HADTUDOMÁNYI SZEMLE

2017. X. évfolyam 2. szám

NYITRAI MIHÁLY[1]

Összehasonlító tanulmány az Európai Unió és az Egyesült Államok kritikus infrastruktúra védelem szabályozása és megvalósítása területein

A Comparative Study of Legislation and Implementation of Critical Infrastructure Protection in the European Union and the United States of America

Absztrakt

A 2012-ben elfogadott Nemzeti Biztonsági Stratégia az Európai Unió és a NATO keretei között határozza meg Magyarország nemzetbiztonsági alapjait. Ahhoz nem férhet kétség, hogy az Egyesült Államok a NATO legmeghatározóbb tagállama, amely a biztonság területein nemcsak a Szövetségen belül, hanem azon kívül is vezető szerepet tölt be a világban. A társadalom zavartalan működése pedig elképzelhetetlen olyan rendszerek nélkül, amelyeket a szakirodalom kritikus infrastruktúrának nevez. A tanulmány áttekinti és elemzi a fenti két, Magyarország biztonsága szempontjából fontosnak tartott entitás, az Európai Unió és az Egyesült Államok kritikus infrastruktúra védelem területén tett erőfeszítéseit.

Kulcsszavak: kritikus infrastruktúra, Európai Unió, Egyesült Államok, terrorizmus, biztonság

Abstract

The National Security Strategy, adopted in 2012, defines Hungary's national security within the framework of the European Union and NATO. There is no doubt that the United States is the most decisive NATO Member State taking a leading role in promoting the security not only within the Alliance, but also outside around the world. The smooth functioning of society is unimaginable without the systems that the literature calls critical infrastructures. The study reviews and analyses the efforts made by these two entities, the European Union and the Uni-

[1] Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola, doktorandusz hallgató/National University of Public Service, Doctoral School of Military Sciences, PhD student, E-mail: nyitrai.mihaly@uni-nke.hu ORCID ID: 0000-0002-7726-9898

ted States, considered important for Hungary's national security, in the field of critical infrastructure protection.

Keywords: critical infrastructure, European Union, United States, terrorism, security

BEVEZETŐ

Napjainkban a kritikus infrastruktúra fogalma és a mögöttes tartalom egyre nagyobb teret hódít, de vajon minek köszönhető ez az érdeklődés és egyáltalán, mi az a kritikus infrastruktúra? Magyarország Országgyűlése 2012. november 12-én fogadta el a saját erre vonatkozó meghatározását, amely szerint „a létfontosságú rendszerelem meghatározott ágazatokba tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna." (OGY 2012) A Gazdasági Együttműködési és Fejlesztési Szervezet,[2] amelynek Magyarország is tagja 1996 óta, e tekintetben például arra az álláspontra helyezkedett, hogy a „kritikus" kifejezés olyan infrastruktúrára vonatkozik, amely a gazdasági és szociális jólét, a közbiztonság és a kulcsfontosságú kormányzati tevékenységek megvalósulását alapjaiban támogatja úgy és oly mértékben, hogy ennek hiánya viszont katasztrofális és messzemenő következményekkel járna. (Poustourli et al., 2015) Már ebből a két definícióból is látszik, hogy maga a fogalom meghatározása, noha tartalmilag roppant hasonlóak, mégis képlékeny.[3] Éppen ezért hazánk szempontjából érdemes kitekinteni azokba az irányokba is, amelyek a biztonságát hosszú távon meghatározzák. Ehhez nyújt iránymutatást Magyarország 2012-ben elfogadott Nemzeti Biztonsági Stratégiája,[4] amely úgy fogalmaz, hogy „Magyarország biztonságpolitikájának alapvető keretét a NATO- és EU-tagság jelenti." (OGY 2012) Kritikus infrastruktúra szempontból a szervezet keretein belül az Európai Unió 2008. december 8-án elfogadott 2008/114/EK tanácsi irányelv[5] (továbbiakban: Irányelv) definícióját kell hivatalosnak tekinteni, amely úgy fogalmaz, hogy a „kritikus infrastruktúra: a tagállamokban található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az em-

[2] Organization for Economic Co-operation and Development, OECD

[3] A későbbiekben látni fogjuk, hogy a kritikus infrastruktúra és védelmének fogalmi körülhatárolása némiképp függ az egyes államok és szervezetek történelmi, gazdasági, kulturális, technikai-technológiai és törvénykezési (!) sajátosságaitól. Éppen ezért a probléma, a kritikus infrastruktúra védelmének megközelítési módja is különbözik. Ebből aztán az is következik, hogy adott esetben egy definíció valódi megértéséhez meg kell vizsgálni a kiváltó tényezőket és az előbb említett környezeti sajátosságokat.

[4] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról, http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf

[5] 2008/114/EK irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32008L0114

berek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna valamely tagállamban." (EU 2008) A magyar nemzeti biztonság másik iránya a NATO, amelynek egyik meghatározó tagállama az Egyesült Államok. Természetesen, az Egyesült Államok is megalkotta a saját kritikus infrastruktúra definícióját, amely, nem véletlenül, az Európai Unió által megadottnál korábbra datálódik. A George W. Bush amerikai elnök által 2001. október 26-án aláírt, röviden USA PATRIOT[6] Act néven emlegetett törvény szerint a kritikus infrastruktúra fogalma alá „azok a fizikai és virtuális rendszerek, eszközök tartoznak, melyek olyannyira létfontosságúak az Egyesült Államok számára, hogy e rendszerek és eszközök működésképtelensége vagy megsemmisülése gyengítené a védelmet, a nemzeti gazdaságbiztonságát, a nemzeti közegészséget és biztonságot vagy mindezek kombinációját." (US Congress 2001, p. 401) A definíciókból összességében látható egyrészt, hogy a kritikus infrastruktúra középpontjában a komplexen értelmezett biztonság humán dimenziója[7] áll (Buzan, 1991, p. 432), másrészt minden szereplő törekvéseinek alanya alapvetően önmaga. Vajon milyen okok állhatnak magyarázatként a háttérben?

A KRITIKUS INFRASTRUKTÚRA VÉDELEM AZ EGYESÜLT ÁLLAMOKBAN

A kritikus infrastruktúra, mint fogalom először az Egyesült Államokban jelent meg nem sokkal az ezredforduló előtt 1996-ban. Ekkor Bill Clinton amerikai elnök bizottságot (President's Commission on Critical Infrastructure Protection, PCCIP[8]) hozott létre a nemzeti kritikus infrastruktúrák kibertérből érkező fenyegetettségekkel szembeni sérülékenységének vizsgálatára. A bizottság jelentését 1997 októberében tette meg, s noha közvetlen veszélyt, fenyegetettségre utaló jelet nem azonosított, ajánlásai mégis korszakalkotónak és iránymutatónak számítottak a következő kormányok és más nemzetközi szervezetek, így az Európai Unió részére is. A bizottság felhívta az elnök figyelmét arra, hogy a lakosság körében rohamosan (gyakorlatilag kontrolálatlanul) terjedő számítástechnika milyen valós veszélyeket hordoz magában. A bizottság véleménye szerint a mindenki, így a bűnözők számára is könnyen hozzáférhető technológiák és technikai vívmányok azok eszközeivel (számítógépek, telefonvonalak, modemek, programok, weboldalak stb.) a közeljövőben olyan fokozott veszélyt jelentenek, amelyre a felkészülést minél hamarabb el kell kezdeni. Akkor ez a felkészülés elsősorban még csak kommunikációt és információcserét jelentett az érdekeltek között, amelyben a kormányra, nem számítva az általa működtetett infrast-

[6] A „PATRIOT" jelentése fordításban „hazafi", de egyben betűszó is. A törvény teljes címe ugyanis „Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001". Ezért a törvény rövidebb nevén történő említése is korrektnek nevezhető.

[7] Barry Buzan, Ole Waever, Jaap de Wilde szerzők egy 1998-ban kiadott munkájukban (Security: A New Framework for Analysis) a biztonság politikai és katonai vetületeit továbbiakkal, gazdasági, társadalmi és környezeti dimenziókkal egészítették ki (szektorelmélet). Az elmélet alapjait azonban először Barry Buzan a „New Patterns of Global Security in the Twenty-First Century" (A globális biztonság új mintái a XXI. században) cikkében fejtette ki 1991 júliusában, ezért is fűződik az elmélet az ő nevéhez.

[8], Kritikus Infrastruktúra Védelmi Elnöki Bizottság

ruktúrákat és azok védelmét, mindössze a koordinátor szerepköre hárult volna. (Moteff, p. 3) Mivel azonban a tengerentúlon sem mindenki érezte volna feltétlenül magától értetődően önmagára nézve kötelezőnek ezt a kommunikációs feladatot, ezért a bizottság szorgalmazta egy megfelelő jogszabályi és kormányzati szintű szervezeti háttér egyidejű megteremtését is, amelynek célja a szereplők együttműködésének koordinációja mellett, annak fokozása, illetve egy valós idejű reagáló képesség megteremtése volt.[9] (Ellis et al., 1997) Így született meg az amerikai kritikus infrastruktúra védelem alfája, a PDD-63 elnöki direktíva[10], amelyet Clinton elnök 1998. május 22-én adott ki.

