XXI. Fiatal Műszakiak Tudományos Ülésszaka, 2016. Kolozsvár, 349–352.
http://hdl.handle.net/10598/29102
DOI: 10.33895/mtk-2016.05.78

KRITIKUS INFRASTRUKTÚRÁK VÉDELME (JOGI SZABÁLYOZÁS)

CRITICAL INFRASTRUCTURES PROTECTION (LEGISLATION)

Rajnai Zoltán[1], Fregan Beatrix[2]

[1]*Óbudai Egyetem, Biztonságtudományi Doktori Iskola, rajnai.zoltan@bgk.uni-obuda.hu*

[2]*Nemzeti Közszolgálati Egyetem, fregan.beatrix@uni-nke.hu*

Abstract

Critical infrastructure protection (CIP) is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation. The systems and networks that make up the infrastructure of society are often taken for granted, yet a disruption to just one of those systems can have dire consequences across other sectors Take, for example, a computer virus that disrupts the distribution of natural gas across a region. This could lead to a consequential reduction in electrical power generation, which in turn leads to the forced shutdown of computerized controls and communications. Road traffic, air traffic, and rail transportation might then become affected. Emergency services might also be hampered.

Keywords: *critical infrastructures, network protection, information and communication systems.*

Összefoglalás

A létfontosságú infrastruktúrák védelme (CIP) egy olyan koncepció, amely a különböző súlyos incidensek elleni felkészülést és válaszlépéseket foglalja magába, és amelyek hatással lehetnek egy adott régió vagy nemzet létfontosságú infrastruktúrájára. A társadalom gyakran magától értetődőnek tartja a rendszerek és hálózatok által alkotott infrastruktúra létét, de ha csak az egyik rendszerben is zavar lép fel, annak súlyos következményei akár más ágazatokban, vagy az egész rendszerben érzékelhető. Vegyük például a számítógépes vírusokat, amelyek megzavarják például a földgázelosztási rendszert egy egész régióban. Ez ahhoz a következményhez vezethet, hogy csökken a villamos energiatermelés, ami viszont azt eredményezheti, hogy kényszerűen leáll akár a számítógépes irányítás és a kommunikáció is. De akár a közúti közlekedés, a légi közlekedés, valamint a vasúti közlekedés is érintett lehet, sőt akadályozhatja a veszélyhelyzeti szolgáltatásokat is.

Kulcsszavak: *kritikus infrastruktúrák, hálózatvédelem, információs és kommunikációs rendszerek.*

1. Bevezetés

A létfontosságú infrastruktúrák a köznyelvben mint kritikus infrastruktúrák jelentek meg az elmúlt alig egy évtizedben. Ezek védelmének fontosságára több olyan veszélyes incidens is felhívta a figyelmet, melyek meggátolták, blokkolták, vagy zavarták olyan, elsősorban informatikai eszközökkel vezérelt hálózatok működésével

biztosítják a bankszektor, az energiaellátás, a közigazgatási hálózatok, vagy más fontos infrastruktúrák szolgáltatásait. Magyarország az Európai Unió tagjaként is szerepet vállalt elsősorban a saját, valamint az összekapcsolt közösségi hálózatok védelme érdekében. A védelemhez kialakításához szükséges volt jogszabályi területen megalkotni és elfogadtatni azon intézkedéseket, melyek megteremtették a feltételeket a kritikus infrastruktúrák védelméhez.

2. Szabályozás alapja az EU-ban és Magyarországon

2004. október 20-án az Európai Bizottság *–az Európai Tanács kritikus infrastruktúrák védelmét célzó átfogó stratégia elkészítésére irányuló felhívására–* közleményt fogadott el „A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben" címmel, amelyben arra tett javaslatokat, hogy hogyan lehetne a megelőzés, felkészültség és reagáló képesség európai dimenzióját javítani a kritikus infrastruktúrákat érintő terrortámadások esetén. [1]

2.1. Kritikus Infrastruktúra Védelem Nemzeti Programja [2]

A modern társadalmak nagymértékben függenek a technikai és virtuális infrastruktúra rendszerektől (energiaellátás, ivóvízellátás, informatikai hálózatok stb.), amelyek komplex rendszerét is egymástól való függőségek jellemzik. E rendszerek működési zavarai, illetve egyes elemeinek ideiglenes kiesése, vagy megsemmisülése jelentős kihatással vannak mindennapi életünkre, a gazdaság és a kormányzat hatékony működésére.

