HADMÉRNÖK

III. Évfolyam 2. szám - 2008. június

Kovács László
Zrínyi Miklós Nemzetvédelmi Egyetem
kovacs.laszlo@zmne.hu

AZ INFORMÁCIÓS TERRORIZMUS ELLENI TEVÉKENYSÉG KORMÁNYZATI FELADATAI

Absztrakt

A kritikus információs infrastruktúráink magukban hordozzák annak a veszélyét, hogy ezeket olyan terroristatámadás éri, amelyek ezeken az információs rendszereken keresztül valósulnak meg, vagy pont azokat célozzák meg. Jelen írás arra keresi a választ, hogy milyen szerepe lehet a kormánynak abban, hogy ezeket az információs infrastruktúrákat a lehető leghatékonyabb védelemmel lássa el.

Our critical information infrastructures include the potential threats of terrorist attack. These systems could become targets of terrorist attack, or the raid will execute through these systems. The main aim this paper to identify the possible action taken by the government to protect our essential infrastructure.

Kulcsszavak: *kritikus információs infrastruktúra, terrorizmus, kormányzat ~ critical information infrastructure, terrorism, government*

BEVEZETÉS

A kritikus információs infrastruktúrák sebezhetősége az egész társadalom számára rendkívül nagy veszélyt jelent. Amennyiben a terrorizmus kihasználja ezt a sebezhetőséget, akkor a 2001. szeptember 11-i támadások következményeinél hatványozottabban nagyobb károkat szenvedhetünk el.

A kritikus infrastruktúrák és azok azonosítása azonban korántsem egyszerű és nagyon sokszor nem is egyértelmű kérdés. A következő nehéz feladat, hogy a kritikus infrastruktúrákon belül megtaláljuk és azonosítsuk, melyek azok a rendszerek, amelyek kritikus információs infrastruktúrának tekinthetők. E kérdés jelentősége abban mutatkozik meg, hogy amíg a kritikus infrastruktúrák esetében a fenyegetések és a veszélyek jórészt a hagyományos támadások (robbantások, fizikai károkozások, stb.) kategóriájába sorolhatók,

addig a kritikus információs infrastruktúrákat ezektől a hagyományos veszélyektől merőben eltérő – az *információs térből*[1] érkező – veszélyek és kihívások fenyegetik.

Hazánkban a kritikus infrastruktúrák vonatkozásában a napokban jelent meg hivatalosan a várva várt, úgynevezett Zöld Könyv[2], amely a hazai kritikus infrastruktúra védelemről rendelkezik. Ez a dokumentum, illetve kormányhatározat már tartalmaz utalásokat és némi kategorizálást a kritikus információs infrastruktúrák vonatkozásában, ugyanakkor a fogalom meghatározása, azaz, hogy mit tekintünk kritikus információs infrastruktúrának, annak részletes felsorolása, osztályozása, valamint a védelem konkrét feladatainak leírása mindezidáig hivatalosan, kormányzati szinten nem történt meg.[3]

Jelen írás azokat a legfontosabb szempontokat igyekszik számba venni, amelyek elengedhetetlenül fontosak ahhoz, hogy a kormányzat és a piaci élet szereplői[4] koordináltan felkészüljenek a kritikus információs infrastruktúrák védelmére, illetve egy esetlegesen bekövetkező támadás esetén a következmények mielőbbi felszámolására.

TÁMADÁSOK AZ INFORMÁCIÓS RENDSZEREKEN KERESZTÜL

Gyakran elhangzó kérdés, hogy amennyiben valóban fennáll az előbb említett információs infrastruktúra sebezhetősége, akkor mindezidáig miért nem következett be komolyabb támadás, amely ezeket a rendszereinket érte volna?

Ennek kiderítése meghaladja jelen írás terjedelmi korlátait és valódi célkitűzéseit is. Az azonban kijelenthető, hogy voltak már kisebb-nagyobb támadások, amelyek elsősorban az interneten keresztül történtek, vagy amelyek éppen annak működésképtelenné tételét próbálták meg elérni. Ezek közül a támadások közül azonban nem mindegyik került nyilvánosságra. Ugyanakkor a nyilvánossá vált támadások közül is számos esetben felmerült a bizonyíthatóság problémája. Mindezek mellett fontos megemlíteni, hogy néhány bekövetkezett információs támadást terrorista szervezetek, vagy az általuk felbérelt csoportok követték el. Ez pedig világosan előrevetíti annak lehetőségét, hogy a különböző terrorszervezetek a jövőben is élni fognak ezzel a hatékony – bár nem mindig egyértelműen „médiásítható” – fegyverrel.

