HADMÉRNÖK

VII. Évfolyam 2. szám - 2012. június

Bonnyai Tünde
bonnyai.tunde@gmail.com

ÚTON A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK AZONOSÍTÁSA ÉS VÉDELMÜK KIALAKÍTÁSA FELÉ

Absztrakt

A XXI. század információs társadalma, a tudástársadalom felé vezető út a kritikus infrastruktúra védelem törekvései mentén, az információs infrastruktúrák függőségének jegyében egyre komolyabb kihívások elé állítja a mindennapok rendszereit. Az alábbi cikk célja, hogy bemutassa a kritikus infrastruktúrák és kritikus információs infrastruktúrák közötti különbségeket és függőségeket, amelyekhez nemzetközi és hazai jogi és szervezeti háttér párosul. Végül a tapasztalatok alapján meghatározza a kritikus információs infrastruktúrák azonosításának és védelmük kialakításának alapvető feltételeit.

The information society of the 21st Century towards the knowledge-based-society, along the efforts of critical infrastructure protection, in the spirit of information infrastructure's dependences pose increasingly serious challenges for systems of everyday life. The identification of critical informational infrastructures, the recognition of the importance of their role, and their safety should be priority. This article aims to present differences and dependencies between critical infrastructures and critical information infrastructures, which coupled with international and domestic legal and institutional background. Finally, based on experiences it defines the basic conditions for identification and protection of critical information infrastructures.

Kulcsszavak: *kritikus infrastruktúra, kritikus információs infrastruktúra, interdependencia, kiberfenyegetés, azonosítás és védelem kialakítása, critical infrastructure, critical information infrastructure, interdependency, cyber threats, identification of critical information infrastructure*

ALAPVETŐ KÜLÖNBSÉGEK A KRITIKUS INFRASTRUKTÚRA ÉS A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA KÖZÖTT

Az ember biológiai evolúciós folyamatának korai szakaszában, az előembernek is nevezett, többféle típusba sorolható emberősök már két lábon jártak, eszközöket használtak, és megjelentek életformáikban az első olyan szükségletek, amelyeket később a homo sapiens – modern emberré válása során – egyre ügyesebben és fejlettebben elégített ki. A környezet kihívásai – az élő szervezet számára legmeghatározóbb tényezők – reakciókat generáltak: eszközhasználat és -fejlesztés, rugalmas alkalmazkodás, hierarchikus létformák, szabálykövető magatartási módozatok alakultak ki. Tekintettel a mai megfogalmazások változatosságára, az őskori kezdeményezéseket (a tűz többcélú alkalmazása, vadászati és védelmi fegyverek készítése, háziasított állatok tartása, stb.) tekinthetjük a klasszikus infrastruktúra kezdeti megjelenési formájának. Az ember és a különböző kultúrák fejlődésével később megjelentek olyan módszerek, amelyeket már korai infrastruktúráknak nevezhetünk. Ilyen volt például az ókori Egyiptom kiterjedt öntöző rendszere, Kína fejlett úthálózata, vagy Hammurapi törvényoszlopa, és ókori, majd középkori birodalmak hadseregei is. Akkoriban – egészen a XX. század közepéig – a társadalmak főként erővel igyekeztek megvédeni azokat a kialakított infrastruktúrákat, amelyek számukra kiemelt fontossággal, vagy létszükségletként funkcionáltak.

A biológiai evolúciós fejlődés mellett kulturális és technikai evolúciós folyamat is megfigyelhető a történelem nyomon követésével, amely során az infrastruktúrák – főként ipari forradalmak hatására – ugrásszerű fejlődésen mentek keresztül. A közlekedési eszközök és módszerek fejlődése, az energia felhasználási módjainak megjelenése, a távközlési eszközök kialakulása, a XIX. századra jellemző tömegtermelésre való áttérés, valamint a tudományos felfedezések lépésről lépésre tették gördülékenyebbé a hétköznapokat és ez által élhetőbbé a közvetlen környezetet. Fontos azonban hangsúlyt helyezni arra, hogy a XX. század nagy áttörései, az emberiség „örökké kíváncsi" jelleme, a technikai fejlődés iránti elkötelezettség egymásrautaltságot és a komplexitás kockázatát hordozzák magukban, miközben az infrastruktúrák léte természetessé és megszokott válik életünkben [1].

Az infrastruktúra

A komplex jellegből, a megannyi funkcionális tulajdonságból, az átfogó és összefüggő megközelítésből adódóan az infrastruktúra nehezen definiálható fogalom. Dr. Cecei Katalin és Mórocz Attila szerzőpáros megfogalmazásában a társadalmat körülvevő környezetet nevezzük infrastruktúrának, amely nem más, mint *„ember alkotta rendszerek és eljárások hálózata, amelyek szinergikusan együttműködve arra törekszenek, hogy folyamatosan alapvető termékeket és szolgáltatásokat állítsanak elő és terjesszenek"*[1]. Dr. Kovács Ferenc úgy fogalmazott, hogy az infrastruktúra *„a termeléshez kapcsolódó azon eszközök és intézmények összessége, amelyek nem részei a közvetlen termelési folyamatnak, de annak nélkülözhetetlen feltételei"* [3].

A meghatározások szerint az infrastruktúra esetében mindig olyan rendszerekre kell gondolnunk, amelyek *célja*, hogy a termelés folyamatában, a társadalom számára termékek és szolgáltatások elérését tegyék lehetővé. Működésük legfőbb *jellemzője* ezzel párhuzamosan az együttműködés, a folyamatosság, a hálózatszerűség és a fenti célok teljesülésének feltétele.

[1] [2] p. 39.

Az információs infrastruktúra

A XXI. századra jellemző technikai, technológiai, szellemi és intellektuális fejlettségi szintnek megfelelően a termelő-ipari berendezkedésű társadalmi rendszert fokozatosan felváltja az információs társadalom[2], amelyet tudásalapú társadalomnak[3] is nevezhetünk. A XX. század közepén bekövetkezett „technológiai forradalomnak" köszönhetően az utóbbi 50-70 év alakulását, változását a számítástechnika térhódítása, az elektronikus eszközök és módszerek terjedése, a távközlés határozta meg. Manapság olyan globális méreteket öltő kommunikációs hálózatok teszik lehetővé a kormányzat, az ipar, a termelés, a kereskedelem, a pénzügyi szféra, az információtechnológia, az oktatás-kutatás-fejlesztés területének folyamatos innovációját, amelyek alapvetően az informatika és a távközlés eszközein és rendszerein alapulnak, létfontosságú információáramlást tesznek lehetővé, miközben létezésüknek nyomát sem látjuk, oly természetes, hogy biztosítják a fenti folyamatok „hátterét". Mindehhez hozzájárul annak a régi mondásnak a tartalma, amely szerint „az információ hatalom, ha jól használod, győzelem", tehát egyre jelentősebb befolyást jelent manapság, ha a fenti folyamatokat lehetővé tevő feltételek feletti ellenőrzés egy-egy hatalmi gócként összpontosul.