Az állam, a gazdaság szereplői, valamint a lakosság részéről elvárás, hogy ezen alapvető létfontosságú, vagy kritikus infrastruktúrák lehető legnagyobb biztonsággal működjenek. A kritikus infrastruktúra elemek terror cselekményekkel, ipari és természeti katasztrófákkal és balesetekkel szembeni védelme érdekében fontos, hogy az infrastruktúrák működésének megzavarása vagy manipulálása megelőzhető, kivédhető, illetve lehetséges mértékben rövid, kivételes és kezelhető legyen.

A közelmúltban bekövetkezett terrortámadások (USA, Madrid, London), természeti katasztrófák (ázsiai szökőár, földrengések) és technikai kihívások (kétezredik évi dátumváltás, nagykiterjedésű áramkimaradások, kiber támadások) felhívták a figyelmet az infrastruktúrák sebezhetőségére, valamint az infrastruktúrák, a társadalom és kormányzati működés kölcsönös egymásrautaltságára.

Az Európai Unió szintjén kiadott Zöld Könyv elsődleges célkitűzése az volt, hogy biztosítsa a nemzeti kritikus infrastruktúrák védelméről (NKIV) szóló nemzeti program megvalósítását és egy olyan jogszabály megalkotását, amely összegzi a kormányzati szereplők NKIV-vel kapcsolatos célokat, szempontokat, alapelveket, fogalmakat és a megvalósítás alapvető formáira vonatkozó álláspontját.

A kritikus infrastruktúrák hatékony védelme tehát megköveteli valamennyi érintett fél - *az infrastruktúrák tulajdonosai és üzemeltetői, a hatóságok, szakmai szervek és érdekszövetségek* - közötti kommunikációt és együttműködést.

Egy széles körű, érdekazonosságon alapuló összefogás nélkül a megváltozott biztonsági környezet által jelentett új típusú veszélyek (aszimmetrikus fenyegetettség, nem hagyományos kockázati tényezők megjelenése) hatékony módon nem kezelhetőek. A Zöld Könyv másik célkitűzése ezért az is volt, hogy a magánszférával történő konzultáció alapjaként, nagyszámú résztvevő bevonásával a kormányzat visszajelzéseket kapjon az NKIV lehetséges megközelítési irányairól.

2.2. Az NKIV általános célja

Az NKIV folyamatos, dinamikus, nemzeti kritikus infrastruktúra tulajdonosok,

üzemeltetők és a kormányzat együttműködésén alapuló rendszert hozott létre, amely hozzájárul a nemzet számára kiemelt fontosságú infrastruktúrák lehetőség szerinti folyamatos működésének biztosításához. Az együttműködés formáin keresztül biztosítja a kritikus infrastruktúrák működésének megszakadása, vagy kiesésének megelőzésére, megszakadás vagy kiesés elleni védelemre vonatkozó képességek fejlesztését.

Az NKIV célkitűzése három irányú:

- megelőzés és védelem: A kritikus infrastruktúrák jelentős kihatású meghibásodásának vagy teljes leállásának hatékony megelőzése a kritikus infrastruktúrák és azok legnagyobb kockázatot képviselő elemeinek beazonosításán, kijelölésén, a kockázatok elfogadott legkisebb mértékűre történő csökkentését biztosító elemzések lefolytatásán és a szükséges védelmi intézkedések alkalmazásán keresztül;
- felkészülés és jelzés: az infrastruktúra tulajdonosok, üzemeltetők és az állami szervek megfelelő felkészítésének biztosítása a kritikus infrastruktúra meghibásodása vagy működésének megszakadása esetére;
- üzemfolytonosság és ellenálló képesség: jelentős kihatású meghibásodás vagy kiesés, teljes leállás esetén a működés lehető legrövidebb időn belül történő visszaállítására, illetve helyettesítő megoldások alkalmazására irányuló képességek, intézkedések tervezése, kialakítása, végrehajtása és fejlesztése.