A következőkben néhány bekövetkezett információs (informatikai) támadást mutatunk be nagyon röviden.

Támadások

Nagyon sokáig az első és egyetlen cyberterrorista akcióként[5] aposztrofálták az LTTE (Tamil Eelam Felszabadító Tigrisei) nevéhez fűződő támadást, amely során 1997-ben a szervezet aktivistái spamekkel árasztották el a világ különböző országaiban működő srí lankai követségek e-mail postaládáit, válaszul néhány tagjuk bebörtönzésére. Az akció nagy kárt

[1] Információs dimenzióból

[2] A Kormány 2080/2008. (VI.30.) Korm. határozata a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.

[3] Általánosságban már több kutatócsoport is meghatározta, majd osztályozta ezeket a rendszereket, amelyek talán a kormányzati munka kiinduló alapjai is lehetnének.

[4] Mivel az infrastruktúrák jelentős része, így a kritikus infrastruktúrák és a kritikus információs infrastruktúrák többsége is gazdasági társaságok tulajdonában vagy üzemeltetésében van, ezért az világosan látszik, hogy azok védelme nem csak kormányzati, hanem közös – a tulajdonosokkal és az üzemeltetőkkel koordinált – tevékenységeket kell, hogy takarjon.

[5] Ezen a helyen azokat a támadásokat is cybertámadásoknak tekintettük, amelyeket hagyományos terrorszervezetek, vagy olyan csoportok, személyek követtek az interneten keresztül, amelyek terrortámadásnak minősíthetőek.

nem okozott, de felhívta a figyelmet az információs rendszerek sebezhetőségére, illetve arra a tényre, hogy a hagyományos terrorista szervezetektől sem áll távol az információs támadás.[1]

1997 júliusában e-mail bombatámadás érte az Institute for Global Communications (IGC) amerikai internetszolgáltatót, akik az Euskal Herria (Baszk Újság) honlapját tartották fenn. A támadás a honlap eltávolítását követelte. [2]

2000 márciusában a Japán rendőrség bejelentett, hogy több mint 150 rendőrségi gépjármű számítógépes rendszerében olyan kémprogramokat találtak, amelyeket többek között követésre, valamint adatlekérésre programoztak. A vizsgálat kiderítette, hogy a gépjárművek fedélzeti szoftvereit az Aum Shinryko[6] terrorista csoporthoz köthető egyik vállalkozás fejlesztette. (Ez a terrorista a csoport követte el a Tokiói metróban, 1995-ben a 12 halálos, és több mint 6000 sérültet okozó szaringáz támadást). A szoftverek segítségével 115 rendőrségi gépjármű helyét követték, amelyek között több civil autó is volt. A további vizsgálatok rámutattak, hogy a csoport több mint 80 japán cég és 10 kormányzati szerv számára szállított szoftvereket korábban. Ezekbe a leszállított szoftverekbe trójai programokat telepíttettek egy későbbi terrortámadás elősegítésére. [3]

2002 októberében az internet legfontosabb infrastruktúrái ellen indult összehangolt támadás. Ekkor a 13 DNS[7] root szerver ellen követtek el DoS[8] illetve DDoS[9] támadásokat. Ez a fajta támadás 2007 februárjában megismétlődött. Szerencsére egyik esetben sem sikerült komoly fennakadást okozni a nemzetközi internet forgalomban, amely egyrészt annak köszönhető, hogy a 13 root szerver több mint 40 helyen tükrözve van. [4]

2003-ban román elkövetők megzsarolták az amerikai National Science Foundation-t (NSF), hogy eladják a szervezet feltört és így nagymértékben feltérképezett számítógépes hálózatának adatait, amennyiben nem kapnak megfelelő anyagi ellenszolgáltatást. Ez a hálózat irányította a Déli-sarkon lévő NSF által fenntartott kutatóbázis energiaellátását és fűtését. Miután bebizonyosodott a fenyegetés valódisága, le kellett választani a kutatóbázis hálózatát. [5]