PDD-63

A tökéletes kritikus infrastruktúra védelemmel kapcsolatos elvárásokat először ez a direktíva tette világossá. E szerint a védelem olyan legyen, hogy eredményeként csak ritka, rövid idejű, földrajzilag elszigetelt, kezelhető és elenyésző hatású működési zavarok fordulhassanak csak elő. (Moteff, p. 4) Ennek megvalósítása érdekében a direktíva minden ágazathoz[11] egy kormányzati szervet ún. Ágazati Felelős Hivatalt[12] rendelt, ahol az államot hivatalonként ágazati összekötők,[13] az ágazatokat pedig civil szféra oldalról ágazati koordinátorok[14] képviselték. Ehhez a rendszerhez társult szövetségi szinten a saját kormányzati hivatali tevékenységek funkcionális koordinátorai,[15] illetve az adott kormányzati hivatal önnön kritikus infrastruktúra biztonságával foglalkozó kritikus infrastruktúra védelmi (CIAO[16]) és vezető információs tisztek (CIO[17]) hálózata. Ez az ágazati összekötő-koordinátori struktúra volt hivatott arra, hogy az általa alkotott ágazati védelmi tervek rendszerén keresztül a nemzeti koordinátor[18] vezérletével 2003-ig létrehozza a Nemzeti Infrastruktúra Védelmi Tervet (NIAP[19]). A struktúra azonban nem önvezérlően, hanem egyrészt a nemzeti koordi-

[9] A bizottság javaslataiból meg kell még említeni egy átfogó, (kiber)tudatosságra (!) nevelő program elindításának szükségességét, illetve a védelmi kutatások és fejlesztések kritikus infrastruktúra irányú kiterjesztését. Ellis et al., 1997

[10] Presidential Decision Directive No. 63

[11] A Clinton kormányzat 1998-ban még csak öt fontos szektort nevezett meg: energiaellátó rendszerek, banki és pénzügyi rendszerek, közlekedés és szállítás, egészségügyi rendszer és segélyszolgálatok, telekommunikációs rendszerek. Bonnyai, 2014

[12] Lead Agency

[13] Sector Liaison Official

[14] Sector Coordinator

[15] Functional Coordinator

[16] Critical Infrastructure Assurance Officer. Ez a személy volt felelős, hogy az elnöki direktíva aláírását követő 180 napon belül a hivatal kritikus infrastruktúra tervét kidolgozza, illetve az abban foglaltak két éven belül megvalósuljanak. A kidolgozott tervek esedékes felülvizsgálatára az elnöki direktíva kétévenkénti ciklust határozta meg.

[17] Chief Information Officer

[18] National Coordinator for Security, Infrastructure Protection, and Counter-terrorism. A szerepkört a PDD-62 hozta létre.

[19] National Infrastructure Assurance Plan

nátor vezette kormányzati-civil összetételű Nemzeti Infrastruktúra Védelmi Tanács (NIAC[20]) koordinációja mellett, illetve szintén a nemzeti koordinátor által elnökölt, hatáskörében hivatalokon és ügynökségeken átívelő Kritikus Infrastruktúra Koordinációs Csoport (CICG[21]) alkotta irányelvek mentén működött. A NIAP kidolgozásának támogatására pedig az elnöki direktíva megalakított még egy további fontos közreműködőt, a Nemzeti Terv Koordinációs Törzset (NPCS[22]), illetve ennek következményeként a Kritikus Infrastruktúra Védelmi Hivatalt (CIAO[23]). Már most látszik, hogy egy egyre inkább szövevényessé váló rendszer kezdett kialakulni, amelyben utat mutatni már a kezdetek elején sem volt egyszerű. Ezért az aktuális kérdésekről, tevékenységekről a Nemzeti Infrastruktúra Védelmi Tanács az elnök részére időről időre jelentéseket terjesztett fel. (Moteff, p. 5)

Összességében tehát felállt egy rendszer, amelyben adott volt egy központi felelős személy (nemzeti koordinátor) egyeztető-kidolgozói szerepkörben tevékenykedő ágazati összekötők és koordinátorok rendszerével, valamint más közreműködő, irányító és koordináló szervezetekkel (CICG, NIAC, NPCS, CIAO), hogy egy átfogó kritikus infrastruktúra védelmi tervet (NIAP) hozzanak létre[24]. Ez a felismerés, hogy ilyen védelmi tervre szükség van, különösen a később történtek ismeretében, kiemelt jelentőségű és a direktíva legfontosabb vívmánya. Mint ahogy az is, hogy máig ható módon ágazati összerendelések jöttek létre a központi kormányzati szervek és a civil szféra érintett képviselői között.

A fentiekhez képest „csak" ráadás, de meg kell említeni, hogy a direktíva a NIAP mellett megfelelő kibervédelmi képesség létrehozását is megcélozta. Ez a képesség elsődlegesen a kibertámadások felfedésére, megakadályozására és válaszreakció kialakítására irányult, amelynek megvalósulását eredetileg két program, a Szövetségi Behatolás Jelző Hálózat (FIDNET[25] és a Szövetségi Számítógép Behatolás Reagáló Képesség – FedCIRC[26] segítette volna. Végül a Szövetségi Nyomozó Iroda (FBI[27]) kapott felhatalmazást arra, hogy a

[20] National Infrastructure Assurance Council. A Tanácsban a (szövetségi állami, helyi) kormányzati oldal mellett a civil szféra képviselői, üzemeltetői is helyet kaptak.
[21] Critical Infrastructure Coordination Group, CICG. A Csoportot csak kormányzati oldal alkotta.
[22] National Plan Coordination Staff
[23] Critical Infrastructure Assurance Office
[24] Fontos megjegyezni, hogy a védelmi terv kidolgozására az elnöki direktíva határidőt nem szabott. A 2003 határidő csak a kritikus infrastruktúra védelemre történő felkészülésre vonatkozott, amelynek részét, természetszerűleg, a NIAP is képezte.
[25] Federal Intrusion Detection Network
[26] Federal Computer Intrusion Response Capability
[27] Federal Bureau of Investigation. Az Iroda kapcsán el kell mondani, hogy már akkor, az elnöki direktíva idején két olyan programot (INFRAGARD, Key Assets Initiative, KAI) működtetett, amelyek ugyan egy egészen más megközelítésben, de ugyancsak a kritikus infrastruktúra védelmet célozták meg. Az INFRAGARD, amelynek középpontjában a hálózatbiztonság állt, alapvetően földrajzi és nem ágazati szemléletű. Az együttműködés ugyanis, amely 2001. szeptember 11. után már a kritikus infrastruktúra védelem fizikai aspektusait is magában foglalja, az Iroda helyi kirendeltségei és az adott földrajzi környezet ipari, gazdasági szereplői között jött létre. A KAI (Key Assets Initiative) kulcsfontosságú létesítmények program célja pedig egy olyan adatbázis kialakítása volt, szintén a területi FBI kirendeltségek felelősségi körében, amely lehetővé tette egyrészt a helyi létesítmények tételes számbavételét, másrészt elősegítette az egyes szereplők közötti kommunikációt, harmadrészt pedig értelemszerűen

számítógépes bűnözés területére szakosodott ágát ezen két program gondolatiságát integrálva Nemzeti Infrastruktúra Védelmi Központot (NIPC[28]) alakítson ki. Ennek megfelelően a NIPC állt a szövetségi fenyegetettség felmérések, a sérülékenység elemzésnek, a korai előrejelzésnek és a válaszképesség koordináció középpontjában. Éppen ezért, hogy ez a központ képes legyen a vele szemben támasztott elvárásoknak megfelelni, minden kormányzati és nem kormányzati hivatal köteles volt a tudomására jutott számítógépes fenyegetettségről és támadásról jelenteni, információkat átadni. Ez az információáramlás azonban nemcsak egy irányban működött. A NIPC a birtokában lévő információkat megosztotta a civil szféra által működtetett (és ma is működő[29]) Információmegosztó és Elemző Központokkal (ISACs[30]). (Károlyi, 2007 pp. 32.)

