Kritikus infrastruktúrák védelme I.

Szerkesztette:
BOGNÁR BALÁZS
BONNYAI TÜNDE

Dialóg Campus

KRITIKUS INFRASTRUKTÚRÁK VÉDELME I.

Vákát oldal

KRITIKUS INFRASTRUKTÚRÁK VÉDELME I.

Szerkesztette:
Bognár Balázs és Bonnyai Tünde

Dialóg Campus Kiadó ❖ Budapest
2019

Szerzők

Bognár Balázs
Bonnyai Tünde
Vámosi Zoltán

Lektorálták

Bleszity János
Vass Gyula

Tartalom

Vákát oldal

Előszó

A 20. század első éveinek biztonságpolitikai kihívásai és a korábbi tapasztalatok alapján 2008 decemberében az Európai Unió tagállamai az Európai Tanács 2008/114/EK irányelvében határozták meg a mindennapi élet gördülékenységét, az államapparátus működőképességét, valamint a gazdasági mechanizmusok folyamatosságát biztosító kritikus infrastruktúrák védelmének alapvető célkitűzéseit. Jelentős mérföldkőnek tekinthetjük ezt a jogi aktust a tagállamok védelmi mechanizmusainak fejlesztésében, hatékonyabbá tételében, amelynek legjobb gyakorlatai napjainkban materializálódnak. A jogharmonizációs kötelezettség alapján Magyarország is jelentős erőfeszítéseket tett – és tesz manapság is – a kritikus infrastruktúrák biztonságának garantálása, fokozása érdekében, amiben a katasztrófavédelem szervezetrendszerének markáns szerepe van.

A 2012. január 1-jével hatályba lépett katasztrófavédelmi törvény és annak végrehajtási rendeletében meghatározott feladatok szakszerű ellátása érdekében a hivatásos katasztrófavédelmi szerv központi szerve egy három pillérre épülő szervezeti struktúrával kezdte meg működését. Az újonnan létrejött integrált katasztrófavédelmi szervezetben az egyes szakterületeket érintő iparbiztonsági, polgári védelmi, illetve tűzvédelmi hatósági és szakhatósági eljárásokat a hivatásos katasztrófavédelmi szerv központi, területi és helyi szervei folytatják le. 2014 szeptemberében ez a tevékenység – hatósági szempontból – kiegészült a vízügyi és vízvédelmi hatáskörök gyakorlásával, míg a 2018-as év újabb, ezúttal az információbiztonság tekintetében rendkívül meghatározó feladat- és hatáskörrel szélesíti a szervezet eddigi spektrumát.

Az elmúlt években végrehajtott szervezeti átalakulás eredményeként a hivatásos katasztrófavédelmi szerv a globális világ valós kihívásaira válaszolni kész, a társadalmi szükségleteket szem előtt tartó, egységes vezetésű rendvédelmi szervezetté vált.

A létfontosságú rendszerek és létesítmények védelmével kapcsolatos feladatok tudatos és következetes végrehajtását, a potenciális kritikus infrastruktúra elemek beazonosítását, a kijelölt elemek hatósági felügyelet alatt tartását, illetve a kiberbiztonság kérdéskörének térnyeréséből adódóan az információbiztonsági hatósági feladatok magas szintű ellátását a katasztrófavédelem prioritásként kezeli.

A katasztrófavédelem egységesített rendszerében a kritikus infrastruktúrák védelmének szakterülete kiemelt helyet foglal el, egyik fő feladata – a szakterület megalakulásakor – a jogalkotási és szabályozási feladatok végrehajtása volt, amelynek eredménye a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény, valamint a hozzá kapcsolódó általános végrehajtási kormányrendelet. Ezen jogszabályok célja egyrészt a létfontosságú rendszerelemek azonosítása, másrészt a kijelölés megtörténte után a megfelelő szintű – humán, fizikai és informatikai – védelem biztosítása. A kritikus infrastruktúrákkal kapcsolatos jogszabályok elfogadása – illetve azok szükségszerű módosításai – megfelelő alapot biztosít ahhoz, hogy Magyarország érdemben legyen képes a létfontosságú rendszerek és létesítmények védelmét garantálni.

A katasztrófavédelem szervei szakhatóságként, központi szerve nyilvántartó hatóságként és általános javaslattevő hatóságként elsősorban monitoring, ellenőrzési, koordinatív, nemzeti kapcsolattartó és hálózatbiztonsági elemző-értékelő feladatokat látnak el.

A létfontosságú rendszerek és rendszerelemek azonosítása, kijelölése és hatósági ellenőrzése a hálózatbiztonsági tevékenységgel kiegészülve olyan európai szintű biztonsági rendszer kialakításához teremt alapot, amely jelentősen elősegíti hazánk közbiztonsági, információbiztonsági, energiabiztonsági, illetve környezetbiztonsági szempontú fejlődését. A potenciális létfontosságú rendszerelemek kijelölésével és felügyelet alatt tartásával csökkenthetők a lakosságot veszélyeztető kockázatok, hatékonyabbá tehetők a társhatóságokkal és az üzemeltetőkkel kialakított együttműködési platformok, valamint a tudatos felkészülés következtében eredményesebbé válhat a rendkívüli események és veszélyhelyzetek kezelése egyaránt.

Az Európai Parlament és Tanács 2016/1148. irányelve (NIS-irányelv) újabb feladatokkal ruházta fel a tagállamokat, amelyek végrehajtása – illetve a hatékony és eredményes végrehajtás körülményeinek megteremtése – jelenleg is zajlik Magyarországon. Ezen rendelkezések kifejezetten a kibertérből érkező fenyegetésekkel szembeni védelem kialakítását és folyamatos fejlesztését határozták meg célkitűzésként, amelyek jelentős mértékben hatással lesznek a kritikus infrastruktúraként már kijelölt, illetve a jövőben kijelölhető rendszerekre. A legfőbb cél továbbra is az üzletmenet-folytonosság biztosítása, a rendkívüli események bekövetkezési valószínűségének lehető legalacsonyabbra csökkentése és a potenciális károk minimalizálása.

A kritikus infrastruktúrák védelme szakterületen az elmúlt években megalkotott jogszabályok hozzájárulnak a lakosságvédelem, a lakosság ellátásának folyamatos biztosításához, a közbiztonság erősítéséhez. A hatályos jogi környezet megköveteli, hogy a hivatásos katasztrófavédelmi szerv szorosabb együttműködést alakítson ki és tartson fenn a létfontosságú infrastruktúrák védelme szakterületen tevékenykedő társhatóságokkal, a kijelölt létfontosságú rendszerelemek üzemeltetőivel, a hálózatbiztonsági feladatokat ellátó eseménykezelő központokkal, illetve az Európai Unió, a NATO és harmadik országok szintjén is.

A *Kritikus infrastruktúrák védelme I.* kézikönyv célja, hogy általános áttekintést adjon a kritikus infrastruktúrák védelme mint tevékenység evolúciójáról nemzetközi és hazai szempontból, összefoglalja a Magyarországon megalkotott jogi környezetet, bemutassa a hatályos jogszabályok által nevesített ágazatokat és azok sajátosságait, illetve betekintést adjon az információ- és hálózatbiztonság égisze alatt végzett tevékenységekbe.

Budapest, 2019. január 1.

Szerkesztők

Bevezető
Biztonságpolitikai aspektusok

Vámosi Zoltán

Magyarország biztonsági környezete szoros összefüggésben van az európai és a legtágabb értelemben vett globális biztonság sajátosságaival, változásának trendjeivel. Napjainkban a világ fejlődését alapvetően meghatározó globális tényezők között meghatározó szerepe van a kiszámítható nemzetközi biztonság érvényesülésének, a globalizáció és az információs kor egyre átfogóbb valóságának, az emberi jogok és méltóság igazságosabb megvalósulásának. Ebből fakadóan az emberiségnek három, egymással összefüggő globális kihívással kell szembenéznie a 21. század elején, amelyek meghatározzák biztonságát: először az egyre szervezettebb és veszélyesebb nemzetközi terrorizmus és a tömegpusztító fegyverek, eszközök ellenőrizhetetlen terjedése (proliferáció), másodszor a gazdasági-politikai egyensúlytalanság által determinált szegénység, harmadszor a környezeti fenntarthatóság egyre súlyosabb, lassan visszafordíthatatlan problémája.

A biztonsági környezet jellemzői és változásai

Napjainkban egy átmeneti korszak megélői vagyunk, amelyben – a fenti kihívások mellett – számos kérdés vár megoldásra helyi (országos), regionális (kontinentális) és globális (világ) szinten egyaránt. Ezek közül a fontosabbak: a gazdasági és tudományos-műszaki eredmények értelmes felhasználása, a népesedés és migráció, az energiaellátás és -felhasználás, a technológiai váltás, a más népek értékeinek, hagyományainak és kultúrájának megismerése és tisztelete, a globális problémák és a nemzetközi együttműködés egész sora, valamint az ezekkel járó értékrendváltás. Ugyanakkor ebben az átmeneti időszakban gazdasági-hatalmi, és az ezzel járó biztonságpolitikai átrendeződés megy végbe, amely egyfelől az Amerikai Egyesült Államok világhatalmi szerepének csökkenését, másfelől a feltörekvő országok, mindenekelőtt Kína és India gazdasági és hatalmi befolyásának vagy Oroszország katonai-haditechnikai képességeinek erőteljes növekedését jelenti. Nyilvánvaló, hogy ez a folyamat nemzetközi feszültségekhez, valamint elkerülhetetlenül kultúra- és civilizációs váltáshoz vezet. Következésképp egy korszerűbb biztonságfelfogás kialakulását eredményezi. Az egymással szoros összefüggésben érvényesülő folyamatok között meghatározó jelentőségű a gazdaság állapota, amely közvetlenül befolyásolja a komplex biztonság minőségét, a katonai biztonság haditechnikai-infrastrukturális szintjét – országok és szövetségek vonatkozásában egyaránt.

A 20. század második felében kibontakozó hidegháború során az Amerikai Egyesült Államok és a Szovjetunió között egyre magasabb szintet ért el a fegyverkezési verseny, amely a Szovjetunió gazdasági-hadigazdasági versenyképtelenségének felismerését követően a nukleáris fegyverkezés leállításához vezetett (1987). A fegyverkezési verseny

megszűnése következtében a szovjet gazdaság összeomlott (1991). A klasszikus háborús fenyegetettség ezáltal megszűnt, helyét az új világrend kialakulása során fokozatosan új típusú kihívások vették át.

A biztonság *gazdasági meghatározottsága* a 2008-ban kialakult globális pénzügyi és gazdasági válság társadalmi hatásait elemezve is megfigyelhető: egyrészt közvetlenül érződött hatása a biztonság különböző területei, mindenekelőtt a katonai fejlesztések és az infrastrukturális beruházások területén, a NATO-tagállamok védelmi kiadásai radikális csökkentése, másrészt a válság biztonsági-védelmi következményei és kezelésének lehetőségei vonatkozásában (a válság által kevésbé érintett Kína és Oroszország folytatták fegyverkezési programjaikat). Ugyanakkor a válság a gazdaság állapotában *strukturális átrendeződésekhez* vezetett a világ egyes országai és régiói között. Mindez egy új, *multipoláris világrend* kialakulását vetíti előre, amelyben az úgynevezett feltörekvő országok, mint például a BRICS-államok: Brazília, Oroszország, India, Kína és Dél-Afrika, valamint a G-20-ak nemzetközi pozícióinak megerősödése várható. Joggal fogalmazhatta meg a mai világ sajátosságait és a 21. század paradoxonát a Világgazdasági Fórum: „Miközben a világ egybenő, aközben mindinkább szétesik" (*Világgazdasági Fórum Jelentése,* 2011).

A gazdaság biztonsági aspektusainak fontosságát bizonyítja az egyre csökkenő természeti erőforrások és energiatartalékok feletti ellenőrzés megtartása/megszerzése érdekében kibontakozó küzdelem, amelynek gazdasági és katonai vonatkozásai egyaránt megtalálhatók.[1] Újfajta *nagyhatalmi vetélkedés* van kibontakozóban, amely ma még beláthatatlan következményekkel járhat a globális érdekérvényesítés új, többek között katonai eszközökkel támogatott formáira nézve. A világméretű érdekszférák változását bizonyítja az a geostratégia, amely Európa helyett Ázsia felértékelődését jelenti az Amerikai Egyesült Államok és Oroszország számára, Kína szempontjából pedig Afrika jelent prioritást, több mint egy évtizede.

A biztonsági környezet változásai az utóbbi évtizedekben felgyorsultak. Olyan trendek, események figyelhetők meg a nemzetközi viszonyokban, amelyek – éppen a kiteljesedő globalizáció következtében – függetlenek az egyes országok és régiók gazdasági-társadalmi képességeitől, földrajzi elhelyezkedésétől, s amelyek következményeinek kezelése csakis *nemzetközi összefogással* lehet eredményes, ugyanakkor hatást gyakorol minden ország jelenére, de még inkább jövőbeni lehetőségeire, bármilyen nagyságú és fejlettségű országról van is szó. A következőkben e tényezőket vesszük sorra.

A 20. század utolsó évtizedében – a Szovjetunió és az általa vezetett szocialista világrendszer összeomlását követően – a bipoláris (kétpólusú) világrend megszűnése lehetővé tette a *kelet-európai rendszerváltás* viszonylag békés végrehajtását. Az uralkodóvá vált kapitalista társadalom eszményképe azonban egyre több ellentmondással és kétellyel párosul, a kelet-európai rendszerváltó országok negyedszázados történelme csak részben – a NATO-tagság révén elsősorban a katonai biztonság területén – igazolta a várakozásokat.

[1] Közel-keleti konfliktusok és nyersanyaglelőhely-viták, például Norvég-tenger, Brazília partjai, Dél-kínai-tenger stb.

Az Amerikai Egyesült Államok ellen 2001. szeptember 11-én végrehajtott *terrortámadás* a globális nagyhatalom, s ezáltal a globális biztonság sebezhetőségének példája. Azt bizonyítja, hogy újra kell gondolni a biztonság értelmezését, a követendő biztonságpolitika prioritásait, a nemzetközi együttműködés formáit és módszereit. Különösen indokolt ez napjainkban, amikor az – Irak és Szíria területén létrejött – *Iszlám Állam*[2] (ISIS) komoly biztonsági kihívást jelent a térségben, de – többek között az öngyilkos merénylők révén – az egész világon. A dzsihadisták térnyerése és globális fenyegetése elleni fellépés nemzetközi összefogást sürget, amelynek részese kell hogy legyen Oroszország és Kína is.

1. ábra
Terrortámadás az ikertornyok ellen

Forrás: digi24.ro

A 2011 tavaszán kibontakozó úgynevezett arab/észak-afrikai mozgalmak nagyhatalmi és geopolitikai megosztó jellege hozzájárul a nemzetközi érdekszférák és biztonságpolitikai befolyási övezetek átalakításához (például Líbia, ahol 5 év után sincs fegyvernyugvás). Az egyes érdekcsoportok autonóm törekvései állandósítják a katonai konfliktusokat, amelyek – nagyhatalmi kapcsolataik és a felerősödő iszlám törekvések révén – túlnőnek az adott régiók határain.

