HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Nagyné Takács Veronika
ntakacsv@t-online.hu

A NEMZETI KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELMÉNEK SZABÁLYOZÁSI ÉS SZERVEZETI KÉRDÉSEI

HELYZETKÉP AZ EU IRÁNYELV 2012-BEN ESEDÉKES FELÜLVIZSGÁLATA ELŐTT

Absztrakt

A kritikus infrastruktúrák – köztük a kritikus információs infrastruktúrák – védelme elméleti és gyakorlati kérdéseinek áttekintése különösen időszerű az Európai Tanács 2008/114/EK Irányelvének 2012-ben esedékes felülvizsgálata előtt.

The theoretical and practical overview of the critical infrastructure including the critical information infrastructure protection is particularly timely before the review of directive 2008/114/EC of the European Council in 2012.

Kulcsszavak: *kritikus információs infrastruktúra, kritikus infrastruktúra védelem nemzeti programja ~ critical information infrastructure, national program for critical infrastructure protection*

1. BEVEZETÉS

A világ legfejlettebb régióiban kialakulóban levő információs (tudásalapú) társadalom alaptétele, hogy az információ (tudás) válik a legfőbb stratégiai erőforrássá. Ebből következően az információt hordozó (létrehozó, tároló, feldolgozó, továbbító) közegek, szervek, szervezetek és személyzetük, valamint mindezek fenntartása és működtetése, irányítása és felügyelete alapvető jelentőségűek a gazdaság fejlődése, a társadalom jóléte és az állam működése szempontjából.

Globalizálódó világunkban nyilvánvaló, hogy nemcsak az információk terjedése/terjesztése válik határtalanná (ide nem értve az üzleti, politikai stb. korlátokat), hanem az információk fenyegetettsége is új dimenziókat kap (például távolról érkező, vagy éppen helyi, váratlan és rendkívül intenzív támadások lehetősége és megvalósulása formájában).

A „minden mindennel összefügg" elvéből következően az információk, az információkat hordozó elemek és eszközök – az információs infrastruktúra – továbbá az információs infrastruktúrákat használó társadalmi, gazdasági és állami szereplők olyan bonyolult egymásra utaltságban léteznek (akár államhatároktól függetlenül), hogy a rendszer bármelyik elemének sérülése vagy kiesése beláthatatlan – kritikus – következményekkel járhat.

Az itt vázolt problémakör elemzése az új évezred első éveiben – a világ különböző pontjain elkövetett terrorcselekmények (New York, Madrid, London) és az informatikai rendszereket ért támadások (Észtország, Litvánia, Egyesült Államok) – után vált intenzívvé, amikortól az államok és a nemzetközi szervezetek komplex, hosszabb távra szóló megoldást kezdtek keresni az átéltekhez hasonló támadások megelőzése, illetve lehetséges hatásaik csökkentése érdekében.

Magyarország folyamatosan együtt haladt az európai törekvésekkel, így a nemzeti és a közösségi eredmények – az állami (közigazgatási) és a tudományos tevékenységet tekintve is – összevethetők.

Érdemes röviden áttekinteni, mi történt eddig, és milyen feladatok vannak előttünk a nemzeti kritikus információs infrastruktúrák védelme terén.

2. A KRITIKUS INFRASTRUKTÚRÁK VÉDELMÉNEK ELMÉLETI MEGALAPOZÁSA

2.1. Fogalmi tisztázás

A *nemzeti kritikus információs infrastruktúrák* kifejezés minden egyes eleme fogalmi tisztázást célzó pontosítások tárgya volt – és az még ma is.

A legegyszerűbbnek tűnik az *infrastruktúrák* meghatározása; e kérdésben viszonylagos konszenzus van a szakirodalomban*: mindazon fizikai létesítmények, eszközök, rendszerek (hálózatok), az ezeket működtető szervezetek és ezek személyi állománya, továbbá az általuk alkalmazott eljárások összessége, amelyet meghatározott társadalmi, gazdasági vagy állami feladat ellátására hoztak létre és működtetnek*. A fogalom meghatározásából két elem – a szervezet és a személyzet – még nem minden definícióban jelenik meg, [1] [2] jóllehet a védelem tervezése és szabályozása során ezeknek is szerepet kell kapniuk. A meghatározásokban több ízben megjelenik a szolgáltatás elem is, [3] [2] ennek szerepeltetése elhatárolási kérdést vet fel az eljárások és az infrastruktúra rendeltetése vonatkozásában.

A *kritikus* jelző tartalmát érintően már nincs ilyen egységes alap. A legáltalánosabb megfogalmazás szerint kritikus az az infrastruktúra, amelynek *működése létfontosságú a társadalom, a gazdaság vagy az állam működése szempontjából*, azaz sérülésének, működésképtelenségének hatása jelentősen túlmutat az infrastruktúra működtetői (és egyes esetekben a felhasználói) körén.

A fenti megfogalmazás konkretizálására három dimenziót (kiterjedés/hatókör, súlyosság/nagyságrend és időbeli hatás) és változó számú elemből álló horizontális szempontrendszert (társadalmi, gazdasági, környezeti, politikai, pszichológiai, közegészségügyi, [4] valamint nemzetbiztonsági, továbbá kölcsönös függőségi [3] hatás alapján történő megkülönböztetést) tartalmaznak a dokumentumok. A legutolsó szempont-elem kicsit megtöri az addigi logikát; az interdependencia nem annyira önálló, inkább az előzőleg említettek súlyosító tényezője.

A dimenziók számszerűsítése – a küszöbértékek meghatározása – már a konkretizálás további lépését jelenti. A hatás földrajzi kiterjedésének meghatározására a globális, nemzetközi, nemzeti, továbbá a nemzetin belül a regionális vagy helyi szint szerinti megkülönböztetés az elfogadott. A súlyosság tekintetében a horizontális szempontok mentén meghatározható mérőszámokban kifejezhető károk nagysága az irányadó. Az időbeliséget az azonnali, 24-48 órás, hetes, éves időtartamban mérhető kiesés/helyreállítás alapján lehet definiálni.

