HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Papp Zoltán
pappz.szeged@gmail.hu

IRÁNYÍTOTT ENERGIÁJÚ FEGYVEREK VESZÉLYEI A KOMMUNIKÁCIÓS HÁLÓZATOKRA

Absztrakt

Az információs társadalmat átszövő infokommunikációs hálózatok folyamatos rendelkezésre állása kiemelt fontosságú, mivel az azok által nyújtott szolgáltatások hozzájárulnak a társadalom, az egyének, illetve a gazdaság szereplőinek egymás közötti kapcsolatainak létrejöttéhez, fenntartásához, valamint a védelmi szféra, az államigazgatás működéséhez. A kérdéses rendszerek biztonságára azonban veszélyt jelenthetnek a különböző motivációkkal rendelkező támadók, akik különböző típusú és fejlettségű elektromágneses fegyverekkel hatékonyan képesek pusztítani a kérdéses hálózat elemeit.

The constant availability of infocommunication networks intertwined with modern information society is of utmost importance, since their services contribute to the establishment and maintenance of relationships among the society, the individuals and the economic actors as well as the operation of the defense sphere and public administration. The security of the systems in question may be threatened by attackers with various motives who can efficiently destroy the elements of such networks by applying various types of radio frequency weapons.

Kulcsszavak: *infokommunikációs hálózatok, infokommunikációs hálózatok pusztítása, rádiófrekvenciás fegyverek, információs társadalom ~ infocommunication networks, destroying of infocommunication networks, radio frequency weapons, information society*

BEVEZETŐ

Napjaink információs társadalmának működéséhez elengedhetetlen az, hogy az infokommunikációs hálózatok technikai eszközei, berendezései megbízhatóan üzemeljenek, mivel ezek biztosítják az egyének, illetve a különböző szervezetek információs folyamatainak a folytonosságát.

A modern félvezető elektronika már lehetővé teszi, hogy ezekbe a hálózatokba beépítésre kerülő eszközök egyre kisebb méretűek legyenek, és egyre nagyobb alkatrész-sűrűségű integrált áramkörökből épüljenek fel, melyek egyre nagyobb hatékonyságot biztosítanak. Az egyre nagyobb műszaki és gazdasági hatékonyság érdekében az infokommunikációs hálózatokat üzemeltető szolgáltatók az elvárt műszaki paraméterekhez pontosan illeszkedő alkatrészeket szereznek be, azok azonban szélsőséges terhelésekre, extrém környezeti viszonyokra nincsenek méretezve. Az eszközök méretének csökkenésének egyik következménye az, hogy – a miniatürizálást lehetővé tevő technológia jellegéből adódóan – csökken a rétegvastagságuk, ami miatt érzékenyebbek válnak a túlfeszültségre. Amennyiben az ilyen berendezések környezetében intenzív elektromágneses térerősség változás történik, akkor a belső vezetékhálózatokon kritikus nagyságú feszültség indukálódhat, ami ennek következtében a félvezető rétegek között átütést okozhat. A villamos átütések a félvezetőkben javíthatatlan károkat idéznek elő.

A fenti jelenséget kihasználva az infokommunikációs hálózatok berendezései hatékonyan rombolhatók lehetnek a különböző elven működő rádiófrekvenciás fegyverekkel. E fegyvertípusok képesek lennének egy adott földrajzi területen kiiktatni a kérdéses rendszereket, illetve minden hasonló elektronikai eszközt, valamint az általuk nyújtott szolgáltatásokat, melyek helyreállítása a nagy költség mellett sok időt is követel.

A veszélyeztetett eszközök

A bázisállomások technológiájának elméletét az amerikai Bell Labs mérnökei már 1947-ben kifejlesztették az AT&T telefontársaságnál, és folyamatosan fejlődik napjainkban is. A bázisállomások kifejlesztésével párhuzamosan hozták létre a rádiótelefonok nulladik (0G) generációját is, azonban ezeket a szakirodalom nem sorolja be a mobiltelefonok közé, mivel még nem voltak képesek a kommunikációs csatorna frekvenciájának automatikus váltására, a beszélgetés csak egy bázisállomáson (cella) keresztül folyt, ami azt jelentette, hogy a beszélgetés ideje alatt folyamatosan a kérdéses bázisállomás hatósugarában kellett tartózkodni. A hívásátadás – a mozgásból adódó cellaváltás lehetőségének – problematikája az 1970-es években oldódott meg, és így vált a rádiótelefon mobiltelefonná. Kezdetekben ezeket a készülékek robosztus méretükből adódóan főleg gépkocsikban alkalmazták, de az elektronika fejlődése révén az 1980-as évektől már kézi kivitelben is elérhetőek lettek, és mivel előállításuk viszonylag olcsó, könnyen fejleszthetők, ezért a mobiltelefon-hálózatok rohamos gyorsasággal terjedtek el a világban.