[2] 2013. április 8-án az Abu Bakr al-Baghdadi által létrehozott, Iraki és Levantei Iszlám Állam elnevezésű terrorszervezet, amely globális szinten folytat az iszlám hit nevében toborzó tevékenységet és hajt végre terrortámadásokat. Az iszlám kalifátus kialakítását célzó szervezet minden muszlim hitű személy feletti vallási fennhatóságot követel, ami a muszlimok által lakott területek politikai irányítását is maga után vonná. (Besenyő et al. 2016)

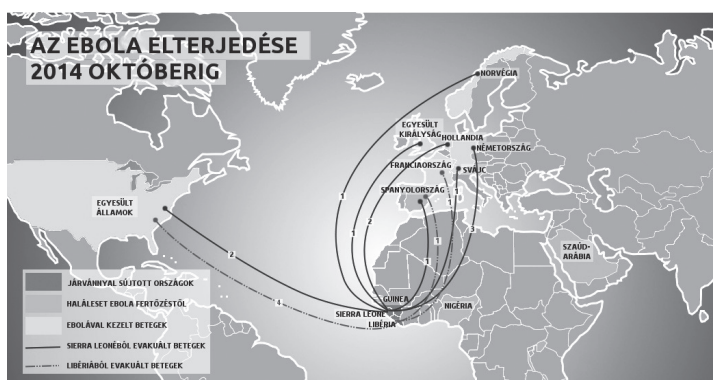
2. ábra

Az arab/észak-afrikai mozgalmak következményei

Forrás: konyvkultura.kello.hu

Az infokommunikációs technológiák (a továbbiakban: IKT) minőségi fejlődése és világméretű térnyerése alapjaiban változtatja meg a biztonságpolitika kihívásait és azok kezelésének lehetőségeit, a felderítő és hírszerzői tevékenység módszereit és formáit. A kiberhadviselés legitimitása, beépülése a hadviselés konvencionális rendszerébe, az űr- és kozmikus hadviselés realitása új dimenziókat nyit a nemzetközi biztonságpolitikában, a diplomáciában, a gazdasági kapcsolatokban és a haditechnikai fejlesztések területén egyaránt.

A biztonsági környezet változásai között új veszélyként jelenik meg az olyan, vírusok által terjesztett betegségek pandémiaszerű terjedése, amelyek a jelenlegi orvostudomány szerint nem kezelhetők. Afrikában 2014-ben nagy áldozatokat követelő járványként söpört végig az Ebola-vírus, amely végül nem terjeszkedett világméretűvé. Mindemellett figyelmet kell szentelni annak, hogy gyorsított ütemben, ellenőrizetlen körülmények között folyik az ilyen és hasonló vírusok biológiai fegyverként történő alkalmazása is.



3. ábra

Az Ebola-vírus terjedése 2014-ben

Forrás: azatlasz.hu

A felsorolt tényezők igazolják, hogy napjaink biztonsági környezete sokszínű és dinamikusan változó, a globalizáció megteremti a lehetőségét annak, hogy a világ bármely térségében, bármely ország biztonságát befolyásolhatják attól függően, hogy az adott ország milyen szinten felkészült a biztonsági környezet jellegének, változásainak és várható következményeinek kezelésére. Érdemes konkrétabban elemezni a biztonság tartalmi változásait és a korszerű biztonságfelfogás sajátosságait, mert a világ még kiszolgáltatottabb lett, s ez már önmagában véve is válság- és konfliktusforrások kialakulásának az előfeltétele lehet. (Vámosi 2018)

A biztonság és a biztonságpolitika tartalmi változásai

Ahhoz, hogy a világ vagy egy adott társadalom működjön, és biztosítottak legyenek az értelmes emberi élet feltételei, mindenekelőtt *biztonságra* van szükség, a legteljesebb értelemben vett kiszámítható és komplex biztonságra. Annak ellenére, hogy napjainkra a biztonság rendkívül tág fogalommá vált a köznyelvben ugyanúgy, mint a szakértők körében, két alapvető fogalmi megközelítést különböztethetünk meg.

A *tradicionális megközelítés* hívei a biztonságot, hasonlóan az elmúlt fél évszázad gondolkodásmódjához, ma is elsősorban a katonai biztonság leszűkített értelemben vett fogalomkörével azonosítják, amely szerint a biztonságpolitika a katonai fenyegetések távoltartását, a védelmi képesség adekvát – a potenciális veszélyforrásokkal megegyező – jellegét hangsúlyozzák. A másik, a *komplex megközelítés,* amely kitágítja a biztonság fogalomkörét mindazokra a veszélyeztető tényezőkre (például: járványok, terrorizmus, klímaváltozás, ipari katasztrófák stb.), amelyek valamilyen formában fenyegetést jelentenek az egyén, a közösség, a társadalom vagy a világ biztonságára nézve. Napjainkban a korszerű értelmezés alapján *a biztonság olyan komplex* társadalmi kategória és állapot, amely

- magában foglalja *a biztonság minden szintjét* – az egyén, a társadalom, a régió és az emberi civilizáció egészének biztonságát, teljes kölcsönhatásukban. Minden biztonság az egyén biztonságával kezdődik, amely az élethez való jog érvényesülésének követelménye. A társadalom biztonságát a nemzetközi biztonság követi, amely regionális (például európai) és globális (az egész világra kiterjedő) biztonságra tagolódik;
- integrálja a biztonság *különböző elemeit és területeit,* úgymint gazdaság és szociális szféra, politikai, katonai, környezet- és katasztrófavédelmi területek, közrend és közbiztonság, informatika stb. Az utóbbi évtizedekben megváltozott világhelyzet, a globális biztonsági környezet – a bipoláris (kétpólusú) világrend megszűnése, a Szovjetunió összeomlása – következtében csökkent a korábban hangsúlyos katonai tényező szerepe, és megnőtt az úgynevezett nem katonai dimenziók jelentősége. Az egyes elemek és területek között szoros kölcsönhatás érvényesül;
- meghatározza és szavatolja a *társadalom működésének és cselekvésének feltételrendszerét:* csak a kiszámítható biztonság megléte esetén képes működni a társadalom, annak intézményei (például: az államigazgatás, a gazdaság, a kultúra, az oktatás) és tagjai. A katonai intézkedéseknek a túlélés megszervezésén túl foglalkoznia kell a társadalmi fejlődés gazdasági-szociális és egyéb kérdéseivel is;

– a komplex, mindent átfogó és integráló biztonság megteremtése és fenntartása *társadalmi feladat,* amely differenciált követelményeket és felelősséget támaszt a társadalom minden tagjával szemben. Erre azonban *fel kell készíteni a társadalom tagjait.* (VÁMOSI 2010, 12–13.)

A biztonság tartalmi változásai természetesen nem jelentik a *katonai biztonság* jelentőségének és veszélyeztetettségének csökkenését, annak szerepe és fontossága megmarad – figyelembe véve a fegyverkezési programokat, a helyi, közöttük napjainkban például az ukrán konfliktusokat. Mégis egyfelől a hidegháborúra jellemző amerikai–szovjet katonai szembenállás s azzal együtt a bipoláris világrend megszűnése, másfelől a biztonságot fenyegető úgynevezett *nem katonai tényezők* (többek között az ökológiai problémák, a demográfiai-migrációs folyamatok stb.) mind nagyobb mértékben befolyásolják az emberiség mindennapi biztonságát. A biztonságot fenyegető veszélyek és veszélyforrások súlyossága és megítélése az emberiség történelme során annak függvényében változott, hogy milyen módon befolyásolták a normális élet feltételeit. Ebből fakadóan a biztonságot befolyásoló tényezők csoportosíthatók aszerint, hogy egy részük *természeti jellegű* (földrengés, szélsőséges időjárás stb.), amelyek függetlenek a közvetlen emberi cselekedetektől. A tényezők másik része vétkes, tudatlan vagy szándékos *emberi tevékenység* közvetlen vagy közvetett, azonnal vagy hosszabb időtávon kialakuló és hatást gyakorló következménye (például: erdőtűz, klímaváltozás stb.). Ugyanakkor mindkettő fenyegetést jelent a lakosság biztonsága szempontjából.

A fentiek alapján a biztonság fogalma legtömörebben úgy definiálható, hogy *az az egyén, a társadalom, illetve az emberi civilizáció létfontosságú érdekeinek és értékeinek a védettségét jelenti a különböző veszélyekkel és fenyegetésekkel szemben.* A biztonság tehát állapot, a biztonságpolitika pedig tevékenység, amely a biztonság megteremtésére és fenntartására irányul.

A biztonságpolitika az általános politika része, amelynek céljait és elveit a törvényhozás határozza meg, gyakorlatát az állami végrehajtó intézmények és szervek által foganatosított rendszabályok és tevékenységek alkotják, s amely a lakosság cselekvő részvételével valósul meg. Ebből fakadóan a biztonság és biztonságpolitika bonyolult összefüggésrendszerében meghatározott szerepe van az államnak, a kormányzati szféra különböző elemeinek, a szakmai és civil szervezeteknek, a médiának, az oktatásnak, a tudományos kutatással és ismeretterjesztéssel foglalkozó szakmai és civil szervezeteknek, azok szakértőinek. A biztonságpolitika hatékonysága és a dinamikusan változó biztonsági környezet *reális értelmezése* érdekében elengedhetetlen:

– a korábbi ismert és az újonnan keletkezett veszélyforrások és fenyegetések okainak, jellegének és összefüggéseinek a feltárása,
– annak tudományos-szakmai elemzése, hogy a máig ható régi és az új veszélyforrások milyen lehetséges fenyegetést, biztonsági kockázatot és következményeket jelenthetnek a társadalomra s annak tagjaira nézve,
– az állami szervek és az állampolgárok várható magatartásának, előre megfontolt és begyakorolt, tudatos reagálásának a kialakítása, a lakosság felkészítése a valószínű fenyegetésekkel szemben.

A korszerű biztonságfelfogás értelmezése szempontjából fontos annak tudatosítása is, hogy a biztonság nem önmagától létezik, annak megteremtéséért és fenntartásáért képességéből és társadalmi státuszából fakadóan mindenkinek tennie kell valamit. Ehhez azonban aktuális ismeretekre, tájékozottságra, az összefüggések felismerésének képességére van szükség. Ugyanis *csak tájékozott,* a szükséges ismeretek tekintetében „naprakész" emberektől várható el a felelős gondolkodás és magatartás, más kifejezéssel a *biztonságkultúra* normáinak megfelelő cselekvés.

Láthatjuk, hogy a nemzeti és nemzetközi biztonsági környezet változásai alapvetően determinálják egy adott ország biztonságát és követendő biztonságpolitikáját, annak tartalmi változásait. Természetesen az adott ország is hatással lehet a nemzetközi biztonsági környezet alakulására – kiterjedése, gazdasági-társadalmi és katonai képességei, geostratégiai helyzete, valamint aktuális kül- és biztonságpolitikai tevékenysége révén –, amely *kölcsönhatásokat* nemzeti biztonsági és katonai stratégiákban, illetve doktrínákban rögzítenek. Másfelől egy állam biztonságpolitikája szerves egységet alkot a társadalmi gondolkodás és szemléletmód, a társadalmi cselekvés módosulásaival, a társadalmi (nemzeti) kultúra változásaival. A biztonsággal és biztonságpolitikával összefüggő vélemények, állásfoglalások és tevékenységek mind az egyén, mind a közösség részéről alapvetően függnek attól a történelmileg kialakult kultúrkörtől, amelyben az egyén/közösség *szocializálódott*, amely meghatározza személyiségjegyeit, értékrendjét és másokhoz való viszonyát. Ezért fontos a lakosság, különösen a fiatalok körében végzett differenciált és következetes tájékoztató- és nevelőtevékenység.

Egy kultúrkörön belül a biztonságkultúrát az adott ország általános kultúrája részének tekintjük, annak egyik fontos részkultúrája. A tudomány – mint az általános kultúra egyik szakmai kultúrája – szorosan kapcsolódik a biztonságpolitikához és a biztonságkultúrához. *A biztonságkultúra általában tehát minden olyan elméletet, nézetet, értéket, hagyományt és gyakorlatot magában foglal, amelyet a társadalom a biztonsággal összefüggésben elfogad és követ, sajátjának tekint.*

Minden kultúra, de leginkább a nemzeti biztonságkultúra szoros kapcsolatban van az aktuális *hatalommal,* elválaszthatatlanul kötődik annak gyakorlásához, vagyis a politikához, a *politikai kultúrához.* Ugyanakkor visszahat az általános politika alakulására, a politikai hatalom jellegére és döntéseire.

Összegezve megállapítható, hogy a korszerűen értelmezett biztonság, s abból fakadóan a biztonságpolitika és biztonságkultúra fogalma sokrétű és összetett, politikai jelentőségén túl minősíti egy adott ország, régió vagy a világ népeinek gondolkodásmódját, illetve cselekvőkészségét a válsághelyzetek kezelésének időszakában.

A biztonság dimenziói

A fentiek alapján láthatjuk, hogy a 21. század elején érvényesülő biztonság rendkívül sokrétű, dinamikusan változó fogalom és állapot, amely egyaránt jellemezhető a hagyományos katonai elem és a korszerűen értelmezett nem katonai tényezők kölcsönhatásával. A múlt század második felére jellemző amerikai-szovjet globális méretű és hatékonyságú nukleáris fegyverkezési verseny, valamint a szembenálló ideológiák ellenére a kétpólusú világrend katonai biztonsága *kiszámíthatóbb* volt, ugyanis a két nagyhatalom a nyolcvanas évek köze-

pére felismerte a lehetséges nukleáris világháború értelmetlenségét, a kölcsönös elpusztítás lehetőségét és várható globális következményeit, ugyanakkor féken tartotta az érdekszférájába tartozó hatalmakat, megfelelő figyelmet fordított a hivatalos propaganda és a média célirányos, tömegtájékoztató szerepére. A biztonság nem katonai tényezőinek biztonságra gyakorolt jelentősége ebben a periódusban pedig még többnyire elhanyagolható volt.

Napjaink multipoláris világában a biztonság – a nemzetközi ellenőrzés hiánya, az új hatalmi központok kialakulása, a vallási, etnikai, ideológiai stb. alapon szerveződő fegyveres csoportosulások akciói, a szélsőséges irányzatok (például: dzsihadista törekvések) növekvő „népszerűsége" az arab és a nyugati országokban, a gyenge és működésképtelen kormányok miatti instabilitás, valamint a nemzetközi bűnözői és terrorista hálózatok térnyerése és egyéb nem katonai tényezők (klímaváltozás, migráció, nyersanyag- és energiatartalékok kimerülése, információtechnológia tömeges alkalmazása stb.) egymást erősítő hatásai következtében – összetettebb, sérülékenyebb, összességében *kiszámíthatatlanabb.*

Ennek hatásait csak felerősíti az a körülmény, hogy napjaink veszélytényezői *kevésbé ismertek* az emberek számára, sőt a politikai döntéshozók többsége sem rendelkezik megfelelő tájékozottsággal, a felelős döntésekhez elengedhetetlen információkkal, elemzésekkel, az összefüggések, valamint a döntések várható következményei felismerésének képességével. (VÁMOSI 2018)

A katonai biztonság

Bármilyen tényezők befolyásolják is az emberiség biztonságát, a katonai biztonság szerepe kiemelkedő jelentőségű. A 21. század első évtizedeiben új *fegyverkezési hullám* bontakozik ki nemcsak a nagyhatalmak, de a fejlődő, különösen a feltörekvő országok vonatkozásában is.

A katonai biztonságra törekvés mindig összefüggésben van a nemzetközi viszonyok alakulásával, a nagyhatalmi globális érdekek vagy regionális befolyásolási politikák érvényesítésével. Következésképp a fegyverkezés egyrészt következménye, másrészt előidézője a nemzetközi hatalmi-politikai és gazdasági törekvéseknek, a fegyveres konfliktusok pedig kiváló hadszínteret biztosítanak az új fegyverek élesben történő teszteléséhez (például Líbia és Mali esetében).

Napjaink fegyveres konfliktusai igazolják, hogy a katonai erő az alkalmazásának technikai és technológiai evolúciója következtében, veszélyessége és lehetséges következményei miatt kiemelt figyelmet követel a biztonságpolitika részéről. A katonai kiadások növekedésének új hulláma, a katonai-haditechnikai kutatások és fejlesztések intenzitása (például: IT-alkalmazások, intelligens és nagypontosságú fegyverek, a „lopakodó" üzemmód stb.) elterjedése folyamatos *minőségi fejlődést* generál a fegyveres erők felszereltségében és alkalmazási lehetőségeiben.