Az *információs* jelző részben ágazati meghatározást takar (lásd később), részben infrastruktúra-jelleget definiál. Haig Zsolt és Várhegyi István rámutat, a különböző rendeltetésű infrastruktúrák között vannak olyanok, amelyek „lehetővé teszik a társadalom valamely információs funkciójának zavartalan működését", azaz „biztosítják az információk megszerzését, előállítását, továbbítását, feldolgozását és felhasználását". Ezeket az információs (és nem szállítási, egészségügyi stb.) rendeltetésű infrastruktúrákat *funkcionális információs infrastruktúrák*nak nevezik, megkülönböztetve azoktól, amelyek egy-egy információs vagy nem-információs (azaz pl. szállítási, egészségügyi stb.) rendeltetésű infrastruktúra működtetésében informatikai („kutató, fejlesztő és ellátó") eszközrendszerként közreműködnek (*támogató információs infrastruktúrák*). [5] A megkülönböztetés megalapozottságát elismerve jelezni szükséges, hogy a közigazgatási tipológiában a tevékenységek jellegének meghatározásakor a funkcionális jelző a támogató jellegű tevékenységet jelöli, szemben a szakmai jelzővel meghatározott alaptevékenységgel. [6]

Az *információs* jelző kapcsán egy hazai sajátosságra is ki kell térni. Az angol *information infrastructure* kifejezésnek két magyar fordítása is létezik: *információs* illetve *informatikai infrastruktúra*. Több szerző foglalkozik a két kifejezés elkülönítésével, aminek lényege, hogy az előbbin az információt (mint adatot, tudást) tartalmazó rendszert, hálózatot stb. értik, utóbbin magát az informatikai (számítástechnikai-elektronikai-elektronikus stb.) (eszköz)rendszert. [1] [7] A 2010-ben közzétett kormányzati stratégiai dokumentum [8] az előbbi, a 2009-ben, 2011-ben közzétett EU bizottsági közlemények [9] [10] magyar fordítása az utóbbi kifejezést alkalmazza. Megfontolandónak tűnik az utóbbi kifejezés elfogadása, mivel így az informatikai közmű – Munk Sándor kifejezésével: az „információs szolgáltatásokat nyújtó technikai hálózat" [7] – és a benne kezelt, tárolt, továbbított információtartalom mind elméleti, mind szabályozási szinten elkülöníthető. Ezt a megközelítést erősítik a kritikus infrastruktúrák informatikai rendszerek általi meghatározottságáról szóló megállapítások is. [11]

A *nemzeti* jelzőnek elsősorban az Európai Unió kritikus infrastruktúrákkal kapcsolatos tevékenységével összefüggésben van jelentősége. A szubszidiaritás elve alapján európai kérdéssé az a probléma válhat, amelynek megoldására a tagállami, azaz nemzeti keretek nem elegendőek. A kritikus infrastruktúrák esetében európainak minősül minden, „a tagállamokban található olyan kritikus infrastruktúra, amelynek megzavarása vagy megsemmisítése jelentős hatással lenne legalább két tagállamra". [12] Ebből következően a kritikus (információs) infrastruktúrák esetében elsődleges a nemzeti szintű megközelítés (meghatározás, azonosítás és védelem), és csak ezt követheti a nemzeti szinten túlnyúló, európai szintű védelem megvalósítása.

Az európai megközelítést Précsényi Zoltán és Solymosi József két tanulmánya részletesen elemzi, [13] [14] és a nemzeti feladatvállalást erősítő következtetésre jut: „a Bizottságnak adott, európai kritikus infrastruktúra-védelmi rendszer megalkotására irányuló mandátummal egyidőben minden tagállam megvizsgálta saját nemzeti rendszereit, s megállapította, hogy ha nem is a "kritikus infrastruktúrák" újszerű terminológiája alatt, de régóta van saját, bejáratott és működő védelmi rendszere, amely egyfelől szuverén stratégiai érdekeken alapul, másfelől pedig közigazgatási, politikai és ezer egyéb oknál fogva összeegyeztethetetlen a többi tagállamban honos rendszerekkel, szemléletekkel". [14]

2.2. Azonosítás és kijelölés

A fogalom kidolgozását az egyes kritikus infrastruktúrák azonosításának kell követnie. Az azonosítás jelenleg azon ágazatok és alágazatok számbavételénél tart, amelyek kritikus infrastruktúrákkal rendelkeznek vagy rendelkezhetnek. A kiválasztási szempontok és a már jelzett horizontális szempontrendszer között nyilvánvalóan és szükségszerűen szoros kapcsolat van. Az egyes államok – hagyományaik, közigazgatási berendezkedésük stb. alapján – eltérő csoportosítást alkalmaznak; tradicionálisan megnevezett szektorok az energiaellátás, közlekedés, távközlés, egészségügy, élelmiszer- és vízellátás, pénzügy, közbiztonság.

Az ágazatok és alágazatok azonosítását követő lépés a kijelölés kell, hogy legyen: azaz a konkrét infrastruktúrák és infrastruktúra-elemek (intézmények, rendszerek, hálózatok stb.) meghatározása. A probléma bonyolultságát szemléletesen mutatja a Bush-adminisztráció 2002-ben tett megállapítása: „a különböző kritikus infrastruktúra szektorokon belüli egyes eszközök, feladatok és rendszerek nem azonosan fontosak ... a közlekedési szektor létfontosságú, de nem minden egyes híd kritikus jelentőségű a Nemzet egésze számára". [15] Ahogyan Bukovics István és Vavrik Antal írja: „ami kritikus 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." [16] Ezen kívül a kritikusság ismérve – ahogyan a fogalmi tisztázás kapcsán már látható volt – térbeli, horizontális és időbeli tényezők módosulása okán folyamatosan változik.