Az infrastruktúrák működését és működtetését tekintve megkülönböztetünk általános feladatú infrastruktúrákat, amelyek egy-egy társadalmi, gazdasági, vagy védelmi funkcióhoz kapcsolhatóak (pl.: egészségügy – kórházak, eszközök, társadalombiztosítás; szállítás – raktárak, utak, gépjárművek), valamint információs rendeltetésű infrastruktúrákat, amelyek az információs társadalom számára szükséges információk előállítását, szállítását, tárolását és alkalmazását biztosítják. Egyik legfontosabb jellemzőjük, hogy önmagukban és az általános feladatú infrastruktúrák részeként is megtalálhatóak a hálózatok rendszerében, tekintettel arra, hogy a legtöbb infrastruktúra alapvető működésének feltételeként szolgálnak [6].

Megállapítható, hogy az információs társadalom sokrétűségének figyelembe vételével és az infrastruktúra definíciójának különböző variációi alapján az információs infrastruktúra fogalmát is többféle módon határozhatjuk meg. Kiindulhatunk az USA Nemzeti Információs Infrastruktúra Bizottsága által adott meghatározásból, amely szerint *„a számítógépek, távközlési hálózatok, szolgáltatások és alkalmazások összeköttetése és kapcsolata jelenti a nemzeti információs infrastruktúrát, amit információs szupersztrádának is hívnak"*[4].

Figyelembe véve azonban azokat a funkciókat, amelyeket az információs infrastruktúrák biztosítanak, indokolt a XXI. századi függőséget jobban ki fejező fogalom megadása, amely kimondja, hogy *„az információs társadalom működéséhez szükséges információk előállítására, szállítására és felhasználásra különböző rendeltetésű, funkciójú és típusú infrastruktúra-rendszerek, hálózatok állnak rendelkezésre. Ezek összessége képezi az információs társadalom komplex információs infrastruktúráját*" [8].

Mindezek alapján kijelenthető, hogy az információs infrastruktúrák működésének legfőbb *célja* az információs társadalomban szükséges információk biztosítása, az általános rendeltetésű infrastruktúrák informatikai jellegű működési feltételeinek folyamatos garantálása, miközben legjellemzőbb *tulajdonság*uk a globális hálózatszerűség és függőség, az információs társadalom egyfajta létszükségleteként való működés.

---

[2] Az információs társadalmak egyszerűen olyan társadalmak, amelyek mára komplex elektronikus információhálózatoktól függnek és erőforrásaik nagy részét információs és kommunikációs tevékenységre fordítják [4].

[3] A tudástársadalom fogalma nem azonos az információs társadalom kategóriájával, mert a tudástársadalom gyakorlatilag az információs társadalom magasabb szintje; a tudástársadalom nem más, mint az ember kapott és a földi létben szerzett szellemének globális tudatként és globális tudástársadalomként való visszafordíthatatlan megvalósulása [5].

[4] Forrás: [7].

Létfontosságú infrastruktúrák

Az Európai Unió, a NATO, a G8-ak[5] is külön foglalkozik manapság a kritikus infrastruktúrák védelmével, amelynek fontosságára elsősorban a jelentős mértékű technológiai fejlődés és a XXI. század hajnalán bekövetkezett terrortámadások adtak okot. A különböző megközelítéseket, de közel azonos célkitűzéseket tartalmazó programok, védelmi mechanizmusok nagymértékben függnek a kidolgozói körülményektől, de alapvetően megegyeznek abban, hogy a kritikus infrastruktúrák tekintetében

- azonosítani kell a gyenge pontokat,
- csökkenteni kell a sérülékenység valószínűségét,
- minimalizálni kell a károkat és a helyreállítás idejét,
- fejleszteni kell a kommunikáció, a koordináció és az együttműködés képességét,
- megfelelő jogi hátteret kell kialakítani,
- figyelembe kell venni a hatályos adatvédelmi szabályokat [9].

A kritikus infrastruktúra definícióját is a fenti célkitűzések tekintetében szükséges megfogalmazni és értelmezni a megfelelő szintű védelem kialakításának érdekében. A korábbi megfogalmazások alapján azok az infrastruktúrák tekinthetőek létfontosságúnak, amelyek lehetővé teszik a nélkülözhetetlen javak előállítását, szállítását és folyamatos rendelkezésre állását, biztosítják az együttműködés és az állandó összeköttetés lehetőségét, valamint együttesen hozzájárulnak a közbiztonság és a gazdasági biztonság megteremtéséhez, fenntartásához. Az általános megfogalmazások érdekek és nemzeti értékek szerinti pontosítását a legtöbb ország (szövetségi tagságoktól függően) önállóan végezte el, így hazánkban az alábbi definíció terjedt el: *„kritikus infrastruktúrák 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 fenntartásában”*[6].

Az eddigiek alapján kijelenthető, hogy – ahogy az infrastruktúrák sem egyeznek meg az információs infrastruktúrákkal, úgy – a kritikus infrastruktúrák definíciója is jelentős mértékben eltér a kritikus információs infrastruktúrák (a továbbiakban: KII-k) fogalmától. Az EU által meghatározott kritikus infrastruktúra védelmi programban azonosított szektorokat tekintve külön találkozhatunk az *Információs és kommunikációs technológiák* szektorával, amely az önmagukban KII-kat foglalja egy csoportba. Ugyanakkor fontos kihangsúlyozni, hogy a KII-k teljes halmaza kiegészül azokkal az informatikai rendszerekkel, hálózatokkal, eszközökkel és folyamatokkal, amelyek egy-egy kritikus infrastruktúra működését informatikai, technikai, technológiai vagy távközlési szempontból támogatják, tehát annak részeként tekintendőek kritikus információs infrastruktúra elemnek. Az EU kritikus infrastruktúra védelemről szóló Zöld könyve szerint a *„kritikus információs infrastruktúrák közé azokat kell sorolni, amelyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak”*[7].