HSPD-7[31]

A 2001. év az Egyesült Államok történetében két szempontból is kiemelkedő jelentőséggel bírt. Egyrészt az elnöki székben Bill Clintont George W. Bush váltotta, másrészt szeptember az al-Kaida több nemzeti, de a nyugati világban is szimbólumnak számító létesítmény ellen terrortámadás sorozatot hajtott végre.[32] Túl a katonai válaszreakción, kritikus infrastruktúra tekintetében újabb elnöki direktíva, a HSPD-7 kiadásának lehettünk tanúi. Azonban addig is, amíg ez a PDD-63 hatálytalanító direktíva nem jelent meg, hiszen kidolgozásához időre volt szükség, Bush elnök rendeletekkel (Executive Orders 13228, 13231) kezdte meg a „tűzoltást". Az új direktíva kiadására pedig azért volt szükség, mert, ahogy a terrortáma-

erősítette a védelemre irányuló kormányzati törekvéseket. Ez a program eredetileg a védelem fizikai szemléletét közelítette meg, de a NIPC integrációja után a kibervédelem is fókuszába került. Moteff, pp. 6–7

[28] National Infrastructure Protection Center Az 1998-ban létrehozott Központot később a Belbiztonsági Minisztérium (Department of Homeland Security, DHS) integrálta, feladatai (elsősorban informatikai hálózatok sebezhető pontjainak vizsgálata, a kibertérben bekövetkező káros események megelőzése, felderítése és elhárítása) pedig a Belbiztonsági Minisztérium Információ Elemző Infrastruktúra Védelem (Information Analysis Infrastructure Protection, IAIP) szervezetei között osztódtak el. http://web.archive.org/web/20041015000154/http://www.nipc.gov/

[29] A Központok és a kormányzati hivatalok közti információáramlás optimalizálását ma már a 2003-ban alapított és 24 szervezetet tömörítő Információmegosztó és Elemző Központok Nemzeti Tanácsa (National Council of ISACs, NCI) végzi. NCI, 2016

[30] Information Sharing and Analysis Center(s). Ha nem is minden ágazat azonos alapon, de működtet egy ilyen saját központot. Itt kell azt is megjegyezni, úgy tűnhet, hogy ezek a folyamatos üzemmódban tevékenykedő csak kibervédelmi kérdésekre összpontosítanak. Ezzel szemben jócskán akadnak ágazati ISACs, amelyek rendeltetésükben a fizikai biztonságra is figyelmet fordítanak, tehát ilyen jellegű információkat is gyűjtenek, osztanak meg. A működési alapot tekintve alapvetően két féle ISACs létezik. Az egyik ISAC modell saját fejlesztésű és szervezetileg integrált vagy szerződéssel alkalmazott vállalkozás alapon működik. A másik ISAC megvalósulási formát többnyire már egy működő kormányzati infrastruktúra használata jelenti, amely vállalja az adott szektor kritikus infrastruktúra védelmét. Ugyanígy a központok gazdasági hátterükben is különböznek. Addig, amíg egyes ágazati ISAC indításához az Ágazati Felelős Hivatal egyszeri vagy folyamatos pénzügyi befektetéssel járult hozzá, más szektorok esetében az ISAC működése teljes mértékben önerős. Moteff, p.6

[31] Homeland Security Presidential Directive 7, HSPD-7

[32] World Trade Center, Pentagon

dás is rámutatott, a kibertér fenyegetettségei mellett igenis számolni kell fizikai dimenzióval is, tehát az információs és a fizikai infrastruktúrák vonatkozásában egyensúly helyreállításra van szükség.

A 2001. október 8-án kelt EO[33] 13228 rendelet megalakította a Belbiztonsági Hivatalt (Office of Homeland Security), illetve a Belbiztonsági Tanácsot (Homeland Security Council). Az USA terrorista fenyegetések és támadások elleni nemzeti stratégiájának fejlesztése, végrehajtásának koordinálása vált az újonnan megalakult Belbiztonsági Hivatal feladatává, míg a Belbiztonsági Tanács (állandó tagjai: USA elnök, elnök-helyettes, pénzügyminiszter, legfőbb ügyész, különböző szövetségi hivatalok (FEMA[34], FBI, CIA[35]) elnökei, az egészségügyi, emberi és közlekedési miniszter, a belbiztonsági miniszter és az elnök belbiztonságért felelős tanácsadója) iránymutatásaival segítette az elnököt belbiztonságot érintő döntések meghozatalában. A belbiztonsági, így a kritikus infrastruktúra védelem szerkezete a 2002. november 25-én a Belbiztonsági Törvény által életre hívott, egyszerre 22 ügynökséget tömörítő és már a korábbiakban a NIPC kapcsán is említett Belbiztonsági Minisztériummal vált teljessé. (Moteff, p. 8) Ugyanis ettől fogva a Nemzeti Infrastruktúra Védelmi Terv kidolgozásáért a felelősség a belbiztonsági minisztert terhelte, mint ahogy a terv neve is most már ténylegesen Nemzeti Infrastruktúra Védelmi Tervre (NIPP[36]) változott.

Az első elnöki rendeletet aztán követte a második. Az Elnöki Kritikus Infrastruktúra Védelmi Testületet (PCIPB[37]) létrehozó EO 13231 rendeletet az elnök 2001. október 16-án adta ki. Ez a testület a kritikus infrastruktúrák információs rendszereit védő különböző szövetségi programok koordinációját végezte, illetve javaslatot tett irányelvek kidolgozására és véleményezte a felelősségi körébe eső ügynökségek vonatkozó költségvetését. Ugyanennek a rendeletnek egy másik kiemelkedő kritikus infrastruktúra védelmi vonatkozása az azóta mintegy 30 taggal[38] működő Nemzeti Infrastruktúra Javaslattételi Tanács (National Infrastructure Advisory Council, NIAC). (DHS, 2017b) A Tanács feladata, hogy a belbiztonsági miniszteren keresztül az elnök részére útmutatásokat adjon a kritikus infrastruktúrák és információs rendszereik védelmével kapcsolatban. Részösszegzésként látható tehát, hogy a 9/11 terrortámadás elnöki rendeletek formájában szükségszerűen azonnali kormányzati reakciókat váltott ki.

[33] Executive Order, Végrehajtási Utasítás
[34] Federal Emergency Management Agency, Szövetségi Veszélyhelyzet-kezelési Ügynökség
[35] Central Intelligence Agency, Központi Hírszerző Ügynökség
[36] National Infrastructure Protection Plan. A tervnek továbbra is részét képezte a szövetségi ágazati felelős ügynökségek által a magánszféra arra kötelezett érintettjeivel együttműködésben kidolgozott Ágazati Tervek (Sector-Specific Plans, SSPs)
[37] President's Critical Infrastructure Protection Board. A testületet később a EO 13286 rendelet megszüntette, és helyét a Kritikus Infrastruktúra Irányelv Koordinációs Bizottság (Critical Infrastructure Policy Coordinating Committee, CIPPCC) vette át.
[38] A Tanács tagjai a tudományos élet, az ipar és az állami szektor különböző területeit képviselik.

2002 júliusában a Belbiztonsági Hivatal kiadta a Nemzeti Belbiztonsági Stratégiát (National Strategy for Homeland Security, NSHS[39]), amely a témában egy újabb mérföldkőnek számít és több lényegi változást, módosítást is hozott a területet illetően. A stratégia egyrészt bővítette az ágazatok rendszerét (közegészségügy, vegyipar, postai szolgáltatások, mezőgazdaság és élelmiszeripar, hadipari bázisok, a kormányzat és kormányzati működés folyamatossága, sürgősségi szolgáltatások), másrészt néhány területen az ágazatok és felelős hivatalaik között átcsoportosítást végzett. Szintén fontosnak számít, hogy a stratégia új fogalmat vezetett be, a kulcsfontosságú létesítmények (Key Assets) intézményét,[40] valamint kimondta, hogy nem csak irányelvek és szervezetek, de prioritások felállítására is szükség van. A prioritások meghatározásakor a stratégia arra utalt, hogy nem minden infrastruktúra egyformán kritikus, köztük fontossági sorrend létezik, és hogy a védelem megvalósításakor költséghatékonysági szempontokat is figyelembe kell venni.[41] (Moteff, p.10)

Ilyen előzmények után adta ki Bush elnök 2003. december 17-én a HSPD-7 direktíváját. Ez a direktíva a hangsúlyt inkább az addigi irányelvek és felelősségi körök pontosítására és finomra hangolására, semmint átrendezésére helyezte. Ettől függetlenül azonban a pontosítások között is akadt néhány említésre méltó változás. Például az Ágazati Felelős Hivatalokat az allokált civil ágazatokkal való együttműködés eredményeiről a Belbiztonsági Hivatal irányába éves jelentés megtételére kötelezte. A direktíva fontos eredményeként kell említenünk, hogy a szövetségi ügynökségek részére határidőt szabott a saját kritikus infrastruktúráikra vonatkozó védelmi tervek elkészítésére. Ez a határidő pedig 2004. (Moteff, pp. 10–11)