2.3. Védelem

A fogalmi tisztázás, az azonosítás és a kijelölés nem öncélú: a helyzetfelmérés célja a megfelelő védelem megtervezéséhez és megvalósításához szükséges elvi és gyakorlati alapadatok meghatározása.

A védelem tervezése során tisztában kell lenni azzal a (többször bebizonyosodott) ténnyel, hogy teljes körű védelem nincs. A védelem szintje, eszközrendszere tökéletes nem, legfeljebb optimalizált (kockázatarányos, fenntartható, költséghatékony stb.) lehet.

Tekintettel kell lenni a fenyegetések típusára és az egyes fenyegetési típusokhoz tartozó események bekövetkezésének valószínűségére. Az elsődleges csoportosításhoz támpontot adhat például Nagy Rudolf tipológiája, amely alapján a zavar, a sérülés forrása lehet technológiai rendellenesség (pl. anyagszerkezeti hiba), külső – természeti – tényező kiváltotta véletlen baleset (pl. természeti katasztrófa) és szándékolt kár (pl. terrortámadás, szabotázs). [17] A zavar jelentkezhet közvetlen vagy közvetett módon is. Az információs rendszerek kapcsán Haig Zsolt és Várhegyi István a konfliktushelyzetek, a technikai lehetőségek és a motivációk (politikai, gazdasági, pénzügyi, katonai, szociális stb. célok) szerint változó fenyegetéseket különböztet meg. [5] Muha Lajos a fizikai és az információs dimenzióból érkező fenyegetéseket különíti el, ez utóbbi csoporton belül a támadó személye (alkalmazott, terrorista stb.) és az elkövetés módja (adathalászat, rosszindulatú programok bejuttatása, elektronikai felderítés stb.) szerint példálózó felsorolást is ad. [1]

A két utóbb említett csoportosítás az információs infrastruktúrák fenyegetettségének egy sajátosságára is felhívja a figyelmet: ezen infrastruktúrák vonatkozásában a fenyegetések, támadások nem feltétlenül a működés megzavarására, az infrastruktúra megsemmisítésére irányulnak, a cél lehet az információtartalom megismerése, ellenőrzés alatt tartása is. A kritikus információs infrastruktúrák elleni támadások módszereit (számítógép-hálózati támadás, elektronikai felderítés és elektronikai támadás) és eszközeit részletesen elemzi Haig Zsolt, Hajnal Béla, Kovács László, Muha Lajos és Sík Zoltán Nándor közös tanulmánya. [18]

A fenyegetéseknek, a kritikus infrastruktúrák sebezhetőségének és a megzavarásuk vagy megsemmisítésük okozta károk lehetséges hatásainak felmérése – a kockázatelemzés – adja a kiindulópontot a védelem megtervezéséhez és megvalósításához.

A fentiek alapján határozhatók meg a védelem céljai is: az infrastruktúrák működésében fellépő zavarok megelőzése, a zavarok elhárítása és a rendeltetésszerű működés helyreállítása. A bekövetkező károk oldaláról: a károk megelőzése, a károk enyhítése, illetve az eredeti állapot helyreállítása. A szándékolt károk (támadások) veszélyének jelentőségét mutatja, hogy a megelőzés – elhárítás – helyreállítás (alapvetően működési szempontú) hármas célján túl Muha Lajos hangsúlyt helyez a támadók elrettentésére, azonosítására, elfogására (és nyilvánvalósan: felelősségre vonására) is. [1]

A védelem tervezésénél törekedni kell arra, hogy minél több szempont számbavételével történjék meg a védelmi rendszer kialakítása.

A védelmi rendszer legyen többszintű és többféle elemből álló. A nemzetközi és a hazai szabványok, legjobb gyakorlatok a szervezeti és személyi, fizikai (környezeti), informatikai és adminisztratív védelmi eszközök, eljárások komplex rendszerét javasolják, amelyben a helyi és a központi feladatok, felelősségi körök összhangja is megvalósul.

A szakma által ismert és alkalmazott fenti szempontrendszer néhány eleme már működő evidencia (pl. a helyi szintű objektumvédelem, amely magában foglalja az őrzésvédelmet, tűzvédelmet, vagyonvédelmet stb., mindezt személyi és biztonságtechnikai elemek belső szabályozókban előírt, kombinált alkalmazásával), mások még csak problémafelvetések. Ez utóbbi körbe sorolható a központi és a helyi, az állami és az önkormányzati, illetve a kormányzati és az üzemeltetői felelősség meghatározása és a terhek megosztása, vagy éppen a nemzeti szabályrendszer és nyilvántartás/számontartás kialakítása és működtetése.

A feladatok, a felelősségek és a terhek megosztása a kormányzati és az üzemeltetői szint között kiemelt jelentőségű. A kritikus infrastruktúrák üzemeltetői (tulajdonosai) gyakran nem állami, hanem piaci szereplők, az ügyfelek viszont az állam polgárai. A kritikus infrastruktúrák kieséséből, megsemmisüléséből keletkező károk nemcsak az üzemeltetőknek okozhatnak veszteséget, hanem az embereket mint ügyfeleket és mint az infrastruktúra környékén élő lakosságot is sújthatják. Ez utóbbi esetek okán az államnak nyilvánvaló kötelezettsége a kármegelőzés és a kárenyhítés. A kritikus infrastruktúrák jelentőségére tekintettel az államnak az is érdeke, hogy az üzemeltetésben közreműködő piaci szereplők érdekeltsége is megmaradjon. A piaci szereplők oldaláról vizsgálva a kérdést leszögezhető, hogy az üzemeltetés mint profittermelő tevékenység része kell legyen a védelmi intézkedések megtervezése és megvalósítása is. A védelemnek pedig komoly költségei vannak. Mindezekből következően a kormányzati és a piaci szereplők egymásra vannak utalva, és előremutató megoldás csak akkor tud születni, ha abban mindkét oldal érdekei érvényesülnek.