Veszélyeztető tényezők

A kritikus infrastruktúra védelem kialakulása és jelenlegi folyamatai során rendkívül meghatározó szerepet töltenek be az egyes infrastruktúrákra vonatkoztatott veszélyeztető tényezők, amelyek lehetséges hatásai kockázatelemzések és kockázatbecslések alapján

[5] A világ, gazdaságilag legfejlettebb 8 országának együttműködési fóruma. Tagjai: Kanada, Franciaország, Németország, Olaszország, Japán, Egyesült Királyság, Amerikai Egyesült Államok és Oroszország.
[6] Forrás: [10]
[7] Forrás: [11]

kerülnek meghatározásra. Az infrastruktúrák sokszínűségéből adódóan a veszélyeztető tényezők tárháza is kifejezetten széleskörű. Az 1. számú táblázatban a veszélyeztető tényezők 3 alapvető csoportosítása alapján a kritikus infrastruktúrák és a KII-k vonatkozásában kerülnek bemutatásra a várható/valószínűsíthető következmények és hatások.

KRITIKUS INFRASTRUKTÚRA	VESZÉLYEZTETŐ TÉNYEZŐK	KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA
• szolgáltatások akadályozása • rendszerek működésének bénítása • figyelemfelkeltés • közvetlenül vagy közvetetten • fizikailag vagy informatikai eszközök útján	**TERRORIZMUS** (zavarkeltés, káosz okozása, kormányzatba vetett hit megingatása)	• új dimenzió • „cyberterrorizmus” • nehezen azonosítható támadási irányok • távolról elkövetett műveletek • fizikai és informatikai védelem szükséges
• fizikai károk keletkeznek • megsemmisülés vagy működő képtelenség követi • egy KI elem, vagy az egész infrastruktúra lehet érintett • láncreakció elindulásának valószínűsége	**TERMÉSZETI EREDETŰ VESZÉLYEZTETETTSÉG**	• rendszer-elemek sérülhetnek leginkább • adatvesztés valószínűséges alacsony • információbiztonság kevésbé veszélyeztetett • működő képtelenség követi
• baleset miatti leállás, sérülés, kiesés • informatikai rendszer miatti leállás, hiba • láncreakció elindulásának valószínűsége	**IPARI VAGY CIVILIZÁCIÓS EREDETŰ VESZÉLYEZTETETTSÉG** (baleset vs. szándékos cselekmény)	• baleset/üzemzavar miatti leállás valószínűsége alacsony • humán képességektől függő károkozás (adatlopás – rendszerleállás) • illetéktelen használat • szakszerűtlen tervezés/üzemeltetés • szakképzetlenség

1. táblázat. Az infrastruktúrák veszélyeztető tényezői
(Szerkesztette: Bonnyai Tünde)

A terrorfenyegetettséget ez esetben speciálisan szükséges értelmezni. A 2004-ben Madridban, majd 2005-ben Londonban elkövetett terrortámadások jellemzői alapján arra lehet következtetni, hogy a terroristák célkitűzése nem a nagy áldozattal járó cselekmények elkövetése volt. Sokkal inkább olyan eseménysorozat generálása, amely hosszabb időre, több szempontból is befolyással van a hétköznapi életre, elrettentő hatást gyakorol az emberekre, és megingatja a mindennapok biztonságába, a közbiztonságba, a közbiztonságot fenntartó szervekbe, ezáltal összességében az állam vezetésébe vetett hitet[8].

[8] A 2004. március 11-én, a madridi pályaudvaron elkövetett robbantásos merényletek az akkori spanyol kormányfő, Jose Maria Aznar bukásához vezettek.

A kritikus (információs) infrastruktúrák esetében manapság – főként a 2007-es észtországi incidenst[9] követően – egyre nyilvánvalóbb a cyberterrorizmus térnyerésének eshetősége, amely kifejezetten informatikai rendszerek kisebb-nagyobb mértékű zavarására irányul.

A természeti eredetű hatások – nehezen prognosztizálható jellegükből adódóan – szélsőséges esetekben veszélyeztetik a KII-kat, tekintettel arra, hogy azok funkcionális működését abban az esetben befolyásolják, ha az adott infrastruktúra fizikai (létesítményi) korlátait fenyegetik. Így az erre történő felkészülés leginkább az infrastruktúrák fizikai kivitelezésben nyilvánulhat meg. Nem feledkezhetünk meg azonban olyan természeti eredetű veszélyeztető tényezőkről sem, mint a napkitörések, amelyek – a média hozzá nem értő megnyilvánulásai miatt – elsősorban utópisztikus gondolatokat szülnek. Valóságos fenyegetésükre azonban egyértelmű példa az 1989-es kanadai áramszünet[10], vagy annak tényszerűsége, hogy 8-10 ezer műhold kering földkörüli pályán, amelyek sérülése jelentős problémákat okozhat például a távközlés, a kommunikációs rendszerek, a műsorszórás, a műhold alapú navigációs rendszerek (GPS) működésében.

Végül, de nem utolsó sorban az ipari és civilizációs hatásokra kell kiemelt figyelmet szentelni, amely magában foglalja a veszélyes ipari balesetek, nukleáris balesetek, a környezetkárosodás, az informatikai rendszerek károsodását, valamint az infrastruktúrák teljesítőképességének kimerülési lehetőségét is. Fentiek közül mind a kritikus infrastruktúrákra, mind a KII-kra egyre fokozottabb veszélyt jelent az informatikai rendszerek szándékos rongálásából, támadásából (nem terror jellegű ártó szándékú cselekmények) származó fenyegetettség. A jelenlegi gazdasági válság miatti kilátástalanság és elkeseredettség, valamint a XXI. századi információs társadalom fiatal rétegének „információéhsége" és a technikai/informatikai tehetségével való kérkedése tesz súlyosabbá. Mindennaposak az adathalász akciók a nagykiterjedésű adatbázisok ellen; a központi honlapok működésének akadályozására irányuló túlterheléses támadások; a megtévesztésre összpontosító, vírusokat terjesztő e-mail láncok. Az ellenük kialakítandó védelem lehetőségei nehezen körvonalazhatóak, tekintettel arra, hogy a kreativitás folyamatosan új és újabb kihívásokkal szembesíti a professzionális védelmi tevékenységet végző szervezeteket.