A direktíva mellett a Bush kormányzat kritikus infrastruktúra fejlesztését illetően az egyik legnagyobb változást annak az összekötő-koordinátori partneri rendszer módosításában eszközölte, miután azt tanácsi szintre emelt. Egészen addig ugyanis, kontakt személyek (Sector Liaison Official, Sector Coordinator) és nem csoportok álltak egymással kapcsolatban. A Bush kormányzat ezt a modellt úgy módosította, hogy az addigi szereplők helyét Kormányzati Koordináló Tanácsok (Government Coordinating Councils, GCCs) és Ágazati Koordináló Tanácsok (Sector Coordinating Councils, SCCs) vették át. A módosítás célja egy szélesebb, közvetlen ágazati konzultációs platform megteremtése volt. Ezekben a civil tanácsokban ugyanis immár nem egy, hanem két szavazati joggal és egy szavazati joggal nem rendelkező delegált tag vehetett részt, akárcsak a kormányzat kibővített testületeiben, ahol a központi rész mellett egyidejűleg megjelenhetett az érdekeltség és érintettség minden szintje. Ezt a kiszélesített konzultációt erősítette a civil interágazati tanácsok (Private Sector Cross-Sector Councils) párhuzamos megjelenése. Azonban ennek az

[39] A Stratégiát a 2005 augusztus 23-31. között tombolt és súlyos károkat okozó Katrina hurrikán hatására 2007-ben felülvizsgálták és módosítottan újat adtak ki. DHS, 2016

[40] A stratégia szerint ezek azok a létesítmények, amelyek megsemmisülése, működési zavara ugyan nem veszélyezteti a létfontosságú rendszereket, de helyi szinten szintén messzemenő következményekkel, hatással járhat.

[41] A védelem fokozásához szükséges ráfordításnak arányban kell állnia a fenyegetettség mértékével.

együttműködési formációnak sem változott az alap küldetése, létre kellett hozni az ágazat specifikus kritikus infrastruktúra védelmi terveket és elősegíteni a NIPP megalkotását, amelyhez a Belbiztonsági Minisztérium az állami és civil szféra közötti nyitott párbeszéd megteremtése érdekében Kritikus Infrastruktúra Együttműködési Javaslattevő Tanács (Critical Infrastructure Partnership Advisory Council, CIPAC) létrehozásával járult hozzá. (DHS, 2017a)

Azonban a kritikus infrastruktúra védelem fejlődésére az idők során nem csak az emberi tevékenység, hanem természeti és technikai események is hatást gyakoroltak. Ilyen kiemelkedő hatásnak számított a Katrina hurrikán 2005-ben. Ezt követően ugyanis 2006-ban a Kongresszus elfogadta az ún. Post-Katrina törvényt, amely egyrészt erősítette a Belbiztonsági Minisztérium alárendeltségébe tartozó Szövetségi Veszélyhelyzet-kezelési Ügynökség FEMA) Nemzeti Felkészültségi Igazgatóságának (National Preparadness Directorate, NPD) keretein belül folyó reagálási és helyreállítási tevékenységet, másrészt megalakította a Vészhelyzet Kommunikációs Hivatalt (Office of Emergency Communications, OEC[42]). (DHS, 2017c) A hivatal az elsőként beavatkozó szervek, szervezetek, hivatalok és ügynökségek között teremt tele- és infokommunikációs kapcsolatot. (109th US Congress 2005-2006)

PPD-21

Barack Obama, az új elnök és újabb direktíva 2013. február 12-én. Igaz, hogy 2017. január 20-án Donald Trump, az Egyesült Államok 45. elnöke tőle is átvette az elnöki mandátumot, de azóta eltelt időben újabb kritikus infrastruktúra védelmi elnöki direktíva nem látott napvilágot. Így minden, amit Obama elnök alkotott, egyben az utolsó is.

Barack Obama 2013. február 12-én adta ki a „Kritikus Infrastruktúra Biztonság és Ellenálló képesség[43]" PPD-21[44] direktíváját, amely egyúttal hatályon kívül helyezte a Bush elnök által kiadott HSPD-7 direktívát. Irányelvekben újat ez a dokumentum már nem jelentett, sőt, bizonyos szempontból a PDD-63 egyfajta reinkarnációjaként is tekinthetünk rá. Ami miatt viszont jelentős, az egyrészt éppen ez a „nincs benne semmi új" (1sz. táblázat), hiszen csak a kormányzati-civil együttműködési modell áttekintésére és értékelésére,[45] egy hatékonyabb információs rendszer követelményeinek lefektetésére, illetve a helyzetismere-

[42] A Hivatallal kapcsolatban több, mint érdekes megemlíteni John Fitzgerald Kennedy elnök nevét és az általa a NSAM 252 számú Nemzetbiztonsági Cselekvési Alapító Okirat (National Security Action Memorandum) útján 1963-ban a kubai rakétaválság idején diplomáciai, katonai és hírszerzői információcsere céljából létrehozott Nemzeti Kommunikációs Rendszert (National Communications System, NCS) John F. Kennedy 1963, amely ma már inkább egy képesség, semmint szervezet, hogy veszélyhelyzetekben az egyes ügynökségek és hivatalok közötti kapcsolattartást és információáramlást segítse elő a különböző telekommunikációs és informatikai rendszerek védelmével.
[43] Critical Infrastructure Security and Resilience
[44] Presidential Policy Directive 21
[45] A direktíva frissítette ugyan az ágazati kijelölést, de az Ágazati Felelős Hivatal hozzárendelések gyakorlatilag nem változtak.

ti és reagálási képesség további fejlesztésére[46] intézkedett. Obama elnökségére tehát kialakult minden, csak felül kellett vizsgálni, illetve a hatékonyságát javítani. Nyilvánvaló tehát, hogy Obama elnök és tanácsadói célja ezzel a felülvizsgálattal az volt, hogy a veszélyhelyzetek okozta fennakadásokat valóban csak a ritka, rövid idejű és kezelhető jelzőkkel lehessen illetni, és hogy a kritikus infrastruktúrák biztonsága és terhelhetősége fokozódjon a fenyegetésekkel szemben. Ettől függetlenül akadtak a direktívában apróbb érdekességek és újdonságok. Például, a PPD-21 a hangsúlyt, a más ágazatok működése szempontjából is meghatározónak számító energia és kommunikációs ágazatokra helyezte, illetve, hogy a kibervédelem ismét teret nyert a fizikai dimenzióval szemben. (Moteff, pp. 14–15)

	HSPD-7	**PPD-21**	**Megjegyzés**
Kiadás éve	2003	2013	
a direktíva fókusza	a kritikus infrastruktúrák közti fontossági sorrend felállítása, illetve azok terrortámadás szembeni védelmének megvalósítása	a kritikus infrastruktúrák biztonságának és ellenálló képességének fizikai és kiber fenyegetésekkel szembeni erősítése	A 9/11 által előtérbe helyezett fizikai védelemről a hangsúly kezd visszatolódni a kibertérből érkező fenyegetések irányába.
a kritikus infrastruktúra meghatározása	USA PATRIOT Act 1016(e) szakasza	USA PATRIOT Act 1016(e) szakasza	nincs különbség
a védelem és a biztonság értelmezése	a kritikus infrastruktúrák terrortámadások elleni sérülékenységének csökkentése	természeti és ember okozta csapások kockázatának csökkentése	lényegi különbség nincs, de már nemcsak a terrortámadás áll a középpontban

[46] Az elnöki direktíva elrendelte a „Nemzeti Kritikus Infrastruktúra Kutatási és Fejlesztési Terv” (National Critical Infrastructure Research and Development Plan) elkészítését, amely 2015 novemberére a Belbiztonsági Minisztérium gondozásában meg is valósult. A terv rendeltetése meghatározni azokat a biztonság és ellenálló képességet növelő kutatási-fejlesztési prioritásokat, amelyek elősegítik a megfelelő innovációk megvalósulását, illetve irányítják a kritikus infrastruktúrákkal kapcsolatos kutatási tevékenységeket.
https://www.dhs.gov/sites/default/files/publications/National%20CISR%20R%26D%20Plan_Nov%202015.pdf

	HSPD-7	PPD-21	Megjegyzés
Kiadás éve	2003	2013	
ágazatok kijelölése	ágazat specifikus hivatalokhoz rendel szektorokat	szektorokhoz rendel ágazat specifikus hivatalokat	az ágazati hozzárendelésekben új szereplő a Belbiztonsági Minisztérium, illetve 18. ágazatként megjelenik a „Kritikus Gyártás[47]", a fontosabb szektorok (bank és pénzügy, védelem, energia) maradtak a korábbi felelősöknél
együttműködés a civil szférával	megerősíti a már korábbi szabályzók által létrehozott modellt	az együttműködési modell felülvizsgálatát és hatékonyabbá tételét rendeli el	a felülvizsgálat nem jelent változtatást
Nemzeti Infrastruktúra Védelmi Terv	első ízben rendeli el átfogó és integrált terv elkészítését[48]	a védelmi terv aktualizálását rendeli el	a hivatkozási alap, a 2002. évi Belbiztonsági törvény mindkét esetben ugyanaz
Kutatás és Fejlesztés (K+F)	éves terv kidolgozása	változatlan felelős szervezetekkel közös K+F erőfeszítések	nincs változás