A védelem központi (állami) szabályozásának, valamint irányításának, felügyeletének és ellenőrzésének szükségessége – a meghatározások alapján – vitathatatlan. A megvalósítást tekintve még van teendő.

3. EURÓPAI UNIÓS EREDMÉNYEK A KRITIKUS INFRASTRUKTÚRÁK VÉDELME TERÉN

3.1. Általános iránymutatás és együttműködés

Mind az eddig tárgyalt elméleti kérdések, mind az ezután említendő gyakorlati eredmények – tagságunkból fakadóan magától értetődően – szoros kapcsolatban voltak és vannak az Európai Unió kritikus infrastruktúrákat érintő tevékenységével.

Az Európai Unió Tanácsa 2004-ben kérte fel a Bizottságot, hogy készítsen átfogó stratégiát a kritikus infrastruktúrák védelmére. 2005-ben a Bizottság *Zöld Könyv*et fogadott el a kritikus infrastruktúrák védelmére vonatkozó európai programról, [19], majd 2006-ban javaslatot dolgozott ki egy tanácsi irányelvre, [4] [20] amelyet az Európai Unió Tanácsa 2008-ban fogadott el. [12]

Az irányelv közös eljárást hozott létre az európai kritikus infrastruktúrák (European critical infrastructure, ECI) azonosítására és kijelölésére, valamint közös megközelítést alakított ki annak értékelésére, hogy szükséges-e az érintett infrastruktúrák védelmét javítani. Célul tűzte ki a bizalmon és biztonságon alapuló, strukturált és következetes információcsere megvalósítását az ECI-k tulajdonosai/üzemeltetői és a tagállam, valamint az egyes tagállamok, továbbá a tagállamok és a Bizottság között. Az ECI-k azonosítása és kijelölése érdekében meghatározta azok fogalmát,

rögzítette a horizontális kritériumokat (a küszöbértékek meghatározását a tagállamokra bízva), kijelölte azokat az ágazatokat és alágazatokat, amelyek európai kritikus infrastruktúrával rendelkezhetnek. A tagállamoknak kötelezte arra, hogy 2011. január 12-éig jelöljék ki az ECI-ket az energia- és a közlekedési ágazatban. Jelezte továbbá, hogy az irányelv (2012. január 12-étől előírt) felülvizsgálata és a további ágazatok meghatározása során elsőbbséget kell biztosítani az IKT – információs és kommunikációs technológiák – ágazatnak.

3.2. Információbiztonsági együttműködés és cselekvési terv

Az együttműködés általános kereteinek kidolgozásán túl a Bizottság a Tanácstól kapott felhatalmazás alapján 2008-ban javaslatot dolgozott ki a kritikus infrastruktúrák figyelmeztető információs hálózatának (Critical Infrastructue Warning Information Network, CIWIN) létrehozására is. [21] A Bizottság javaslatában megállapította, hogy az Európai Unióban számos ágazati sürgősségi riasztórendszer létezik, de ágazatokat átfogó jellegű nincs, ezért egy biztonságos, önkéntes és többszintű kommunikációs/riasztórendszer létrehozását indítványozta, két elkülönült – „sürgősségi riasztórendszer és a kritikus infrastruktúrák védelmével kapcsolatos vélemények és bevált módszerek cseréjére szolgáló elektronikus fórum” – funkcióval.

A „Közösségen belüli magas szintű és hatékony hálózat- és információbiztonság biztosítása”, valamint a „hálózat- és információbiztonsági kultúra kifejlesztése” érdekében az Európai Parlament és a Tanács létrehozta az Európai Hálózat- és Információbiztonsági Ügynökséget (European Network and Information Security Agency, ENISA), meghatározta feladatait, szervezetét és működési rendjét. [22] Az ENISA információcserét, együttműködést lehetővé tevő és koordináló, tanácsadó feladatokat is ellátó szervezetként jött létre öt éves időtartamra. 2009-ben megbízatási idejét 2012. március 13-áig meghosszabbították. [23] 2010-ben a Bizottság az ENISA megerősítésére és modernizálására, továbbá tevékenysége további öt évre történő meghosszabbítására vonatkozó rendelettervezetet készített, mivel „szükség van egy olyan szakpolitikai eszközrendszerre, amely proaktív módon képes azonosítani a hálózat- és információbiztonság területén jelentkező kockázatokat és rendszereink gyenge pontjait, amely létrehozza a válaszadás mechanizmusait, és amely képes

gondoskodni arról, hogy ezeket a válaszadási mechanizmusokat az érdekeltek ismerjék és alkalmazzák". [24]

Az információcserén és a koordináción túl az Európai Unió *Cselekvési terv*et is készített [9] és annak végrehajtását is figyelemmel kíséri. [10] A *Cselekvési terv* öt pillére a Felkészülés és megelőzés, az Észlelés és reagálás, a Hatások enyhítése és a helyreállítás, a Nemzetközi együttműködés és az Európai kritikus infrastruktúrákra vonatkozó követelmények az IKT-ágazat számára. Az utóbbi kérdéskör kapcsán a 2011-es közlemény rögzíti, hogy elkészült a vezetékes és mobiltávközlésre, valamint az internetre vonatkozó kritériumrendszer tervezete, az IKT-ágazatspecifikus kritériumok műszaki vitáját 2011 végén tervezik lezárni, konzultációkat terveznek a magánszférával az ágazati kritériumokról és a Bizottság megtárgyalja a tagállamokkal a 2008/114/EK irányelv 2012-ben esedékes felülvizsgálata során megfontolandó elemeket is. [10]

4. GYAKORLAT: A KRITIKUS INFRASTRUKTÚRÁK VÉDELMÉVEL KAPCSOLATOS SZABÁLYOZÁS ÉS SZERVEZETRENDSZER

4.1. Elvi keretek, programok: országgyűlési és kormányhatározatok, stratégiai dokumentumok

A kritikus infrastruktúrák (köztük a kritikus információs infrastruktúrák) védelmének céljait, irányait, kereteit, továbbá a védelemmel kapcsolatos kormányzati feladatokat országgyűlési és kormányhatározatok, továbbá különböző stratégiai dokumentumok rögzítik.