A fegyverkezési törekvések ellenére a biztonság katonai tényezői korábbi jelentőségének csökkenése a múlt század végén számos körülménnyel függött össze:

– először a Szovjetunió gazdasági-politikai összeomlása és felbomlása (1991) következtében megszűnt a 20. század második felére jellemző bipoláris katonai, politikai és ideológiai szembenállás a nyugati szövetségi rendszer (Amerikai Egyesült

Államok vezetésével) és a keleti blokk (Szovjetunió) gazdasági és katonai tömbjei között,
– másodszor a szocialista világrendszer összeomlása, a szovjet/orosz beavatkozás lehetőségének megszűnése következtében felerősödtek a globális demokratizálódás folyamatai Kelet-Európában, Ázsiában és Latin-Amerikában,
– harmadszor lényeges hangsúlyeltolódás ment végbe a katonai biztonság területén: elsősorban az úgynevezett feltörekvő országok (India, Brazília) érezték szükségét, hogy fejlesztve katonai képességeiket közelebb kerüljenek a vezető triádhoz (USA, Kína, Oroszország). Ezzel hozzájárulnak a globális katonai biztonság multipoláris jellegének erősödéséhez.

A fegyverkezés új hullámának kialakulása, ezáltal a katonai biztonság reneszánsza mellett a múlt század vége felé olyan új típusú fenyegetések kezdtek kibontakozni, amelyek nincsenek összefüggésben a katonai tényezőkkel, s amelyek többnyire világméretű és váratlan veszélyt jelentenek az emberiség biztonságára, túlélő képességére nézve – ezek a biztonság úgynevezett nem katonai dimenziói.

A biztonság nem katonai tényezői

A világ fejlődésének jelenlegi szakaszára jellemző új folyamatok, mint például az ökológiai, demográfiai, információtechnológiai stb. változások új típusú kihívásokat jelentenek az emberiség általános biztonsága tekintetében – fogalmában, értelmezésében és a biztonságot fenyegető körülmények, valamint következményeik kezelésének módjában. Bevezetésként elegendő itt csak a gyökeresen megváltozott *természeti jelenségekre*[3] utalni: a hazai és európai szélsőséges időjárási események, a kínai és japán földrengések, a délkelet-ázsiai és japán cunamik stb., amelyek kiszámíthatatlanságukkal és kivédhetetlenségükkel, az ember kiszolgáltatottságával új helyzetet teremtenek a biztonság szempontjából.

A biztonság nem katonai dimenziói számos *sajátossággal* rendelkeznek:
– folyamatosan bővítik a biztonság és biztonságpolitika fogalomkörét,
– nem csupán a biztonságot befolyásolják, hanem az emberiség létét,
– hatásaik helyi, regionális és globális szinten érvényesülhetnek (járványok, szélsőséges időjárás),
– kialakulásuk körülményeit és lehetséges hatásaik összefüggéseit az emberiség többnyire még nem ismeri,
– következményeik elhárítására, kezelésük módszereire az emberiség még nem készült fel (klímaváltozás, cunamik, aszteroidák vagy űrszemét becsapódása),

[3] A svájci Swiss Reinsurance Co. biztosítótársaság adatai szerint 2011-ben a természeti katasztrófák okozta károk összege meghaladta a 350 milliárd dollárt. A legnagyobb kárt a 2011. márciusi japán földrengés és cunami okozta, amelynek kárértéke lényegesen meghaladta a 35 milliárd dollárt. Jelentős anyagi károk keletkeztek más természeti jelenségek következtében is: Új-Zéland, 2011, földrengés; Thaiföld, 2011, árvíz; USA, 2011, erős viharok.

– egy részük (nyersanyag- és energiaforrások kimerülése, klímaváltozás) már – egyre több szakértő véleménye szerint – eljutott a visszafordíthatatlan folyamat fázisába, amelyek tekintetében ezért az ember tehetetlen,[4]
– nem előzhetők meg és nem oldhatók meg katonai eszközökkel, megoldást elsősorban a katasztrófavédelmi módszerek hozhatnak,
– a szükséges információk és tudás hiánya miatt ismeretük nem képezi az általános műveltség és biztonságkultúra szerves részét.

A globális problémák biztonsági aspektusai

A 2008/2009-ben kibontakozott világméretű *pénzügyi és gazdasági válság* ráirányította a figyelmet arra a körülményre, hogy a globális *gazdasági folyamatok* elválaszthatatlanul összefüggnek olyan társadalmi problémákkal, mint a munkanélküliség, a fejlett országok elöregedő társadalma, a munkaerőpiaci ellentmondások, a gazdag és a szegény országok közötti gazdasági-szociális és társadalmi-egzisztenciális megosztottság növekedése, a természeti környezet stb. pusztulása. A világgazdaság nem csupán piacgazdasági jelenség, annak nagyon szoros társadalompolitikai, szociális és egyéb összefüggései is vannak.

A gazdasági folyamatok globálissá válása mellett egyre nagyobb szerepet kap az IKT globalizálódása: az utóbbi néhány évtizedben rohamosan terjedő technológiák, a digitális kommunikáció egyeduralkodóvá válása számtalan, ma még talán fel sem ismert lehetőséget kínál az ember számára a tudományban, az oktatásban, a kultúrában, a személyiség sokoldalú ffejlődésében vagy akár a védelmi szférában. Ugyanakkor rossz szándékú emberek kezében ártalmas lehet az emberiség egészének vagy egyes csoportjainak biztonságára nézve.

Századunk az információs kor százada, amelyben az információtechnológiai eredmények széles körű és tömeges alkalmazása felerősíti a globalizációs folyamatokat a gazdasági, termelési, kereskedelmi, fogyasztási, tudományos, kulturális és egyéb területeken, hozzájárulva a világméretűvé válás, az integráció és a kölcsönhatás, valamint az *interdependencia* elmélyüléséhez. A *globalizáció* következtében megváltozik a tér és idő dimenziója, megszűnnek a zárt társadalmak, lerövidülnek a földrajzi távolságok és időbeli különbségek. Az információk másodpercek alatt jutnak el a világ egyik részéből a másikba. Amennyiben a globalizációt úgy értelmezzük, mint társadalmi (világ-) fejlődési folyamatot, s a fejlődési folyamatok kölcsönhatásait, akkor nyomon követhetjük azokat a társadalmi és technikai változásokat, amelyek a fenntartható fejlődés során globálissá válnak. Ezek egy része globális problémává alakulhat, sőt nemzetközi konfliktushoz is vezethet.

A globális problémák között egyre nagyobb jelentősége van a *szegény országokat* sújtó szegénységnek, az élelmiszer- és vízhiánynak, a természeti és energetikai erőforrások folyamatos kimerülésének, hozzájárulva tömeges megbetegedésekhez, illetve a megélhetési migráció globális kibontakozásához. Miközben a Föld lakossága az évszázad közepére elérheti a 9 milliárdot, tovább növelve a veszélyeztetett népcsoportok számát (elsősorban a szegény országokban), hozzájárul a globális népvándorlás felerősödéséhez – belső társa-

[4] A Kormányközi Klímaváltozási Panel 2014. október végén kiadott összegző jelentése szerint 2100-ra gyakorlatilag be kell fejezni a kőolaj és a földgáz, valamint a szén energetikai célú felhasználását. Sőt, a Földön felhasznált elektromos áram négyötödét már 2050-re megújuló forrásokból (szél-, víz- és napenergia), illetve atomerőművekben kell előállítani. (*Népszabadság,* 2014. november 3.)

dalmi és szociális feszültséget, konfliktusokat gerjesztve a helyi lakosság és a bevándorlók között (például: 2015. Európai Unió országai).

A biztonsági aspektusok fentiekben bemutatott bővülése miatt megnő a követendő *biztonságpolitikai tevékenység* szerepe az alábbiak szerint:

- összehangolt, célirányos tudományos kutatások, a hazai és nemzetközi tapasztalatok és tudományos eredmények gyakorlati alkalmazása,
- törekvés a válság- és katasztrófahelyzetek tervszerű előrejelzésére, megelőzésére és szakszerű kezelésére,
- az operatív tevékenység szakmai, szervezeti és technikai-infrastrukturális feltételeinek folyamatos biztosítása és fejlesztése,
- a vezetők/menedzserek vezetői felkészültségének, képességének és készségének speciális, rendszerszerű fejlesztése,
- a lakosság tájékoztatásának, gyakorlati felkészítésének és orientálásának kompetenciája,
- a katasztrófavédelem, a Magyar Honvédség, a Rendőrség és a közigazgatás érintett személyi állománya társadalmi presztízsének és motiváltságának biztosítása.

A globális környezet változásai

A világ fejlődésének irányait és lehetőségeit a 21. század elején döntően azok a globális környezeti változások határozzák meg, amelyekre elsősorban nemzetközi összefogással lehet válaszolni. A globális méretű környezeti változások biztonsági aspektusainak részletesebb elemzése előtt át kell tekinteni – társadalmi hatásaik és következményeik alapján – *a globális problémák csoportosítását:*

- közvetlen ökológiai problémák: alapvetően hatnak az emberiség létezésének körülményeire (például: globális felmelegedés, környezetszennyezés, az élővilág diverzitásának pusztulása, az újra nem termelhető természeti erőforrások [kőolaj, földgáz, ivóvíz] kimerülése stb.),
- ökológiai és társadalmi problémák: idetartozik többek között a népességnövekedéssel közvetlen összefüggésben a világ élelmezése és az egyre csökkenő ivóvízellátás,
- gazdasági természetű, globális problémák: többek között a gazdasági javak igazságtalan eloszlása, a gazdagság és a szegénység fokozódó egyenlőtlensége, a fejlett és fejletlen országok, régiók (centrum és periféria) közötti szakadék mélyülése, az anyagi és szellemi javakhoz való hozzáférés végletesen kiélezett lehetőségeinek megjelenései (amelyeket az információs kor kiteljesedése csak tovább mélyít),
- társadalmi-tudati problémák: idesorolhatók az ideológiai, vallási, politikai megosztottságból fakadó konfliktusok, amelyek fegyveres összetűzésekhez, terrorista akciókhoz vagy akár tömegpusztító fegyverek alkalmazásához vezethetnek. Kiváltó okokként azonosíthatjuk például a szélsőséges nacionalizmust, a fajgyűlöletet, az egyéni és kollektív emberi jogok megsértésével összefüggő törekvéseket.

Napjainkban két olyan meghatározó *világtrendet* láthatunk, amelyek hozzájárulnak a globális problémák kialakulásához:

– az egyik a népesség világméretű növekedése, amely egyre több természeti erőforrást igényel,
– a másik a Föld számos természeti erőforrásainak gyorsuló ütemű kimerülése és biológiai diverzitásának a károsodása.

Mindkét folyamat olyan fázisába jutott századunk elejére, hogy semmiféle emberi beavatkozás *nem képes a fenti trendek megállítására,* a bolygó fizikai lehetőségei, valamint a szüntelenül növekvő népesség szükségletei közötti összhang pozitív trendjének kialakítására, ezáltal a globális egyensúly megteremtésére.

A globális problémák mint biztonsági kockázatok elméleti összefüggéseinek áttekintése mellett szükséges a legfontosabb *területek sajátosságaival* és a *lehetséges következményekkel* kapcsolatos biztonsági-biztonságpolitikai aspektusok összefoglalása.

Ökológiai problémák

A negatív trendek miatt egyre gyarapodó tudományos kutatások eredményei azt bizonyítják, hogy a növekvő világméretű természeti károsodás következtében *romlanak az emberiség természeti* életfeltételei.

A természeti erőforrások rövid távú érdekeket szolgáló kiaknázása (például a fogyatkozó erdőterületek, a világméretűvé vált ivóvízválság, a kimerülőben lévő energiaforrások), valamint az alternatív megoldások halogatása tovább súlyosbítják a méltatlan körülmények között élők helyzetét, és nem ritkán *fegyveres konfliktusok kialakulásához* vezethetnek (például: Darfur, Mali, Marokkó stb.).

Abban egységes vélemény alakult ki a témakörrel foglalkozó szakértők körében, hogy amennyiben a gazdasági-társadalmi fejlődés a múlt század második felében kialakult pályán folytatódik, a világgazdasági rendszer a 21. században komoly változásokon fog keresztülmenni. Az emberi élet *romló természeti feltételeinek* a megnyilvánulásai a következők:

– a meg nem újítható természeti és energiaforrások csökkenése,
– a népesség robbanásszerű növekedése,
– az egy főre jutó termőföld csökkenése,
– az esőerdők irtása,
– a víztartalékok apadása,
– a halászterületek csökkenése,
– számos növény- és állatfaj kihalása,
– a hőmérséklet emelkedése miatt veszélybe kerülő ökorendszerek stb.

A növekvő társadalmi igény, az életminőség szüntelen javítására törekvés különösen a múlt század második felében oda vezetett, hogy *a bolygó ökológiai rendszere túlterhelődött,* a hagyományos gazdasági-társadalmi fejlődés önpusztítóvá vált, kockára téve ezzel az ember életben maradását. Ugyanakkor a természeti források kiaknázásának eltérő mértéke mellett a megtermelt javak elosztásának igazságtalansága is tovább mélyült. Jól mutatja ezt a népesség és a természet eltartóképességét kifejező „ökológiai lábnyom" differen-

ciáltsága. A mértéktelen és felelőtlen természetkárosítás gazdasági és fogyasztási-jóléti következményei mellett – hosszabb távon – *biztonsági kockázatot* jelent. Ennek többféle megnyilvánulási formája várható. Fegyveres konfliktusokat gerjeszthet:

- a természeti kincsek egyenlőtlen és igazságtalan kitermelése, amely „forrásháborúkhoz" vezethet,
- a gazdasági és politikai hatalommal, a katonai erőfölénnyel való visszaélés,
- a különböző politikai és korrupciós manipuláció,
- az eltérő földrajzi adottságokkal való visszaélés,
- az afrikai, illetve közel-keleti fegyveres konfliktusok elől (az ISIS által fenyegetett területekről, polgárháborús övezetekből) menekülő, vagy létbiztonságot és megélhetést kereső tömegek megjelenése az európai határokon, valamint az egyre nagyobb számban megjelenő latin-amerikai népesség beáramlása az USA-ba, vagy az orosz–kínai határon zajló vitás kérdések. (Vámosi 2001)

Klímaváltozás

Az elmúlt évtizedek során lezajló éghajlatváltozás – a fokozatos felmelegedés következtében – egyre nagyobb valószínűséggel vetíti előre a földi klíma átalakulásának visszafordíthatatlan folyamatát, annak számos, ma még pontosan meg nem határozható hatásaival együtt. Az ENSZ vezetésével folyó kutatások eredményei világméretű nemzetközi összefogást és gyökeres szemléletváltást sürgetnek.

Élelmiszerből kevesebb, konfliktusból több lesz a következő évtizedekben – hangzik az Intergovernmental Panel on Climate Change (a továbbiakban: IPCC), az ENSZ klímaügyi tanácsadó testülete ötödik jelentésében (2014). A dokumentum újdonsága, hogy már nem a jövőről, hanem a jelenről szól: gyakorlatilag azokat a *veszélyeket* mutatja be és igyekszik számszerűsíteni, amelyeket már napjainkban érzékelhetünk. A klímaváltozás következtében csökkentek a terméshozamok búzából és kukoricából, miközben az emberiség létszáma növekszik. Ezzel párhuzamosan azonban a termőterület – részben éppen a klímaváltozás okozta sivatagosodás, illetve erózió, részben a szintén klimatikus okok következtében egyenlőtlenebbé vált csapadékeloszlás, aszályok miatt – csökken. Hasonló folyamat mehet végbe a halászat területén, csak lényegesen súlyosabb mértékben.

