelmezése. Robothadviselés 6. tudományos konferencia kiadványa. Hadmérnök különszám 2006. nov. 22. ISSN 1788-1919. http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles6/haig_rw6.htm (Letöltve: 2009. 08. 30.)

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

[8] Haig Zsolt: Az információs hadviselés kialakulása, katonai értelmezése. Hadtudomány XXI. évf. 1-. sz. 2011. május ISSN 1215-4121 12-28 p.

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

[10] National Military Strategy for Cyberspace Operations. December, 2006. http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf (Letöltve: 2012. 07. 24.)

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

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

[13] Fahrenkrug, David T.: Cyberspace Defined. http://www.au.af.mil/au/archive/0209/Articles/CyberspaceDefined.html (Letöltve: 2008. 02. 24.)

[14] Bourque, Jesse: The Language of Engagement and the Influence Objective. The Journal of Electronic Defense. November 2007. Vol. 30. No.11. p. 30-35 ISSN 192429X

[15] Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína. A Magyar Honvédség kiadványa, 2004.

[16] AJP-3.10 Allied Joint Doctrine for Information Operations. 2009

[17] Kovács László: Az információs terrorizmus eszköztára. HADMÉRNÖK Robothadviselés 6. tudományos szakmai konferencia különszám. 2006. http://zrinyi.zmne.hu/hadmernok/kulonszamok/ robothadviseles6/kovacs_rw6.html ISSN 1788–1919 (Letöltve: 2012. 07. 25.)

[18] http://www.ezenanapon.hu/main.php?reszletes=414=9=5 (Letöltve: 2007. 11. 23.)

[19] http://www.origo.hu/tudomany/tarsadalom/20011106iraes.html (Letöltve: 2012. 07. 25.)

[20] http://www.enc.hu/1enciklopedia/fogalmi/poltud/vor_brig.htm (Letöltve: 2012. 07. 25.)

[21] Hadtudományi Lexikon MHTT Budapest, 1995.

[22] Townshend, Charles: A terrorizmus. Magyar Világ kiadó, 2003. 174p. ISBN 963907523X

[23] http://www.fas.org/sgp/news/2003/01/dodweb.html (Letöltve: 2012. 07. 25.)

[24] http://konfliktus.index.hu/sritigrisek.html (Letöltve: 2012. 07. 25.)

[25] Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004 http://www.fbi.gov/congress/congress04/lourdeau022404.htm (Letöltve: 2007. 11. 23.)

[26] Russian Cyberwar on Georgia. http://georgiaupdate.gov.ge/doc/10006922/CYBERWAR-%20fd_2_.pdf (Letöltve: 2012. 04. 06.)

[27] http://english.aljazeera.net/news/archive/archive?ArchiveId=24098 (Letöltve: 2007. 11. 23.)

[28] http://electronicintifada.net/v2/article1387.shtml (Letöltve: 2007. 11. 23.)

[29] http://www.enc.hu/1enciklopedia/fogalmi/poltud/intifada.htm (Letöltve: 2012. 07. 25.)

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

[31] Gyányi Sándor: DDoS támadások veszélyei és az ellenük való védekezés. Hadmérnök, Robothadviselés 7 tudományos szakmai konferencia különszám. http://hadmernok.hu/kulonszamok/robothadviseles7/gyanyi_rw7.html (Letöltve: 2009. 08. 30.)

[32] Kovács László: Az elektronikai felderítés korszerű eszközei és eljárásai és azok alkalmazhatósága a Magyar Honvédségben, PhD értekezés, ZMNE, 2004

[33] ÁLT/27 Magyar Honvédség Összhaderőnemi Doktrína, 2. kiadás. A Magyar Honvédség kiadványa, 2007.

[34] WTC – LIDAR Three Dimensional Model. http://www.loc.gov/exhibits/911/911-maps.html (Letöltve: 2009. 08. 26.)

[35] Hand Held Thermal Imager. http://www.ir55.com/hhti.html (Letöltve: 2009. 08. 26.)