2004-ben történt, a később Titan Rain-nek keresztelt támadás, amelynek során feltételezhetően kínai hackerek bejutottak az amerikai védelmi minisztérium számára is fejlesztő Lockheed Martin számítógépes hálózatába és onnan érzékeny adatokat szereztek meg. [6]

2007 áprilisában és májusában DDoS támadások érték Észtország számítógépes hálózatait. Az egyébként igen fejlett információs infrastruktúrával rendelkező, és az e-kormányzat területén komoly sikereket elért Észtország, a több mint kéthetes támadás során komoly anyagi károkat szenvedett, mert számos kormányzati, minisztériumi és több bank internetes oldala vált elérhetetlenné a támadások következtében. A támadások a tallinni orosz emlékmű elmozdítása után kezdődtek, és nagy részük többé-kevésbé beazonosíthatóan Oroszországban működtetett szerverekről indult. Az észt miniszterelnök az orosz kormányt tette felelőssé a támadások miatt. Oroszországot korábban Ukrajna és az Egyesült Államok is megvádolta hasonló támadások végrehajtásával, de Moszkva minden alkalommal határozottan tagadta részvételét az akciókban. Az online támadások alatt összesen 128 túlterheléses támadás történt, a legkomolyabbak öt-tíz órán át, több száz megabitnyi sávszélességen bombázták folyamatos adatlekérésekkel a megtámadott szervereket, addig amíg azok össze nem omlottak. Az észt hálózaton az adatforgalom esetenként órákon át a normális ezerszerese volt. Ehhez egyes források szerint valószínűleg az internetes alvilágtól kellett erőforrásokat bérelnie a támadóknak. Érdemes megjegyezni, hogy közel fél évvel a támadások után csak

[6] Ez a terrorista a csoport követte el a Tokiói metróban, 1995-ben a 12 halálos, és több mint 6000 sérültet okozó szaringáz támadást.
[7] Domain Name Server
[8] DoS: Denial of Service, azaz túlterheléses támadás.
[9] DDoS: Distributed Denial of Service, azaz elosztott túlterheléses támadás.

egyetlen támadót sikerült bizonyíthatóan azonosítani. Meglepő módon azonban ez a támadó egy észt fiatalember volt, akit a bizonyítékok alapján pénzbüntetésre ítéltek. [7]

A cyber- és az információs terrorizmus

A fenti információs (informatikai) támadások tanulmányozása esetén nyilvánvalóan kitűnik, hogy a terrorista szervezetek is egyre inkább használják az információs rendszereket, magát az internetet, sőt támadásaikat azon keresztül is kivitelezhetik. Ennek kapcsán felmerül a cyberterrorizmus kérdése.

A témában a cyberterrorizmusra vonatkozó egyik legelső meghatározás az FBI úgynevezett cyber részlegének volt vezetőjétől – Keith Lourdeau-tól – származik: „*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.*" [8]

Mindezek alapján az nyilvánvaló és jól következtethető, hogy a hagyományos terrorizmus, illetve a cyberterrorizmus közös, esetenként egymást kiegészítő, párhuzamos támadásai a legsebezhetőbb és 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 definíciószerűen megfogalmazva: „*a cyber-támadásokat és a hagyományos terrortámadásokat egyszerre alkalmazó olyan terrortevékenység, amely az információs infrastruktúrákat felhasználva, a kritikus információs infrastruktúra elleni támadásokkal próbálja meg célját elérni*." [9]

A KRITIKUS INFRASTRUKTÚRA ÉS A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA MEGHATÁROZÁSA MAGYARORSZÁGON

Kutatók már korábban megállapították, hogy 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."* [10]

Ugyanakkor, amennyiben a kritikus infrastruktúrák illetve a kritikus információs infrastruktúrák részleges, időleges, vagy akár teljes kiesése vagy leállása esetén megvizsgáljuk azokat a hatásokat, amelyek ennek következményeként fellépnek, akkor a következő kategorizálást tudjuk megtenni [11; 12]:

- Kiterjedés[10]: a kritikus infrastruktúra, illetve azok egyes elemeinek kiesése esetén jelentkező negatív hatás annak a földrajzi területnek nagysága alapján jellemezhető és osztályozható, amelyet a veszteség vagy az adott szolgáltatás megszűnése érinthet. Mivel infrastruktúráink több földrajzi régiót érintve egymással kapcsolatban vannak, több földrajzi régiót érintve, ezért ezt a kategóriát nemzetközi, nemzeti és regionális szintekre is fel lehet osztani.
- Nagyságrend: az infrastruktúra meghibásodásából vagy kieséséből fakadó hatás mértékét jelenti, amely a társadalom, a gazdaság és a kormányzat esetében jelenik meg. Ezt a

[10] A kiterjedést sok esetben hatókörként is értelmezik, melynek tartalma megegyezik az itt leírtakkal.

következőképpen lehet értékelni: nincs hatás, minimális, mérsékelt vagy jelentős hatás. A nagyságrend megállapításához a következő szempontokat szükséges figyelembe venni:
    - társadalmi hatás (népességre gyakorolt hatás): a szolgáltatás kiesése miatt érintett lakosság, azaz a szolgáltatást igénybe vevők száma;
    - gazdasági hatás: a gazdasági veszteség jelentősége, illetve a termékek és szolgáltatások színvonalában mérhető negatív változás mértéke. Ebbe a hatásba tartozik az infrastruktúra fizikai sérüléséből, elvesztéséből fakadó közvetlen (azaz a sérült infrastruktúra értéke, annak pótlásának költsége) vagy a közvetett (pl. piacra gyakorolt negatív hatás) károk;
    - környezeti hatás: az infrastruktúra működésképtelensége miatt bekövetkezett környezeti kár mértéke;
    - politikai hatás: az állami intézmények iránti bizalom csökkenése, vagy az állami szervek működőképességének csökkenése;
    - közegészségügyi hatás: áldozatok száma, betegségek, esetleges járványok, súlyos sérülések, stb. hatása;
    - pszichológiai hatás: lakosság magatartásának megváltozása;
    - kölcsönös függőségi hatás: azoknak az interdependáns rendszereknek, illetve elemeknek az elemzése és értékelése, amelyek az adott infrastruktúrát, az adott vagy tágabban kapcsolódó szektort, illetve a nemzeti és nemzetközi viszonylatban felmerülő függéseket meghatározzák, befolyásolják.
- Időbeli hatás: annak meghatározása, hogy az adott infrastrukturális rendszerrel, vagy rendszer-elemmel kapcsolatos veszteség mennyi idő elteltével fejt ki komoly hatást (azonnali, 24–48 óra, egy hét, stb.), illetve mennyi ideig tart ez a hatás.

A már említett hazai Zöld Könyv immár hivatalosan is meghatározza a kritikus infrastruktúra fogalmát: „*Kritikus infrastruktúra alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot feltárásában*.” [12]

Az 1. Táblázat bemutatja, hogy a hazai Zöld Könyv milyen ágazatokra és alágazatokra bontja a hazai kritikus infrastruktúrákat. Érdemes megjegyezni, hogy a kormányhatározat 2. melléklete felelősöket is hozzárendel – hasonlóan az USA ilyen irányú rendelkezéséihez[11] – a felsorolt ágazatokhoz.

Mielőtt a táblázatban felsorolt kritikus infrastruktúrákat kritikus információs infrastruktúra szempontból megvizsgálnánk, célszerű meghatározni, hogy mit is értünk a kettő különbségén. A kritikus infrastruktúra meghatározást már láthattuk. Ugyanakkor a kritikus információs infrastruktúra nem minden esetben egyezik meg a kritikus infrastruktúrával. 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.)”*. [13]

[11] pl.: a Bush elnök által kiadott 7/HSPD-7 elnöki direktíva [14]

