Munk Sándor

A kritikus infrastruktúrák védelme információs támadások ellen

Napjainkban a fejlett társadalmak egyre nagyobb mértékben függenek a különböző (energetikai, kommunikációs, informatikai, közlekedési, ellátási, stb.) infrastruktúráktól, így a társadalmi, gazdasági és hétköznapi élet működési folyamatai, biztonsága így egyre inkább veszélyeztetettek a legfontosabb – kritikusnak nevezett – infrastruktúrák működésének, szolgáltatásainak megszakadása esetén. A szerző e tanulmányban elemzi a kritikus infrastruktúra védelem egyes alapfogalmait, rámutat a fogalomhasználat problémáira; vizsgálja a kritikus infrastruktúra védelem újszerűségét és az információs támadások specifikumát; végül bemutatja a kritikus infrastruktúrák információs támadások elleni védelme és a védelmi szféra közötti viszonyrendszer egyes összefüggéseit.

A kritikus infrastruktúrák védelme napjaink egyik rendkívül aktuális, népszerű témaköre mind a mindennapi életben, mind a tudományos kutatásban. A fejlett XXI. századi társadalmak egyre nagyobb mértékben függenek a különböző (energetikai, kommunikációs, informatikai, közlekedési, ellátási stb.) infrastruktúráktól és ezek az infrastruktúrák maguk is kölcsönösen függenek egymástól. A társadalmi, gazdasági és hétköznapi élet működési folyamatai, biztonsága így egyre inkább veszélyeztetettek a legfontosabb – kritikusnak nevezett – infrastruktúrák működésének, szolgáltatásainak megszakadása esetén.

Ez utóbbira az elmúlt években számos példával találkozhattunk terrortámadások (New York, Madrid, London), természeti katasztrófák (New Orleans, dél-kelet ázsiai szökőár), vagy technikai problémák (közlekedési balesetek, áramkimaradás) következtében. A kritikus infrastruktúrák működésének, szolgáltatásainak ma már kiemelt a terrorfenyegetettsége is, amelyen belül a jövőben – viszonylagos „egyszerűsége", „olcsósága" miatt – jelentős szerepet játszhatnak az információs, informatikai jellegű támadások is.

* „A nemzetközi terrorizmus elleni küzdelem időszerű társadalmi, katonai és rendvédelmi kérdései" konferencián 2007. november 6-án elhangzott előadás szerkesztett változata

A tanulmányban a szerző az alábbi vizsgálatokra vállalkozott:
– a kritikus infrastruktúra védelem egyes fogalmi kérdéseinek elemzése;
– a kritikus infrastruktúra védelem újszerűsége, az információvédelemmel, informatikai védelemmel fennálló viszonyrendszere;
– a kritikus infrastruktúra védelem és a védelmi szféra, ezen belül a katonai és a rendvédelmi alkalmazás összefüggései, kapcsolatrendszere.

Miről beszélünk? Kritikus infrastruktúrák egyes fogalmi kérdései

A kritikus infrastruktúra fogalmának mindmáig nincs egységesen elfogadott értelmezése, a számos rendelkezésre álló definíció azonban szemmel láthatóan azonos elemekre épül. Az első ilyen elem az *infrastruktúra*, amelynek általános fogalma viszonylag egységesen értelmezett. A fogalom a gazdaságtudományban jelent meg, mint „olyan gazdasági feltételek (úthálózat […], kikötők, közművek, közoktatás stb.) gyűjtőneve, amelyek nem vesznek részt közvetlenül a termelési folyamatban, de közvetve befolyásolják a termelés fejlesztésének lehetőségeit". Ennek alapján a műszaki infrastruktúra „alapvető létesítmények[..], létesítményrendszerek[..], hálózatok[..], amelyek […] alapjai – létesítési és üzemeltetési feltételei – […] konkrét cél végett megvalósítandó létesítményeknek.", illetve a társadalmi értelemben vett infrastruktúra „mindazon szervezetek, létesítmények, létesítményrendszerek, hálózatok összessége, amelyek egy országon belül a lakosság szellemi és tárgyi életfeltételeit megteremtik, a gazdaság működését elősegítik, ill. lehetővé teszik."[1]

A kritikus infrastruktúra fogalom másik alapvető összetevője, a szűkítő tartalmú '*kritikus*' jelző. A különböző definíciók kritikus infrastruktúra alatt azon infrastruktúrákat értik, amelyek megsemmisülése, működésének vagy szolgáltatásainak alacsonyabb szintje, elérhetőségének megszűnése vagy csökkenése valamilyen támogatott objektumra, folyamatra jelentős (negatív) hatást gyakorol. Ilyenek lehetnek például a következőek: [egy ország esetében] „a társadalmi és gazdasági jólét, vagy a nemzetbiztonság", „az állampolgárok egészsége, biztonsága és gazdasági jóléte, vagy a kormányzat hatékony működése", „a nemzet egésze, vagy a lakosság nagy része", [az Európai Unió esetében] „a tagállamok állampolgárainak egészsége, biztonsága és gazdasági jóléte, vagy kormányzataik hatékony működése"[2], vagy [egy nemzeti haderő esetében] „a katonai erők és műveletek kihelyezése/előkészítése, támogatása és fenntartása"[3].