Az Országgyűlés 1998-ban fogadta el a *Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről* szóló határozatot, amely a biztonságot átfogó módon értelmezi, és fogalmába beleérti annak „információs és technológiai dimenzióját" is. [25]

A határozat alapján dolgozta ki és fogadta el a kormány a *Magyar Köztársaság nemzeti biztonsági stratégiáját*, amely a terrorizmus elleni küzdelem keretein belül szól a kritikus infrastruktúrák védelmének szükségességéről, *Az információs társadalom kihívásai* alfejezetben pedig leszögezi „az informatikai infrastruktúra technikai és szellemi feltételeinek biztosítása mellett ügyelni kell e rendszerek védelmére és a megfelelő tartalékok képzésére is", és szoros koordinációt ír elő „mind a szövetségesekkel, mind az informatikai és távközlési szolgáltatók, valamint kutatóközpontok között". [26]

2004 és 2007 között három kormányhatározat született a terrorizmus elleni küzdelem aktuális feladatairól, amelyek az *Európai Unió Terrorizmus Elleni Cselekvési Tervé*nek hatékony végrehajtása érdekében a kritikus infrastruktúrák védelmével kapcsolatos ágazatközi koordinációs feladatokat határoztak meg. [27] [28] [29]

Szintén az európai folyamatokat képezte le az a 2008-ban közzétett kormányhatározat, amelynek 1. sz. melléklete a *Zöld Könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról*, 2. sz. melléklete a *Szektorok és felelősök listája*. [3] A *Zöld Könyv* a kritikus infrastruktúrák meglehetősen tág, a kölcsönös függőséget hangsúlyozó meghatározását adja, azonban a kritikus információs infrastruktúrák definíciójával – ellentétben az európai *Zöld Könyv*vel – adós marad. Tartalma értelemszerűen szoros kapcsolatot mutat az európai *Zöld Könyv*vel, az alapfogalmak leírásán túl meghatározza a védelem céljait és alapelveit, iránymutatást ad a kritikus infrastruktúrák kijelöléséhez, rögzíti a védelemben részes szereplők feladatait és felelősségét, együttműködési formáit. A *Szektorok és felelősök listája* felsorolja az érintett ágazatokat és alágazatokat; a kritikus információs infrastruktúrákat a kilenc alágazatot tartalmazó infokommunikációs technológiák ágazat képviseli.

Az Európai Unió Tanácsa által meghatározott feladatok teljesítése érdekében 2010-ben újabb kormányhatározat született. [30] A dokumentum az ECI-k védelmével kapcsolatos koordinációs feladatok ellátására nemzeti kapcsolattartó pontként (European Critical

Infrastructure Protection Contact Point) a belügyminisztert jelöli ki, munkacsoportot hoz létre az ECI-k azonosításához szükséges kritériumrendszer kidolgozására (2011. január 5-ei határidővel) és az ECI-k kijelölésére vonatkozó javaslat megfogalmazására, az ECI-k kijelölésével a nemzeti fejlesztési minisztert bízza meg (2011. február 15-ei határidővel), rendelkezik az Európai Bizottság felé fennálló jelentési kötelezettség teljesítéséről (első alkalommal 2011. január 12-ei határidővel).

Ez a kormányhatározat az európai uniós teendőkön túl a nemzeti kritikus infrastruktúrák védelmével kapcsolatos feladatokat is rögzít, így az említett munkacsoportot bízza meg a nemzeti kritikus infrastruktúra védelem intézmény- és kritériumrendszerének kidolgozásával, továbbá a kormányzati szereplők és a civil szféra kritikus infrastruktúra védelemmel kapcsolatos együttműködésének megteremtése érdekében konzultációs fórum felállítását rendeli el (2011. március 31-ei határidővel). A dokumentum külön hangsúlyt helyez a honvédelmi érdekből kritikus infrastruktúrák védelmére: a honvédelmi minisztert felhívja a vonatkozó intézmény- és követelményrendszer kidolgozására (2011. február 28-ai határidővel).

2011. február 2-ai keltezésű a tárgyban közzétett legutóbbi kormányhatározat. [31]

A kritikus információs infrastruktúrák védelmét önálló alfejezetben tárgyalja az egyik legutóbbi, a Nemzeti Fejlesztési Minisztérium által készített stratégiai dokumentum. [8] A szakmai műhelyek által kidolgozott, valamint a nemzeti *Zöld Könyv*ben megjelent elméleti megközelítés rövid áttekintése után négy akcióban foglalja össze a tennivalókat, amelyek lényege a központi (állami) szerepvállalás növelése a védelem vezetésében és a védelmi stratégia kidolgozásában, a nemzeti és az európai kritikus infrastruktúrák kijelölésében és a kijelölések felülvizsgálatában, a feladat-meghatározásban és a szabályozásban, továbbá összkormányzati szinten a tudatosság növelése, az oktatás és a képzés.

4.2. Ágazati jogszabályok

A stratégiai jellegű, programadó dokumentumokon túl meghatározó jelentőségűek az egyes ágazatokra vonatkozó jogszabályok. Ezek már jóval a kritikus infrastruktúrák fogalmának megjelenése előtt stabil alapot képeztek az egyes szektorok tevékenységéhez, beleértve a védelmi feladatokat is. Igaz ez a kritikus információs infrastruktúrák esetében is. Sőt, a kritikus infrastruktúrák első hazai normatív megfogalmazását egy ágazati védelmi jogszabály tartalmazza. [32]

Az ágazati jogszabályok – törvények, kormány- és miniszteri rendeletek – számbavétele meghaladná jelen munka kereteit.