1. Táblázat: Kritikus infrastruktúra ágazati, alágazati és felelősi besorolás a hazai Zöld Könyv alapján [12]

Ágazat	Alágazat	Felelős
I. Energia	1. kőolaj kitermelés, finomítás, tárolás és elosztás 2. földgáztermelés, tárolás, szállítás és rendszerirányítás, elosztás 3. villamosenergia-termelés, átvitel és rendszerirányítás, elosztás	KHEM
II. Infokommunikációs technológiák	4. információs rendszerek és hálózatok 5. eszköz-, automatikai és ellenőrzési rendszerek 6. internet, infrastruktúra és hozzáférés 7. vezetékes és mobil távközlési szolgáltatások 8. rádiós távközlés és navigáció 9. műholdas távközlés és navigáció 10. műsorszórás 11. postai szolgáltatások 12. kormányzati informatikai, elektronikus hálózatok	MeH EKK, KHEM
III. Közlekedés	13. közúti közlekedés 14. vasúti közlekedés 15. légi közlekedés 16. vízi közlekedés 17. logisztikai központok	KHEM
IV. Víz	18. ivóvíz szolgáltatás 19. felszíni és felszín alatti vizek minőségének ellenőrzése 20. szennyvízelvezetés és -tisztítás 21. vízbázisok védelme 22. árvízi védművek, gátak	KvVM
V. Élelmiszer	23. élelmiszer előállítás 24. élelmiszer-biztonság	FVM
VI. Egészségügy	25. kórházi ellátás 26. mentésirányítás 27. egészségügyi tartalékok és vérkészletek 28. magas biztonsági szintű biológiai laboratóriumok 29. egészségbiztosítás	EüM
VII. Pénzügy	30. fizetési, értékpapírklíring- és elszámolási infrastruktúrák és rendszerek 31. bank és hitelintézeti biztonság	PM
VIII. Ipar	32. vegyi anyagok előállítása, tárolása és feldolgozása 33. veszélyes anyagok szállítása, 34. veszélyes hulladékok kezelése és tárolása, 35. nukleáris anyagok előállítása, tárolása, feldolgozása 36. nukleáris kutatóberendezések 37. hadiipari termelés 38. oltóanyag és gyógyszergyártás	KHEM, HM, ÖM (OKF), IRM (OAH) NFGM
IX. Jogrend – Kormányzat	39. kormányzati létesítmények, eszközök 40. közigazgatási szolgáltatások 41. igazságszolgáltatás,	IRM, ÖM, HM
X. Közbiztonság – Védelem	42. honvédelmi létesítmények, eszközök, hálózatok 43. rendvédelmi szervek infrastruktúrái	IRM, HM, ÖM (OKF)

Amennyiben ez utóbbi megfogalmazást elfogadjuk a kritikus információs infrastruktúrára vonatkozónak, akkor az előbbi táblázatból – azaz a hazai kritikus infrastruktúrák felsorolásából – jól látszik, hogy bár a *II. Infokommunikációs technológiák* ágazat, illetve az itt meghatározott alágazatok – információs rendszerek és hálózatok; eszköz-, automatikai és ellenőrzési rendszerek; internet, infrastruktúra és hozzáférés; vezetékes és mobil távközlési szolgáltatások; rádiós távközlés és navigáció; műholdas távközlés és navigáció; műsorszórás; postai szolgáltatások; kormányzati informatikai, elektronikus hálózatok – kritikus információs infrastruktúráknak tekinthetők, mégis számos más ágazatban is találhatunk olyan rendszert vagy elemet, amely kritikus információs infrastruktúrának minősül. Többek között ilyen rendszer vagy elem az *Energia* ágazatban több alágazatnál említett rendszerirányítás is.

Korábbi tanulmányok már többször – természetesen esetenként a vizsgálatot végző csoport szakmai kompetenciáját, vagy megközelítési módszereit tükröző módon, de többnyire egyöntetűen, illetve egymástól csak kis mértékben eltérve – megállapították, hogy hazánkban melyek minősülhetnek kritikus információs infrastruktúrák. Ezek közül a kritikus információs infrastruktúra-csoportosításokból kettőt kívánunk bemutatni.