A felsorolt példák alapján megfogalmazható *a kritikus infrastruktúra általános fogalma*, amely mindazon infrastruktúrák (működtető személyzet, folyamatok, rendszerek, szolgáltatások, létesítmények, és eszközök összessége), amelyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése egy adott felhasználói kör létére, lét- és működési feltételeire jelentős negatív hatással jár. A kritikus infrastruk-

1 Közgazdasági Kislexikon – 232.o.; Műszaki Lexikon, II. kötet, G–M – 354.o.; Magyar Nagylexikon, 9. kötet, Gyer-Iq – 871.o.

2 Lásd International CIIP Handbook 2006. Vol 1.

3 DoD Directive 3020.40 Defense Critical Infrastructure Program (DCIP), 2005.

túra ezen általános fogalmán belül az érintett felhasználói körtől függően meg kell különböztetnünk specifikus fogalmakat, mint például nemzeti kritikus infrastruktúra, európai kritikus infrastruktúra, [nemzeti] védelmi/katonai kritikus infrastruktúra, szövetségi kritikus infrastruktúra, vagy szervezeti kritikus infrastruktúra.

Ebből következően a kritikus infrastruktúra fogalmat – a jelenlegi gyakorlattól eltérően – tulajdonképpen nem szabad minősítő jelző nélkül használni. Napjainkban a szakirodalom tanúsága szerint a legnagyobb figyelem a nemzeti kritikus infrastruktúrákra irányul, de nem lehet figyelmen kívül hagyni az európai kritikus infrastruktúrák, vagy a [nemzeti] védelmi kritikus infrastruktúra szerepét sem. Az osztályozás tovább is folytatható, például egy nemzeti közigazgatás szintjeinek megfelelően beszélhetünk regionális, területi és lokális (pld. települési) kritikus infrastruktúráról.

Azt, hogy egy adott infrastruktúra – az adott felhasználó kör szempontjából – kritikus-e, vagy sem, az érintett felhasználói kör határozza meg. Így értelemszerűen ugyanazon infrastruktúra, vagy infrastruktúra összetevő kritikussága eltérő lehet/lesz európai, magyar nemzeti, NATO, vagy magyar védelmi szempontból. Emellett megítélésem szerint a 'kritikusság' egy adott felhasználói kör számára is dinamikusan változó sajátosság: meg kell/lehet különböztetni az általánosságban, illetve egy adott helyzetben kritikus infrastruktúrákat. Például egy természeti katasztrófa, veszélyhelyzet (pld. Katrina hurrikán, tiszai árvíz) esetén egyes, korábban nem kritikus, területi, vagy helyi infrastruktúra összetevők válhatnak nemzeti szempontból is kritikussá.

A kritikus infrastruktúrák fogalmából értelemszerűen következik, hogy biztonságuk megőrzése, a fenyegetések elleni védelmük – vagyis a *kritikus infrastruktúra védelem* (Critical Infrastructure Protection, CIP) – az érintett felhasználói kör számára alapvető jelentőségű feladat. A kritikus infrastruktúra védelem fogalma sokféle változatban, de tartalmilag lényegében azonos módon a kritikus infrastruktúrák védelmére irányuló programokat, rendszabályokat és tevékenységeket rögzítik. Bár ezzel kapcsolatban érdemi értelmezési problémákkal nem találkozunk, de szükségesnek látom hangsúlyozni, hogy a kritikus infrastruktúra védelme valójában nem, pontosabban funkciója szerint nem elsősorban a kritikus infrastruktúra, hanem az általa nyújtott szolgáltatások meghatározott szintjének és elérhetőségének védelme. A szolgáltatások biztosítandó szintjét a korábban már említett felhasználói kör határozza meg.

A kritikus infrastruktúra védelem feladatrendszerének egyik első, általánosan elfogadott feladata az adott felhasználói kör, illetve alkalmazási terület szempontjából *kritikus infrastruktúrák azonosítása*. Ennek legmagasabb szintjét a gyakorlatban a kritikus infrastruktúrák ágazatonkénti, szektoronkénti felsorolása képezi. A kritikus infrastruktúrák szektorális szintű meghatározása azonban csak a kezdő lépés lehet, önmagában nem elegendő annak kimondása, hogy például a villamosenergia-ellátó rendszer (vagy a bankszektor) a nemzeti kritikus infrastruktúra összetevője. Ezen belül megítélésem szerint elsőként – például a nemzeti biztonsági stratégiában és a kapcsolódó ágazati stratégiákban – meg kell határozni a villamosenergia-ellátó rendszerrel (bankszektorral stb.) szemben támasztott általános követelményeket. A stratégiai szintű követelményeket ezt követően le kell bontani részletesebb, konkrét külső szolgáltatás-szint jellegű követelményekre. Ennek alapján lehet majd dinami-

kusan meghatározni, hogy az adott szektor, vagy infrastruktúra mely összetevői minősülnek kritikusnak és hogy ezekkel szemben milyen belső szolgáltatási-szint követelményeknek kell eleget tenniük.