Mindezek alapján kijelenthető, hogy a kritikus infrastruktúrák és a kritikus információs infrastruktúrák között működés és veszélyeztetettség tekintetében markáns különbségek és jelentős párhuzamok egyaránt felfedezhetőek. A 2. sz. táblázat a főbb jellemzők összesítését tartalmazza.

[9] Észtország fővárosában, a szovjet hősi emlékmű eltávolítása miatt 2007 áprilisában zavargások törtek ki, majd az eseményt követő napokban belül jelentős károkkal járó kibertámadások indultak az észt parlament, kormányhivatalok, minisztériumok, bankok, telefontársaságok és médiacégek szerverei ellen. Szakértők szerint a támadások célja a balti állam online infrastruktúrájának kiütése, és ezen keresztül az észt gazdaság és telekommunikáció megbénítása volt.

[10] 1989-ben Kanadában egy űrvihar következtében összeomlott a villamosenergia-hálózat és kilenc óra időtartamra hatmillió ember maradt áram nélkül.

Hatás	Kritikus infrastruktúra	Kritikus információs infrastruktúra
MŰKÖDÉS		
primer	önállóan	rendszerként
szekunder	informatikai rendszer alapján	rendszerelemként
FŐ VESZÉLYEZTETETTSÉG		
primer	fizikai sérülés	informatikai jellegű károkozás, cyberterrorizmus
szekunder	dominóhatás	dominóhatás
INTERDEPENDENCIA		
primer	jelentős	szinte mindennel függőségben áll
szekunder	önállóan is működhet	rendszerként önállóan is működhet
LAKOSSÁGI HATÁSOK		
primer	kiterjedéstől függő hatások	közvetlen érintettség miatti hatások
szekunder	közvetlen hatások	közvetett hatások

2. táblázat. Különbségek és párhuzamok
(Szerkesztette: Bonnyai Tünde)

A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELMÉRE IRÁNYULÓ NEMZETKÖZI ÉS HAZAI JOGSZABÁLYI ÉS SZERVEZETI HÁTTÉR

A kritikus infrastruktúra védelem európai programja kidolgozásának kezdeti fázisaiban is egyértelműsítésre került, hogy az interdependenciák tekintetében az infokommunikációs-technológiák (a továbbiakban: IKT) szektora (akkor még nem azonosított ágazatként) kiemelt szerepet játszik a tagállamok gazdasági szereplőinek, ágazatainak, hatóságainak folyamatos működésében. A felsoroltak közötti és azokon belüli függőségek figyelembe vétel az IKT technológiákon alapuló infrastruktúrák és infrastruktúra elemek veszélyeztetettségét kiemelten szükséges kezelni. A 2005 decemberében napvilágot látott Zöld Könyv több helyen is külön nevesíti a KII-kat, különösen az üzemeltetők és használók szerepét taglaló 8. fejezetben, ahol az információs hálózatokat emeli ki példaként az azonos védelmi szint biztosításának szükségessége vonatkozásában. A Zöld Könyv kimondja, hogy ilyen kiterjedt és összefüggő hálózat esetében az azonos szintű védelem biztosítása nem elvárható, így az üzemeltetőket/tulajdonosokat, valamint a hatóságokat arra ösztönzi, hogy azonosítsák a hálózat létfontosságú pontjait és arra összpontosítsák a biztonsági intézkedéseiket [11]. E megállapítások tükrözik, hogy az IKT szektor jelentőségét és széleskörű függőségét már

idejekorán felismerte az Európai Unió, mégsem azonosította a prioritásként kezelendő szektorok listájában a 2008-ban kiadásra került Irányelvben.

Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességéről szóló 2008/114/EK irányelv a Zöld Könyv alapján határozta meg a kritikus infrastruktúra védelem európai alapjait, azonosítva az energia- és a közlekedési szektor prioritásait. Az Irányelv az IKT ágazatra vonatkozóan még nem tartalmaz kötelező elemeket, illetve ajánlásokat, mindössze javasolja, hogy kerüljenek végrehajtásra olyan vizsgálatok és kutatások, amelyek értékelése alapján az IKT szektor az Irányelv hatálya alá vontható [12].

A Világgazdasági Fórum 2008-ban készített becslését[11] figyelembe véve az Európai Bizottság közleményt adott ki 2009 márciusában a KII-k védelméről, amelyben hangsúlyozta a megelőzés és felkészülés szükségességét, valamint a KII-k ellenálló-képességének megerősítését egyaránt. A közlemény kimondja, hogy a KII-k nélkülözhetetlenek az EU gazdasági és társadalmi növekedése szempontjából, tekintettel arra, hogy az IKT technológiák az innováció szerves részei és a termelékenység mintegy 40 %-át adják. Fontos továbbá, hogy ellenálló-képességüket az információs társadalomba vetett bizalom megtartása és megerősítése érdekében is fejleszteni szükséges. Mindezekre való különös tekintettel a Bizottság feladatokat határozott meg a tagállamok számára a nemzeti szemléletmódok összehangolására, a reagáló képesség javítására, a nemzetközi együttműködési képesség fejlesztésére vonatkozóan. A közlemény tartalmazza továbbá a Kritikus Információs Infrastruktúrák Védelmének Cselekvési Tervét, amelyben az alábbi célkitűzések szerepelnek:

FELADAT	CÉL	HATÁRIDŐ
Közös alapképességek és szolgáltatások kidolgozása	Európára kiterjedő együttműködés	2011 vége
Köz-magán partnerség kialakítása	Ellenálló-képesség javítása	2010 vége
Európai információ-megosztási és figyelmeztető rendszer (EISAS)	érintettek és a lakosság értesítése, információcsere	2010 vége
Nemzeti vészhelyzeti tervek és gyakorlatok	hálózatbiztonságot veszélyeztető nagyszabású eseményekre való reagálás és a keletkező károk helyreállítása rutinjainak kialakítása	2010 vége
Nemzeti/kormányzati CERT-ek létrehozása	nemzetközi együttműködés fejlesztése	2010 vége
Az internet ellenálló képessége és stabilitása	az internet létfontosságú alkotóelemeivel és vonatkozásaival kapcsolatos uniós prioritások meghatározása	2010 végéig
IKT-ágazatra vonatkozó kritériumok kidolgozása	IKT szektor Irányelv hatály alá helyezése	2010 eleje