1.sz. táblázat HSPD-7 és PPD-21 elnöki direktívák összehasonlító táblázata (saját szerkesztés)

NEMZETI INFRASTRUKTÚRA VÉDELMI TERV

Már a Clinton elnök PDD-63 direktívája is kritikus infrastruktúra védelmi tervért kiáltott, akkor még (lásd fentebb) National Infrastructure Assurance Plan néven, ráadásul konkrét határidő és tartalmi meghatározás nélkül, de hozzátéve, hogy határidő tekintetében látens módon 2003-ig fel kellett készülni bizonyos kockázatok kezelésére. A Bush kormányzat HSPD-7 direktívája ezeket a határidő hiányosságokat alapvetően kiküszöbölte, ugyanis 2004-ig el kellett készíteni a négy fő területre koncentráló „Kritikus Infrastruktúra és Kulcs-

[47] Critical Manufacturing
[48] National Plan for Critical Infrastructure and Key Resources Protection (Kritikus Infrastruktúra és Kulcsfontosságú Források Védelmének Nemzeti Terve)

fontosságú Erőforrások Védelmének Nemzeti Tervét.[49] Noha nem lehet figyelmen kívül hagyni, hogy időközben a Clinton kormányzat 2000-ben kiadta „Az amerikai kibertér védelme. Nemzeti Terv az Információs Rendszerek Védelmére 1.0 Felhívás egy párbeszédre.[50]" kezdeményező dokumentumát, illetve 2003-ban Bush elnök az Elnöki Kritikus Infrastruktúra Védelmi Testületen[51] keresztül a „Nemzeti Stratégia a Kibertér Védelmére[52]" útmutatását, a tervek elkészítése késedelmet szenvedett. A Belbiztonsági Minisztérium csak 2005 februárjában tett közzé egy Ideiglenes Nemzeti Infrastruktúra Védelmi Tervet,[53] amelyet a civil szféra szerint megfelelő egyeztetés nem előzött meg. Az első valódi védelmi tervet az elnök 2006. június 30-án hagyta jóvá, amelyet aztán három évvel később, 2009-ben egy felülvizsgálat követett. A terv kidolgozásában résztvevő felek (Belbiztonsági Minisztérium és ágazati koordinációs bizottságok) akkor abban egyeztek meg, hogy a NIPP és annak mellékletét képező ágazati tervek (SSPs[54]) felül- és esetleges átdolgozására elegendő egy négyéves ciklus kialakítása is. Így történt az, hogy 2009 után a NIPP újabb felülvizsgálata csak 2013-ban történt meg, illetve ugyanebben a négyéves ciklusban jelenleg, 2017-ben folyik ismét munka.[55] (Moteff, pp. 21-22)

[49] National Plan for Critical Infrastructure and Key Resources Protection. A terv négy fő területe: stratégia kidolgozása a kritikus infrastruktúra/kulcsfontosságú erőforrások azonosítására és azok fontossági sorrendjének felállítására; mindazon tevékenységek meghatározása, amely az iménti stratégia kidolgozásához szükségesek; olyan programok, projektek és kezdeményezések áttekintése, amelyek az érintett kritikus infrastruktúra üzemeltetőkkel együttműködésben egyrészt előrejelzést, másrészt az információmegosztást segítenek elő; és szövetségi szintű kritikus infrastruktúra védelmi tevékenységek koordinációja.

[50] Defending America's Cyberspace. National Plan for Information Systems Protection. Version 1.0. An Invitation to a Dialogue https://fas.org/irp/offdocs/pdd/CIP-plan.pdf

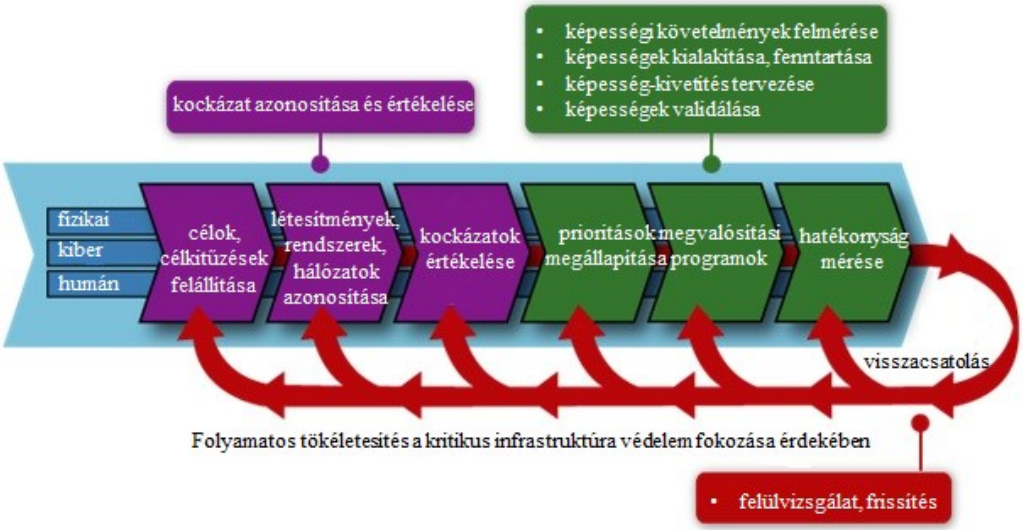
[51] President's Critical Infrastructure Protection Board

[52] National Strategy to Secure Cyberspace https://www.dhs.gov/national-strategy-secure-cyberspace

[53] Interim National Infrastructure Protection Plan https://www.hsdl.org/?abstract&did=451406

[54] Sector Specific Plans

[55] A 2006-ban elsőként kiadott NIPP védelmi terv mellékletét képező ágazati tervek (Ez akkoriban 17 ágazatot jelentett, de a DHS csak hetet minősített nyilvánosan elérhetőnek, a többit csak hivatali felhasználók számára.) vizsgálata után az Egyesült Államok Számvevőszéke (Government Accountability Office, GAO) tapasztalatai azt mutatták, hogy az ágazati tervek kidolgozottsága (SSPs), bár az elvárásokat és követelményeket teljesítik, nem mutat egyenszilárdságot. Így pedig azt sem lehetett megállapítani, hogy az egyes szektorok milyen messze jutottak saját területük kritikus infrastruktúráinak azonosításában, fontossági sorrendjük felállításában, illetve a kulcsfontosságú létesítményeik védelmében. Ezért a terv és mellékleteik éves, illetve rendszeres felülvizsgálata vált indokolttá (Ezt az éves felülvizsgálatot egyébként a HSPD-7 is megkövetelte). Moteff, p. 23



1.sz. ábra: NIPP Kockázatkezelési Keretrendszer (forrás: FEMA, 2004)[56]

BELBIZTONSÁGI MINISZTÉRIUM

Az eddigiek alapján azt láthattuk, hogy a kritikus infrastruktúra védelem szálai a Bush adminisztráció idején a 2002-ben a Belbiztonsági törvény által alapított Belbiztonsági Minisztériumhoz vezetnek. A minisztérium egyik alapvető feladata, hogy azonosítsa a kritikus infrastruktúra kritériumainak megfelelő objektumokat, támogassa azok védelmének megvalósulást és előmozdítsa az érintett szereplők közötti kommunikációt. Az előzőekben említetteken kívül ezen folyamat megvalósulását további különböző alárendelt szervezetek és az általuk támogatott programok segítik még, mint, például, a Nemzeti Infrastruktúra Szimuláció és Elemző Központ (NISAC[57]) és az Kiber és Infrastruktúra Elemző Hivatal

[56] A NIPP Kockázatkezelési Keretrendszere a kockázatértékelés és kezelés érdekében folyamatszerűen egyesíti a fenyegetés, a sérülékenység és a "következmény információ" kapcsolatát a fizikai, kiber és humán dimenziókban. A folyamatos visszacsatolás (pirossal) a kritikus infrastruktúra védelmének állandó fokozását teszi lehetővé. Magyarázat: lilával a kockázatok azonosítása és értékelése folyamat részei (célok és célkitűzések felállítása; létesítmények, rendszerek és hálózatok azonosítása; kockázatértékelés: következmények, gyenge pontok és fenyegetések/veszélyek), zölddel a védelem kialakításához szükséges képességek megállapítása, kialakítása, fenntartása és validálása (fontossági sorrend megállapítása, programok kivitelezése, hatékonyság mérése) tartozik.

[57] National Infrastructure Simulation and Analysis Center http://www.sandia.gov/nisac/

(OCIA[58]) által támogatott Nemzeti Kritikus Infrastruktúra Prioritási Program (NCIPP[59]) vagy az Országhatáron túli Kritikus Függőségek Kezdeményezés (CFDI[60]).