A kritikus infrastruktúrák fogalmi alapjainak tisztázása során találkozhatunk a következő *fogalmi keveredés* problémájával is: a gyakorlatban a kritikus infrastruktúra védelem fogalma alatt sok esetben a kritikus információs infrastruktúrák védelmét, vagy a kritikus infrastruktúrák információs támadások, veszélyeztetések elleni védelmét értik. Nyilvánvaló azonban, hogy a három fogalom egymással nem keverhető össze. Egyrészt a kritikus információs infrastruktúrák a kritikus infrastruktúráknak csak egy, bár az információs korszakban egyre nagyobb jelentőséggel bíró csoportját alkotják, másrészt a kritikus infrastruktúrák nyilvánvalóan fizikai úton is támadhatóak, veszélyeztetettek.

A kritikus infrastruktúra védelem és a kritikus információs infrastruktúra védelem számos más szakterülethez is kapcsolódik. Ezek közé tartozik többek között a működésfolytonosság (Business Continuity), a kormányzati tevékenység folyamatossága (Continuity of Government), a biztonság az információs színtéren (Cyber Security), vagy az információs és az informatikai védelem (Information Security, IT Security).

Bár a jelen előadás témája a kritikus infrastruktúrák információs támadások elleni védelme és mindez egy terrorizmussal foglalkozó konferencián hangzik el, hangsúlyozni szeretném hogy a kérdéskör összetettségéből következően a tudományos kutatás és a gyakorlati megvalósítás egyedül helyes megközelítése a valamennyi veszélyforrásra kiterjedő módszer. A kritikus infrastruktúra védelem kérdéseit nem lehet leszűkíteni az információs támadások elleni védelemre, illetve a terrorizmus elleni védelemre.

Mi az új? Az információs támadások elleni védelem újdonsága

A kritikus infrastruktúrák védelme általában és ezen belül *az információs támadások elleni védelem* tulajdonképpen *nem új dolog*. Egy nemzet hadviselési képességei szempontjából kritikus infrastrukturális erőforrások támadása és védelme gyakorlatilag egyidős a hadviseléssel magával. Az információs támadások sem a XXI. században jelentek meg, az információs hadviselés, az információs műveletek fogalomrendszere már 1992-ben megjelent az Egyesült Államok haderejének egy szigorúan titkos utasításában.

A tágabb értelemben vett informatika – az információkkal és kezelésükkel, az információs tevékenységekkel foglalkozó tudomány és technikaterület – eredményeinek gyors ütemben bővülő, terjedő alkalmazása is a múlt század utolsó évtizedeitől tapasztalható, amivel együtt járt az információvédelem, informatikai védelem szerepének előtérbe kerülése, elméletének, eszközeinek és módszereinek kialakulása. A kritikus infrastruktúrák elleni információs veszélyeztetések, támadások nem különböznek az informatikai rendszerek elleni, már korábban jól ismert támadásoktól, hiszen a kritikus infrastruktúrák informatikai összetevői (önálló infrastruktúrák, vagy más infrastruktúrák részét képező összetevők) sem különböznek más informatikai rendszerektől, eszközöktől.

Akkor viszont miben áll a kritikus infrastruktúrák információs támadások elleni védelmének sajátossága, milyen sajátos tudományos kutatási problémákat vet fel, milyen sajátos megoldásokat, eszközöket és módszereket igényel (ha egyáltalán vannak ilyenek)? Jelen előadás egyik hipotézise, hogy *a kritikus infrastruktúrák információs támadások elleni védelme az információvédelem, informatikai védelem egyik* – napjainkban jelentős szerepet játszó – *alkalmazási területe*. Vagyis e szakterületen is érvényesek az információvédelem, informatikai védelem általános elvei, törvényszerűségei, alapvetően alkalmazhatóak kidolgozott eszközei és módszerei, azonban léteznek alkalmazási terület specifikumok is.

Az alkalmazási terület sajátosságainak rendszerezéséhez induljunk ki a biztonság/védelem alapmodelljéből, amelynek alapvető elemeit a veszélyeztetett objektum, a belső és külső veszélyeztető hatások és a veszélyeztetést kiváltó objektumok képezik. Az alapmodell részét képezik a veszélyeztetett objektum sebezhetőségei is: olyan összetevői, tulajdonságai, amelyek lehetővé teszik a veszélyeztető hatások érvényesülését, az objektum létének, tulajdonságainak, működésének káros módon történő befolyásolását.

A veszélyeztető hatások forrásai, kiváltói a természeti környezet, az épített és technikai környezet, valamint a társadalmi környezet objektumaira csoportosíthatóak. A veszélyeztető hatások két nagy csoportját pedig – a rendszerek környezetükkel fenntartott kapcsolatainak rendszerelméleti osztályozásából kiindulva – a fizikai (anyagi), illetve az információs hatások képezik.