3. táblázat. Cselekvési terv 2009. [13] (Szerkesztette: Bonnyai Tünde)

A fenti Cselekvési Tervvel kapcsolatban 2009 decemberében az Európai Tanács állásfoglalást adott ki, amelyben megerősítette és fokozottan hangsúlyozta a hálózat- és információbiztonság kiemelkedő szerepét a demokratikus rend fenntartása, a magánélet védelme, a gazdasági növekedés és a politikai stabilitás vonatkozásában. A Tanács felhívta a tagállamok figyelmét arra, hogy az IKT technológiákon alapuló infrastruktúrák súlyos

[11] A Világgazdasági Fórum előrejelzése szerint 2020. előtt 10-20%-os esély mutatkozik az IKT technológiákon nyugvó kritikus információs infrastruktúrákon belül bekövetkező üzemzavarra, amely kiterjedése révén – hozzávetőlegesen – 250 milliárd dolláros kár okozását idézheti elő a gazdaság vonatkozásában [13].

zavarása, meghibásodása, vagy kiesése a technológiában, a hálózatokba, a szolgáltatásokba és összességében az információs társadalomba vetett közbizalmat rendítheti meg, így a fenyegetések folyamatosan változó jellegére és egyre nagyobb területekre való kiterjedésük megakadályozására kiemelt figyelmet kell szentelni. Ennek érdekében az IKT technológiák felhasználóinak tájékozottságát és érzékenységét növelni, valamint a KII-kkal kapcsolatosan azonosított és feltételezett veszélyeket globális kihívásként szükséges kezelni, ezért az egységes, határokon átnyúló együttműködést fokozatosan fejleszteni és erősíteni kell. A Tanács megállapította, hogy a nemzeti és európai szintű hálózat- és információbiztonságra irányuló gyakorlatok minden résztvevő számára kifejezetten hasznosak, ezért felkérte a tagállamokat további gyakorlatok tervezésére, szervezésére és értékelésére, továbbá a kutatás-fejlesztési tevékenység fokozására egyaránt. Végül az állásfoglalás keretében az EU megerősítette az Európai Hálózat- és Információbiztonsági Ügynökség[12] szerepét is [14].

A 2009-ben elfogadott Cselekvési Terv végrehajtásának értékelésére, aktualizálására és újabb feladatok meghatározására 2011. március 31-én az Európai Bizottság közleményt adott ki, amelynek 3 fő célkitűzése az alábbiak szerint foglalható össze:

- az IKT technológián alapuló KII-k biztonságának, ellenálló-képességének növelése;
- magas szintű felkészültség elérése;
- kapacitásfejlesztés.

A közlemény ismételten hangsúlyozza az állami és magánszektor együttműködésének szükségét és fontosságát, amelynek jegyében – figyelemmel a célkitűzésekre – az 5 alappillérhez kapcsolhatóan az alábbi feladatokat határozza meg:

PILLÉR	FELADAT
felkészülés & megelőzés	legjobb szabályozási gyakorlatok megosztása
észlelés & válasz	Európai Információ-megosztási és figyelmeztető rendszer fejlesztése
kárenyhítés & helyreállítás	kríziskezelési tervek készítése és gyakorlatok szervezése
együttműködés	nemzeti – uniós – nemzetközi szintű szervezetek kapcsolatrendszerének fejlesztése
IKT kritériumok	IKT szektor kritikus infrastruktúráinak azonosítása

4. táblázat. Javasolt feladatok a tudatosság fokozására [15]
(Szerkesztette: Bonnyai Tünde)

A KII-k vonatkozásában az Állampolgári Jogi, Bel- és Igazságügyi Bizottság adott ki legutóbb egy véleményt, amelyben a 2011-es közleményhez tettek kiegészítő javaslatokat. A véleményben markánsan megjelenik a megfelelő tagállami döntéshozatali és jogszabályi környezet kialakításának igénye és szükségessége, valamint a kockázatkezelési eljárások alkalmazásának fontossága, amely egyben erősítheti is a nemzeti és nemzetközi szintű, horizontálisan és vertikálisan is megvalósítandó együttműködéseket. Mindezekhez a tagállamok figyelmébe ajánlja a készülő internet-biztonsági stratégiát, amelyhez a későbbiekben szervesen kapcsolódhatna egy közös, európai kiber-biztonsági stratégia is. Az

[12] ENISA – European Network and Information Security Agency

ajánlás emellett megfogalmazza a párhuzamosságok feltérképezésének szükségességét, amelyek megszüntetése és elkerülése érdekében felveti egy koordinátor jellegű szerepkör kialakítását (pl.: uniós kiber-biztonsági koordinátor), valamint folyamatos és széleskörű kiber-biztonsági oktatási és gyakorlatszervezési tevékenységet javasol az érintettek számára [16].

Nemzetközi szervezetek a kritikus információs infrastruktúra védelem rendszerében

A KII-k tekintetében – ahogy már korábban többször rögzítésre került – kiemelkedő fontosságú az állami és a civil szféra együttműködése, tekintettel arra, hogy a legtöbb kritikus elem a magánszektorban található, de interdependeciái révén kiemelten érintheti az állami infrastruktúrák működését is. Ennek felismerése vezetett oda, hogy manapság több nemzetközi szintű szervezet is rendszeresen és hivatásszerűen foglalkozik a KII-k védelmével. Ezzel kapcsolatban meghatározó szerepet kapnak az ún. CERT[13]-szervezetek, amelyek célja a hálózati problémák hatásának minimalizálása, segítségnyújtás az elhárításban, további ártó jellegű események akadályozása [17].

A CERT-szervezetek tevékenységét támogatják és hangolják össze az alábbi nemzetközi szerveződések [18]:

IWWN – International Watch and Warning Network: a világ 14 legfejlettebb gazdasággal bíró országa és Magyarország tagságával működő szervezet. Célja, hogy közös fórumot biztosítson a jogszabályalkotás, a kormányzati CERT szervezetek és a bűnüldözési szervezetek részére a nemzetgazdaságot érintő kockázatok és kihívások kezelésében.