Az NKIV nem irányul a kritikus infrastruktúrák kis kihatású működési zavaraira, sem az infrastruktúrákra veszélyt jelentő összes tényezőt kizáró teljes védelemre, hanem a sebezhető pontok csökkentésével, valamint a kockázati tényezők tudatos felmérésével és beazonosításával biztosítja a kritikus infrastruktúrák számára a megfelelő védelmet.

2.3. A 1249/2010 Kormányhatározat [3]

Ez a 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 új fejezetet nyitott a hazai kritikus infrastruktúrák védelmének tekintetében.

Bevezette a létfontosságú információs rendszer és létesítmény fogalmát, mely alatt: a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszereit, eszközeit és módszereit értjük, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek.[4]

3. Következtetések

Nemzetközi példákat látva hazánkban is kormányzati szinten, globálisan kell foglalkozni a kritikus információs infrastruktúrák elleni támadások összehangolt védelmével. A Kritikus infrastruktúrák védelme kiemelt jelentőségű, melyben több hazai kormányzati szervezet is feladatot vállal. Közülük is kiemelkedik a Kormányzati Eseménykezelő Központ (govCERT) és a Nemzeti Kibervédelmi Intézet.[5] A Kormányzati Eseménykezelő Központ a magyar és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezetekkel mint az országon belüli koordinációs szervezet végzi az Internetet támadási csatornaként felhasználó incidensek kezelését és elhárításának koordinálását, továbbá közzéteszi a felismert és publikált szoftver sérülékenységeket.[6]

A Nemzeti Kibervédelmi Intézet szolgáltatásait (preventív információ-megosztás és operatív incidens-kezelés) a kormányzati

szervezetek és önkormányzatok részére nyújtja. Az Intézetnek kiemelt szerepe van a nemzetgazdaság és az állami működőképesség szempontjából létfontosságú informatikai rendszerek védelmében, ezzel összefüggésben a nemzetközi szervezeteknél Magyarország képviseletében, és a hálózatbiztonsági tudatosításában egyaránt. [7, 8]

Szakirodalmi hivatkozások

[1] www.kurt.hu/wp-content/uploads/2013/03/KURT_KIV_elemzes.pdf

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

[3]http://www.katasztrofavedelem.hu/index2.php?pageid=pvl_kritikus_infrastruktura

[4] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról, http://www.njt.hu/cgi_bin/njt_doc.cgi?docid=159312

[5] Farkas Tibor: *A honvédség tervezett kommunikációs hálózata*, KARD ÉS TOLL, 1:(1) pp. 53-57. (2006)

[6] Tóth András, Farkas Tibor, Pándi Erik: *A válságreagáló műveletek híradó- és informatikai rendszerének megszervezése* Hírvillám- Signal Badge 1:(1) pp. 13-31. (2010)

[7] Farkas Tibor: *Signal Officer Training at the National University of Public Service* (Budapest, Hungary) In: Mikuláš Šostronek, Roman Berešik, Marián Babjak, Danuša Spilá (szerk.): New Trends in Signal Processing 2014: Proceedings of the International Conference Liptovski Mikulas: Armed Forces Academy of General Milan Rastislav Štefánik, 2014. pp. 37-43.

[8] Farkas Tibor, Hronyecz Erika: *The infocommunication system requirements and analysis of the communication of the deployable rapid diagnostic laboratory support „sampling group”* II. Academic and Applied Research In Public Management Science XIV:(1) pp. 53-61. (2015)