A Belbiztonsági Minisztérium tevékenysége azonban nemcsak nemzeti, hanem regionális szinten is számottevő. Például a minisztérium Regionális Ellenállóképesség Értékelő Program (RRAP[61]) programja egy adott földrajzi területen belüli kritikus infrastruktúra és a kulcsfontosságú létesítmények csoportos sérülékenységi és tűrőképességi vizsgálatára irányul. A programban való részvétel és a vizsgálati eredmények feldolgozása utáni kockázatcsökkentési ajánlások adaptálása a résztvevők részéről ugyan önkéntes, de a minisztérium figyelemmel kiséri az adaptált ajánlások gyakorlati alkalmazhatóságát és a hatékonyságot. (Moteff, pp. 26-27)

KRITIKUS INFRASTRUKTÚRA VÉDELEM SZABÁLYOZÁSA ÉS MEGVALÓSULÁSA AZ EURÓPAI UNIÓBAN, ÖSSZEHASONLÍTÁSBAN AZ EGYESÜLT ÁLLAMOKKAL

Azt láthattuk, mi és hogyan (terrortámadás, természeti katasztrófa) alakította Egyesült Államokban a kritikus infrastruktúrák védelmét, de mi a helyzet Európában? Ezen a területen Európában 2004. március 11-ig említésre érdemes esemény nem történt.[62] A madridi terrortámadás következményeként azonban az Európai Unió Tanácsa 2004. július 17-18-i ülésén az Európai Bizottságot az európai társadalom biztonságérzete növelése érdekében a kritikus infrastruktúrák védelmére vonatkozó átfogó stratégia elkészítésére kérte fel. Ugyanis egyértelművé vált, hogy a tagállamok és állampolgáraik biztonságát, jólétét, működését garantáló infrastruktúrák, létfontosságú létesítmények, szolgáltatások döntő jelentőséggel bírnak, így azok védelmére sajátos intézkedések, programok és stratégia szükségesek.

A felkérésnek megfelelően az Európai Bizottság 2004. október 20-án közleményt fogadott el „A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben” címmel, amely a kritikus infrastruktúrákat érintő terrortámadások tekintetében javaslatokat tett az európai megelőzés, felkészültség és reagálás javítására. (EU 2008) Alig egy hónappal később, a Hágai Program[63] második szakaszának elindítása keretében az Európai Tanács megbízást adott az Európai Bizottságnak, hogy segítse a tagállamokat létfontosságú inf-

[58] Office of Cyber and Infrastructure Analysis https://www.dhs.gov/office-cyber-infrastructure-analysis
[59] National Critical Infrastructure Prioritization Program
[60] Critical Foreign Dependencies Initiative
[61] Regional Resiliency Assessment Program https://www.dhs.gov/regional-resiliency-assessment-program
[62] 2004. március 11-én Madridban négy vonatszerelvényen végrehajtott összesen 10 robbantás 191 halálos áldozatot és mintegy 1800 sérültet követelt. Európa történetében ez a legnagyobb terrortámadás, amelynek következményeként néhány nappal később a kormányzó párt elvesztette a választásokat és a spanyol csapatok kivonultak az iraki műveletekből. (Euronews, 2017)
[63] A Hágai Programot az Európai Bizottság 2004. november 4-5.-i ülésén fogadták el. A program tíz prioritást határozott meg, többek között a terrorizmus elleni küzdelem részeként a kritikus infrastruktúrák védelmét.

rastruktúráik védelmével kapcsolatos erőfeszítésekben, a tagállamokat pedig, hogy a védelem 2006. I. félév végéig megvalósuljon. (Council of the European Union, 2004 pp. 6)

A folyamat innentől kezdve felgyorsult. 2005. november 17-én az Európai Bizottság elfogadta a kritikus infrastruktúrák védelmére vonatkozó európai program Zöld Könyvét,[64] majd egy hónappal később, decemberben a Bel- és Igazságügyi Tanács felkérte az Európai Bizottságot egy, a kritikus infrastruktúrák védelmére vonatkozó európai programról (EPCIP) szóló javaslat előterjesztésére. Az Európai Tanács 2007. április 19-20-i ülésén következtetéseket fogadott el az EPCIP-ről, amelyben a tagállamok felelőssége az országhatárokon belül található kritikus infrastruktúrák védelmének megszervezése terén külön hangsúlyt kapott. (Council of the European Union, 2007) Ezen az ülésen az Európai Bizottság bemutatta az európai kritikus infrastruktúrák (ECI)[65] azonosítására és kijelölésére, valamint védelmük javítása szükségességének értékelésére vonatkozó európai eljárás kialakítására vonatkozó javaslatát. (Council of the European Union, 2006)

Az EPCIP az Európai Bizottság által 2006. december 12-én meghirdetett program általános célkitűzése, hogy javítsa a létfontosságú infrastruktúrák védelmét az Európai Unióban és két részből áll: jogi keret és cselekvési terv. A jogi keret alatt kell érteni, többek között, az EPCIP végrehajtását megkönnyítő szakértői csoportok létrehozásáról, cselekvési terv kidolgozásáról, információcseréről és pénzügyi támogatásról szóló intézkedéseket, az azonosítási és kijelölési eljárások összességét és magát a 2008/114/EK Irányelvet is. A cselekvési terv pedig három fő folyamatból áll: (1) horizontális intézkedések kidolgozása, (2) az európai létfontosságú infrastruktúrák sebezhetőségének csökkentése, (3) nemzeti keret, amely a tagállamokat segíti a saját, nemzeti kritikus infrastruktúrák védelmében. Az eddigiekhez képest a fentiekből némileg újólag hathat az ún. szakértői csoport. Itt egyszerűen csak arról van szó, amennyiben különleges szakértelemre van szükség, az Európai Bizottság felállíthat uniós szintű szakértői csoportokat kérdések, problémák megvizsgálására. Az adott létfontosságú infrastruktúra ágazatától függően a szakértők segítséget nyújthatnak sebezhető pontok, kölcsönös függőségek és bevált ágazati gyakorlatok azonosításához, védelmet növelő intézkedések és teljesítménymutatók kidolgozásához, illetve esettanulmányok készítéséhez. (EU, 2006)

Az EPCIP kapcsán fontos megjegyezni, hogy megvalósításának egyik eszköze az ún. Európai Referencia Hálózat a Kritikus Infrastruktúrák Védelmére (European Reference Network for Critical Infrastructure Protection, ERNCIP) vonatkozó többéves projekt. A project célja, hogy kísérleti létesítmények, laboratóriumok rendszerén keresztül keretet bizto-

[64] Green Paper on a European programme for critical infstructure protection A Zöld Könyvben foglaltak szerint a kritikus infrastruktúra védelem három pilléren alapszik: megelőzés, felkészülés, ellenálló képesség. A dokumentum az irányelvek kidolgozásához három védelmi stratégiát kínált: (1) mindenfajta veszéllyel szembeni, (2) mindenveszéllyel szembeni, különös tekintettel a terrorizmusra és (3) a terrorveszélyekkel szembeni védelem. Már a Zöld Könyvben megjelenik az a későbbi öt alapelv (szubszidiaritás, kiegészítő jelleg, együttműködés, titkosság, arányosság), amelyet a 2008/114/EK Irányelv is megerősített. (Európai Bizottság, 2005, p. 4)