A kritikus infrastruktúrák információs támadások elleni védelme helyett gyakran önálló kifejezéssel, az Egyesült Államokban többnyire – az eredeti jelentésétől eltérő tartalmat hordozó jelzőjű – 'kibernetikai' védelemmel (cyber security), vagy 'kibernetikai térbeli' védelemmel (cyberspace security) is találkozhatunk.[4] A magyar terminológiában ezen kifejezéseket véleményem szerint az 'információs védelem', illetve a 'védelem az információs színtéren' formában célszerű megjeleníteni. A fentieknek megfelelően a fizikai hatások (támadások) ellenpárját a szakirodalomban sok esetben az úgynevezett 'cyber' hatások (fenyegetések, támadások) képezik, amelyek összetevői között azonban sokszor találkozhatunk fizikai hatásokkal is.[5]

Az információs hatásokat megítélésem szerint a veszélyeztetett objektumok által átvett, vagy kezelt információ-reprezentációkhoz kell kötnünk, függetlenül az adott reprezentációt hordozó fizikai (anyagi) reprezentációtól. Ennek megfelelően *információs hatás* az a hatás, amely a veszélyeztetett rendszer által értelmezhető, feldolgozható információt juttat be, vagy a rendszer által kezelt információt, megvalósított információs tevékenységet módosít, töröl az adott (hagyományos információfeldolgozási, vagy informatikai) rendszer saját folyamatai, résztevékenységei útján. Ebből következően nem tartom információs hatásnak az elektronikai támadás legtöbb hagyományos lehetőségét, pl. az elektronikai zavarást, lefogást, megsemmisítést, vagy egy mágneses adathordozó tartalmának külső behatásra történő törlését.

---

4 The National Strategy to Secure Cyberspace, 2003.

5 Lásd pl. „elektronikai, rádiófrekvenciás, vagy számítógép-alapú támadások", Executive Order 13010, Critical Infrastructure Protection. President of the USA, 1996.

Az előadás témájához kapcsolódó legfontosabb, alapvető változást – a szakirodalom egyöntetű véleménye szerint is – az informatika eszközeinek és szolgáltatásainak folyamatosan bővülő alkalmazása, a legkülönbözőbb technikai rendszerekbe történő beépülése, ehhez kapcsolódóan a hálózatok megjelenése, világméretű elterjedése és erre épülően a rendszerek közötti információcsere kibővülése, a szolgáltatások együttműködő alkalmazásokra épülő megvalósítása jelentette. Ennek következménye *az információs infrastruktúra 'kritikussá válása'*, a társadalmi, szervezeti és magánéletbeli folyamatok egyre fokozódó informatikai szolgáltatás-függősége.

A 'mindenütt jelenlévő' (ubiquitous) informatika, hálózat-elérhetőség és összekapcsolódás – elsőként az Interneten, majd a helyi és nagykiterjedésű, illetve vezetéknélküli és hibrid hálózatok segítségével – korábban nem látott szolgáltatásokat nyújt, új iparágakat teremtett, megváltoztatta többek között a hadviselés, a munkavégzés és a tanulás formáit és módszereit. Ugyanakkor – mint a történelemben már oly sokszor – az új lehetőségek új problémák megjelenésével is együtt jártak. Az informatikai rendszerek és összetevők új sebezhetőségeket hordoznak, új – elsősorban információs jellegű – veszélyeztető hatások számára teremtenek lehetőségeket. Ennek kiemelt részét képezik például a hagyományos infrastruktúrák, rendszerek informatikai alapú felügyeleti és adatgyűjtő (supervisory control and data acquisition, SCADA) rendszerei.

Az *információs támadások sajátossága*, hogy a hálózati kapcsolatoktól elszigetelt – de ezzel egyben az együttműködési előnyökből kizárt, alacsonyabb szintű eredményességet, hatékonyságot biztosító – rendszerektől eltekintve a veszélyeztető hatások egyszerűbben, olcsóbban, nehezebben felderíthető módon, a földrajzi távolságtól általában függetlenül kiválthatóak. Mindez egyben jelentős mértékben kiszélesítette a veszélyeztetést előidézni képes szereplők körét is. A biztonságpolitikai színtéren ez is hozzájárult a nem-hagyományos szereplők (pld. terrorista csoportok, szervezett bűnözői csoportok) lehetőségeinek, eszköztárának kibővüléséhez.

Ha végiggondoljuk, akkor az előzőekben elmondottak egyaránt érvényesek a kisebb szervezetek informatikai rendszereire és egy nemzet, vagy az Európai Unió kritikus infrastruktúráira. Az alapvető különbség, a kritikus infrastruktúrák információs támadások elleni védelmének sajátosságai megítélésem szerint a veszélyeztetett objektum összetettségében, heterogenitásában, a támadások következményeinek súlyosságában, valamint a potenciális támadók szélesebb körében található.

A vonatkozó hivatalos dokumentumok[6] egységesen hangsúlyozzák, hogy a nemzeti kritikus infrastruktúrák és annak informatikai összetevői gyakorlatilag minden szervezeti informatikai rendszernél összetettebbek és ami talán még ennél is fontosabb, jelentős részük – piacgazdaságra épülő államokban mintegy 80–90%-uk – az adott államtól teljes egészében, vagy részben független magánvállalkozások kezelésében van.

Nyilvánvaló, hogy a nemzeti kritikus infrastruktúrák védelmét, ezen belül információs támadások elleni védelmét az adott állam igényei, követelményei alapján, irányítása és koordinálása mellett, az államon kívül számos más szereplő együttműködésével kell

6 Pl. Green Paper on a European Programme for Critical Infrastructure Protection, 2005; Executive Order on Critical Infrastructure Protection, 2001.

megvalósítani. A kritikus infrastruktúrák védelme tehát egy olyan tevékenységrendszer, amelynek jelentős része az adott állam hatáskörén kívül kerül megvalósításra.