TF-CSIRT – Task Force-Computer Security Incident Response Team: európai CERT szervezeteket tömörítő szervezet, amely a CERT-ek közötti, a globális fenyegetésekkel szembeni egységes fellépés érdekében történő hatékony információcsere biztosítását tűzte ki célként.

FIRST – Forum of Incident Response Team: a CERT szervezetek világszintű szervezete, amelynek célja, hogy elősegítse a CERT-ek együttműködését nemzetközi (EU feletti) szinten.

EGC – European Governmental CERTs: az EU tagállamaiban létrehozott kormányzati CERT szervezetek együttműködésének biztosítására alakult, jelenleg azonban még csak 7 tagja van.

Információs társadalom kialakítása Magyarországon

Hazánkban – tekintettel a történelmi tényekre és a szolid gazdasági fejlődési mutatókra – a 2000-es évek elején merül fel először stratégiai szinten az információs társadalommal kapcsolatos igények, tervek, célkitűzések megfogalmazása. 2001 májusában jelent meg, a Miniszterelnöki Hivatal Informatikai Kormánybiztossága által készített Nemzeti Információs Társadalom Stratégia (NITS), amely megállapította, hogy Magyarország az infokommunikációs piac európai átlagon felüli bővülése ellenére jelentős hátrányban van a nyugat-európai, versenyképes tagállamokkal szemben. Lemaradásunk főként a technológiai és gazdasági fejlettség, a piaci környezet, az internet használata és az információs társadalommá válásra való felkészültség tekintetében mutatkozott meg. A stratégia elsődleges céljául tűzte ki a meghatározott akciótervek mentén történő felzárkózás mielőbbi megvalósítását, kormányzati beavatkozás segítségével. A NITS ezzel kapcsolatos legfőbb célkitűzései:

- szabályozás és szabványosítás, az EU-s normáknak megfelelő szinten és módon;
- innováció és K+F tevékenység támogatása;
- IKT eszközök oktatásban történő alkalmazásának elősegítése;

[13] CERT – Computer Emergency Response Team, olyan szervezet, amelynek tevékenysége a hálózatbiztonság fenntartására, a biztonság szintjének fokozására, a hibák azonosítására és kiküszöbölésére, az elhárítás koordinációjára, a felhasználók képzésére és a tudatosításra irányul.

– elektronikus – szolgáltató – kormányzat kialakítása és folyamatos fejlesztése [19].

A két évvel később napvilágot látott Magyar Információs Társadalom Stratégia (MITS) hosszabb távú akcióterveket és programokat hirdetett meg. Helyzetelemzéseken alapuló célkitűzései az alábbiak szerint foglalhatóak össze:

– biztosítani Magyarország belépését az információs korba;
– operatív programok útján támogatást nyújtani a tervek megvalósításához;
– versenyképesebbé tenni a magyar gazdaságot.

Mindezek megvalósíthatósága érdekében a MITS illeszkedett az Európai Unió eEurope+ és az eEurope 2005 akciótervekhez, valamint a Nemzeti Fejlesztési Tervhez egyaránt. Tartalmában elsősorban az infrastrukturális fejlesztések, a jogi-társadalmi környezet biztosítása, az esélyegyenlőség megteremtése és a digitális írástudatlanság csökkentése, valamint a K+F tevékenységek és az oktatás szerepel prioritásként [20].

A Nemzeti Fejlesztési Minisztérium 2010 decemberében készítette el a 2010-2014. közötti időszakra vonatkozó kormányzati kommunikációs tervet, amely egységes keretrendszert hivatott biztosítani az infokommunikációs technológiák részére és széleskörű szakmai és társadalmi konszenzus övezi. A Digitális Megújulás Cselekvési Terv a digitális megújulást nemzeti ügyként kezeli, tekintettel arra, hogy kulcsszerepet játszhat a gazdaság talpra állításában és tényleges kitörési pontként szolgálhat. A cselekvési terv illeszkedik az Új Széchenyi Tervhez és az Európa 2012 Digitális Menetrend Stratégia által meghatározott ajánlásokhoz. Mindezek alapján 4 fő eleme:

– állampolgárok digitális esélyegyenlőségének biztosítása,
– vállalkozások versenyképességének növelése,
– modern közigazgatási informatika megteremtése,
– informatikai infrastruktúra széleskörű fejlesztése [21].

A kritikus információs infrastruktúra védelem hazai jogszabályi és szervezeti háttere

Magyarország, 2004. május 1-jei európai uniós csatlakozásával teljes jogú részesévé vált az akkor épp kidolgozás alatt álló kritikus infrastruktúra védelmi folyamatnak. A tagállami egyeztetések keretében a kritikus infrastruktúra fogalma, jelentősége és védelmének fontossága egyre markánsabban jelent meg a hazai jogszabályi környezetben is:

– a személyes adatok védelméről szóló törvény az uniós elvárásoknak megfelelően szigorú rendszerbe foglalja a védendő adatra vonatkozó szabályokat, amelyek a kritikus infrastruktúrák (így a KII-k) szempontjából is kiemelkedő jelentőségűek [22];
– a Magyar Köztársaság biztonság és védelempolitikájának alapelveiről szóló országgyűlési határozat külön foglalkozik az információs társadalom kihívásaival és a nemzet részéről adható válaszokkal [23];
– az első kritikus infrastruktúra definíciót egy, az Informatikai és Hírközlési Minisztérium által kiadott 2004-es rendelet határozta meg hazánkban, amely szerint a kritikus infrastruktúra alatt létesítmények és szolgáltatások értendőek, beleértve informatikai rendszereket is, amelyek működésképtelenné válása jelentősen befolyásolhatja a nemzetbiztonságot, a nemzetgazdaság és a közszolgáltatások működését [24];
– a kritikus infrastruktúrák védelemére irányuló tudatos tevékenység a terrorizmus elleni küzdelemmel kapcsolatban 2004-ben kiadott kormányhatározat, az európai megközelítések alkalmazására történő felhívással és a kritikus infrastruktúra védelem keretrendszerbe foglalására való felszólítással kezdődött [25];