Napjainkban a mobiltelefonok, illetve az egyéb mobilkommunikációs berendezések már a legelterjedtebben és a leggyakrabban használt eszközeink közé tartoznak. A készülékekbe integrált, illetve általuk a kibernetikus térben elérhető szolgáltatásokra az információs társadalom tagjai, valamint gazdasági, közigazgatási és rendészeti szervezetei életük és működésük során fontosabb és kevésbé fontosabb részterületén egyaránt számítanak. Az információs társadalom egyre növekvő igényei miatt a városok – ahol az információ felhasználói legnagyobb létszámban vannak jelen – egyre sűrűbben be lesznek hálózva az infokommunikációs hálózatok eszközeivel.

A nagyfokú fejlettség az infokommunikációs infrastruktúrákban egyben kiszolgáltatottá is teszi a társadalmat, mivel a hálózatokban keletkezett véletlen vagy épp szándékosan előidézett zavarok azonnal a társadalom széles körét érintik, és más infrastruktúrákba is átgyűrűznek, így tovább szélesítve a negatív hatások körét. A jelenség, miszerint az információs társadalom számos folyamata a mobilkommunikációs eszközök révén is elérhető kibernetikus térben zajlik, értelemszerűen elhozta azt a következményt, hogy a különböző indíttatású támadók igyekeznek hozzáférni, befolyásolni az infokommunikációs hálózatokban kezelt információkat, adatokat, illetve a rendszer szolgáltatásaiban zavarokat okozni, ezáltal másodlagos következmény formájában érni el a kívánt célt.

Az infokommunikációs rendszerekben zavart okozni kívánó támadónak számos eszköz és módszer állhat rendelkezésére, hogy célját elérje. Az érintett rendszerekben kezelt információ bizalmasságát, titkosságát számos módszerrel (például titkosítással) védik, így az információ tartalma ellen indított támadások nagy szakértelmet, modern eszközparkot és számítási kapacitást igényelnek. Azokban az esetekben, amikor a támadó nem a rendszerekben kezelt információ tartalmát kívánja megváltoztatni, manipulálni, hanem csak magának az információnak az elérhetőségét, hozzáférhetőségét akarja akadályozni, kevésbé szofisztikáltabb lehetőségek is rendelkezésére állnak. A szóba kerülhető módszerek nagyban függnek a támadó támadási potenciáljától, mely azt mutatja meg, hogy a fenyegető tényezők összessége mennyire képes kompromittálni az információs rendszer biztonságát. A potenciál mértékét befolyásolja a támadó szakértelme, a rendelkezésére álló erőforrások és technikai eszközök, valamint motivációja.

Elektromágneses fegyverek

A fizikai pusztítás eszközeivel a mobiltelefon-technológia sajátosságaiból adódóan egy földrajzi területen egy időben elérhető, szétszórtan elhelyezkedő bázisállomások lerombolása nehezen kivitelezhető. További nehézség, hogy a felhasználóknál lévő mobil kommunikációs eszközök – nagy számuk, szétszórt és rejtettnek tekinthető elhelyezkedésük révén – e módszerrel egy időben nem iktathatók ki.

Egy kérdéses területen a mobil kommunikációs rendszerek elemei azonban nagy hatékonysággal pusztíthatók elektromágneses fegyverekkel. A nagy energiájú rádiófrekvenciás sugarak alkalmazásának célja a felvezetők károsítása, a mikroáramkörök (processzorok, memóriák) túlterhelése, a villamos alkatrészek szigeteléseinek átütése és ezáltal az elektronikai eszközök tönkretétele. [1] Az elektromágneses impulzusok elleni védekezésnek csupán gazdasági korlátai vannak, a berendezések gyártóinak – elsődlegesen a megrendelők gazdaságossági szempontjainak tükrében – kell azt eldönteniük, hogy mit és mi ellen védjenek.