[65] European Critical Infrastructure

sítson egyezményes európai teszt eljárások elfogadásához és biztonsági megoldások kidolgozásához. A projektet az Állampolgárok Védelmét és Biztonságát szolgáló Intézeten (Institute for the *Protection* and *Security* of the Citizen, IPSC) keresztül az Európai Bizottság Belügyi Főigazgatósága (Directorate-General Migration and Home Affairs, DG Home) finanszírozza. (EU Commission, 2009) Itt érdemes megjegyezni, hogy ezen programok és projektek mellett az Európai Unió rendelkezik még egy olyan további szervezettel is, amelynek rendeltetése középpontjában a kommunikációs hálózatok és információs rendszerek védelme áll. A 2014-ben létrehozott Európai Hálózat- és Információbiztonsági Ügynökség (European Network and Information Security Agency, ENISA) feladata, hogy az Európai Bizottság és a tagállamok részére tanácsot adjon hálózataik és információs rendszereik biztonsága érdekében, hogy fokozottabb mértékben legyenek képesek a hálózat- és információbiztonsággal kapcsolatos problémák megelőzésére, kezelésére és az azokra történő reagálásra. (EU, 2004) Funkciójában az ENISA részben és áttételesen hasonlít a már korábban ismertetett amerikai Elnöki Kritikus Infrastruktúra Védelmi Testülethez (PCIPB), amelynek szintén a feladatai közé tartozott a kritikus infrastruktúrák információs rendszereit védő különböző szövetségi programok koordinációja.[66] E tekintetben szorosan az ENISA működéséhez kapcsolódnak még az európai információ-megosztási és figyelmeztető rendszer (European Information Sharing and Alerting *System,* EISAS) részét képező uniós számítógépes vészhelyzeti reagáló csoportok (Computer Emergency Response Teams, CERTs) is. Ilyen csoport kormányzati szinten ma már valamennyi tagállamban működik, sőt, néhol ágazati szinten is. A CERT csoportokat olyan számítástechnikai szakemberek alkotják, akik az információ biztonsági eseményekre és fenyegetésekre folyamatos munkarendben képesek hatékonyan reagálni. A 2010. május 19-én útjára indított Európai Digitális Menetrend 2010-2020[67] alapján az Európai Bizottság az EU intézmények vonatkozásában is elkötelezte magát egy ilyen vészhelyzet reagálási csoport létrehozására. Egy évnyi sikeres kísérleti működés és tapasztalatok után döntöttek úgy az EU intézmények, hogy ezt a számítógépes vészhelyzeti reagáló csoportot 2012. szeptember 11-én véglegesítik. Az így megalakult CERT-EU szorosan együttműködik a tagállamok azonos csoportjaival és az információs technológiai biztonságra szakosodott intézményekkel, vállalkozásokkal. (CERT-EU, 2016) Emellett az Európai Parlament és Tanács 2016/1148 irányelve[68] alapján a határokon átnyúló együttműködés elősegítése érdekében minden EU tagállam köteles a hálózati és információs rendszerek biztonságának vonatkozásában nemzeti kapcsolattartó pontot kijelölni. (EU, 2016) CERT-EU „hasonmás" azonban az Egyesült Államokban is létezik United States Computer Emergency Readiness Team, US-CERT), illetve az európai információ-megosztási és figyelmeztető rendszer (EISAS) analó-

[66] Csakhogy, amíg a PCIPB 2001-ben alakult és más feladatokkal is bírt, addig az ENISA 2004. március 14-én jött létre.
[67] Europe's Digital Agenda 2010-2020
[68] Szokás az irányelvet az angol megnevezésben előforduló „network and Information systems" (hálózati és információs rendszerek) kifejezés kezdőbetűiből alkotott mozaikszóval NIS irányelvként is emlegetni.

giájaként az EO 13691 elnöki rendelettel létrehozott Információ-megosztási és Elemző Szervezetek (Information Sharing and Analysis Organizations, ISAOs) rendszere[69] fogható fel.

Az európai kritikus infrastruktúra szabályozása történetében 2008. december 8. az a dátum, amikor az Európai Unió Tanácsa az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK Irányelvét lefekteti. Ez az Irányelv jelenti az első lépést az európai kritikus infrastruktúrák azonosítása és kijelölése, valamint védelmük javítása szükségességének terén. (EU 2008) Az Irányelv kijelöli mindazon kereteket, amelyek Unió és tagállami szinten a megfelelő kritikus infrastruktúra védelem megvalósításához szükségesek. Az európai kritikus infrastruktúrák védelmében ilyen keret, hogy a hatékony kommunikáció, koordináció és együttműködés érdekében valamennyi tagállam kapcsolattartó pontot (ECIP[70]) köteles kinevezni, amely az európai kritikus infrastruktúrák védelmével kapcsolatos kérdéseket nemzeti szinten, valamint a többi tagállammal és az Európai Bizottsággal is koordinálja. (EU 2008) Részösszegzésként elmondható tehát, hogy az Európai Unióban is egyfajta összekötő-kapcsolattartói rendszer jött létre. Azonban amíg az Egyesült Államokban ez ágazatonként valósult meg kijelölt felelős hivatallal párba rendezve, addig az Unióban ez tagállami, azaz összágazati képviseletet jelent.

Az uniós irányelv is, hasonlóan az amerikai szabályozáshoz, a kritikus infrastruktúra védelméhez, pontosabban magához az infrastruktúrához, üzemeltetői biztonsági terveket (OSPs[71]) és biztonsági összekötő tisztviselőket rendel. Némi különbség tehát itt is tapasztalható, hiszen az Egyesült Államokban ez a biztonsági összekötő tisztviselő egyrészt ágazati és nem infrastruktúra szinten, másrészt nem egyszemélyi, hanem tanácsi[72] szinten jelenik meg.

A kritikus infrastruktúra védelem újabb állomását jelentette az Európai Tanács 2010. március 25-26-i ülésén elfogadott EU Belbiztonsági Stratégia.[73] A stratégia tovább erősítette a kritikus infrastruktúrák védelmének szükségességét és napirenden tartását, különös tekintettel a modern technológiák által biztosított lehetőségeket is kiaknázó szervezett bűnözésre. Ugyanakkor, ha az Egyesült Államok irányába tekintünk, azt kell megállapítani, hogy ott ugyanez a szabályozás[74] már 2002-ben megjelent, sőt, 2007-ben már egyszeri felülvizsgálaton is átesett.

[69] A korábban ismertetett civil működtetésű, ágazat specifikus Információmegosztó és Elemző Központokkal (ISACs) ellentétben az ISAOs kormányzati működtetésűek és nem ágazat specifikusak, ezért módszereikben ez utóbbiak rugalmasabbak és általános hatóerejűek.
[70] European Critical Infrastructure Protection Contact Point. Magyarország képviseletét a CIP POC (Critical Infrastructure Protection Point of Contact) üléseken a BM Országos Katasztrófavédelmi Főigazgatóság látja el.
[71] Operator Security Plans
[72] Kormányzati/Ágazati Koordináló Tanácsok (Government/Sector Coordinating Councils, G/SCCs)
[73] Internal Security Strategy for the European Union: Towards a European security model https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf
[74] National Strategy for Homeland Security

Továbbhaladva az Európai Unió kritikus infrastruktúra védelmében, hamar nyilvánvalóvá vált, hogy egy EPCIP jellegű program során nélkülözhetetlen egy biztonságos információcsere lehetővé tevő értesítési hálózat az érintett résztvevők között. A létfontosságú infrastruktúrák figyelmeztető információs hálózata (Critical Infrastructure Warning Information Network, CIWIN) az EPCIP sikeres végrehajtása érdekében a bevált gyakorlatok cseréjének céljából jött létre, valamint, hogy fakultatív jelleggel platformot nyújtson az Európai Bizottság ARGUS[75] rendszerével kapcsolatos sürgősségi riasztások továbbításához. (EU Council, 2008) Az internet alapú CIWIN portál a prototípus tesztelése után 2013 január közepe óta működik.

ÖSSZEGZÉS ÉS KÖVETKEZTETÉSEK

A kritikus infrastruktúra védelem elsősorban (de nem kizárólag) a terrorizmus elleni harccal kapcsolatos ellenintézkedések és akció tervek részeként indult el. Összehasonlítva az Európai Unió és az Egyesült Államok jogszabályi hátterét, rögtön megállapítható, hogy mindkét esetben egy központi szabályzó irányelvet találunk. Nem járunk messze az igazságtól akkor sem, ha az konstatáljuk, hogy az Egyesült Államok esetében az elnöki direktíva gyakorlatilag ciklusonként változik. Azonban ennél sokkal helyénvalóbb megállapítás, hogy ez a változás az Európai Unióhoz képest inkább a tendenciákhoz és az aktualitásokhoz való rugalmasságot fejez ki. Például, amíg a Clinton adminisztrációnak nem kellett fizikai fenyegetettséggel számolni, ezért nyugodtan koncentrálhatott a kibertérből érkező fenyegetésekre, addig a Bush kormányzatnak azzal kellett szembesülni, hogy a kritikus infrastruktúra más dimenzióit sem szabad elhanyagolni, tehát egyfajta súlypont helyreállítást kell végrehajtani. Azonban az egyensúly megteremtése után, Obama elnök irányítása alatt a kibervédelem ismét teret nyert a fizikai védelemmel szemben.

Amíg az Egyesült Államokban minden elnök az elmúlt évtizedekben megalkotta a maga irántyűként ható direktíváját, addig az Európai Unió 2008-ban fektette le a napjainkig változatlan 2008/114/EK Irányelvét. Az irányelvek közös vonásaként azonban elmondható, hogy megalkotásuk óta gyakorlatilag nincsenek bennük nagyobb mélyreható változások, ami azt mutatja, hogy a kialakított elvek és szervezetek rendszere megfelel a jelenlegi kihívások támasztotta elvárásoknak. Az irányelvek mellett azonban fontos az is, hogy mindkét esetben a kritikus infrastruktúra védelem szempontjából meghatározó stratégiák vannak jelen és kísérik az alap- és irányelvek megvalósulását.