A megváltozó éghajlati körülmények negatív hatásai meghatározott *biztonsági kockázatokat* jelenthetnek, mint például:

- a meleg égöv fokozatos északra húzódása következtében megváltozik a mezőgazdasági termelés jellege, módosul a növényi kultúra, a mezőgazdasági tevékenység jellege, ezáltal a lakosság étkezési szokásai és étkezési kultúrája,
- átalakul az élelmiszer-kereskedelem struktúrája, az export-import jellege és iránya,
- megváltozik a nemzeti és nemzetközi kereskedelmi és gazdasági kapcsolatok érdekrendszere, ami
- nemzetközi politikai és fegyveres konfliktusokhoz, helyi és regionális háborúkhoz, globális válságokhoz vezethet.

Népességrobbanás

Látható, hogy a fentiekben vázlatosan bemutatott két terület szorosan összefügg a szintén fokozatosan növekvő és feltartóztathatatlan népességnövekedéssel. Különböző szociológiai és statisztikai felmérések, valamint tudományos kutatások tapasztalatai alapján egyértelműen előrejelezhetők a népesség számában és összetételében végbemenő jelentős változások, mindenekelőtt az ázsiai és afrikai földrészen.

A népesség számának folyamatos emelkedése és az eddig hozott mérséklési intézkedések (például Kínában a születésszabályozás) eredménytelensége következtében egyre markánsabban fogalmazódik meg az a vélemény, hogy képtelenség megállítani ezt a folyamatot.

A gazdasági és társadalmi fejlődés különbözősége és színvonala, valamint a népesség gyarapodásának szabályozására hozott intézkedések hatására a fejlett országokban növekszik a születéskor várható élettartam, ugyanakkor csökken a gyermekhalandóság. A statisztikai adatok azonban nem tükrözik az országok és régiók közötti olyan különbségeket, mint például azt, hogy a fejlett országokban – a jólét, a színvonalas egészségügyi ellátás, a prevenció, a megfelelő nyugdíjasellátás rendszere stb. hatására – *megnő az átlagéletkor,* ugyanakkor a szegény országokban – a szegénység, az ivóvíz és az élelmiszer hiánya, a higiéniás és egészségügyi ellátás hiányosságai, a betegségek, fegyveres konfliktusok, elvándorlás következtében – *csökken az emberek átlagéletkora.*

A fenti társadalmi problémák mellett a fejlődő országok nagy részében a népességrobbanással összefüggő globális probléma a demográfiai egyensúly kérdése. Az ENSZ adatai szerint 2000-ben a világ több mint száz országában volt úgynevezett *ificsúcs,* azaz amikor a felnőtt lakosság több mint negyven százaléka 15 és 29 év közötti volt.

A globálisan egyre fenyegetőbb népességrobbanás negatív hatásainak csökkentése és egy radikális, az új technológiák lehetőségeit észszerűen kihasználó életmódváltás végrehajtása érdekében megfogalmazódnak lehetséges megoldási módszerek is, közöttük olyanok, mint:

- az energiamegújítás új formáinak és módjainak kidolgozása és alkalmazása a gazdasági és társadalmi élet különböző területein,
- a természeti erőforrások felhasználásának fokozatos csökkentése, az esőerdők és halászati területek regenerálódásának biztosítása,
- a bolygó teherbíró képességét fokozatosan terhelő és növekvő mennyiségű hulladék újrahasznosításának megoldása.

A század közepére/második felére előre jelzett népességrobbanás komoly *biztonsági kihívásokat* rejt magában, ugyanis várhatóan tovább mélyíti és szélesíti a gazdag és szegény országok, régiók között meglévő gazdasági, szociális és társadalmi szakadékot. ENSZ-adatok szerint – *tömeges migráció* révén – mintegy 500 millió ember tervezi lakhelyének megváltoztatását, hazája elhagyását egy „élhetőbb" ország reményében. A szegény, de a népesség növekedésében élenjáró országokban a legnagyobb a *belső fegyveres konfliktusok* veszélye, amely – éppen a migráció által – könnyen átterjedhet a szomszédos országokra (például: Afrika országai).

A fentiekben bemutatott környezeti változások csak a legfontosabb globális problémák vizsgálatára irányulnak, amelyek differenciáltan, de hatást gyakorolnak a világ legtöbb országára. Idesorolhatjuk még az információs társadalom és a terjeszkedő terrorizmus,

valamint a szervezett bűnözés világméretű térhódítását, amelyek azonban *inkább függnek* egy adott ország gazdasági és társadalmi fejlettségétől, belső rendjétől, a közrend és közbiztonság minőségétől. Egy technikai-technológiai színvonalon felkészült, szervezett rendvédelmi és magas színvonalú nemzetközi együttműködést megvalósító, motivált felderítő szervekkel rendelkező ország képes időben felderíteni és kezelni a megjelenő deviáns jelenségeket, elejét venni a társadalom biztonságára nézve fenyegetést jelentő cselekedeteknek.

Biztonsági kihívások napjainkban

A globális problémák néhány évtizedes felerősödése ráirányította a tudomány és a szakértők, valamint egyre meggyőzőbben a döntéshozók figyelmét a korszerűen értelmezett biztonság új összefüggéseire, a szemléletváltás szükségességére. Az utóbbi évtizedek eseményei bebizonyították, hogy nem lehet a hidegháborús időszakra jellemző gondolkodásmóddal szemlélni felgyorsult világunk történéseit:

- míg a hagyományos biztonsági kockázatok, mint a fegyveres konfliktusok, a háborúk több-kevesebb előkészítést (logisztikai, kommunikációs, díszlokációs, mozgósítási és egyéb feladatokat) követelnek, addig
- az új, nem katonai biztonsági kihívások (szélsőséges időjárási anomáliák, földrengések és cunamik, földcsuszamlások és iszapkatasztrófák, aszteroida- és űrszemét-becsapódások stb.), amelyek többnyire függetlenek az emberi szándéktól és cselekvéstől, rövid időn belül, váratlanul következnek be, és velük szemben az ember kevésbé képes hatékonyan fellépni.

A komplex biztonság sajátosságainak és összefüggéseinek ismerete napjainkban egyre fontosabb követelmény, ugyanis az új típusú biztonsági kockázatok *megváltoztatták a biztonság fogalmát és értelmezését,* emiatt megváltozott azok felismerésének, megelőzésének és kezelésének módja. Olyan trendek kibontakozásának vagyunk tanúi, amelyek a drasztikusan változó környezeti feltételek miatt nem csupán az emberiség nyugalmát, mindennapi biztonságát fenyegetik, hanem a létét, a katasztrófák túlélését, amelyek többségére – még – nem készültek forgatókönyvek.

Mindehhez jelentős mértékben járultak hozzá azok az elmúlt 2 évben bekövetkezett események, amelyek biztonságpolitikai szempontból minden egyes nemzet, illetve a szövetségi rendszerek vonatkozásában is egyedülálló és szigorú védelmi célú intézkedéscsomagok elfogadását tették szükségessé. A londoni terrortámadás (2005) óta az európai emberek biztonságérzete helyreállt, viszont a 2015. november 13-i párizsi terrorcselekmény-sorozat mindezt ismételten ingatta meg. Az ezt követő brüsszeli robbantások 2016 tavaszán egyre sürgetőbbé tették a terrorizmus elleni harc újragondolását, a tömeges migráció által hordozott kihívások csökkentését, összességében a biztonság megteremtésének, visszaállításának kérdését. A legtöbb EU-tagállam szigorította a közbiztonság fenntartására irányuló nemzeti jogszabályait, több esetben visszaállították a schengeni övezeten belüli határellenőrzést, egyre nagyobb figyelmet fordítottak a terrorizmussal okkal gyanúsítható, a közel-keleti térségből visszatérő „harcosok" nyomon követésére, és összességében növelték a közbiztonság fenntartásáért felelős szervek létszámát. Mindezek ellenére újra és újra bekövetkeztek olyan események, amelyeket az Iszlám Állam mint terrorszervezet nevében követtek el

úgynevezett magányos farkas terroristák (például: 2016. július 14. nizzai teherautós támadás; 2016. július 22. müncheni lövöldözés; 2016. december 19. berlini teherautós támadás). Látható, hogy a módszer egyre inkább az egy személy által elkövethető, könnyen tervezhető, áldozatokat és tömeges sérüléseket követelő terrorcselekmények irányába mozdult el. Rendkívüli kihívás az ilyen dinamikusan változó körülményekre hatékony és eredményes válaszokat kialakítani mind nemzeti, mind nemzetközi szinten.

A fenti elemzések alapján érthető, hogy a biztonság nem katonai elemeinek erőteljes előtérbe kerülése többnyire tükröződik az országok és nemzetközi szervezetek (ENSZ, EU, NATO, OECD) hivatalos dokumentumaiban, tudományos és szakmai szervezetek állásfoglalásaiban, javaslataiban. Az új típusú fenyegetéseket az aktuális nemzetközi viszonyok, trendek sokoldalú tudományos elemzése alapján definiálják annak megfelelően, hogy azok elemei és kölcsönhatása milyen módon és mértékben befolyásolják a biztonságot. A nagyhatalmak (és egyes más országok) nemzeti biztonsági stratégiái és katonai stratégiái/doktrínái már tükrözik a biztonság nem katonai dimenzióinak az elemzését (például: USA – 2010, Oroszország – 2010, NATO – 2010, Magyarország – 2012).

A nemzetközi összefüggések és a szövetségesi stratégiák elemzése alapján megfogalmazhatók a Magyarország biztonsága szempontjából legfontosabb aktuális *biztonsági kihívások:*

- az elsősorban Európa irányába intenzívebbé váló migrációval felerősödő nemzetközi terrorizmus és vallási/iszlám szélsőségek (például: Iszlám Állam, Al-Kaida stb.),
- a regionális konfliktusok nemzetközi következményei (például: Ukrajna, Szíria, Izrael),
- a szervezett bűnözés (fegyver-, kábítószer-, embercsempészet stb.),
- kibertámadások (Irán, Grúzia, Észtország, Magyarország stb. ellen),
- kritikus infrastruktúrák elleni támadások,
- a tömegpusztító fegyverek és a katonai technika-technológia proliferációja,
- az ipari és természeti katasztrófák,
- járványok és egészségügyi problémák,
- a meg nem újítható természeti erő- és energiaforrások (kőolaj és földgáz) csökkenése és kimerülése,
- az ökológiai problémák és klímaváltozás. (ENDRESZ–VÁMOSI 2012)

A felsorolás alapján látható, hogy a korszerű biztonsági kihívások többsége nem katonai jellegű, következésképp azok megelőzése és kezelése sem csupán katonai eszközöket igényel. Napjainkban a biztonsági kockázatok döntő többsége elsősorban *rendészeti és katasztrófavédelmi eszközöket* és módszereket kíván, valamint a lakosság kellő szintű felkészültségét és differenciált tájékozottságát.

Végezetül levonható az a következtetés, hogy biztonsági környezetünk megteremtése és fenntartása – megfelelő nemzetközi együttműködés mellett – *komplex* társadalmi feladat és felelősség, amely a szükséges ismeretek mellett korszerű gondolkodásmódot és megalapozott biztonságkultúrát igényel. Erre azonban *fel kell készíteni a társadalmat, mert csak felelős társadalom* képes reális döntéseket hozni biztonsága érdekében is.

***

A 21. században az információs társadalom kiteljesedése globalizálja az egész világot, ugyanakkor megismerhetővé teszi a világ biztonságát befolyásoló tényezők jellegét, összefüggéseit és várható hatásaikat. A globális trendek megismerése lehetőséget ad az ember számára, hogy felismerje természeti és társadalmi környezetének új típusú törvényszerűségeit, a létfenntartáshoz szükséges biztonsági környezet megteremtésének és fenntartásának lehetőségeit és feladatait.

Felhasznált irodalom

Besenyő János – Prantner Zoltán – Speidl Bianka – Vogel Dávid (2016): *Az Iszlám Állam – Terrorizmus 2.0. Történet, ideológia, propaganda.* Budapest, Kossuth Kiadó.

Endresz Ernő – Vámosi Zoltán összeáll. (2012): *Biztonság és biztonságkultúra.* Budapest, TIT HABE.

Vámosi Zoltán (2001): *Politológia.* Tankönyv. Budapest, LSI.

Vámosi Zoltán (2010): A 21. század valósága. In Vámosi Zoltán szerk.: *A biztonságról – fiataloknak.* Budapest, TIT HABE.

Vámosi Zoltán szerk. (2018): *Gondolatok és vélemények a biztonságról (A biztonságkultúra kérdései).* Budapest, TIT HABE.

Hivatkozott jogszabályok és dokumentumok

Világgazdasági Fórum Jelentése (2011). Davos. Elérhető: www.weforum.org/reports?page=28 (Letöltés ideje: 2014. 11. 20.)

Az ábrák forrása

1. ábra: www.digi24.ro/stiri/externe/mapamond/au-trecut-12-ani-de-la-atentatele-de-la-11-septembrie-2001-in-care-si-au-pierdut-viata-peste-3-000-de-oameni-117006 (Letöltés ideje: 2018. 07. 24.)
2. ábra: http://konyvkultura.kello.hu/kritika/2015/09/arab-tavasz (Letöltés ideje: 2018. 07. 24.)
3. ábra: http://azatlasz.hu/2014/10/ebola_veszelyt_jelentenek-e_az_illegalis_hataratlepok (Letöltés ideje: 2018. 07. 24.)

Vákát oldal

1. fejezet
Történeti áttekintés

Bonnyai Tünde

1.1. A kritikus infrastruktúra jelentése és kapcsolódási pontjai

Az ember és környezete folyamatos fejlődésével jelentek meg azok a módszerek, hálózat jellegű rendszerek, amelyeket megalapozottan nevezhetünk korai infrastruktúráknak. Idesoroljuk például az ókori vízvezetékeket, öntöző- és gátrendszereket, Kína összefüggő úthálózatát és csatornáit, az athéni Akropoliszt vagy Hammurápi törvényoszlopát. Mindemellett ideérthetjük az ókori, majd középkori birodalmak hatalmas hadseregeit, illetve az újkor tömeghaderőit is. Egyes társadalmak hosszú ideig az ellenséges szándékra koncentrálva alakították védelmi tevékenységüket, így főként erővel igyekeztek megóvni számukra létszükségletként funkcionáló infrastruktúráikat. Az urbanizáció kezdeti szakaszában elsősorban a fizikai védelem élvezett prioritást, ami a katonai módszerek alkalmazásában nyilvánult meg. Az ókori egyiptomi, görög, római és távol-keleti birodalmak kezdeményezései, illetve találmányai igazolták az emberiség fejlődésének tapasztalati úton történő megvalósulását. Összességében olyan fejlődési irányokat vetítettek elő, amelyek később fokozatosan növelték a szükségleteket kielégítő eszközök, módszerek és rendszerek kialakulásának lehetőségeit.

Mindebből egyértelműen látható egy olyan dinamikusan változó folyamat, amely az ember fejlődése által magával hozta az infrastruktúrák változását is. Kiemelkedő történelmi fordulatnak tekinthetjük az ipari forradalmak időszakát és a nagy háborúk éveit, amelyek hatására ugrásszerű fejlődés következett be. A közlekedési lehetőségek bővülése, az elektromosság megjelenése, a távközlési eszközök kialakulása, a tömegtermelésre való áttérés, valamint a kémiai-fizikai-biológiai tudományos felfedezések mind gördülékenyebbé tették az emberek hétköznapjait és élhetőbbé a környezetet. Ritkán esett azonban szó arról, hogy az új találmányok, a 20. század nagy áttörései, a technikai és virtuális infrastruktúrák – külön-külön és együttesen is – a függőség, az egymásrautaltság és a komplexitás kockázatát hordozzák magukban.