Ennek során az *állami igények, követelmények* természetesen általában nem esnek egybe az adott infrastruktúrát, vagy annak egy szegmensét működtető szervezet – különösen gazdasági – szempontjaival, aminek feloldása elsősorban jogi, gazdasági és szervezési feladat. Emellett a követelmények megfogalmazása önmagában egy rendkívül összetett feladat tekintettel a szakirodalomban szintén sokat hangsúlyozott egymásra épülésre, hatás-tovaterjedésekre. Jelenleg úgy tűnik, nincs kialakult hatékony módszertana az ilyen összetett rendszerek egyes összetevőivel szemben támasztott szolgáltatás-szint követelmények meghatározásának.

Önmagában egy olyan követelmény megfogalmazása, hogy egy adott infrastruktúra-összetevő (pl. egy mobil-, vagy egy Internet-szolgáltató rendszere) 'legyen védett az információs támadások ellen' (esetleg ezen belül egyes részterületeket konkrétan megnevezve, pld. rendelkezzen számítógépes vírusvédelemmel) nem lehet alapja egy védelmi feladat- és eszközrendszer kialakításának és nem is számonkérhető, pontosabban könnyen és olcsón teljesíthető. Ebből következően a tudományos kutatás egyik fontos feladata az infrastruktúra védelmi mérési és mértékrendszerek, értékelési eszközök és módszerek kialakítása.

Ha a kritikus infrastruktúra védelemmel kapcsolatos állami követelményeket sikerül is pontosan megfogalmazni és elfogadtatni, újabb feladatot, sőt problémát jelent a magasfokú autonómiával rendelkező szereplők által alkalmazott heterogén fogalomrendszerek, eszközök és módszerek összehangolása, egységes rendszerbe illesztése. Mindez elengedhetetlen egy közös kritikus infrastruktúra helyzetismeret folyamatos fenntartásához, az egyes szereplők közötti jelentésmegőrző információáramláshoz és védelmi tevékenységeik összehangolásához.

Miért a védelmi szféra? Az információs támadások elleni védelem egyes kérdései

A védelmi, katonai informatika kutatójában értelemszerűen merülhet fel a kérdés, hogy – a védelem kifejezés azonossága mellett – milyen viszony áll fent a kritikus infrastruktúrák információs támadások elleni védelme és a védelmi szféra között. Van-e és ha igen, milyen érintettsége a hadtudományi, rendvédelem-tudományi kutatásnak és gyakorlatnak a kritikus infrastruktúra védelem informatikai vonatkozásaiban. A következőkben a teljesség igénye nélkül e kérdéskör néhány kérdésére térek ki.

Az első és legfontosabb, a különböző doktrínális dokumentumokban is gyakorlatilag egységesen elfogadott megállapítás, hogy *a kritikus infrastruktúrák biztonsága a nemzeti biztonság egyik alapvető összetevője*. A Magyar Köztársaság Nemzeti Biztonsági Stratégiája szerint „… Magyarország számára kiemelt feladat a felzárkózás a fejlett világ információs és telekommunikációs színvonalához. … Az informatikai infrastruktúra technikai és szellemi feltételeinek biztosítása mellett ügyelni kell e rendszerek védelmére és a megfelelő tartalékok képzésére is."[7] A terrorizmus elleni védekezéshez kapcsolódóan pedig úgy fogalmaz, hogy „A terrorizmus elleni küzdelem

7 2073/2004. (III. 31.) Korm. határozat, A Magyar Köztársaság nemzeti biztonsági stratégiája. [5.o.]

integrált megközelítést kíván meg, amely magában foglalja a megelőzés és beavatkozás eszközeit, a terrorizmus anyagi alapjainak ellehetetlenítésére irányuló közös nemzetközi erőfeszítéseket, a kritikus infrastruktúra védelmét."[8] Az információs rendszerek védelme a stratégiában önálló alpontot (III.3.7) képez, benne azzal, hogy „… új feladatként jelentkezik a korszerű és biztonságos informatikai infrastruktúra kialakítása …"[9].

Az európai biztonsági stratégia is a globális kihívások közé sorolja, hogy a globalizációs folyamatok „megnövelték Európa függőségét – és így sebezhetőségét – a szállítási, energia-, információs és más infrastruktúráktól."[10] Ezt követően a Tanács felkérésére az Európai Bizottság 2005-ben dolgozta ki a 26 oldalas zöld könyvet a kritikus infrastruktúra védelem európai programjáról.[11]

Az elmondottakból egyértelműen következik, hogy a kritikus infrastruktúrák védelmének kérdései a védelmi szféra, a hadtudományi és rendvédelem-tudományi kutatás vizsgálati körébe tartoznak és ezen belül is kiemelt szerepet játszanak. Ennek során természetesen szoros együttműködésre van szükség az általános értelemben vett információ-, illetve informatikai biztonsági szakterülettel is, azonban a kritikus infrastruktúra védelem a szűkebb értelemben vett informatikai védelmi megközelítésnél komplexebb – a támadások, fenyegetések, illetve a védelmi tevékenységek, rendszabályok szélesebb körére kiterjedő és integrált – megközelítést igényel.