A kritikus információs infrastruktúrák vonatkozásában a legjelentősebb jogszabályok az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény (Ekszt.) [33] és végrehajtási rendeletei, így különösen a *223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról*. [2] Ez utóbbi rögzíti, hogy az elektronikus közszolgáltatások nyújtását, illetve igénybevételét támogató központi informatikai és kommunikációs rendszerek együttese, azaz „*a központi rendszer – a kritikus infrastruktúra része*, védelmét a kritikus infrastruktúrára vonatkozó, nemzetközileg kialakult biztonsági követelményeknek megfelelően kell kialakítani”. [2] A jogszabály meghatározza a kritikus infrastruktúra és az információbiztonsági fenyegetés fogalmát, minőségirányítási, biztonsági, szabályozási és ellenőrzési követelményeket fogalmaz meg, rendelkezik az informatikai biztonság irányításáról és a működtetéssel kapcsolatos felelősségi viszonyokról. Bár a rendelet csak az elektronikus közszolgáltatás vonatkozásában szabályoz(hat), előírásai – némi fogalmi pontosítás után – irányadóak lehetnek általánosabb szabályozás esetében is. A dokumentum kétségtelen érdeme, hogy a korábban csak legjobb gyakorlatként illetve szabványokban megjelenő informatikai biztonsági előírásokat normatív szintre emelte. A jogszabály rendelkezik a Nemzeti Hálózatbiztonsági Központ létrehozásáról is (lásd később).

4.3. Új megközelítés: az adatvagyon törvény

A nemzeti adatvagyon körébe tartozó állami nyilvántartások védelméről szóló 2010. évi CLVII. törvény (Nav. tv.) [34] és végrehajtási rendelete [35] adatvédelmi okokból – tehát nem az infrastruktúra védelme érdekében – rögzít a közigazgatásban végzett elektronikus adatfeldolgozásra vonatkozóan biztonsági előírásokat. Ezek az előírások meghatározzák a védendő adatállományt kezelő informatikai rendszerek elvárt védelmi szintjét (*Korlátozott terjesztésű* minősítési szintű adatot kezelő rendszerre egyébként irányadó személyi, fizikai, adminisztratív és elektronikus biztonsági követelmények teljesítése), illetve korlátozzák ezen rendszerek működtetőinek körét (csak államigazgatási szerv vagy kizárólagos állami tulajdonú gazdálkodó szervezet lehet). A korábban kifejtettek alapján ezek a rendelkezések a kritikus információs infrastruktúrák egy típusára vonatkozó konkrét védelmi intézkedéseknek is tekinthetők.

4.4. Szervezetrendszer

A közigazgatás szervezetrendszerén belül az érintett szereplők, feladataik, felelősségeik, együttműködési formáik – az előbbiekben tárgyalt stratégiai-koordinációs illetve ágazati-operatív szinten – azonosíthatók.

A már idézett, 2010-ben közzétett kormányhatározat két új együttműködési fórum kialakításáról rendelkezett. A (korábban már említett) közigazgatási munkacsoport létrehozására a belügy-, a nemzeti fejlesztési, a nemzetgazdasági, a közigazgatási és igazságügyi és a honvédelmi minisztert hívta fel, a kormányzat és a civil szféra közötti együttműködés megteremtésére az érintett miniszterek részéről kijelölt vezetők, valamint az infrastruktúra-tulajdonosok, üzemeltetők, érdekvédelmi szervezetek, tudományos testületek bevonásával konzultációs fórum működtetését írta elő. [30]

A kritikus információs infrastruktúrák védelmében meghatározó szerepet játszó Nemzeti Hálózatbiztonsági Központ (NHBK) tevékenységének előzményei 2004-re nyúlnak vissza, amikor a Puskás Tivadar Közalapítvány (PTA) az Informatikai és Hírközlési Minisztérium támogatásával programot indított egy magyarországi hálózatbiztonsági központ létrehozása érdekében. [36] A PTA-CERT Hungary Központ 2005. januártól kezdte meg működését a Miniszterelnöki Hivatal Elektronikuskormányzat-központ felügyelete alatt, 2010. január 1-jétől – a már idézett kormányrendelet alapján, „a magyar kritikus információs infrastruktúrák védelme, valamint a központi rendszeren megvalósuló kommunikációs biztonság, a vírus- és más támadások káros hatásainak korlátozása érdekében nemzetközi együttműködéssel” – az NHBK feladatait is ellátja, továbbá magyar Nemzeti Kapcsolattartó Pontként (NKP) és kormányzati számítástechnikai sürgősségi reagáló egységként (kormányzati CERT) működik. [2] Ez utóbbi minőségében együttműködést folytat más nemzeti (német, holland, lengyel stb.) és nemzetközi CERT szervezetekkel (Forum of Incident Response and Security Teams, FIRST, European Government CERTs group, EGC).

4.5. Hazai szakmai - tudományos eredmények

A kritikus infrastruktúrák és a kritikus információs infrastruktúrák védelmével foglalkozó (az előzőekben többször idézett) szakértői kör az elmúlt években az elméleti kérdések vizsgálatán túl tevékeny szerepet vállalt a kormányzati jogalkotás és jogalkalmazás támogatásában is. Az ismertetett tudományos publikációk, stratégiai dokumentumok és jogszabályok kevés különbséggel ugyanazon gondolatmenetet tükrözik, viszonylag egységes kiindulási pontot biztosítva a gyakorlati megvalósításhoz.