1.1.1. Az infrastruktúra értelmezése

Fentiek egyértelműen utalnak az infrastruktúra definíciójának szerteágazó jellegére, többféle értelmezés alapján történő megközelítésének lehetőségére. Számtalan különböző szempontot kell figyelembe venni, amikor fogalmi kereteket adunk az infrastruktúra meghatározására. Ahhoz, hogy megfelelő módon értelmezhetővé váljon a kifejezés, néhány egymástól független céllal megfogalmazott definíciót kell vizsgálni.

A világháló idegen szavak gyűjteményének megfogalmazása szerint az infrastruktúra „egy adott szervezet vagy szolgáltatás működéséhez szükséges eszközállomány hálózata" (idegen-szavak.hu). A definíció magában foglal minden olyan eszközt, elemet, módszert és rendszert, amely bármely szervezetet és szolgáltatást lehetővé tesz. Nincs meghatározva, hogy milyen tevékenységet biztosít e tekintetben az adott szervezet vagy szolgáltatás, de nem derül ki az sem, hogy mit értünk eszközök alatt. Ez a kifejezés nem alkalmas arra, hogy a kritikus infrastruktúrák védelme rendszerében jelentkező feladatok alapjául szolgáljon, mert túl tág és változatos értelmezést ad.

A Bakos Ferenc által szerkesztett *Idegen szavak és kifejezések szótárá*ban az infrastruktúra kifejezés „a gazdaság működésének üzemen kívüli előfeltételeit biztosító állóés forgóeszközök; a lakásállomány és a legkülönfélébb szolgáltatások (művelődésügy, közlekedés, közművek, hírközlés, egészségügy, kereskedelem stb.) állóeszközei, illetve ezek hálózataként" szerepel. (BAKOS 1983) Ez a körülírás konkrétabb utalásokat tartalmaz, mint az előző, ugyanakkor olyan megfogalmazásokkal él, amelyek elsősorban a közgazdaságtan terminológiájában használatosak. A szolgáltatások értelmezését tekintve továbbra is széles megközelítésre ad lehetőséget, a példákkal szemléltetett felsorolás nem teljes, a fogalom megalkotója fenntartotta a lehetőségét az igény szerinti kiegészítésnek. A leírásban ugyan jelen esetben is szerepel a hálózatszerűségre utaló kifejezés, de a definíció nem eléggé egzakt ahhoz, hogy a kritikus infrastruktúrák védelme rendszerében viszonyítási alapul szolgálhasson.

A Cecei Katalin és Mórocz Attila szerzőpáros szerint 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" (CECEI–MÓROCZ 2004). Ebben a megfogalmazásban már szerepelnek azok a célirányos jelzők, amelyek lehetővé teszik az infrastruktúra mint komplex kifejezés megértését. Kulcsfontosságú, hogy a szerzőpáros az infrastruktúrát ember alkotta létesítésnek tekinti, és nyomatékosan hangsúlyozza az összekapcsolt függőségi viszonyokat. Ugyanakkor a fogalom magában foglalja a célkitűzést is, amiért a megnevezett rendszerek és eljárások léteznek. Ez a megközelítés a jelentés szerves részeként kezeli a funkciót és a folyamatosságot egyaránt. Ahhoz azonban, hogy a kritikus infrastruktúrák védelme rendszerében általánosságban értelmezhető legyen az infrastruktúra jelentése, még egy további tényezőt figyelembe kell venni.

Kovács Ferenc úgy fogalmazta meg az infrastruktúra fogalmát, hogy az „a termeléshez kapcsolódó azon eszközök és intézmények összessége, amelyek nem részei a közvetlen termelési folyamatnak, de annak nélkülözhetetlen feltételei". (KOVÁCS 2012) A meghatározásban a korábbi tartalmi elemekhez képest egy jelentős kiegészítés, a „nélkülözhetetlen feltétel" szóösszetétel is megtalálható, amelyből – a kritikus infrastruktúrák védelme szempontjából – már teljes képet kapunk az infrastruktúra jelentéséről.

1. ábra

Az infrastruktúra értelmezése

Forrás: a szerző szerkesztése

Új fogalom megalkotása azonban nem volt indokolt, tekintettel arra, hogy a fentiekben vizsgált tartalmi elemeket az Európai Unió megfelelően alkalmazta. A tagállamok számára is egyértelműsített infrastruktúra kifejezés alatt jelenleg kölcsönösen egymástól függő hálózatok rendszerét kell érteni, amely magában foglalja a kritikus infrastruktúrák védelme rendszerében azonosított ágazatokat, intézményeket (ideértve a humán erőforrást) és képességeket. Mindezek az általuk keletkezett termékek és szolgáltatások megbízható áramlásáról, a kormányok minden szinten történő zavaratlan működéséről és a társadalom egészéről gondoskodnak. Ez a meghatározás áll legközelebb ahhoz, hogy mindenre kiterjedő fogalmi keretet adjon az infrastruktúra definíciójának, ugyanakkor tételes megfogalmazására az időközben végrehajtott felülvizsgálati időszak keretében sem került sor. A fenti értelmezés az Európai Unió jogalkotási folyamata során készített *Zöld Könyv* megállapításai alapján alakult ki. [Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról. COM (2005) 576 final.]

Összességében mindegyik definíció kifejezi az infrastruktúrákra jellemző hálózatszerűséget, de a részletesebb megfogalmazások a célkitűzéseket is hozzárendelik a működés jellegéhez. Láthatóvá válik, hogy napjaink információs társadalma és a technikai (virtuális) infrastruktúra között többoldalú, komplex függőség áll fenn.

A definíciók egyértelművé teszik ugyanakkor azt is, hogy az infrastruktúrákat alapvetően gazdasági szempontból szükséges vizsgálni, tekintettel arra, hogy elsősorban termékeket állítanak elő, amelyek igénybevétele nyomán egy folyamatosan működő rendszer jön létre. Az infrastruktúra által rendelkezésre bocsátott termék vagy szolgáltatás valamilyen formában eljut a fogyasztóhoz, akinél újra és újra szükségletként jelentkezik a szolgáltatásra irányuló igény. E tekintetben két csoportra oszthatjuk az infrastruktúrákat, attól függően, hogy gazdasági szempontból milyen típusú szolgáltatásokat tesznek elérhetővé.

2. ábra

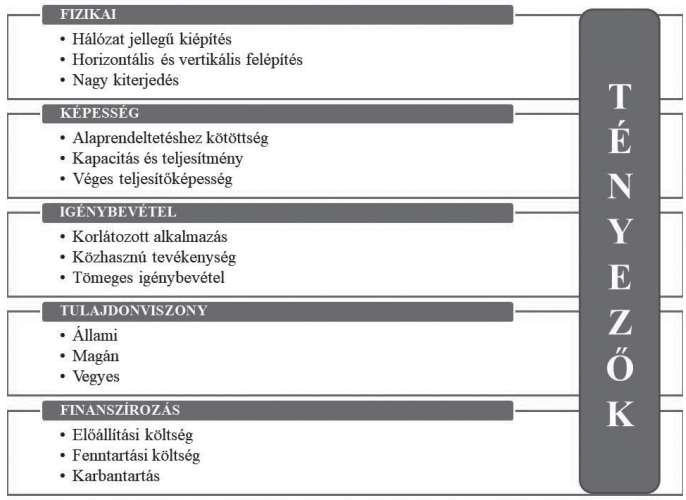
Az infrastruktúrák csoportosítása

Forrás: BONNYAI 2014

Az anyagi szolgáltatások közé elsősorban a gazdasági folyamatok működőképességét garantáló tevékenységek sorolhatók, úgymint pénzügy, kereskedelem, idegenforgalom, logisztika, szállítás (áru és személy), információszolgáltatás. Mindezek a gazdasági szektor állandó körforgását biztosítják, ténylegesen termékeket és szolgáltatásokat állítanak elő, amelyeket a fogyasztók részére szolgáltatási díj ellenében biztosítanak. Emellett a másik nagy kategória a nem anyagi szolgáltatások halmaza, amelybe a társadalom működését és fejlődését lehetővé tevő tevékenységek tartoznak. Az egészségügyi ellátás, a közigazgatás, a szociális ellátás, a védelmi igazgatás, valamint a közoktatás és a kutatás-fejlesztés azonban elsősorban szolgáltatási díj nélkül, alapvető jogként illeti meg a fogyasztót, amelyet ez esetben lakosságnak, társadalomnak nevezünk. Természetesen az effajta szolgáltatások léteznek önköltséges formában is, de elsősorban az állami gondoskodás keretében biztosítandó szolgáltatásként jellemzőek. (KOVÁCS 2012)

1.1.2. Az infrastruktúrák legfőbb jellemzői

Szintén a fogalmi meghatározásokból vezethetők le azok az alapvető tulajdonságok, amelyek az infrastruktúrákat – a szolgáltatás típusától függetlenül – jellemzik. A főbb sajátosságok már több szempontból utalnak azokra a specifikumokra, amelyek révén egy-egy infrastruktúrát kritikusnak tekinthetünk. A vizsgálat során öt alapvető tényező, és minden tényezőn belül három-három jellegzetesség különíthető el, amit a következő ábra szemléltet:



3. ábra

Az infrastruktúrák legfőbb tulajdonságai

Forrás: Bonnyai 2014

Fizikai létesítés szempontjából az infrastruktúrák *hálózat jellegű kialakítása, horizontális* és *vertikális felépítése,* valamint jellemzően *nagy kiterjedése* meghatározó (például: villamosenergia-hálózatok), ami a kölcsönös függőséget támasztja alá.

E tulajdonságokhoz szervesen kapcsolódnak az infrastruktúrára jellemző képességek. Az *alaprendeltetés szerinti alkalmazás* korlátozottsága különösen fontos, hiszen egy-egy infrastruktúra általában egy-egy szolgáltatás biztosítására képes (például: fűtési célra használjuk a vezetékes gázszolgáltatást és a távhőszolgáltatást is, de az infrastruktúrához tartozó elemek csak és kizárólag a saját termék továbbítására alkalmasak). Átfedéseket viszonylag ritkán találhatunk, csökkentve ezzel az alternatív lehetőségek kínálatát. Emellett meghatározó képesség a *kapacitás,* amely megadja, hogy időegység alatt milyen mennyiségű szolgáltatási *teljesítményt* képes nyújtani az adott infrastruktúra. Ennek rendkívüli jelentősége lehet, ha az – külső tényezők hatására – nem képes a megszokott teljesítmény biztosítására. Mindezzel szoros összefüggésben áll ugyanakkor a *véges teljesítőképesség,* amely minden egyes infrastruktúránál a sajátos működési feltételektől függ. E tulajdonság kifejezi, hogy a szolgáltatás határai – ez által a *korlátozott alkalmazás* – pontosan definiálhatók.

Az igénybevételi tényező szempontjából két, egymással jelentős mértékben összefüggő jellegzetességet kell kiemelni. A *közhasznú tevékenységet* ellátó infrastruktúrák (például: mobilkommunikációs hálózatok) kifejezetten a *tömeges igénybevétel* révén gyakorolhatnak hatást a lakosság nagyobb hányadának mindennapjaira. A közhasznú szolgáltatások ugyanis rendkívül széles körben elérhetők, ebből adódóan magas a fogyasztók száma. Mindez a normál működéstől eltérő esetekben hatványozott igénybevételt, esetenként működési zavart vagy leállást eredményezhet (például: szilveszteri telefonhívások számának ugrásszerű növekedése).

Mind nemzetközi, mind hazai viszonylatban igaz az a megállapítás, hogy az infrastruktúrák eltérő arányban vannak állami, önkormányzati és magántulajdonban, de több

szolgáltatástípus esetén előfordul, hogy *vegyes kezelés* jellemző. Ez bizonyos esetekben – a jogi szabályozástól függően – akár eltérő értelmezést és működést is előidézhet, amely a működési problémák kezelése során nehézségeket is okozhat.

Végül a finanszírozás kérdése merül fel. Tekintettel az ellátott feladatokra és a tömeges alkalmazásra, az infrastruktúráknak *előállítási és fenntartási költségeik* vannak, amelyekhez hozzátartozik a folyamatos és biztonságos működés garantálása érdekében történő *karbantartási tevékenység* is. Ezek olyan költségek, amelyekkel a tulajdonosok és üzemeltetők természetesen számolnak. Fontos azonban, hogy a szolgáltatási díj, amelyet a fogyasztók fizetnek, önmagában nem fedezi a működtetés, a fenntartás és a fejlesztés költségeit. Emiatt különösen fontos lehet, hogy ha az adott szolgáltatás kapcsán felmerül a kritikus infrastruktúrává történő kijelölés lehetősége, akkor az további anyagi kötelezettségekkel járhat.

Bizonyos infrastruktúrák működési zavarai a társadalom széles spektrumát érinthetik, amire a lakosság kifejezetten érzékenyen reagálhat. A hétköznapi életvitel folyamatosságát akadályozva az infrastruktúrákkal kapcsolatos rendkívüli események jelentős hatást gyakorolhatnak az érintettek mindennapjaira. Bizonyos esetekben, például a működési zavar elhárításának elhúzódása esetén, a nagyobb károk okozásának valószínűsége is növekszik, így a kialakuló helyzet lakosság életére gyakorolt hatása egyaránt súlyosbodhat (például az elhúzódó energiaellátási problémák és hatásaik más szolgáltatások működésére). (KOVÁCS 2012)

Az alapvető jellemzők és tulajdonságok mellett kiemelkedő jelentőségű az egyes infrastruktúrákat *veszélyeztető tényezők* köre. Olyan körülményeket értünk ezek alatt, amelyek az adott infrastruktúrára potenciálisan hatást gyakorló fenyegetés[1] jellege szerint különböztethetők meg. A 20. századra még jellemző, klasszikus háborús események és fegyveres konfliktusok a mai világ fejlett országaiban már kevésbé számottevőek. Egyre nagyobb jelentősége van azoknak a hadviselési módszereknek és egyéb eredetű kockázatoknak,[2] amelyek nehezen azonosítható veszélyforrásból származnak, hatásuk az emberi életre és az anyagi javakra előre nem prognosztizálható.

Mind a természetes, mind az épített környezetre jelentős hatást gyakorolhatnak olyan kihívások,[3] amelyeket az infrastruktúrák veszélyeztető tényezőiként azonosíthatunk. A hazai, modern értelemben vett kritikus infrastruktúra védelmi folyamatok első mérföldköve volt a nemzeti kritikus infrastruktúrák védelméről szóló *Zöld Könyv,* amely a veszélyeztető tényezők egyes csoportjait bevezette a szakmai terminológiába. Ezek alapján az infrastruktúrák potenciális veszélyeztető tényezőinek besorolása a következő:

Ártó szándékú cselekmények – alapvetően a tudatos károkozás céljából végrehajtott cselekedetek, amelyeknek az okozott anyagi kár mellett főként a társadalomra gyakorolt pszichológiai hatása lehet rendkívül jelentős:

---

[1] „A fenyegetések az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek legmagasabb megnyilvánulási szintjén, amikor a nemzeti érdekek sérülhetnek, és közvetve hatással lehetnek a nemzeti értékek megőrzésére." (BOGNÁR 2009, 14.)

[2] „A kockázatok az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek olyan megnyilvánulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek." (BOGNÁR 2009, 15.)

[3] „A kihívások az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek legalacsonyabb megnyilvánulási szintjén, amelyek eredői általában hátrányosan befolyásolják a belső és külső stabilitást és kihatással lehetnek egy adott régió hatalmi viszonyaira." (BOGNÁR 2009, 15.)

a) terrorcselekmények (például: 9/11 USA; 2004. Madrid; 2005. London; 2015. Párizs; 2016. Brüsszel),
b) kibertámadások (például: 2007. észtországi támadások; 2017. Wannacry),
c) társadalmi eredetű események (például: 2014. őszi zavargások Missouriban),
d) fegyveres konfliktus előidézése (például: 2014. polgárháború Ukrajnában, Szíriában),
e) gazdasági, politikai okkal elkövetett visszaélés.