- a korábban hatályos nemzeti biztonsági stratégia kifejezetten az információs infrastruktúrák feltételeinek biztosítását, védelmét és az ezzel kapcsolatos tartalékok kialakítását helyezte előtérbe, valamint felhívta a figyelmet a technológiai fejlődés által generált kockázati tényezőkre [26];
- a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala létrehozásáról, szóló kormányrendelet feladatul szabta az újonnan létrehozott szervezetnek, a hatáskörében lévő kritikus információs infrastruktúra elemek védelmét [27];
- a Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló kormányhatározat a teljes hazai kritikus infrastruktúra védelmi folyamat alapjait határozta meg, bár célirányosan nem foglalkozott a KII-k védelmével mégis megfelelő alapot teremthet a jövőben a KII-k védelmének jogszabályi alapokra helyezése során [10];
- a végrehajtandó feladatokról szóló kormányhatározat az azonnal elvégzendő feladatokra és azok körülményeinek megteremtésére irányult, ezáltal nem tartalmaz KII-k védelmével kapcsolatos rendelkezéseket [28];
- a megújított honvédelmi és az új alapokra helyezett katasztrófavédelmi törvény szintén ismeri és alkalmazza a kritikus infrastruktúra fogalmát, de nem tér ki részleteiben a KII-k védelmével kapcsolatos ágazati feladatokra [29-30];
- Magyarország új Nemzeti Biztonsági Stratégiájában – a korábbi stratégiához hasonlóan – markánsan jelenik meg a KII-k szerepe és veszélyeztetettsége. Kimondja, hogy a kibervédelemre és a nemzeti KII-k működésének biztosítására készen kell állni. Ezzel kapcsolatban olyan feladatokat határoz meg, mint a kibertér fenyegetéseinek felmérése és priorizálása, a kormányzati koordináció erősítése, a társadalmi tudatosság fokozása, illetve a nemzetközi együttműködések erősítése és kiaknázása [31].

Hazánkban a kritikus információs infrastruktúrák jogszabályi alapokra történő helyezése láthatóan nem valósult még meg. A szervezeti hátteret jelenleg a Puskás Tivadar Közalapítvány látja el, amely 2005-ben jött létre és azóta nemzetközi szinten elismert CERT-szervezetévé nőtte ki magát. A Magyar Kormány döntése alapján a Közalapítvány 2010. január 1-jétől ellátja a Nemzeti Hálózatbiztonsági Központ szerepét is, amelynek keretében az Országos Informatikai és Hírközlési Főügyelettel együttműködésben felelős a magyar KII-k védelméért, a központi rendszeren végbemenő kommunikáció biztonságának szavatolásáért [32]. A Puskás Tivadar Közalapítvány Nemzeti Hálózatbiztonsági Központ (PTA CERT-Hungary) akkreditált szervezet, amely tagja a 2. 1. pontban ismertetett nemzetközi szervezeteknek. Tevékenysége szempontjából három fő rendeltetése van:

1. állami koordináló szerv,
2. szituáció-kezelő központ,
3. nemzeti CERT-szervezet.

2005 óta Incidenskezelési Munkacsoportot működtet a pénzügyi szektorral, amelyben a Magyar Bankszövetség, a Pénzügyi Szervezetek Állami Felügyelete és bankok vesznek részt. A munkacsoport információ-megosztást tesz lehetővé az érintettek számára és évente gyakorlatokat szervez a pénzügyi szektort veszélyeztető tényezőkre való hatékony felkészülés érdekében. Az energia szektorral működtetett Információmegosztó Csoport munkájában erőművek, elosztók, szolgáltatók, irányítók, valamint a Nemzeti Fejlesztési Minisztérium, a Nemzeti Média- és Hírközlési Hatóság vesz részt. Együttműködésük keretében 2009-ben került végrehajtásra egy törzsvezetési gyakorlat, amely forgatókönyvek alapján, szimulált környezetben feltételezett informatikai támadások kezelésének gyakorolását tette lehetővé [17].

Napjainkban zajlik a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvénytervezet egyeztetése, amelynek célja kifejezetten a

kritikus infrastruktúrák azonosítási és kijelölési folyamatának meghatározása az uniós irányelv és már meglévő hazai dokumentumok (pl.: Zöld Könyv) alapján. A tervezet nem tartalmaz a KII-k védelmére irányuló rendelkezést, tekintettel átfogó jellegére. A törvénytervezethez kapcsolódó végrehajtási rendelet 2012 augusztusában készül el. A KII-k védelmével kapcsolatos konkrét jogszabályi háttér kidolgozása valószínűleg csak a fent említett csomag elfogadását követően veheti kezdetét.

A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK AZONOSÍTÁSÁNAK ÉS VÉDELMÜK MEGTEREMTÉSÉNEK FELTÉTELEI

A következőkben röviden összegzésre kerül egy, a KII-kra vonatkozó azonosítási folyamat [33], amely – tekintettel arra, hogy a kritikus infrastruktúrák azonosítási és kijelölési módszertanát horizontális és ágazati kritériumok határozzák meg – nem egy újfajta azonosítási eljárást tartalmaz, sokkal inkább egy olyan metódust, amely elősegítheti az információs infrastruktúrák felmérését és kiválasztását a kritikusság meghatározása során. Mindezekhez az alábbi lépések megtétele javasolt:

- definíciók, szereplők megnevezése és meghatározása,
- rendelkezésre álló információs infrastruktúrák veszélyeztetettségének feltárása,
- védelmi célkitűzések megfogalmazása az adott infrastruktúrák vonatkozásában,
- kockázatbecslések készítése és kockázatértékelés összeállítása az adott infrastruktúrák vonatkozásában,
- priorizálás a kockázatértékelése eredményei tükrében,
- védelmi megoldások kidolgozása és megvalósítása az azonosításra kerülő infrastruktúrák részére.