Az első felosztás alapvetően az információs rendszereket – ezek közül is az egyik legsérülékenyebbeket, a számítógép-hálózatokat – vette alapul a felosztás megalkotásakor. E felosztás szerint a következők minősülhetnek kritikus információs infrastruktúrának:

- 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 információs rendszerek. [9; 15]

A másik bemutatandó felosztás már nem csak a számítógép-hálózatokat, hanem a tágabb értelemben vett infokommunikációs eszközöket és rendszereket helyezte a vizsgálat homlokterébe. Ennek megfelelően a Magyar Köztársaság kritikus információs infrastruktúrái közé tartoznak:

- informatikai rendszerek és hálózatok;
- automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek, stb.);
- internet szolgáltatás (infrastruktúra is);
- vezetékes távközlési szolgáltatások;
- mobil távközlési szolgáltatások;
- rádiós távközlés és navigáció;
- műholdas távközlés;
- műsorszórás;
- közigazgatási informatika és kommunikáció;
- a kritikus infrastruktúrák létfontosságú infokommunikációs rendszerei. [11]

A két felosztás – bár látszik a vizsgálati szempontok alapján a különbség – mégis nagyon sok hasonlóságot, sok átfedést tartalmaz.

Összességében tehát megállapíthatjuk, hogy számos kritikus infrastruktúra önmagában, vagy egyes részeiben és elemeiben is kritikus információs infrastruktúra, ugyanakkor a fenti két felosztást kiemelve a kritikus információs infrastruktúrák alapvetően infokommunikációs rendszerek. Ezek sérülékenysége – a hathatós védelmi intézkedések, ajánlások és szabályzók ellenére – igen magas. Tovább nehezíti a kérdést, hogy sok esetben ezek az infokommunikációs rendszerek azok, amelyek a már említett kritikus infrastruktúrák közötti interdependenciát jelentik, azaz pont ezek azok a rendszerek, amelyeken keresztül

infrastruktúráink összekapcsolódnak. Ez az összekapcsolódás lehet fizikai, de lehet logikai is, hiszen sok esetben az infokommunikációs rendszerek által összegyűjtött, feldolgozott, majd a megfelelő helyre eljutatott adat vagy információ jelenti a kapcsolatot.

Abban az esetben, amennyiben ezek az infokommunikációs rendszerek, azaz kritikus információs infrastruktúrák sérülnek – akár csak időlegesen, vagy akár csak lokálisan –, akkor az a kritikus infrastruktúrák működésére komoly negatív hatással van, azaz azok is működésképtelenné válhatnak.

Ennek megfelelően kijelenthető, hogy a kritikus információs infrastruktúrák jelentik azokat a kulcspontokat, amelyek védelme érdekében mindent meg kell tenni, azaz a kritikus infrastruktúrák védelem területén kiemelt helyen kell kezelni ezeket a rendszereket.

A VÉDELEM KORMÁNYZATI FELADATAI

A már idézett EU Zöld Könyv szerint a kritikus információs infrastruktúra védelme: „a *tulajdonosok, üzemeltetők, gyártók és használók, valamint a hatóságok programjai és tevékenységei, melyek célja fenntartani a kritikus információs infrastruktúra teljesítményét meghibásodás, támadás vagy baleset esetén a meghatározott minimális szolgáltatási szint felett, illetve minimálisra csökkenteni a helyreállításhoz szükséges időt, valamint a károkat.*" [13]

Az EU a védelem érdekében különböző szervezeteket (hálózatokat és projekteket) is létrehozott, illetve a közeljövőben létre fog hozni. Ilyen szervezetek például:

- Kritikus Infrastruktúra Figyelmeztető Információs Rendszer (Critical Infrastructure Warning Information Network — CIWIN[12]);
- Európai Hálózati És Informatikai Biztonság Ügynökség (European Network and Information Security Agency — ENISA);
- Kritikus Információs Infrastruktúra Kutató Koordináció projekt (Critical Information Infrastructure Research Co-ordination — CI2RCO). [13]

A kritikus infrastruktúra illetve a kritikus információs infrastruktúra védelem nem új keletű feladat hazánkban sem. A védelemről már a terrorizmus elleni küzdelem aktuális feladatairól szóló 2112/2004. (V.7) Korm. határozat, illetve annak módosításáról szóló 2046/2007 (III. 19.) Korm. határozat 1. sz. melléklet 2.3.1. pontja is rendelkezik, amely előírja a Kritikus Infrastruktúra Védelem Európai Programjának (EPCIP – European Programme for CIP) megközelítését tükröző, a különböző ágazati feladat- és hatáskörbe tartozó kritikus infrastruktúra védelmi tevékenységek közös keretrendszerbe foglalásáról, ágazatközi összehangolásáról szóló előterjesztés elkészítését. További lépések megtételét írja elő a katasztrófavédelemmel összefüggő 2007. évi feladatokról szóló 1/2007. (III.29.) Kormányzati Koordinációs Bizottság határozat 5. b) pontja, amely értelmében meg kell kezdeni a kritikus infrastruktúra védelem nemzeti programjának kidolgozását, elő kell készíteni a kritikus infrastruktúra védelem hazai koordinációjáról, feladatairól szóló kormány előterjesztést.