A nagy erejű professzionális fegyverek elvileg csak a hadseregek eszköztárában lelhetők fel, de léteznek kisebb erejű, készre gyártott, sőt elvileg megvásárolható változatok is:

1. ábra. EMP mikrohullámú sütőből
(forrás: www.fegyverlabor.hu)

2. ábra. Az Internetről rendelhető EMP eszközök (forrás: http://www.amazing1.com/emp.htm)

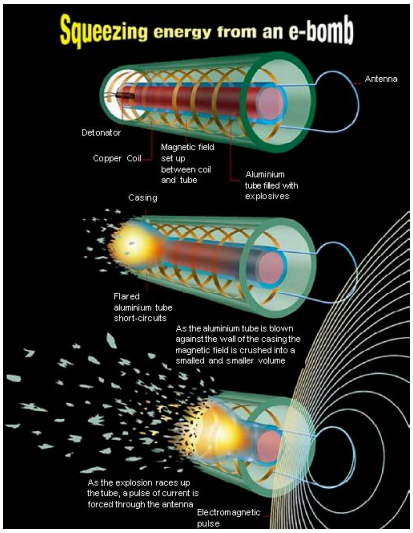
Ugyanakkor ezek az eszközök kereskedelemi forgalomban kapható alkatrészekből is összeállíthatók, melyeket a támadók (terroristák) könnyedén felhasználhatnak céljaik elérése érdekében. Felhasználható az egyszerű mikrohullámú sütő magnetronjától kezdve, régi televíziós készülékek feltöltött képcsövéig, a fényképezőgépek nagyteljesítményű vakujáig minden.

Ezen eszközök működési elve csaknem azonos. Feltölteni egy energiatárolót, ami akár egy egyszerű fényképezőgép vakujában található kondenzátor is lehet, és adott időben és helyen a lehető legrövidebb idő alatt kisütni. [1]

A nagy energiájú rádiófrekvenciás fegyverek közül az elektromágneses impulzusbomba (EMP) a leghatékonyabb, melynek vannak nukleáris (NEMP) és nem nukleáris (NNEMP) alapú implementációi is. A hidegháború elmúltával a nukleáris alapú elektromágneses impulzus fegyverek háttérbe szorultak, de a nem nukleáris alapú eszközök fejlesztése töretlen. A NNEMP fegyverek lényegesen szűkebb tartományban (kisebb hatóerővel, kisebb hatókörrel) működnek, azonban másodlagos hatásaik (például radioaktivitás) nincsenek, vagy elhanyagolhatók, így alkalmazhatók precíziós csapásokat igénylő műveletekben. A nem nukleáris elektromágneses impulzusfegyverek többféle megoldást használnak a nagy energiájú elektromágneses lökéshullám előállítására.

A rádióhullámok fegyvertechnikai alkalmazása esetén meg lehet különböztetni:

- impulzusüzemű, és
- periodikusan rádióhullámokat sugárzó rádiófrekvenciás fegyvereket.



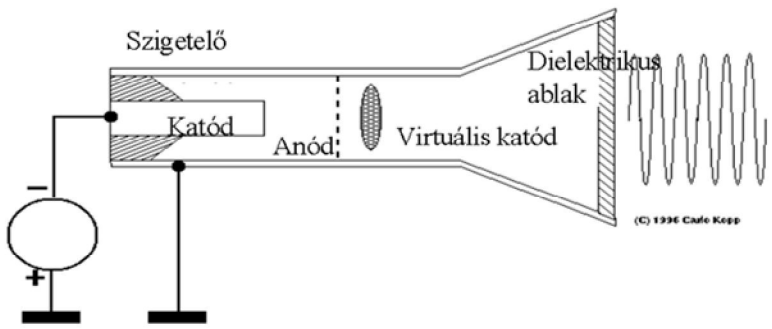
3. ábra. Az E-bomba működése (forrás: www.countdown.org/end/pix/ebomb.jpg)