A második megállapítás alapját az a tény képezi, hogy napjainkban a kritikus infrastruktúrákhoz hasonló, *összetett rendszerek informatikai védelmében leginkább* a többnemzeti műveletekben résztvevő *katonai erőknek vannak tapasztalatai*. A kritikus információs infrastruktúrák védelmének egyik alapvető sajátossága, hogy összetevőik különböző – teljes, vagy részleges autonómiával (döntési szabadsággal) rendelkező – szervezetekhez tartoznak, amelyek ennek megfelelően a hatáskörükbe tartozó összetevők biztonságát (működésfolytonosságát) is különböző célkitűzések érdekében, eltérő elvek, módszertanok, eszközök segítségével teremtik meg és tartják fent.

A viszonylagos önállósággal rendelkező szervezetek közötti együttműködési problémák elsőként a katonai alkalmazásban és ezen belül az Egyesült Államok hadseregében merültek fel. A jelentős önállósággal rendelkező haderőnemek közötti kommunikációs problémák már a koreai háborúban (1950–1953), a dominikai partraszállás során (1965), Vietnamban (1965–1973) és majdnem húsz évvel később a grenadai beavatkozás alatt (1983) alatt is jelentkeztek.

A hosszú távú informatika-alkalmazási stratégia alapjait az 1992-ben a Vezérkari Főnökök Egyesített Bizottságának J–6 Csoportfőnöksége által kibocsátott „Informatika a harcos számára" (C4IFTW)[12] koncepció fogalmazta meg. A koncepció központjában egy olyan globális informatikai infrastruktúra – az úgynevezett infoszféra – állt, amelybe a harcoló bármely feladat végrehajtása során, bárhonnan, bármikor

8 U.o. [13.o.]

9 U.o. [15.o.]

10 A Secure Europe in a Better World. European Security Strategy. 2003 [3.o.]

11 Green Paper on a European Programme for Critical Infrastructure Protection, 2005.

12 *C4I for the Warrior.* 1992.

„bekapcsolódhat". A C4IFTW infrastruktúrája egy olyan „globális háló", amely átszövi az ipari, tömegkommunikációs, kormányzati, katonai és más nem-kormányzati szervezeteket. A koncepció célkitűzéseinek lényeges elemét képezte a helyzethez igazodó védelmi eszközök (az informatikai rendszer védett és megszakítás nélküli működését – fejlett technológiával rendelkező ellenség esetében is – biztosító személyi, fizikai és elektronikai védelmi eszközök) alkalmazása.

Az 1990-es évek második felére a biztonságpolitikai környezetben bekövetkezett gyökeres változások és az informatika szinte forradalmi fejlődése a védelmi szférában és a katonai alkalmazásban is új helyzetet teremtett. A 21. század elejének sajátossága a katonai műveleteket végrehajtó erők összetételének megváltozása és az együttműködési kör kibővülése, a multilaterális jelleg uralkodóvá válása. Korunk katonai műveletei összhaderőnemi, többnemzetiségű – szövetségi, sőt leggyakrabban az adott feladatra létrehozott, a résztvevő nemzetek eseti felajánlásaira épülő koalíciós – keretekben kerülnek végrehajtásra. Emellett a műveletet végrehajtó csoportosításoknak küldetésük eredményes megvalósítása érdekében egyre szorosabb együttműködést kell kialakítaniuk más – nemzetközi, kormányzati, nem-kormányzati és civil – szervezetekkel is.[13]

Az előzőekből következően – a polgári és a más védelmi alkalmazási területeket megelőzően – a katonai erők kerültek elsőként abba a helyzetbe, hogy autonóm, egymással együttműködő informatikai rendszerek együttes biztonságát, működésfolytonosságát és együttműködési képességét kell megteremtsék és fenntartsák. Ezen a területen egyébként még a katonai informatika sem ért el végleges, mindenre kiterjedő eredményeket, de mindenképpen előbbre jár, mint pld. a közigazgatás, vagy a katasztrófa- és rendvédelem.

A harmadik kérdéskör központi gondolata az a megállapítás, hogy a kritikus infrastruktúrák elleni *információs támadásokat végrehajtók felderítése*, az *információs támadások detektálása* (majd 'helyszínelése'), illetve a *támadók elleni fellépés*, de legalábbis e feladatok nagyobb része és egészének koordinációja *a védelmi szféra feladata*.

A hagyományos értelemben vett informatikai védelem ma még – a szervezetek túlnyomó többsége esetében alapvetően jogi okokból is – bizonyos értelemben passzív jellegű: nem, vagy csak alig foglalkozik az informatikai védelmi célú felderítéssel, illetve ellentevékenységgel. Ezek a tevékenységek a katonai alkalmazásban már régóta az információs műveletek integráns részét képezik, egyes végrehajtó elemeik az elektronikai védelem analógiájára is építve folyamatosan jelennek meg a fejlett haderők szervezetében. Bár napjainkban a szakirodalomban többet szerepelnek az informatikai úton végrehajtott támadások, a katonai hacker-hadviselés műveletei, azonban bizonyíthatóan megjelentek a felderítés és az ellentevékenység erői és eszközei is.