Mindezeket figyelembe véve született meg a hazai Zöld Könyv, azaz a Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló kormányhatározat. A dokumentum alapján szükségessé válik az állami és a tulajdonosi feladatok szétválasztása, majd ennek megfelelően a konkrét védelmi tennivalók meghatározása. A Zöld Könyv a következő feladatokat határozza meg a kormány számára:

[12] A hazai Zöld Könyv meghatározza, hogy egy adott konkrét veszély megléte esetén az információknak, illetve a veszélyjelzéseknek a kritikus infrastruktúra tulajdonosok és üzemeltetők, illetve az állami szervek számára is rendelkezésre kell, hogy álljanak. Ezért meg kell vizsgálni azt, hogy a hazai veszélyjelző és jelentő informatikai és kommunikációs rendszer alkalmas-e arra, hogy a CIWIN-nel együtt tudjon működni.

- a nemzeti koordináló szerv és feladatainak meghatározása:
  a hatékonyság és a koherencia megteremtésére szükséges egy nemzeti koordináló szerv felállítása (pl.: Miniszterelnöki hivatalban), amely összefogja, irányítja és elősegíti az eltérő ágazatokban, illetve a kormány és a különböző tulajdonosok közötti kritikus infrastruktúra védelem feladatait;
- a kritikus ágazatok és az ágazati koordináló minisztériumok kijelölése;
- javaslattétel az európai szintű kritikus infrastruktúra elemek kijelölésére. [12]

A Zöld Könyv nem csak a kormány, hanem a központi államigazgatási szervek, illetve a különböző kritikus infrastruktúra elemek tulajdonosainak és üzemeltetőinek is meghatároz számos – a védelem területén igen fontos – feladatot. Ezek azonban többnyire általános, nagyvonalakban meghatározott tevékenységek.

Kritikus információs infrastruktúra szempontból elemezve a dokumentumot, elmondható, hogy a hazai Zöld Könyv nem határoz meg külön feladatokat a hazai kritikus információs infrastruktúrák védelmére, azokat mintegy a kritikus infrastruktúra védelembe érti. Ezt támasztja alá az is, hogy a kormányrendelet a kritikus infrastruktúrákat veszélyeztető tényezők között megemlíti *„a gazdasági, vagy politikai indítékból, kritikus informatikai rendszerek és hálózatok ellen elkövetett visszaélések, illetve cyber-támadások (cyber-terrorizmus, DDOS támadások, tömeges phising incidensek)”* [12] jelentette veszélyeket,[13] ugyanakkor ezekhez a veszélyekhez konkrét védelmi feladatokat nem rendel hozzá.

Mindezek alapján a hazai kritikus információs infrastruktúrák védelmének területén a következő kormányzati feladatok válnak szükségessé:

- meg kell határozni a kritikus információs infrastruktúra hazai fogalmát;
- az ágazati kritikus infrastruktúrák mellett meg kell határozni azokat az elemeket, amelyek kritikus információs infrastruktúraként jelentkeznek;
- fel kell tárni a hazai a kritikus információs infrastruktúrákat fenyegető konkrét veszélyeket;
- elemezni kell, hogy a feltárt veszélyforrások közül, melyik és milyen mértékben érinti a meghatározott kritikus információs infrastruktúrákat, illetve azok egyes elemeit;
- konkrét szimulációkat kell tervezni és szervezni az információs infrastruktúrák körében, amelyek alapján fel lehet tárni azokat a pontokat, kulcsfontosságú elemeket, amelyek a gazdaság, a társadalom és a kormányzat szempontjából létfontosságúak;
- meg kell határozni, és fel kell térképezni a hazai információs infrastruktúrák egymásra, illetve a kritikus infrastruktúrákra gyakorolt közvetlen és közvetett hatásait;
- meg kell határozni, és fel kell térképezni a hazai információs infrastruktúrák környező országok infrastruktúráira gyakorolt hatását;[14]
- a kormányzati koordináló szerv feladatait és résztvevőit ki kell egészíteni a kritikus információs infrastruktúra tulajdonosainak, üzemeltetőinek, illetve a hazai CERT-ek képviselőivel;
- meg kell vizsgálni, hogy alkalmas-e egy esetleges terrortámadás esetén a hazai információs és kommunikációs infrastruktúra a riasztás és a jelzés, majd a vészhelyzeti kommunikáció menedzselésére;
- a tudatos és biztonságos internet-, illetve infokommunikációs eszközhasználatának oktatása, az erre való lakossági felkészítés az eddiginél hatékonyabb és nagyobb szerepet kell, hogy kapjon.