Az ilyen fegyverek három részből állnak: egy energiaforrásból, melyek a mikrohullámok generálásához szükséges nagy mennyiségű statikus energiát tárolják, egy mikrohullámot generáló eszközből, és egy antennából, mely a kívánt irányba sugározza a generált mikrohullámokat. Az energiát tároló eszköz lehet Marx generátor vagy fluxus kompressziós generátor. A fluxus kompressziós generátor több MJ energiájú elektromos energiát képes előállítani rövid (10-100 μs) ideig. A viszonylag kisméretű eszköz több MW impulzusteljesítményű energiaforrásnak számít. Működési elve azon alapul, hogy egy induktív energiatárolóban tárolt elektromágneses energiát robbantással, a tekercs meneteinek rövidre zárásával áramimpulzussá alakítja. Mivel az impulzusbombában alkalmazott fluxus kompressziós generátort a robbanótöltet hozza működésbe, ennek következtében az eszköz megsemmisül. [2]

A Marx generátor számos kaszkádba kapcsolt kondenzátort alkalmaz, melyek mindegyike párhuzamosan kapcsolódik a töltőrendszerre, így ugyanarra a feszültségre van feltöltve. A kondenzátorok szikraközökkel vannak elválasztva egymástól. A generátor elsütésekor a szikraközök begyújtanak és az addig párhuzamosan kapcsolt kapacitásokat a kimenet felől tekintve sorba kapcsolják, így nagyfeszültséget generálnak ezzel. Az impulzus időtartama 4-100 ns, de ez idő alatt több száz A nagyságú áram folyhat az elektromágneses hullámot gerjesztő eszközben. [1]

A folytonos, periodikus jel előállítására alkalmas eszközök közül legelterjedtebb a virtuális katódú oszcillátor, amely a rádiófrekvenciás fegyverek abba a csoportjába tartozik, amely – a fluxus kompressziós generátort használó fegyverekkel ellentétben – többször is felhasználható. [3]

4. ábra. Vircator
(forrás: www.amazing1.com/emp.htm)



5. ábra. Elvi felépítése
(forrás: www.amazing1.com/emp.htm)

Az NNEMP fegyverek talán legveszélyesebb tulajdonsága az, hogy viszonylag távolról is alkalmazhatóak, a támadásra való felkészülés nehezen észlelhető, a támadásnak pedig külső jele nincs. A sikertelen támadásnak nyoma nem marad, egy sikeres támadásnál pedig a megtámadott kommunikációs rendszerek üzemeltetői és felhasználói csak a hatást, azaz eszközeik tönkremenetelét érzékelik.

ÖSSZEGZÉS

Az információs társadalom modern nagyvárosaiban az infokommunikációs hálózatok eszközei a speciális környezeti jellemzőkből adódóan nagy sűrűséggel vannak telepítve, így egy elektromágneses támadás nagyszámú berendezésben tehet kárt, melyek helyreállítási költségei jelentősek lehetnek. A fizikai károkon túl további veszteségek jelentkezhetnek a kieső szolgáltatások révén, valamint szervezetek esetében számolni kell a jelentkező bizalomvesztéssel is.

Ilyen típusú fegyverek alkalmazásának lehetősége egyre valószínűbb, mivel a megalkotásukhoz szükséges tervrajzok megtalálhatók az Interneten, a szükséges alkatrészek kereskedelmi forgalomban beszerezhetők és kisebb gyakorlattal házilag is megalkothatók, így pedig a potenciális támadók köre – túl a hadseregeken, terroristákon – lényegesen kiszélesedhet. A kevésbé elszánt, kisebb támadó potenciállal rendelkező támadók részéről nem az egyszer használható, robbanással működésbe hozható eszközök alkalmazására lehet elsősorban számítani, hanem a többször felhasználható – bár kisebb hatótávolságú és hatékonyságú – berendezések használata merülhet fel.

Prognosztizálható, hogy az információs infrastruktúrák üzemeltetőinek, illetve az ő hálózatukon kiemelt jelentőségű szolgáltatásokat nyújtó felhasználóknak a fontosabb elektronikus eszközeik védelmének szintjének emelésére az elkövetkezendő időszakban fokozott figyelmet kell fordítaniuk.

Felhasznált irodalom

[1] Dr. Kovács Tibor - A terroristák láthatatlan fegyverei (ZMNE Terrorizmus Konferencia 2006.)

[2] Csuka Antal, Előházi János - Irányított energiájú fegyverek és veszélyeik a számítógépes rendszerekre (Hadmérnök, III. Évfolyam 3. szám. 2008. szeptember, ISSN 1788-1919);

[3] Dr. Ványa László - Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre (Doktori (PhD) értekezés, ZMNE, Budapest, 2001.)