Az informatikai támadók és támadások felderítése, 'nyomrögzítése' természetes, bár újszerű feladata a rendvédelem ún. számítógépes bűnözés[14] elleni küzdelmet

13 Strategic Vision. The Military Challenge. By NATO's Strategic Commanders. 17., 21–23. pontok [7–9. o.].

14 Számítógépes bűnözés: azon bűncselekmények összessége, amelyek információ-technológiai eszközök, rendszerek, illetve rendszerelemek ellen irányulnak, vagy információ-technológiai eszközöket, rendszereket használnak a bűncselekmény elkövetése eszközeként.

folytató szervezeteinek és szakembereinek is. A világon az első számítógépes bűnözéssel foglalkozó rendőri egységet a Scotland Yard állította fel 1971-ben (igaz egyetlen tiszttel). Magyarországon az ORFK 2000-ben hozott létre egy Internet-figyeléssel foglalkozó munkacsoportot. 2007 februárjában az Internet-csoportot a kibővített feladat- és hatáskörű, nagyobb létszámú Csúcstechnológiai bűnözés elleni osztály váltotta fel, amely már önálló nyomozati jogkörrel is rendelkezik. A számítógépes bűnözés elleni küzdelem a rendőrség mellett természetesen a nemzetbiztonsági szolgálatok feladatköréhez is kapcsolódik.

Míg a felderítés az elmondottakból láthatóan több, a védelmi szférához tartozó szervezet feladatrendszerében is szerepel, az ellentevékenység – vagyis a saját rendszereinket, a kritikus infrastruktúrát fenyegető támadók elleni támadás, vagy tevékenységük akadályozása – a magyar gyakorlatban egyenlőre gyakorlatilag nem jelent meg. Mivel ez a feladat a kormányzati és azon belül kiemelten a védelmi szférabeli információs infrastruktúra védelme esetén nem mellőzhető, előbb-utóbb ki kell alakítani az erre alkalmas erőket, amelyre megítélésem szerint célszerűen a Magyar Honvédség állományában kerülhet sor, de a katonai alkalmazási területet meghaladó feladat- és hatáskörrel.

Összegzés, következtetések

Összességében tehát megállapíthatjuk, hogy a kritikus infrastruktúra fogalmat még a szakirodalomban is eltérő tartalommal – az érintett felhasználói kör (egy adott állam, az Európai Unió, egy adott haderő, vagy katonai szövetség) megjelölése nélkül – használjuk. Ebből következően szükség van a kritikus infrastruktúra általános fogalmára, illetve konkrét esetekben – a jelenlegi gyakorlattól eltérően – a fogalom minősítő jelzővel (nemzeti, európai, védelmi stb.) kiegészített alkalmazására.

A kritikus infrastruktúra fogalmán belül a 'kritikusság' fogalma is figyelmet érdemel. Alkalmazása során tisztában kell lenni azzal, hogy ez a jelző egyrészt felhasználói kör függő (pl. egy adott infrastruktúra[összetevő] lehet kritikus nemzeti szempontból, de nem kritikus európai szempontból), másrészt egy adott felhasználói kör esetében is a körülményektől függő, dinamikusan változó sajátosság (egy adott infrastruktúra[összetevő] általánosságban nem kritikus, vagy egy adott helyzetben, pl. árvíz esetén az).

Fontos hangsúlyozni azt is, hogy a kritikus infrastruktúra védelme valójában nem, pontosabban funkciója szerint nem elsősorban a kritikus infrastruktúra, hanem az általa nyújtott szolgáltatások meghatározott szintjének és elérhetőségének védelme. A szolgáltatások biztosítandó szintjét az érintett felhasználói kör és annak valós igényei határozzák meg.

A szakirodalom tanulmányozásából levonható fontos következtetés az is, hogy a fogalomhasználatban gyakran keveredik a kritikus infrastruktúra védelem, a kritikus információs infrastruktúrák védelme, illetve a kritikus infrastruktúrák információs támadások elleni védelme. E három, eltérő tartalmú jelenség vizsgálata egymástól nem elválasztható. Véleményem szerint ennek során csak a valamennyi veszélyeztetett objektumra és valamennyi veszélyforrásra kiterjedő komplex megközelítés lehet eredményes.

Szükségesnek tartom hangsúlyozni azt is, hogy a kritikus infrastruktúrák és ezek információs támadások elleni védelme nem új dolog. A hadviselési képességek szempontjából kritikus infrastrukturális erőforrások támadása és védelme gyakorlatilag a hadviseléssel egyidős. Az információs támadások, az információs hadviselés, az információs műveletek fogalomrendszere pedig már 1992-ben megjelent. A kritikus infrastruktúrák információs támadások elleni védelme lényegét tekintve az információvédelem, informatikai védelem egyik alkalmazási területe, így érvényesek rá ez utóbbi általános elvei, törvényszerűségei, azonban léteznek alkalmazási terület specifikumok is.

A kritikus infrastruktúrát veszélyeztető hatások két nagy csoportját a fizikai (anyagi), illetve az információs hatások képezik. Ez utóbbit megítélésem szerint a veszélyeztetett objektumok által átvett, vagy kezelt információ-reprezentációkhoz kell kötnünk. Ennek megfelelően információs hatás az a hatás, amely a veszélyeztetett rendszer által értelmezhető, feldolgozható információt juttat be, vagy a rendszer által kezelt információt, megvalósított információs tevékenységet módosít, töröl az adott (hagyományos információfeldolgozási, vagy informatikai) rendszer saját folyamatai, résztevékenységei útján.