Katasztrófa jellegű események – természeti, ipari vagy civilizációs eredettel bekövetkező események, amelyek bekövetkezési valószínűsége és gyakorisága csekély mértékben prognosztizálható, de jelentős következményekkel járhatnak:

a) természeti eredetű veszélyek (kiterjedést és anyagi kártételt figyelembe véve az egyik legsúlyosabb következménnyel járó eseménytípus, amely az elmúlt évtizedekben egyre szélsőségesebb formákat ölt),
   aa) hidrológiai események (például: ár- és belvíz, villámárvíz miatti korlátozások),
   ab) meteorológiai események (például: szélsőséges jelenségek miatti kiesések),
   ac) geológiai események (például: 2013. fonyódi partfalcsúszás miatti útlezárás),
   ad) kiterjedt vegetációs tűzesetek,
   ae) napkitörések (például: 1989. akadozások a kanadai távvezeték-hálózaton).
b) ipari eredetű veszélyek (technológiai hiba, helytelen emberi beavatkozás vagy baleset miatt az ipari termelés létesítményeiben, illetve azokkal kapcsolatosan bekövetkező helyzetek):
   ba) veszélyes anyagokkal foglalkozó üzemben bekövetkező esemény (például: 2012. Bad Fallingbostel, Németország, Kraft Foods),
   bb) közlekedési baleset veszélyes áru szállítása során (például: 2013. veszélyes anyagot szállító vonat balesete Baltimore-ban),
   bc) környezetkárosodással járó esemény (például: 2010. olajfúró platform elsüllyedése a Mexikói-öbölben),
   bd) egyéb ipari létesítményben bekövetkező esemény (például: hőerőmű-leállás),
   be) nukleáris létesítményben bekövetkező esemény (például: 2011. fukusimai atomerőmű földrengést követő nukleáris üzemzavara).
c) civilizációs eredetű veszélyek (a modern társadalom sajátosságaiból eredő események, amelyek az alkalmazott rendszerek és a társadalom működőképességére egyaránt hatást gyakorolhatnak):
   ca) informatikai, kommunikációs vagy navigációs rendszerek károsodása (például: űrobjektum becsapódása),
   cb) humánegészségügyi és állategészségügyi járványok (például: H5N1-pandémia),
   cc) éhínség és vízkészletekért folyó harc (például: migráció erősödése),
   cd) infrastruktúrák teljesítőképességének kimerülése.

Napjaink fejlettsége, a társadalmi rétegek között tapasztalható különbségek, a szélsőséges vallási és politikai nézeteket valló csoportok számának növekedése és időszakos megerősödésük, a világ terrorveszélyeztetettségének exponenciális növekedése mind okot szolgáltatnak arra, hogy a prevenciós szemlélet erősödjön.

1.1.3. A kritikus infrastruktúra mint fogalomrendszer

A korábbi definíciókból adódóan a kritikus infrastruktúra fogalmára is többféle meghatározás létezik. A kritikus infrastruktúra kifejezés új terminológiát jelent, de korántsem új keletű tevékenységet takar. A modern társadalmak igénytől, lehetőségtől, érdektől és szükségességtől függően eddig is tettek olyan védelmi célú intézkedéseket, amelyek a létfontosságúnak tekinthető rendszerek és az azok működését garantáló létesítmények biztonságát szavatolta. Ennek keretében a fejlett országok már a 20. század végén megalkották saját szempontrendszereik alapján a számukra létfontosságúnak minősíthető infrastruktúrák halmazát, tehát a kritikus infrastruktúra definícióját is.

Az *Amerikai Egyesült Államok* 1998-ban, a 63. elnöki irányelvben fogalmazta meg a kritikus infrastruktúrák védelmének alapjait, amely a fizikai és a kibertér olyan rendszereit tekintette kritikusnak, amelyek a gazdaság és a kormányzat működéséhez nélkülözhetetlenek (White Paper 1998). Ezt a megfogalmazást 2001-ben, a terrorellenes törvény szerves részeként pontosították, így az USA kritikus infrastruktúrának tekinti „mindazon fizikai vagy virtuális rendszereket és berendezéseket, amelyek oly létfontosságúak az Amerikai Egyesült Államok számára, hogy azok korlátozása vagy megsemmisülése meggyengítő hatással lenne a nemzetbiztonságra és a nemzetgazdaság biztonságára, a közegészségre, közbiztonságra vagy ezek bármely kombinációjára" (USA PATRIOT Act 2001, a szerző fordítása).

Szövetségi szinten az Észak-atlanti Szerződés Szervezete (a továbbiakban: NATO) 2001 óta minden stratégiai szintű dokumentumában szerepelteti a kritikus infrastruktúrák védelmének fontosságát. Ennek alapján a tapasztalatcserét, a kutatási folyamatokat, a nemzetközi együttműködés erősítését szorgalmazták elsősorban. Két évvel később, a 2003-ban elfogadott *Kritikus Infrastruktúra Védelmi Irányelvek* című dokumentumban a NATO is megalkotta saját, rendeltetéséhez illeszkedő kritikus infrastruktúra fogalmát, amely „azokat a létesítményeket, szolgáltatásokat és információs rendszereket jelenti, amelyek olyan létfontosságúak a nemzetek számára, hogy működésképtelenné válásuknak vagy megsemmisülésüknek gyengítő hatása lenne a nemzet biztonságára, a nemzetgazdaságra, a közegészségre, a közbiztonságra és a kormány hatékony működésére" (MUHORAY – BARTÁNÉ MUHARAY 2009).

Az elsősorban nem katonai célú szövetségi jellegre való tekintettel az *Európai Unió* kritikus infrastruktúra fogalma részletesebb, kifejezetten az Unió egységére irányul, de mégis általánosságban fogalmaz. Ennek megfelelően „azok a fizikai eszközök, szolgáltatások, információs technológiai létesítmények, hálózatok és vagyontárgyak" tekinthetők kritikus infrastruktúrának, „melyek megrongálása vagy elpusztítása súlyos hatással lenne az európaiak egészségére, békéjére, biztonságára, vagy gazdasági jólétére, illetve az EU és a tagállamok kormányainak hatékony működésére". [Green Paper, COM (2005) 576 final]

Hazánkban a kritikus infrastruktúrák azonosításáról és kijelöléséről szóló európai uniós irányelv alapján szintén kiemelt célkitűzés volt egy saját kritikus infrastruktúra definíció megalkotása. A szupranacionális szinttől a nemzeti önállóság felé haladva fokozatosan bővül a fogalom tartalma, ennek eredményeként egyre pontosabb és értelmezhetőbb lesz a meghatározás. Hazánkban a jogharmonizáció során többféle definíciót is nevesítettek, legkorábban a már említett hazai *Zöld Könyv*ben, majd később *a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény*

végrehajtási rendeletében (a továbbiakban: Kat. vhr.), illetve *a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényben* (a továbbiakban: Lrtv.) egyaránt. A kritikus infrastruktúra magyar értelmezését a hazai *Zöld Könyv* által megfogalmazottak írják le a legpontosabban. Eszerint „kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére" [Zöld könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról. A Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) kormányhatározat 1. sz. melléklete].

A kritikus infrastruktúrák legfontosabb jellemzőit a következő ábra szemlélteti:

4. ábra

A kritikus infrastruktúrák legfőbb jellemzői

Forrás: Bonnyai 2014

A kritikus infrastruktúra szempontjából legfontosabb jellemző a *függőség,* amely kettős eredetű lehet. Egyfelől az infrastruktúrák egymással való összekapcsolódását, *hálózatszerűségét,* másfelől a társadalom és az infrastruktúra kapcsolatát jellemezheti. Az egymástól való függőség, más néven az egymásrautaltság magában hordozza a lehetőségét annak, hogy mindkét érintett infrastruktúra megfeleljen a kritikusság feltételeinek. A mai fejlett, tudásalapú társadalom egyre több ilyen interdependenciát generál maga körül, amelyet az energetikai és informatikai rendszerektől való függőség határoz meg elsősorban.

A kölcsönös függőség miatt a rendszer sérülése során tényleges valószínűsége van annak, hogy az esemény „dominóelv"-szerűen egyfajta láncreakciót generáljon, és több infrastruktúra hálózatszerű működését, rendelkezésre állását befolyásolja. A villamos energia iránti szükséglet például az élet minden terén jelentkezik, rendelkezésre állása nemcsak az állami működés, hanem a lakossági fogyasztás szempontjából is kiemelkedő jelentőségű.

Egy bekövetkező esemény rosszabb szcenáriója esetén egy lokális probléma akár regionális kiterjedésű rendkívüli eseményt vagy veszélyhelyzetet is eredményezhet.

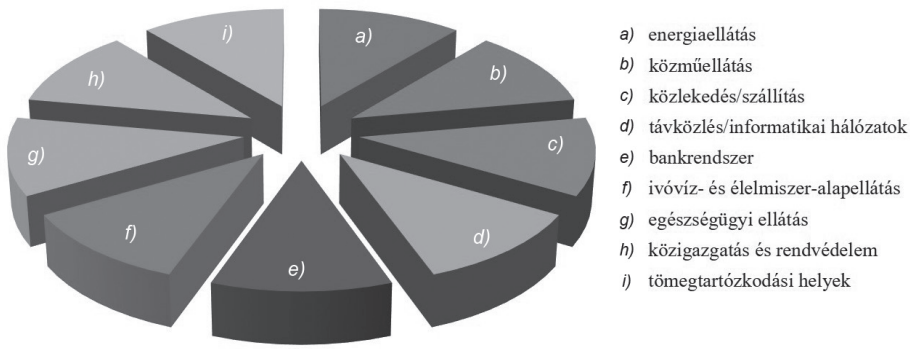
A függőséget további két sajátosság súlyosbíthatja. Egyrészt az adott infrastruktúra *sajátos működéséből* fakadóan is különböző veszélyeztetettségű lehet, tehát az üzemeltetésből eredő kockázati szint eleve magasabb. Az ilyen infrastruktúrák önmagukban is veszélyeket hordoznak, aminek eredményeként létesítésüktől kezdve veszélyforrásként tartják számon őket. Másrészt az adott infrastruktúra *kiterjedését és elhelyezkedését* vehetjük alapul, amelynek akkor van jelentősége, ha természeti eredetű kockázatok szempontjából nagyobb veszélynek van kitéve (például lemeztektonikai törésvonalak környékén, ár- és belvízzel veszélyeztetett területeken fekszik). Ez esetben az infrastruktúra normál működése alapvetően biztonságos, ugyanakkor a természetes környezetben bekövetkező, előre nem vagy ritkán prognosztizálható események következményei súlyosabb hatásokkal járhatnak.

A kritikus infrastruktúrák vonatkozásában külön specifikumnak tekintjük a fizikai védelemmel (létesítéssel, működéssel, üzletmenettel) kapcsolatos információk kezelési módját. Tekintettel arra, hogy egyes szolgáltatások – amelyeket kritikus infrastruktúrák biztosítanak – nélkülözhetetlenek a gördülékeny életvitelhez, kiemelt figyelmet kell szentelni a velük kapcsolatos *titokvédelemnek.* Az egyes infrastruktúrák azonosítási és a kijelölési eljárásában olyan információk alapján történik a döntéshozatal, amelyek érzékeny, minősített vagy titkos adatokat tartalmazhatnak. Megismerésük emiatt csak korlátozott körben történhet, figyelembe véve, hogy az ilyen adatokkal történő visszaélés alapjaiban ingathatja meg az adott infrastruktúra működőképességét. Ugyanakkor a titokvédelemnek nem kell kiterjednie azokra az alapvető információkra, amelyek az adott kritikus infrastruktúra működési sajátosságait, kiesésének következményeit a lakosság tájékoztatása szempontjából tartalmazza, tehát hozzájárulhat az érintett fogyasztók megfelelő információkkal történő ellátásához.

Végül az információs társadalom sajátos jellemzője, vagyis az informatikai rendszerektől való nagyfokú függősége teszi szükségessé, hogy az *informatikai védelem* fogalma szintén specifikum legyen. Az információs társadalom sajátossága, hogy működőképességét alapjaiban meghatározzák a rendelkezésére álló információs infrastruktúrák, amelyek önmagukban és más rendszerek részeként is képesek működni. Figyelembe véve azokat a funkciókat, amelyeket az információs infrastruktúrák biztosítanak, definiálásuk megfelelő módon fejezi ki a 21. századi függőség jelentőségét. E szerint „az információs társadalomnak […] szüksége van […] az információkat előállító, feldolgozó, továbbító stb. rendszerekre is, amelyeket gyűjtőnéven információs infrastruktúrának nevezünk. Ez a megkülönböztetés […] azt jelenti, hogy az általános infrastruktúra-halmazból kiemeltünk és kitüntetett szerepet adtunk egy olyan komplex infrastruktúra-részhalmaznak, amely az információs társadalom információellátásával és kezelésével foglalkozik" (VÁRHEGYI–MAKKAY 2000). A definíció alapján az információs infrastruktúrák megkülönböztetésének oka, hogy védelmük sajátos megközelítést igényel. Működésük legfőbb célja az információs társadalomban szükséges adatok, információk biztosítása, az általános rendeltetésű infrastruktúrák informatikai jellegű működési feltételeinek folyamatos garantálása. Emiatt legjellemzőbb tulajdonságuk a globális hálózatszerűség és függőség, az információs társadalom egyfajta létszükségleteként való működés. Mindez kellő alátámasztást ad az informatikai védelem kiemelt szerepének, amelyet mind az Európai Unióban, mind Magyarországon stratégiai szintű tervezési dokumentumokkal fejlesztenek. Az Európai Unió kiberbiztonsági straté-

giája az első olyan átfogó szakpolitikai dokumentum, amelyet az Európai Unió a témában létrehozott. A stratégia kiterjed a belső piacra, a bel- és igazságügyre, valamint a virtuális térrel kapcsolatos kérdések külpolitikai vetületeire. Magyarország Nemzeti Kiberbiztonsági Stratégiáját a Kormány a 1139/2013. (III. 21.) kormányhatározattal[4] fogadta el és tette közzé azzal a céllal, hogy a kibertérből érkező fenyegetésekkel kapcsolatban célkitűzéseket, alapelveket fogalmazzon meg, és a védekezés megvalósítása érdekében kormányzati eszközök útján megfelelő intézkedéseket tegyen.

A fentiekben ismertetett fogalmak és speciális jellemzők alapján a kritikus infrastruktúrák az általuk nyújtott szolgáltatások elsődleges rendeltetése szempontjából csoportosíthatók. A következő ábra olyan fő csoportokat szemléltet, amelyek a jogszabályi környezet megalkotása során nevesített szektorokkal harmonizálnak.



5. ábra

A kritikus infrastruktúrák általános csoportosítása a működés jellege szempontjából

Forrás: Bonnyai 2014

1.2. A kritikus infrastruktúrák védelme kialakulásának mérföldkövei

A kritikus infrastruktúrák védelmének új típusú megközelítése az elmúlt tíz év vívmánya, de már sokkal korábban is kiemelt védelmi célú tevékenységnek számított. Minden – ma már kritikusnak nevezett – infrastruktúra működéséért felelős állami vagy magánkézben lévő szervezet eddig is törekedett arra, hogy az általa biztosított szolgáltatás folyamatosságát szavatolni tudja. Minden állam alapvető érdeke, hogy a működőképességét biztosító államigazgatási apparátus és gazdasági rendszer fenntartásáról, valamint az állampolgárai élet- és vagyonbiztonságáról gondoskodjon. Ahhoz azonban, hogy a kritikus infrastruktúrák védelme érdekében szövetségi és közösségi szintű egységes fellépés valósuljon meg, olyan globális hatású eseményeknek kellett bekövetkezniük, amelyek ráirányították a nemzetek figyelmét a célirányos infrastruktúra-védelem szükségességére.