[13] Érdemes megjegyezni, hogy a dokumentum informatikai rendszerek és hálózatokat említ ehelyütt, a tágabb értelemben vett információs rendszerek helyett.

[14] Ezt a feladatot előírja az Európai Bizottság 9403/08-as, az európai kritikus infrastruktúra azonosításáról és megjelöléséről, és azok védelmének növeléséről szóló határozata is. [16]

ÖSSZEFOGLALÁS

Természetesen a fent megfogalmazott kormányzati feladatok önmagukban még nem hozzák meg a kívánt eredményt, azaz nem lesznek „sebezhetetlenek” a kritikus információs infrastruktúráink.

Az azonban teljes bizonyossággal látszik, hogy a védelem lehető legmagasabb szintűre emelése érdekében egy széleskörű, érdekközösségen alapuló összefogásra van szükség, amelyben a kormány mellett a különböző kormányzati szerveknek, a kritikus információs infrastruktúrák tulajdonosainak és üzemeltetőinek, valamint a társadalomnak is komoly szerepe és faladatai vannak.

Ugyanakkor a védelem megteremtése kormányzati és tulajdonosi oldalról sem történhet máshogy, csak koordináltan. E koordináció, pedig a hatékonyság maximalizálása érdekében centralizált kell, hogy legyen.

A védelem hármas célját, azaz a felkészülést a védelemre, a riasztás és jelzés, valamint a folyamatos és kiesés nélküli üzemeltetést, csak abban az esetben lehet megvalósítani, amennyiben a különböző résztvevők – kormány, kormányzati, vagy ágazati szervek, tulajdonosok, üzemeltetők, riasztást és az együttműködők közötti kommunikációt biztosító információs rendszert üzemeltetők – képviselői közösen vesznek részt a koordinációs szerv munkájában.

FELHASZNÁLT IRODALOM:

[1] http://konfliktus.index.hu/sritigrisek.html (2008.06.10.)

[2] http://www.bbc.co.uk/politics97/news/07/0719/eta.shtml (2008.06.10.)

[3] http://fas.org/irp/threat/terrorism/sup2.pdf (2008.06.10.)

[4] http://index.hu/tech/biztonsag/hekk0207/ (2008.06.10.)

[5] http://www.fbi.gov/page2/july03/071803backsp.htm (2008.06.10.)

[6] http://www.time.com/time/magazine/article/0,9171,1098961,00.html (2008.06.10.)

[7] http://index.hu/tech/jog/eszt250108 (2008.06.10.)

[8] http://www.fbi.gov/congress/congress04/lourdeau022404.htm (2008.06.10.)

[9] Kovács László: Kritikus információs infrastruktúrák. Egyetemi jegyzet. ZMNE, 2007.

[10] 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 (2008.06.10.)

[11] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. Doktori értekezés. ZMNE, Budapest, 2007.

[12] 2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

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

[14] Homeland Security Presidential Directive 7/HSPD-7, Washington, December 17, 2003.

[15] Haig Zsolt – Kovács László – Ványa László: Kritikus információs infrastruktúrák támadása, védelme. Dunaújvárosi Főiskola Közleményei, XXIX/1. ISSN 1586-8567

[16] European Council directive on the identification and designation of European Critical Infrastructure (ECI) and the assessment of the need to improve their protection (9403/08).

Jelen írás a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.