Az előbbi fejezetek, valamint a kapcsolódó források tanulmányozásából fakadó tapasztalatok alapján a kritikus információs infrastruktúrák azonosítása és védelme megfelelő szintű kialakításának és fenntartásának feltételrendszere négy pilléren alapul, amelyeket az 5. számú táblázat foglal össze:

PILLÉR	OK-OKOZAT	EMPIRIKUS ALÁTÁMASZTÁS
Jogszabályi háttér	alkalmazható, egységes, átfogó jogi alapok nélkül nem létezik feladat, felelősség, kötelezettség	• Az európai program nem tartalmazott kötelező elemeket az IKT-ra. • Nemzetközi események (Észtország) indították el az EU Bizottság közleményeit. • CERT-szervezetek 2007 után kezdtek gyarapodni.
Szervezeti keretek	működő, jogszabályi alapokon nyugvó szervezet életre hívása hiányában a célkitűzések nem megvalósíthatók	• Az EU kezdeményezései elméleti síkon maradtak az első célirányosan létrehozott CERT-szervezet megalakulásáig. • A szervezetek együttműködése erősíti a nemzetközi együttműködést akár nem azonos gazdasági szinten lévő országok között is (pl.: IWWN)

PILLÉR	OK-OKOZAT	EMPIRIKUS ALÁTÁMASZTÁS
Együttműködés	horizontális és vertikális, illetve nemzeti és nemzetközi szintű közösségi tevékenység nélkül nincs egységes védelmi mechanizmus	• Nemzeteken átívelő jellege miatt a KII-k védelme nem értelmezhető csak nemzeti szinten. • Az interdependenciára való tekintettel az állam és a magánszektor együttműködése kiemelten szükséges az eredményesség érdekében.
Megelőzés és felkészülés	globális kihívásra adandó válasz első lépése a felkészülés, amely az érintettek intenzív bevonása nélkül nem lehet hatékony	• Állami és magánszektor együttműködésének lehet a működő szervezeti háttér. • Felhasználói szintig megvalósuló oktatási programok és a tudatosság növelése erősíti a védelmi képességet.

5. táblázat. Az azonosítás és védelem feltételrendszere
(Szerkesztette: Bonnyai Tünde)

Összességében megállapítható, hogy mind az Európai Unió, mind Magyarország szempontjából folyamatos előrehaladás mutatkozik a kritikus infrastruktúra védelem terén, de a kritikus információs infrastruktúrák vonatkozásában még jelentős hiányosságok fedezhetők fel, amelyek révén – a témakör komplexitását tekintve –a megfelelő védelmi szint kialakításának és fenntartásának követelményei nem elégíthetők ki teljes mértékben.

Felhasznált irodalom

[1] Bonnyai Tünde: A kritikus infrastruktúra védelem fogalmi rendszere, hazai és nemzetközi szabályozása; pályamunka a Katasztrófavédelmi Tudományos Tanács pályázatára, 2011.

[2] Cecei Katalin – Mórocz Attila: Klímaváltozás és a kritikus infrastruktúra; AGRO-21 Füzetek, 2004. 36. szám, Budapest. pp. 32-63.

[3] Kovács Ferenc: A kritikus infrastruktúra védelme I. c. tantárgy előadás vázlat; Nemzeti Közszolgálati Egyetem

[4] Denis McQuail: A tömegkommunikáció elmélete; Osiris kiadó, Budapest 2003. p. 112.

[5] Varga Csaba: Egységkor vízió – posztmodern utáni jövőkép, poszt-neokonzervatív szemlélettel;
http://www.inco.hu/inco3/tudas/cikk0h.htm – letöltés ideje: 2012. június 10.

[6] Kovács László: Kritikus információs infrastruktúrák; Zrínyi Miklós Nemzetvédelmi Egyetem, egyetemi jegyzet. Budapest 2007. pp. 9-19.

[7] http://www.ofi.hu/tudastar/oktatas-informacios – letöltés ideje: 2012. június 15.

[8] Várhegyi István – Makkay Imre: Információs korszak, információs háború, biztonságkultúra; OMIKK, Budapest, 2000.

[9] A G8 alapelvei a kritikus információs infrastruktúra védelmére; http://www.kiiv.hu/node/5 – letöltés ideje: 2012. május 29.

[10] 2080/2008. (VI. 30.) kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.

[11] Green Paper on a European Programme for Critical Infrastructure Protection (COM(2005) 576 final).

[12] Az Európai Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről

[13] Az Európai Bizottság Közleménye a kritikus információs infrastruktúrák védelméről: „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása" címmel (COM(2009) 149 final), 2009. március 30.

[14] Az Európai Tanács Állásfoglalása (2009. december 18.) a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről (2009/C 321/01)

[15] Az Európai Bizottság Közleménye a kritikus informatikai infrastruktúrák védelméről: „Eredmények és következő lépések: a globális kiberbiztonság felé" címmel (COM(2011) 163 final), 2011. március 31.

[16] Állampolgári Jogi, Bel- és Igazságügyi Bizottság Véleménye a kritikus infrastruktúrák védelméről szóló Európai Bizottsági Közleményről (2011/2284(INI)), 2012. március 22.

[17] Angyal Zoltán: A Puskás Tivadar Közalapítvány keretein belül működő Nemzeti Hálózatbiztonsági Központ szerepe a kritikus információs infrastruktúra védelemben c. előadása. A Hírközlési és Informatikai Tudományos Egyesület Távközlési Klub Szakosztálya szakmai rendezvénye, Budapest, 2010. január 28.

[18] Kovács László: Kritikus információs infrastruktúrák; Zrínyi Miklós Nemzetvédelmi Egyetem, egyetemi jegyzet. Budapest 2007. pp. 168-169.

[19] Nemzeti Információs Társadalom Stratégia, Budapest, 2001. május 17.

[20] Magyar Információs Társadalom Stratégia, Budapest, 2003. november.

[21] Digitális Megújulás Cselekvési Terv, Budapest, 2010. december 23.

[22] A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény.

[23] A Magyar Köztársaság biztonság és védelempolitikájának alapelveiről szóló 94/1998. (XII. 29.) kormányhatározat.

[24] 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 kötelezettségeiről.

[25] 2112/2004. (V. 7.) kormányhatározat a terrorizmus elleni küzdelem aktuális feladatairól.

[26] 2073/2004. (III. 31.) kormányhatározat a Magyar Köztársaság Nemzeti Biztonsági Stratégiájáról.

[27] A Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala létrehozásáról, feladatairól és hatásköréről szóló 276/2006. (XII. 23.) kormányrendelet módosításáról szóló 81/2008. (IV. 4.) kormányrendelet.

[28] 1249/2010. (XI. 19.) kormányhatározat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról;

[29] A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény.

[30] A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény.

[31] 1035/2012. (III. 21.) kormányhatározat Magyarország Nemzeti Biztonsági Stratégiájáról.

[32] 223/2009. (X. 14.) kormányrendelet az elektronikus közszolgáltatásról és annak igénybevételéről.

[33] Haig Zsolt, Hajnal Béla, Kovács László, Muha Lajos, Sik Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana, ENO Avisory Kft. 2009.