A tudományos tevékenység a fogalmi tisztázáson túl módszertani alapot is kívánt nyújtani a kritikus infrastruktúrák kijelöléséhez és azonosításához, [1] [18] sőt egyes információs infrastruktúrák esetében konkrét rendszerek elemzéséig is eljutott. [37] A módszertani javaslatok a már ismertetett elméleti alapvetésből kiindulva igyekeznek konkretizálni az

azonosítás és kijelölés folyamatát. Azon ágazatok meghatározása, amelyek kritikus infrastruktúrákkal rendelkezhetnek – különösen az EU és a nemzeti *Zöld Könyv* ismeretében – egyszerű feladatnak tűnik. Megjegyzendő, hogy éppen az információs infrastruktúrák területe az, ahol már az alágazatok elhatárolása is problémát okoz. Muha Lajos külön alágazatként nevesíti az informatikai rendszerek és hálózatok, valamint a közigazgatási informatika és kommunikáció területét, továbbá négy távközlési területet, vegyítve az infrastruktúra-jelleg és a rendeltetés fogalmát. [1] Ugyanez a csoportosítás jelenik meg némi módosítással a nemzeti *Zöld Könyv*ben is. [3] A kritikusság értékelése minőségi és mennyiségi jellemzőkön alapulhat. Többször idézett alaptétel, hogy a nemzeti szempontból kritikus és a helyi szinten kritikus fogalma nem esik egybe. A megkülönböztetéshez segítséget nyújthat a számszerűsítés: a javaslat megfogalmazói – külföldi példa alapján – a küszöbértékeket egy háromfokozatú skála (alacsony - közepes - magas) szerint határoznák meg. [18] Az ilyen típusú kategorizálás szolgálhat alapul a kritikus infrastruktúrák kijelöléséhez és rangsorolásához. A végeredményt minőségi (nem mérhető vagy pontosan nem mérhető) jellemzők is befolyásolhatják. Ez utóbbi körbe tartozik az államba vetett bizalom megrendülése, az állampolgárok társadalmi-politikai környezethez viszonyulása (az Egyesült Államokban 2003-ban kiadott elnöki direktíva – morális jelentőségükre tekintettel – a nemzeti emlékműveket és szimbólumokat is a nemzeti kritikus infrastruktúrák körébe sorolja). [39] További pontosítást eredményezhet a kölcsönös függőségi mutató, vagyis az tény, hogy egy adott infrastruktúra kiesése kihat-e, és ha igen, mennyiben, további egy vagy több infrastruktúra működésére. Végül pedig a kialakult sorrendet egy új horizontális elem, vagy a dimenziókban bekövetkező módosulás felülírhatja.

A szakértők a kormányzati, társadalmi és gazdasági szereplőknek a kritikus infrastruktúrák védelmével kapcsolatos feladatait is számba vették. Kovács László 2008-ban írt, kormányzati feladatokat áttekintő tanulmányának megállapításai ma is időszerűek. [38] A feladatok meghatározása és végrehajtása tekintetében kettősség tapasztalható: az egyes szektorok tradicionálisan vagy jól felfogott gyakorlati érdekből rendelkeznek stratégiával, szervezetrendszerüket, tevékenységüket, együttműködésüket leíró és keretbe foglaló jogszabályokkal, működésük feltételeit meghatározzák és igyekeznek teljesíteni (teljesíttetni) is – a rendszer működik. Az ágazatok közötti és feletti szintet azonban – egyelőre – a sokszereplős koordinációs fórumok jelentik. Márpedig a téma jelentőségére tekintettel az ennél határozottabb – az érintettek konszenzuson alapuló véleményét tükröző –, központi szabályozás, a felelősségi körök nemzeti szintű elhatárolása, az irányításhoz szükséges szakmai kompetencia és a pontos feladat- és hatáskör-meghatározás is szükséges lehet.

5. ÖSSZEGZÉS

A kritikus infrastruktúrák (köztük a kritikus információs infrastruktúrák) védelmének tervezése és megvalósítása során alapvető jelentőségű elv az egységesítés és az ágazatfelettiség.

A hazai és a külföldi dokumentumok, jogszabályok, szabványok, ajánlások, tudományos publikációk nyomán a fogalomrendszer egységesíthető. A normatív keretrendszer megalkotása és a már létező jogszabályok felülvizsgálata, egységesítése és kiegészítése az egyik első lépés lehet a kritikus infrastruktúrák védelmének kormányzati feladatai között. A (végre) konzisztens és kötelező fogalomrendszer alapján, a jogszabályban (részben már) rögzített szervezetrendszer és eljárásrend keretein belül biztosított lehet a részletes feladat-meghatározás és -elhatárolás a közigazgatás, a piaci szféra és a társadalmi szereplők számára.

A kritikus infrastruktúrák azonosítása és rangsorolása, majd az eredmények folyamatos aktualizálása a kijelölt kormányzati felelős rendszeres egyeztetést igénylő – nem könnyű – feladata lehet.

Ezt követheti a védelem központi szervezési feladatainak kiteljesítése a már ismertetett elvek szerint.

Ami újszerű: az egységes szemléletmód és megközelítés, az ezen alapuló elemzés és összehasonlítás, az azonos elvek és módszertanok szerinti tervezés és végrehajtás kívánalma.

A „mi és mennyire kritikus infrastruktúra” kérdésre adandó válasz megfogalmazásához minőségi és mennyiségi jellemzők ismerete, közigazgatási és piaci számítások elvégzése és nem utolsósorban az érintettek szakmai alapú konszenzusa szükséges. A „hogyan védjük” kérdésre pedig a már létező eredmények felmérésén, összehasonlításán, szintetizálásán, jobbításán keresztül adható megnyugtató válasz.

Mindez nagy kihívás: túl kell lépni évtizedes hagyományokat és beidegződéseket, újra kell gondolni a saját és a közös értékeket és érdekeket, újfajta – még nem ismert vagy nem elterjedt – módszereket, eljárásokat kell kialakítani és meghonosítani, ráadásul egy sokszereplős – kormányzati és civil, nemzeti és nemzetközi – együttműködés keretében.