[36] Infrared Thermal Imaging: Unattended Ground Sensor Package. http://www.iecinfrared.com/Products/IEC-Infrared-products-accessories-ground-sensors.html (Letöltve: 2009. 08. 26.)

[36] Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai. MTA SZTAKI, 2004.

[37] GSM Jammer. http://www.tayx.co.uk/jmf-mobile-phone-jammer.html (Letöltve: 2009. 08. 26.)

[38] Horváth Tamás: „GPS Jamming" a GPS jelek szándékos zavarása http://www.agt.bme.hu/tantargyak/gpselm/eloadas/HT_26apr.pdf (Letöltve: 2009. 08. 30.)

[39] Raise Hell With A GPS/GSM Jammer From DetectNu. http://www.crunchgear.com/2007/01/30/raise-hell-with-a-gpsgsm-jammer-from-detectnu/ (Letöltve: 2009. 08. 26.)

[40] Ványa László: Elektronikai ellentevékenység. Kézirat

[41] Kopp, Carlo: The E-bomb – A Weapon of Electrical Mass Destruction http://www.jya.com/ebomb.htm (Letöltve: 2009. 08. 30.)

[42] Cereijo, Manuel: The E-bomb. http://www.lanuevacuba.com/archivo/manuel-cereijo-115.htm (Letöltve: 2009. 08. 30.)

## IV. Fejezet

[1] Abele-Wigert, Isabelle– Dunn, Myriam: International CIIP Handbook 2006, VOL. I, An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies, Center for Security Studies, ETH Zurich, 2006.

[2] Critical Foundations Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection, Washington, 1997. október

[3] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

[4] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.
http:// www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf (Letöltve: 2012. 07. 25.)

[5] The Comprehensive National Cybersecurity Initiative

http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (Letöltve: 2012. 07. 25.)

[6] A Strong Britain in an Age of Uncertainty: The National Security Strategy, http://direct.gov.uk/nationalsecuritystrategy (Letöltve: 2012. 07. 25.)

[7] Muha Lajos: A Magyar Köztársaság információs infrastruktúráinak védelme. Doktori (PhD) értekezés tervezet, ZMNE, Budapest, 2007.

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

[9] Précsényi Zoltán–Solymosi József: Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé. Hadmérnök, 2007. március.
http://zrinyi.zmne.hu/hadmernok/archivum/2007/1/2007_1_precsenyi.html ISSN 1788-1919 (Letöltve: 2012. 07. 25.)

[10] Európai Unió Tanácsa, az Elnökség konklúziói a 2004. június 18-19-i brüsszeli csúcstalálkozó nyomán, 10679/2/04 REV2, 2004. június 19.

[11] Commission of the European Communities: Communication from the Com-mission to the Council and the European Parliament – Critical Infrastruc-ture Protection in the fight against terrorism, Brussels, 20.10.2004 COM(2004) 702 final
http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf (Letöltve: 2012. 07. 25.)

[12] Európai Unió Tanácsa, az Elnökség konklúziói a 2004. december 16-17-i brüsszeli csúcstalálkozó nyomán, 16238/1/04 REV1, 2005. február 1.

[13] NATO stratégiai koncepciója 2010 a Biztonságpolitikai szakkollégium fordításában: http://www.biztonsagpolitika.hu/documents/1291766875_NATO_Strat_Koncepcio_2010_hun_BSZK.pdf (Letöltve: 2012. 07. 25.)

[14] Chicago Summit Declaration

http://www.nato.int/cps/en/SID-D95FAE1D-99C8ECE1/natolive/official_texts_87593.htm

[15] Summit Declaration on Defence Capabilities: Toward NATO Forces 2020

http://www.nato.int/cps/en/natolive/official_texts_87594.htm

[16] Muha, Lajos: A Magyar Köztársaság információs infrastruktúráinak védelme. Doktori (PhD) értekezés. ZMNE, Budapest, 2007.

[17] Útmutató az IT biztonsági szintek meghatározásához**.**

http://www.ekk.gov.hu/hu/emo/EKK_ekozig_ITbiztonsagiszintekmeghatarozasa_080822_V101.doc (Letöltve: 2009. 08. 30.)