[4] Módosítása a jegyzet készítése időszakában is folyamatban van, várható megjelenése: 2018.

1.2.1. A védelmi célkitűzések változása a hidegháborútól napjainkig

A védelmi stratégiák kialakítása mindenkor a biztonság értelmezéséből indult ki. A biztonság olyan alapfeltétel, amely a létezés fenyegetettség nélküli állapotát fejezi ki, tehát vizsgálható az egyén szintjétől egészen a globális kiterjedés szemszögéig. Jelentése azonban az elmúlt évszázad során, a bekövetkezett történelmi fordulatoknak köszönhetően időről időre változott.

A *Bevezető – Biztonságpolitikai aspektusok* című fejezetben kifejtett változási tendenciák alapján kijelenthető, hogy a korábbi katonai veszélyeztetettség átfordult a tömeghadseregek és konvencionális háborúk időszakából a terrorizmus, a szervezett bűnözés megfékezését, a természeti csapások és az IT-rendszerek kihívásainak tudatos kezelését biztosítani képes korszakba. Ebből a biztonságpolitikai aspektusból nézve a biztonság összetevői (dimenziói) ma már komplex módon értelmezhetők, amibe a társadalmi, a politikai, a belügyi (rend- és katasztrófavédelmi), a gazdasági, a pénzügyi, a környezeti, a katonai, az informatikai, az egészségügyi biztonság egyaránt beleértendő. (BOGNÁR 2009)

Az elmúlt évtized tapasztalata azt mutatja, hogy a technikai és technológiai fejlődés a modern társadalom javát szolgálja, azonban ezek a rendszerek a természetes környezeti életfeltételek helyébe lépve a társadalom jelentős függőségét okozzák. Az effajta dependencia létét az ártó szándékú cselekmények elkövetői is felismerték. Ennek eredménye, hogy a biztonságos és megszokott életvitelt biztosító infrastrukturális háttér a 21. század hajnalára terrortámadások célpontjává vált. Ezek a támadások olyan nemzetközi szintű kezdeményezéseket indítottak útnak, amelyekből nemzetközi, uniós és tagállami konzultációk eredményeként megszületett egy új terminológia: a kritikus infrastruktúrák védelme.

A kritikus infrastruktúrák védelmének szükségessége olyan korba vezeti az emberiséget, ahol a komplex megközelítés, az egységes elvek alapján történő reagálás különösen nagy jelentőségű. A veszélyeztető tényezők szerteágazó jellege, a veszélyforrások különbözősége és a lehetséges következmények sajátosságai a kockázatfelmérés-kockázatbecslés-kockázatértékelés hármas tevékenysége által válnak azonosíthatóvá, a rendkívüli eseményekkel kapcsolatos reagálóképesség pedig tudatos tervezéssel alakítható ki.

1.2.2. Önálló kezdeményezések a 21. század hajnalán

A fejlett világ nemzetei az 1990-es években is rendelkeztek saját védelmi mechanizmusokkal, amelyekkel a folyamatos életvitelhez nélkülözhetetlen rendszereiket óvták bizonyos hatásokkal szemben. Az egyes országok különbözőségéből és sajátosságaiból fakadóan azonban ezek a rendszerek nehezen egyeztethetők össze egymással.

Az *USA* a hidegháború idején – főként a Varsói Szerződés országai[5] részéről feltételezett atomtámadások elleni védelemre összpontosítva – alkotta meg azokat az irányelveit, amelyek a kritikus infrastruktúrák védelmének mai szempontjaihoz hasonlóan a megelőzésre, felkészülésre irányuló kezdeményezések voltak. Az 1990-es években jelentek meg az első olyan elnöki rendeleti úton megtett intézkedések, amelyek főként az informatikai

[5] Egykori tagállamai: Szovjetunió, Albánia, Bulgária, Csehszlovákia, Lengyelország, Magyarország, Német Demokratikus Köztársaság, Románia.

és távközlési hálózatok védelmére irányultak. Mindemellett megkezdődött azon infrastruktúrák felmérése és meghatározása, amelyek az ország biztonsága, a nemzetgazdaság akadálytalan működése, valamint a mindennapi élet folyamatossága szempontjából létfontosságúak. A felmérés eredményeként a Clinton-kormány öt fontos szektort (energiaellátó rendszerek, banki és pénzügyi rendszerek, közlekedés és szállítás, egészségügyi rendszer és segélyszolgálatok, telekommunikációs rendszerek) nevezett meg 1997-ben, majd a következő évben kiadta a kritikus infrastruktúrák védelméről szóló elnöki iránymutatást (White Paper 1998). A 2001. szeptember 11-i eseményeket követően rövid idő alatt elfogadták az új terrorellenes törvényt *(Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. – USA PATRIOT ACT),* amely már konkrétabban és szélesebb körben határozta meg a kritikus infrastruktúrákat. A 2003-ban kiadott, majd többször módosított kritikus infrastruktúrák fizikai védelmére irányuló nemzeti stratégia *(The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets)* szektorokat és ágazatokat különített el, amelyek között az együttműködés koordinálását egy központi szövetségi kormányszerv, az Egyesült Államok Nemzeti Infrastruktúravédelmi Központja *(National Infrasturcture Protection Center – NIPC)* végzi napjainkban is. Még 1998-ban erre a feladatra hozták létre a Szövetségi Nyomozóiroda *(Federal Bureau of Investigation – FBI)* szervezetén belül működő Nemzeti Infrastruktúravédelmi Központot, amelynek feladatát 2004 óta a *Nemzeti Infrastruktúra-koordinációs Központ (National Infrastructure Coordinating Center – NICC)* látja el. Az NICC a kritikus infrastruktúrák védelmi rendszere országos hálózatának információs és koordinációs központja, koordinálja a 2003-ban nevesített 16 szektor védelmi célú tevékenységét. A központ 24 órás ügyeleti rendben készenléti megfigyelést végez, amelynek keretében elsősorban a veszélyeztető tényezőkkel kapcsolatos információk megosztásáért felelős. Funkcióját tekintve egyszerre lát el megelőzési, felkészülési, információmegosztási, elemző és értékelő, valamint döntéstámogató feladatokat. Az USA a kibertér biztonságára irányuló politikáját is fejlesztette, aminek révén a költségvetés 2009-ben és 2010-ben 40 milliárd dollárt különített el hálózatbiztonsági célokra.

Napjainkban az USA nyomatékossá tette a kritikus infrastruktúrák védelme kapcsán az együttműködés jelentőségét. Ennek értelmében a működőképesség biztosításának felelőssége közös érdek, amely szövetségi, állami, területi és helyi szinten, állami és magánkézben lévő intézmények összehangolt tevékenységén alapul. Emellett a Belbiztonsági Minisztérium *(US Department of Homeland Security)* fő feladata maradt, hogy a kritikus infrastruktúrák védelme tizenhat elkülönített szektora vonatkozásában a köz- és magánszféra részére stratégiai útmutatást nyújtson, illetve koordinálja a szövetségi szintű biztonsági intézkedések fejlesztését a kritikus infrastruktúrák ellenálló képességének növelése és biztonságuk szavatolása érdekében.

Nagy-Britannia és Észak-Írország Egyesült Királysága kritikus infrastruktúra értelmezése kismértékben tér el az amerikai meghatározástól, alapvető jellemzője, hogy a kritikusság fogalmát az egész ország nemzeti érdekeihez köti, és ez alapján alakított ki tíz szektort. A szektorokat fizikai és elektronikus/informatikai támadások által okozott károk hatásai alapján különböztették meg. Központi szinten a *Nemzeti Infrastruktúra Védelmi Központ (Center for the Protection of National Infrastructure – CPNI)* foglalkozik a kritikus infrastruktúrák védelmével, amelyet 2007-ben a Nemzeti Infrastruktúra Biztonsági Koordinációs Központ és a Nemzetbiztonsági Tanácsadó Központ egyesítésével hoztak

létre. A központ tanácsadó jellegű feladatköröket lát el az egyes szektorokba tartozó infrastruktúrák tulajdonosai, üzemeltetői felé, függetlenül attól, hogy azok köz- vagy magántulajdonban vannak-e. A szervezet tevékenységének fő célja a kritikus infrastruktúrák működőképességének fenntartása és védelme a fizikai, belső és informatikai eredetű támadásoktól, különös tekintettel a terrorizmusra. Ennek megfelelően napjainkban a fizikai, a személyi és a kiberbiztonság játszik főszerepet az Egyesült Királyság kritikus infrastruktúra védelmi tevékenységében. Kiemelt hangsúlyt fektetnek az együttes/kombinált hatásokra történő felkészülésre, azokra a veszélyeztető tényezőkre, amelyek akár egymás felerősítése által is jelentős fennakadásokat okozhatnak. Az elmúlt évek eredménye, hogy az állam működése szempontjából nélkülözhetetlen infrastruktúrák védelme ma már a Nemzeti Biztonsági Stratégia, a Terrorellenes Stratégia, a Kibervédelmi Stratégia szerves része. Mindehhez olyan nemzeti kockázatértékelési tevékenység párosul, amelynek eredménye egy *Országos Kockázati Nyilvántartás (National Risk Register),* amely a legmeghatározóbb potenciális veszélyhelyzeteket és azok körülményeit tartalmazza. Jelenleg tizenkét szektort tartanak nyilván, amelyekben kritikussági skála szerint azonosítják az egyes infrastruktúrákat. A besorolás három tényezőt vesz alapul: alapvető szolgáltatások szállítási rendszereire gyakorolt hatás, gazdasági hatás (veszteségek), alapvető szolgáltatások kiesésének hatása a mindennapi életre.

Németországban is a hidegháborús évek lezárását követően ismerték fel a kritikus infrastruktúrák védelmének fontosságát. 1990-ben alakult, majd 2001 augusztusában vált önálló intézménnyé az Információbiztonsági Szövetségi Hivatal *(Bundesamt für Sicherheit in der Informationstechnik – BSI),* amely a kritikus infrastruktúrák védelmével kapcsolatos feladatok koordinációját végzi a *Polgári Védelmi és Katasztrófa-elhárítási Szövetségi Hivatallal (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe)* szoros együttműködésben. A 2001. évi terrortámadás után a szervezet átértékelte az addig meghatározott és alkalmazott definíciókat, és nyolc ágazatot alakított ki. Ezt követően 2003-ban – az alapvető közműszolgáltatók állami szintű bevonásával – újradefiniálták a kritikus infrastruktúrák fogalmát, és kilenc szektort azonosítottak. A nemzetközi folyamatok előrehaladása által 2005-ben elkészült a *Nemzeti Kritikus Infrastruktúra Védelmi Terv (National Plan for Information Infrastructure Protection),* amely az infokommunikációs technológiák térnyerésére helyezte a hangsúlyt. Ezt követte a Kritikus Infrastruktúra Védelmi Stratégia 2009-ben, majd a kibervédelmi tevékenységek jelentőségének erősödése révén 2011-ben a Kiberbiztonsági Stratégia. Az érintettek közötti együttműködés elősegítése érdekében kidolgozták a Kritikus Infrastruktúra Védelmi Megvalósítási Tervet, és létrehoztak egy internetalapú platformot is, amely a központi szintű koordinációért felelős. Németországban a kritikus infrastruktúrák több mint 90%-a magánkézben van, ezért a német rendszer kevésbé centralizált, és különösen nagy figyelmet szentel az egyes infrastruktúra-tulajdonosok és -üzemeltetők szerepének hangsúlyozására, a köz- és magánszféra közötti koordináció és együttműködés erősítésére.

Szövetségi szempontból jelentős az Európai Unió mellett a *NATO,* amely rendeltetéséből fakadóan más típusú elvek és prioritások mentén kezeli a kritikus infrastruktúrák kérdéskörét. A NATO *Felsőszintű Polgári Veszélyhelyzeti Tervező Tanácsa (Senior Civil Emergency Planning Committee – SCEPC)* amerikai és kanadai kezdeményezésre dolgozta ki a kritikus infrastruktúrák védelmével összefüggő koncepcióját, és meghatározta a létfontosságú kritikus infrastruktúrák fogalmát. 2001-ben megtörtént a NATO-tagállamok

infrastruktúráinak feltérképezése, valamint az ezzel kapcsolatos tervezési tevékenység és készültségi szint felülvizsgálata. A kritikus infrastruktúrák védelmének égisze alatt a lakosságvédelem, a gazdaság működőképességének fenntartása, a katonai helyzetekben történő polgári segítségnyújtás és a polgári feladatokban való katonai szerepvállalás kapott hangsúlyt. Az elmúlt években a NATO-tagországok kutatási tevékenységeket folytattak a függőségek feltérképezésére, fejlesztették a CIMIC-képességet, meghatározták a kockázatkezelés elméleti alapjait, és megteremtették a szükséges szakértői hátteret is. 2003-ban a SCEPC elfogadta a Kritikus Infrastruktúrák Védelmével Kapcsolatos Vitaanyagot. A dokumentum azzal a célkitűzéssel jött létre, hogy a tagállamok rendelkezésére álló, a CBRN-eseményekkel kapcsolatos felkészülésre és a következmények kezelésére – illetve bizonyos mértékig a természeti katasztrófák elhárítására és a kritikus infrastruktúrák védelmére is – szolgáló eszközök fejlesztését ösztönözze. Kiemelt tevékenységként ismerte el továbbá

- a közreműködők közötti információmegosztás támogatását,
- az oktatási és képzési programok fejlesztésében történő közreműködést,
- a kritikus infrastruktúrák azonosításában való részvételt, valamint
- a fentieket támogató kutatási és fejlesztési projektek keresését egyaránt.

A NATO ez irányú tevékenységének másik pillére a 2004-ben elfogadott Terrorizmus Elleni Harc Munkaprogramja *(Programme of Work on Defence Against Terrorism),* amelynek célja a katonai eszközök és alakulatok védelmét szolgáló legmodernebb technológiák fejlesztésének elősegítése. A munkaprogram tíz prioritása közül a kritikus infrastruktúrák védelme az egyik, amelynek keretében a katonai „know-how" és a stratégiai célpontok (például: repülőterek, kommunikációs hálózatok stb.) védelmének fokozásával kapcsolatos képességek fejlesztése zajlik. Az egyes Tervező Tanácsok és Bizottságok a Miniszteri Irányelvek alapján munkatervüknek megfelelően szintén foglalkoztak a kérdéskörrel. A NATO Felszíni Közlekedés Tervező Tanácsa 2005-ben kérdőívet juttatott el a nemzetekhez a vasúti, közúti és belvízi hajózás területén a közlekedési infrastruktúra kritikus elemeinek, ezek védelmének szabályozása, valamint a kapcsolatos szervezeti háttér és információáramlás feltérképezése érdekében. A NATO Ipari Tervező Tanácsa külön ad hoc munkacsoportja foglalkozik az energetikai vonatkozású kritikus infrastruktúrák védelmével, és vizsgálja a NATO szerepvállalásának lehetőségeit.