Az információs infrastruktúrák 'kritikussá válása' a társadalmi, szervezeti és magánéletbeli folyamatok egyre fokozódó informatikai szolgáltatás-függősége. Az információs támadások sajátossága a veszélyeztető hatások egyszerűbb, olcsóbb, nehezebben felderíthető, a földrajzi távolságtól általában független kiválthatósága, ami jelentős mértékben kiszélesítette a veszélyeztetést előidézni képes szereplők (pld. terrorista csoportok, szervezett bűnözői csoportok) körét. A kritikus infrastruktúrák alapvető sajátossága tehát a veszélyeztetett objektumok összetettségében, heterogenitásában, a támadások következményeinek súlyosságában, valamint a potenciális támadók szélesebb körében találhatóak.

A kritikus infrastruktúrák védelmével kapcsolatos uniós, állami, szövetségi stb. igények, követelmények általában nem esnek egybe az adott infrastruktúrát, vagy annak egy szegmensét működtető szervezet – különösen gazdasági – szempontjaival, aminek feloldása elsősorban jogi, gazdasági és szervezési feladat. A követelmények megfogalmazása önmagában egy rendkívül összetett feladat tekintettel és jelenleg nem rendelkezik kialakult hatékony módszertannal sem. Ebből következően a tudományos kutatás egyik fontos feladata az infrastruktúra védelmi mérési és mértékrendszerek, értékelési eszközök és módszerek kialakítása.

Végül a teljesség igénye nélkül összegezzük a kritikus infrastruktúrák információs támadások elleni védelme és a védelmi szféra közötti viszonyrendszer egyes összefüggéseit. Ezen belül a legfontosabb megállapítás, hogy a kritikus infrastruktúrák biztonsága a nemzeti biztonság egyik alapvető összetevője, így a kritikus infrastruktúrák védelmének kérdései a védelmi szféra, a hadtudományi és rendvédelem-tudományi kutatás vizsgálati körébe tartoznak, ezen belül is kiemelt szerepet játszanak. *A második megállapítás* az, hogy a kritikus infrastruktúrákhoz hasonló, összetett rendszerek informatikai védelmében leginkább a többnemzeti műveletekben résztvevő katonai erőknek vannak tapasztalatai. A XXI. század elején a katonai erők kerültek elsőként abba a helyzetbe, hogy autonóm, egymással együttműködő informatikai rendszerek együttes biztonságát, működésfolytonosságát és együttműködési képességét kell megteremtsék és fenntartsák.

Harmadik megállapításként megfogalmazhatjuk, hogy a kritikus infrastruktúrák elleni információs támadásokat végrehajtók felderítése, az információs támadások detektálása, illetve a támadók elleni fellépés, de legalábbis e feladatok nagyobb része és egészének koordinációja a védelmi szféra feladata. A hagyományos értelemben vett informatikai védelem alapvetően passzív jellegű: nem, vagy csak alig foglalkozik az informatikai védelmi célú felderítéssel, illetve ellentevékenységgel.

Ezek a tevékenységek a katonai alkalmazásban – legalábbis a legfejlettebb hadseregekben – már régóta az információs műveletek integráns részét képezik. Az informatikai támadók és támadások felderítése, 'nyomrögzítése' természetes, bár újszerű feladata a rendvédelem, illetve a nemzetbiztonsági szervezetek ún. számítógépes bűnözés elleni küzdelmet folytató szervezeteinek és szakembereinek is. Az ellentevékenység a magyar gyakorlatban egyenlőre még nem jelent meg, de a kormányzati és azon belül kiemelten a védelmi szférabeli információs infrastruktúra védelme esetén nem mellőzhető, előbb-utóbb ki kell alakítani az erre alkalmas erőket.

FELHASZNÁLT IRODALOM

2073/2004 (III. 31.) Korm. Határozat, *A Magyar Köztársaság nemzeti biztonsági stratégiája.*

Abele-Wigert, Isabelle-Dunn, Myriam: *International CIIP Handbook, 2006. Vol 1.* – Center for Security Studies, ETH Zurich, 2006.

C4I for the Warrior. – Joint Staff C4 Architecture and Integration Division, 1992.

DoD Directive 3020.40 Defense Critical Infrastructure Program (DCIP). – United States Department of Defense, August 19, 2005.

Executive Order 13010, Critical Infrastructure Protection. – President of the USA, July 15, 1996.

Executive Order on Critical Infrastructure Protection. – Office of the Press Secretary, October 16, 2001.

Green Paper on a European Programme on Critical Infrastructure Protection. – Comission of the European Communities, Brussels, 17.11.2005.

Közgazdasági Kislexikon. (Negyedik bővített és átdolgozott kiadás) – Kossuth Könyvkiadó, Budapest, 1987.

Műszaki Lexikon, II. kötet G–M. – Akadémiai Kiadó, Budapest, 1972.

Magyar Nagylexikon, 9. kötet, Gyer-Iq. – Magyar Nagylexikon Kiadó, Budapest, 1999.

The National Strategy to Secure Cyberspace. – The White House, Washington, February 2003.

A Secure Europe in a Better World. European Security Strategy. – European Council, Brussels, 12 December 2003.

Strategic Vision: The Military Challenge. By NATO's Strategic Commanders. – Allied Command Transformation Information Office-Allied Command Operations Public Information Office, Norfolk-Mons, 2004.