[18] Az informatikai biztonság kézikönyve. Verlag Dashöfer Szakkiadó. ISBN 963 9313 12 2

[19] Haig, Zsolt–Várhegyi, István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005. ISBN 963 327 391 9

[20] Haig, Zsolt – Kovács, László – Makkay, Imre – Seebauer, Imre – Vass Sándor – Ványa, László: Az információs társadalom veszélyforrásai. A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban. Tanulmány. MEH Informatikai Kormánybiztosság, 2002.

[21] Holdaway, Eric J.: Active Computer Network Defense: An Assessment. Air Command and Staff College. Maxwell Air Force Base, Alabama, 2001.

[22] Thomas, Tom: Hálózati Biztonság – Panem Könyvkiadó Kft, 2005. ISSN 1785-3346, ISBN 963-545-425-2

[23] Szirota, Csaba: Adatvédelem kérdései az Interneten, tekintettel az e-mail és World Wild Web-en keresztüli adatforgalomra. http://www.vcsk.hu/~szistvan/linux/biztonsag/dolgozat.html (Letöltve: 2009. 08. 30.)

[24] Dravecz, Tibor – Párkányi, Balázs: Hogyan védjük hálózatra kötött számítógépes rendszereinket? NIIF Információs Füzetek II./8. Budapest, 1996.

[25] Szimmetrikus kulcsú titkosítás folyamata. https://onlinessl.netlock.hu/hu/tudasbazis/hogyan-mkoedik/a-szimmetrikus-titkositas.html (Letöltve: 2009. 08. 26.)

[26] Aszimmetrikus kulcsú titkosítás folyamata. https://onlinessl.netlock.hu/hu/tudasbazis/hogyan-mkoedik/az-aszimetrikus-titkositas.html (Letöltve: 2009. 08. 26.)

[27] Digitális aláírás. http://www.biztostu.hu/mod/resource/view.php?id=243 Letöltve: 2009. 08. 26.

[28] Balajti, István – Vass, Sándor: Elektronikai védelem. Egyetemi jegyzet, ZMNE, 2000

[29] Kassai Károly Az elektronikus információk védelmének területei. http://www.zmka.hu/kulso/mhtt/hadtudomany/2002/3/kassaikaroly/chapter1.htm (Letöltve: 2009. 08. 30.)

[30] Van Eck-Phreaking. http://hu.wikipedia.org/wiki/Van_Eck-phreaking (Letöltve: 2009. 08. 30.)

[31] Video Eavesdropping Demo at CeBIT 2006. http://www.lightbluetouchpaper.org/2006/03/09/video-eavesdropping-demo-at-cebit-2006/ (Letöltve: 2009. 08. 30.)

[32] Géczy Gábor: Fémezett szövetek alkalmazása az elektronikában. Elektronet, Budapest, 1998/6-7

[33] Vass Sándor: Az elektronikai berendezéseinket fenyegető terrortámadások és az ellenük való védekezés kérdései. Budapest, ZMNE, Nemzetvédelmi Egyetemi Közlemények, 2006. X. évf. 3.(tematikus) szám, 228-236 p.

[34] EMC villámvédelem és túlfeszültség-védelem V. rész: http://epa.oszk.hu/00000/00025/00001/feher.html (letöltve: 2009. 08. 30.)

[35] Raymond, Eric Steven: Szünetmentes tápegység HOGYAN. http://tldp.fsf.hu/HOWTO/UPS-HOWTO-hu/index.html (Letöltve: 2009. 08. 30.)

[36] Elemental Faraday Cage. http://www.boltlightningprotection.com/Elemental_Faraday_Cage.htm (Letöltve: 2009. 08. 30.)

[37] Kopp, Carlo: The E-bomb – A Weapon of Electrical Mass Destruction http://www.jya.com/ebomb.htm (Letöltve: 2009. 08. 30.)

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Regionális Fejlesztési Alap társfinanszírozásával valósul meg.