Felhasznált irodalom

[1] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. Doktori (PhD) értekezés. Budapest, 2007

[2] 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról

[3] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[4] Javaslat - a Tanács irányelve az európai létfontosságú infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (COM (2006) 0787 végleges), 2006. december 12.

[5] Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005.

[6] Magyary Zoltán Közigazgatás-fejlesztési Program (MP 11.0), Közigazgatási és Igazságügyi Minisztérium, Budapest, 2011. június 10.

[7] Munk Sándor: Információs szolgáltatásokat nyújtó hálózatok alapjai – Hadmérnök, 2011. (VI.)/2., 227-243. o. http://www.hadmernok.hu/2011_2_munk.php; (2011. 11. 22.)

[8] Digitális Megújulás Cselekvési Terv 2010-2014., Nemzeti Fejlesztési Minisztérium, Budapest, 2010.

[9] A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről – „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása” (COM (2009) 149 végleges), 2009. március 30.

[10] A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről – „Eredmények és következő lépések: a globális kiberbiztonság felé” (COM (2011) 163 végleges), 2011. március 31.

[11] Munk Sándor – Fleiner Rita: Adatbázisok kritikus infrastruktúrákban – Hadmérnök, 2009. (IV.)/1., 225-234. o. http://www.hadmernok.hu/2009_1_fleiner.php; (2011. 11. 22.)

[12] A Tanács 2008. december 8-i 2008/114/EK Irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (EGT-vonatkozású szöveg), 2008. december 8.

[13] Précsényi Zoltán – Solymosi József: Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé – Hadmérnök, 2007. (II.)/1., 227-243. o. http://www.hadmernok.hu/archivum/2007/1/2007_1_precsenyi.html; (2011. 11. 22.)

[14] Précsényi Zoltán – Solymosi József: Kritikus infrastruktúrák azonosítása: körkép az EU-ban és az USA-ban tapasztalható nehézségekről – Hadmérnök, 2008. (III.)/1., 59-67. o. http://www.hadmernok.hu/archivum/2008/1/2008_1_precsenyi.html; (2011. 11. 22.)

[15] The President's National Strategy for Homeland Security, 2002. július 16. Idézi: Précsényi Zoltán – Solymosi József: Kritikus infrastruktúrák azonosítása: körkép az EU-ban és az USA-ban tapasztalható nehézségekről – Hadmérnök, 2008. (III.)/1., 59-67. o.

[16] Bukovics István – Vavrik Antal: Infrastruktúrák kockázata és biztonsága: kritikai problémaelemzés – Hadmérnök, 2006. (I.)/3. http://www.hadmernok.hu/archivum/2006/3/2006_3_bukovics.html; (2011. 11. 22.)

[17] Nagy Rudolf: A kritikus infrastruktúra védelme és katasztrófavédelmi aspektusai a terrorizmus tükrében – Kard és toll 2006/3., 56-64. o.

[18] Dr. Haig Zsolt - Hajnal Béla - Dr. Kovács László - Dr. Muha Lajos - Sík Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana. ENO Advisory Kft., 2009.

[19] Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról (COM (2005) 0576 végleges), 2005. november 17.

[20] A Bizottság közleménye – A létfontosságú infrastruktúrák védelmére vonatkozó európai programról (COM (2006) 0786 végleges), 2006. december 12.

[21] Javaslat - a Tanács határozata a létfontosságú infrastruktúrák figyelmeztető információs hálózatáról (COM (2008) 0676 végleges), 2008. október 27.

[22] az Európai Parlament és a Tanács 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról (EGT-vonatkozású szöveg), 2004. március 10.

[23] az Európai Parlament és a Tanács 1007/2008/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendeletnek az Ügynökség megbízatási ideje tekintetében történő módosításáról (EGT-vonatkozású szöveg), 2008. szeptember 24.

[24] Javaslat – Az Európai Parlament és a Tanács rendelete az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA) (COM (2010) 521 végleges), 2010. szeptember 30.

[25] 94/1998. (XII. 29.) OGY határozat a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről

[26] 2073/2004. (IV. 15.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról

[27] 2112/2004. (V. 7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól

[28] 2151//2005. (VII. 27.) Korm. határozat a Terrorizmus Elleni Nemzeti Akcióterv felülvizsgálatáról

[29] 2046/2007. (III. 19.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól szóló 2112/2004. (V. 7.) Korm. határozat módosításáról

[30] 1249/2010. (XI. 19.) Korm. határozat 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

[31] 2003/2011. Korm. határozat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelv végrehajtásáról és az Európai bizottság számára történő jelentésről

[32] 27/2004. (X. 6.) IHM rendelet az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségéről

[33] Az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény (Ekszt.)

[34] A nemzeti adatvagyon körébe tartozó állami nyilvántartások védelméről szóló 2010. évi CLVII. törvény

[35] 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról

[36] http://www.cert-hungary.hu Letöltés: 2011.11. 22.

[37] Kovács László: Kritikus infrastruktúrák Magyarországon. Robothadviselés 7. tudományos szakmai konferencia 2007. november 27. Hadmérnök Különszám http://www.hadmernok.hu/kulonszamok/robothadviseles7/kovacs_rw7.html; (2011. 11. 22.)

[38] Kovács László: Az információs terrorizmus elleni tevékenység kormányzati feladatai – Hadmérnök, 2008. (III.)/2., 138-148. o. http://www.hadmernok.hu/archivum/2008/2/2008_2_kovacsl.html; (2011. 11. 22.)

[39] Homeland Security Presidential Directive 7/HSPD-7, Washington, 2003. december 17. Idézi: Dr. Haig Zsolt - Hajnal Béla - Dr. Kovács László - Dr. Muha Lajos - Sík Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana. ENO Advisory Kft., 2009.