Azt is láthattuk, hogy a kritikus infrastruktúrák védelmében, tekintettel, hogy azok tulajdonosai, üzemeltetői javarészt a civil szférához tartoznak, viszont a humán biztonság letéteményese pedig az állam, mennyire kiemelt szerep jut egy központi szereplőnek és a megfelelő információáramlásnak. A központi szereplő és szabályozás már csak azért is

[75] Az ARGUS egy általános rendeltetésű Európai gyorsreagálású riasztó rendszer, amelyet az Európai Bizottság a különböző jellegű vészhelyzetek esetére hozott létre, hogy az egyes uniós vészhelyzet- és válságkezelő központokat összekösse.
https://ec.europa.eu/health/preparedness_response/generic_preparedness/planning/argus_en

fontos tényező mindkét esetben, mert ennek hiányában az egyes szövetségi/uniós tagállamok és meghatározó civil üzemeltetők erőfeszítései céljuk elérése nélkül veszhetnének el a kihívások labirintusában. A kritikus infrastruktúra védelem végpontja az Egyesült Államokban minisztériumi szint (Belbiztonsági Minisztérium), míg az Európai Unióban a tagállamok után az Európai Bizottsághoz kötődik.

A két entitás kritikus infrastruktúra védelmében nemcsak szabályozási, de megvalósulás vonatkozásában is a fentiekben számos analógiát láthattunk, amelyből legalább két fő momentum vonható le. Az egyik, hogy már a kezdetektől Európa „fáziskésésben" van az Egyesült Államokhoz képest. A másik, hogy a kihívások globalizációja nem meglepő módon azonos válaszlépéseket váltottak ki mindkét szereplőből. Ezáltal az is nyilvánvaló, bár a tanulmány erre nem tért ki, hogy a két fél közötti együttműködés (például információcsere, szabványosítás) természetszerű és költséghatékony.

Az Európai Unió esetében a kihívások globális jellege mellett azonban arról sem szabad megfeledkezni, hogy a kritikus infrastruktúrák védelmével szembeni felelősség továbbra is nemzeti hatáskörben maradt.

FELHASZNÁLT IRODALOM

1. 109th US Congress (2005-2006): S.3721 - Post-Katrina Emergency Management Reform Act of 2006. Elérhető: https://www.congress.gov/bill/109th-congress/senate-bill/3721, letöltve: 2017.05.24.
2. Bonnyai, Tünde (2014): A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében. katonai műszaki. Nemzeti Közszolgálati Egyetem, Budapest. Katonai Műszaki Doktori Iskola. Elérhető: http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2014/bonnyai_tunde.pdf, letöltve: 2017.05.10.
3. Buzan, Barry (1991): New Patterns of Global Security in Twenty-First Century. International Affairs (Royal Institute of International Affairs 1944-) (No.3). Elérhető: http://home.sogang.ac.kr/sites/jaechun/courses/Lists/b7/Attachments/10/New%20Patterns%20of%20Global%20Security%20in%20the%20TwentyFirst%20Century_Buzan.pdf, letöltve: 2017.05.24.
4. CERT-EU (2016): About Us CERT-EU. CERT-EU. Elérhető: https://cert.europa.eu/cert/plainedition/en/cert_about.html, letöltve: 2017.05.25.
5. Council of the European Union (2004): Adoption of Council conclusions on prevention, preparedness and response to terrorist attacks. Council of the European Union. Elérhető: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015232%202004%20INIT, letöltve: 2017.05.25.
6. Council of the European Union (2006): Comission Staff Working Document. Accompanying document to the Proposal for a COUNCIL DIRECTIVE on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. Summary of the Impact Assessment (16933/06). Elérhető:

https://www.eerstekamer.nl/eu/documenteu/sec_2006_1648_working_document/f=/vjm2lbtwymsq.pdf, letöltve: 2017.05.25.

7. Council of the European Union (2007): Adoption of the Council Conclusions on a European Programme for Critical Infrastructure Protection. 7743/07. European Union. Elérhető: http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%207743%202007%20INIT, letöltve: 2017.05.25.
8. DHS, Department of Homeland Security (2016): The Nationa Strategy For Homeland Security, October 2007. Department of Homeland Security. Elérhető: https://www.dhs.gov/national-strategy-homeland-security-october-2007, letöltve: 2017.05.24.
9. DHS, Department of Homeland Security (2017a): Critical Infrastructure Partnership Advisory Council. Department of Homeland Security. Elérhető: https://www.dhs.gov/critical-infrastructure-partnership-advisory-council, letöltve: 2017.05.24.
10. DHS, Department of Homeland Security (2017b): National Infrastructure Advisory Council. Elérhető: https://www.dhs.gov/national-infrastructure-advisory-council, letöltve: 2017.05.24.
11. DHS, Department of Homeland Security (2017c): Office of Emeregency Communications. Department of Homeland Security. Elérhető: https://www.dhs.gov/office-emergency-communications, letöltve: 2017.05.24.
12. Ellis, James; Fisher, David et al. (1997): Report to the President's Comission on Critical Infrastructure Protection. Special Report. CMU/SEI-97-SR-003. Carnegie Mellon University. Pittsburgh. Elérhető: http://resources.sei.cmu.edu/asset_files/SpecialReport/1997_003_001_16538.pdf, letöltve: 2017.05.17.
13. EU (2004): Európai Hálózat- és Információbiztonsági Ügynökség (ENISA). 460/2004/EK. European Union. Elérhető: http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l24153&from=GA, letöltve: 2017.05.25.
14. EU (2006): Létfontosságú infrastruktúrák védelmére vonatkozó európai program. EU Commission. Elérhető: http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=URISERV%3Al33260, letöltve: 2017.05.23.
15. EU (2008): A Tanács 2008/114/EK Irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. Elérhető: http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32008L0114, letöltve: 2017.05.17.
16. EU (2016): Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. European Union. Elérhető: http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=EN, letöltve: 2017.05.25.
17. EU Commission (2006): Communication from the Comission on a European Programme for Critical Infrastructure Protection. COM(2006) 786 final. Elérhető: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF, letöltve: 2017.05.23.
18. EU Commission (2009): European Reference Network for Critical Infrastructure Protection (ERNCIP). EU Commission. Elérhető: https://ec.europa.eu/jrc/en/network-bureau/european-reference-network-critical-infrastructure-protection-erncip, letöltve: 2017.05.25.

19. EU Commission (2013): Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. SWD(2013) 318 final. EU Commission. Elérhető: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf, letöltve: 2017.05.23.
20. EU Council (2008): A Tanács határozata a létfontosságú infrastruktúrák figyelmeztető információs hálózatáról (CIWIN). COM(2008) 676. EU Commission. Elérhető: http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52008PC0676&from=EN, letöltve: 2017.05.25.
21. Euronews (2017): 13 éve történt a madridi terrortámadás. Spanyolország. Elérhető: http://hu.euronews.com/2017/03/11/13-eve-tortent-a-madridi-terrortamadas, letöltve: 2017.05.25.
22. Európai Bizottság (2005): Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó Európai Programról. COM(2005) 576 végleges. Európai Unió. Elérhető: http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52005DC0576&from=GA, letöltve: 2017.05.25.
23. FEMA (2004): Lesson Summary. Lesson 4: Managing Risk. Incorporating the National Preparadness System. Federal Emergency Management Agency. Elérhető: https://emilms.fema.gov/is921/CIPP0104summary.htm, letöltve: 2017.05.25.
24. John F. Kennedy (1963): National Security Action Memorandum 252. Elérhető: https://www.jfklibrary.org/Asset-Viewer/mOsd6HP9gkG_mqGvJhY1qA.aspx, letöltve: 2017.05.24.
25. Károlyi, László (2007): A kritikus infrastruktúrák védelme és az operatív erők tevékenységirányítása a honi katasztrófavédelemben, különös tekintettel az EU konformitásra. katonai műszaki. Bolyai János Katonai Műszaki Kar, Zrínyi Miklós Nemzetvédelmi Egyetem. Katonai Műszaki Doktori Iskola. Elérhető: http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2007/karolyi_laszlo.pdf, letöltve: 2017.05.24.
26. Korm.hat. (2012): A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról. Elérhető: http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf, letöltve: 2017.05.24.
27. Moteff, John D.: Critical Infrastructures: Background, Policy, and Implementation. Elérhető: https://fas.org/sgp/crs/homesec/RL30153.pdf.
28. NCI (2016): National Council of ISACs. National Council of ISACs. Elérhető: https://www.nationalisacs.org/, letöltve: 2017.05.24.
29. OGY (2012): 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Elérhető: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv, letöltve: 2017.05.15.
30. Poustourli, Aikaterini; Ward, David et al. (2015): An Overview of European Union and United States Critical Infrastucture Protection Policies. Koaceli University. 12th International Conference on „Standardization, Prototypes and Quality: A Means of Balkan Countries' Collaboration". Elérhető: https://www.researchgate.net/publication/304777687_AN_OVERVIEW_OF_EUROPEAN_UNION_AND_UNITED_STATES_CRITICAL_INFRASTRUCTURE_PROTECTION_POLICIES, letöltve: 2017.04.27.

31. US Congress (2001): Uniting and Strenghtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. Elérhető: https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf, letöltve: 2017.05.17.