2006-ban a tagállamok megerősítették a kritikus infrastruktúrák védelmében betöltött szerepüket, hangsúlyozták, hogy az alapvető szolgáltatások folyamatos rendelkezésre állását érintő zavarok a Szövetség érdekeit is érinthetik. A NATO-nak tehát nem célja önálló szabályozás kialakítása, ugyanakkor természetesen nem hagyhatja figyelmen kívül a tagállamokban potenciálisan bekövetkezhető események határon átnyúló, akár szövetségi érdekeket is befolyásoló jellegét. (Bonnyai 2014)

A kibervédelmi képességek egyik fő letéteményese ma a NATO. 2008 elejére körvonalazódott a NATO új kibervédelmi stratégiája, amely lefektette a szövetség kiberpolitikájának három alappillérét: a biztonság, a szubszidiaritás és a párhuzamosságok kiiktatása. A 2010-es lisszaboni döntés értelmében a kibervédelem kiépítése folyamatosan és önállóan napirenden lesz a NATO stratégiai célkitűzései között. Az új stratégiai célok kidolgozása mellett a NATO végrehajtja olyan már meglévő struktúrák szükséges megújítását, mint amilyen például a NATO Számítógépes Biztonsági Események Kezelése *(Computer Incident Response Capability – CIRC).* Fő cél egy továbbfejlesztett „Kibervédelem 2.0"

kialakítása a teljes körű védelem érdekében. Érdemes megemlíteni azt is, hogy a válságövezetekben a NATO olyan „ernyőt" hozott létre, amely a kommunikáció biztonságát hivatott szavatolni.

Lényegében minden biztonsággal összefüggő uniós tevékenység az ENSZ-célkitűzésekhez kapcsolódik. Az ENSZ Európai Gazdasági Bizottsága (a továbbiakban: ENSZ EGB) 2006 februárjában tartott kerekasztal-megbeszélésén foglalkozott első ízben, alapvetően a közlekedési infrastruktúra terrortámadások elleni védelmének kérdéseivel. Az ENSZ EGB egyetért az ENSZ Közgyűlésének 58/199. sz. határozatában foglalt felhívással, amely szerint szükséges *a kibervédelem globális kultúrájának megteremtése és a kritikus informatikai infrastruktúrák védelme*. Tekintettel arra, hogy a kritikus informatikai infrastruktúrák biztonsága és ellenálló képessége szempontjából az országok kölcsönösen függnek egymástól – ahogyan egy lánc is csak annyira erős, amennyire a leggyengébb láncszeme –, aggodalomra adhat okot, hogy mindeddig csupán 9 tagállam alakított ki számítástechnikai eseménykezelő csoportot *(Computer Emergency Response Team – CERT),* és lépett be az Európai Kormányzati CERT-ek Csoportjába (EGC).

1.2.3. Terrortámadások és következményeik

A kritikus infrastruktúrák védelme mai értelemben vett folyamatainak megjelenését a 21. század nagyobb terrortámadásaihoz vezethetjük vissza. Az új generációs terrorizmus egyik legmeghatározóbb eseménye a *2001. szeptember 11-én* az USA ellen elkövetett támadássorozat volt, amely igazolta, hogy a terroristák is felismerték a társadalom mindennapjaira közvetlen hatással lévő rendszerek sebezhetőségét. A hajdani Világkereskedelmi Központ ikertornyai és a Védelmi Minisztérium székhelyeként működő Pentagon ellen intézett támadások több aspektusból alátámasztották, hogy a legnagyobb gazdasági és katonai potenciállal rendelkező ország sincs megfelelően felkészülve olyan eseményekre, amelyek egyik pillanatról a másikra, azonosítatlan eredettel következnek be, és jelentős következményeket idéznek elő.

2004 tavaszán a terrorizmus globális jellegét alátámasztó robbantások rázták meg a világot, ezúttal európai földön, Madridban. A *spanyolországi terrorcselekmény* célkitűzése azonban túlmutatott az elrettentés szándékán, és sokkal inkább a kormányba vetett bizalom megtörését célozta. A támadás elsősorban nem a nagyszámú emberáldozatra, hanem a minél jelentősebb károkozásra és pánikkeltésre irányult. E szándéknak kifejezetten megfelelt a madridi nagy kiterjedésű, stratégiailag fontos és fejlett főpályaudvar, amelynek hálózatszerűsége miatt a robbantások közvetett hatása országszerte érezhető volt. A robbantást követően oly mértékben megrendült a társadalom kormányba vetett bizalma, hogy az akkori spanyol kormányfő 8 éves kormányzás után megbukott a terrortámadást követő héten tartott választásokon. Az új elnök első intézkedései között gondoskodott a spanyol katonai erők Irakból történő kivonásáról, amellyel jelezte Spanyolország közel-keleti konfliktusoktól való távolmaradási szándékát. Ebben az esetben konkrétabban látható, hogy a lakosságot kiszolgáló létesítmények sebezhetőségi indexe magas, így a védelmüket garantáló biztonsági intézkedéseket különösen magas prioritással kell kezelni.

A kulcsfontosságú események másfél év elteltével tovább bővültek, amikor *2005 júliusában* újabb robbantásos merényletek erősítették fel az európai nemzetek félelemérzetét.

A *londoni* metróhálózat ellen intézett támadás több hasonlóságot mutatott a madridi eseményekkel. A *robbantás* időzítése egy jelentős nemzetközi-politikai döntéshez is köthető. A robbantások előtt egy nappal derült ki, hogy a brit főváros elnyerte a 2012. évi, nyári olimpiai játékok rendezési jogát. A támadás magas színvonalú szervezettségét támasztja alá, hogy a hat metróállomás felrobbantása után egy olyan buszon történt detonáció, amely a leállított metróforgalom pótlására indult. A terroristák tehát azonosítottak egy olyan szolgáltatáscélú rendszert, amelynek sérülése jelentős káoszt, és a lakosság körében pánikot eredményezett. Mindezt tovább fokozta, hogy a túlterheltség miatt a támadásokat követő órákban nemcsak a közel tízmilliós lélekszámú Londonban, hanem a környéken is összeomlott a mobiltelefon-szolgáltatás.

***

Ezek az események rövid idő alatt egyértelműsítették, hogy egy állam biztonságát, a nemzetgazdaság működését, valamint az állampolgárok jólétét garantáló infrastruktúrák, illetve az azok által nyújtott szolgáltatások létfontosságúak, így azok védelmére különleges jogrendi szabályozás vagy sajátos intézkedések szükségesek.

Felhasznált irodalom

Bakos Ferenc (1983): *Idegen szavak és kifejezések szótára.* Budapest, Akadémiai Kiadó.

Bognár Balázs (2009): *A Magyar Köztársaság védelmi igazgatási rendszerének lehetséges korszerűsítése.* Doktori értekezés. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem.

Bonnyai Tünde (2014): *A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében.* Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem.

Cecei Katalin – Mórocz Attila (2004): Klímaváltozás és a kritikus infrastruktúra. *AGRO-21 Füzetek,* 36. sz. 32–63.

Idegen szavak gyűjteménye. http://idegen-szavak.hu/infrastrukt%C3%BAra. (Letöltés ideje: 2011. 08. 08.)

Kovács Ferenc (2012): *„A kritikus infrastruktúra védelme I." c. tantárgy.* Jegyzet. Budapest, Nemzeti Közszolgálati Egyetem.

Muhoray Árpád – Bartáné Muharay Irén (2009): A kritikus infrastruktúra védelem társadalmi és gazdasági kihatásai. *Szakmai Füzetek,* 26. sz. 14–19.

Várhegyi István – Makkay Imre (2000): *Információs korszak, információs háború, biztonságkultúra.* Budapest, Országos Műszaki Információs Központ és Könyvtár.

Hivatkozott jogszabályok és dokumentumok

Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról. COM (2005) 576 final, Brussels, 17. 11. 2005. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52005DC0576&from=HU (Letöltés ideje: 2018. 07. 24.)

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003). Washington, The White House. Elérhető: www.hsdl.org/?view&did=1041 (Letöltés ideje: 2018. 07. 24.)

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). Elérhető: www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (Letöltés ideje: 2018. 07. 24.)

White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection. Presidential Decision Directive 63, May 22, 1998. Elérhető: https://fas.org/irp/offdocs/paper598.htm (Letöltés ideje: 2018. 07. 24.)

Zöld könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról. A Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) kormányhatározat 1. sz. melléklete.

2. fejezet
Európai uniós szabályozás

Bonnyai Tünde

2.1. Globalizáció a védelmi tevékenység kapcsán

Az elmúlt évtizedben a kritikus infrastruktúrák védelme nemzetközivé válásának lehettünk tanúi. Világossá vált, hogy ebben a feladatrendszerben az állam alapvető feladata a belső rend megteremtése, a társadalmi és gazdasági viszonyok fenntartása, alapvető szolgáltatások biztosítása, a külső védelem biztosítása, de az is látható, hogy a globalizáció folyamatának tulajdoníthatóan a világ fokozatosan egységessé és egymástól függővé válik. A hidegháborút követően kialakult környezetet az egyre nyitottabb határok jellemzik, ahol a belső és külső biztonsági szempontok feloldhatatlanul összekapcsolódnak.

A 2001. szeptember 11-i New York-i merénylet sokkolta az egész világot, de Európa ekkor még nem számolt azzal, hogy bármely uniós tagállam is célponttá válhat. A 2004. márciusi madridi terrortámadás eseménye azonban rávilágított arra, hogy az egyes szolgáltatások, infrastruktúrák működési zavarai, a köztük fellelhető interdependenciák révén milyen pusztítás okozható a társadalomban mind humán, mind gazdasági tekintetben. Az esemény rávilágított arra is, hogy globálisan új típusú, új megközelítésű és aktívabb biztonsági intézkedésekre van szükség.

A globalizáció nem egyformán hat életünk minden területén, de a biztonság területén markánsan érzékelhető. Ennek kapcsán a kritikus infrastruktúrák védelme olyan prioritást élvező, kiemelten kezelt biztonságpolitikai kérdéskörnek tekinthető, amelynek kapcsolódási pontjai a biztonság minden szegmensét érintik. A kritikus infrastruktúrákterrorcselekményekkel, természeti katasztrófákkal és balesetekkel szembeni védelme érdekében fontos, hogy az infrastruktúrák működésének megzavarása vagy manipulálása megelőzhető, kivédhető, illetve lehetséges mértékben rövid idő alatt kezelhető legyen.

A létfontosságú infrastruktúrák védelme tekintetében az USA, az ENSZ, a NATO és az EU vitathatatlanul globális szereplő. Az USA elsősorban műszaki aspektusból, majd később általános biztonságpolitikai kontextusban foglalkozott e témával. A következőkben az Európai Unió módszertanát vizsgáljuk meg részletesen.

2.1.1. A kritikus infrastruktúrák védelmének fejlődése Európában

A 2001-ben elkövetett terrortámadások indították meg közvetlenül azt a napjainkban is zajló cselekvési hullámot, amely az Európai Unió történetében elhozta a kritikus infrastruktúrák védelmére irányuló egységes jogi szabályozás igényét. A visszaszoruló hagyományos

hadviselés helyét az új, nehezen azonosítható fenyegetések vették át, amelyek egyre inkább a lakosság elrettentésére és károkozásra irányulnak.

A tengerentúli tapasztalatok és néhány uniós tagállam meglévő gyakorlata alapján kezdődött meg az kritikus infrastruktúrák védelemre vonatkozó uniós projekt kidolgozása. A kezdeményezés elsődleges célja volt, hogy nem tagállami, hanem együttműködésen alapuló, közösségi szintű program alakuljon ki, amely ötvözi az uniós szabályozást a tagállami jellegzetességekkel. *2003-ban* első lépésként elfogadták az *Európai Biztonsági Stratégiát*.

Az Európai Tanács 2004. júliusi ülésén, a közelmúlt terrortámadásai révén, nyomatékos hangsúlyt kapott az európai állampolgár biztonságérzete, vagyis az, hogy egy európai átlagember mit vár el a hétköznapok biztonságával kapcsolatban. Az a tény, hogy erre a kérdésre eltérő válaszok adhatók, rávilágított arra, hogy új típusú, új megközelítésű és aktívabb biztonsági intézkedésekre van szükség. Ennek érdekében megerősítették a nemzetközi együttműködési módszerek (ENSZ, USA, harmadik országok) fontosságát, továbbá egyetértés született arról, hogy a tagállamoknak fel kell mérniük a potenciális terrortámadásokra vonatkozó reagálási képességük szintjét. Ezzel párhuzamosan az Európai Bizottság felkérést kapott a kritikus infrastruktúrák védelmére összpontosító, átfogó stratégia 2004. év végéig történő előkészítésére.

2004 októberében az Európai Bizottság közleményt adott ki a terrorizmus elleni küzdelem és a kritikus infrastruktúrák védelmének összefüggéseiről. A közleményben az európai szintű megelőzés és felkészültség javítására vonatkozó javaslatokat fogalmaztak meg, különös tekintettel a kritikus infrastruktúrákat érő potenciális támadásokra. Alig egy hónappal később az Európai Tanács megbízást adott az Európai Bizottság részére, hogy a tagállamok integrált és koordinált megállapodások útján, 2006. I. félév végéig gondoskodjanak kritikus infrastruktúráik védelméről.

Az Európai Tanács *2004. decemberi* ülésén elfogadták a *Kritikus Infrastruktúrák Európai Programjának* (European Programme for Critical Infrastructure Protection, a továbbiakban: EPCIP) kialakítására vonatkozó *előterjesztést,* amely alapján meghatározták a terrorizmus elleni harc jövőbeli főbb irányvonalait:

- gyakorlati és operatív együttműködés erősítése,
- igazságügyi és hírszerzésbeli együttműködés, határbiztosítás,
- terrorizmus anyagi vonzatainak hatékony akadályozása,
- polgári védelmi tevékenységek fejlesztése,
- külpolitikai tárgyalások folytatása a harmadik országokkal,
- magán- és közszféra közötti partnerség kialakítása.

A terrorizmus elleni harccal kapcsolatos akcióterv részeként jelent meg az EPCIP mint a potenciális, határokon átnyúló hatásokkal szembeni védelem alapja, amelyet 2005 végéig kellett kidolgozni. *2005 januárjában* a Hágai Programot[1] és a közös kezdeményezést üdvözölve egy konkrétabb célkitűzéseket tartalmazó *javaslatot* dolgoztak ki. Mindez egy többéves kutatási projekt megkezdését szorgalmazta az unió területén található kritikus infrastruk-

[1] A Hágai Programot az Európai Bizottság 2004. november 4–5-i ülésén fogadták el. A program tíz prioritást határozott meg, amelynek keretében további együttműködést szorgalmazott a menekültügy és a bevándorláspolitika területén, kitért a határokon átívelő válságok közös kezelésének szükségességére, különös tekintettel a szervezett bűnözés és a terrorizmus kihívásaira, ugyanakkor a terrorizmus elleni küzdelem részeként kezelte a kritikus infrastruktúrák védelmét.

túrák sebezhetőségének feltérképezésére. A projekt egy közös európai kockázatelemzési rendszer kidolgozását, valamint olyan információmegosztásra alkalmas felület kialakítását javasolta, amely révén a tagállamok, a Bizottság és a Tanács az említett infrastruktúrákkal kapcsolatos tevékenységet folyamatosan nyomon tudja követni. Tartalmazta egy állandó válságkezelő központ életre hívását is, a tagállami és európai szinten működésben lévő korai figyelmeztetési *(early warning system)* és sürgősségi rendszerek *(emergency system)* összefogására vonatkozóan. Fentiek alapján 2005 júniusában az Európai Parlament kiadta *a terrorizmus elleni küzdelem keretében a létfontosságú infrastruktúra védelméről szóló EP ajánlását (2005. június 7.).* A dokumentumban hangsúlyozták az egységes uniós módszer létrehozásának szükségességét, a kritikus infrastruktúrák meghatározásának igényét, valamint a veszélyeztetett infrastruktúrák védelmére vonatkozó közösségi megoldások kidolgozásának elvárását egyaránt.

A londoni robbantások utáni, *2005. július 13-án* tartott rendkívüli tanácsülésen a tagállamok megerősítették a *terrorizmus elleni harc melletti határozott elkötelezettségüket.* Ehhez kapcsolódóan hangsúlyozták, hogy az uniós állampolgárok és a kritikus infrastruktúrák védelmére irányuló egységes fellépéssel törekedni kell a fenyegetettség és kiszolgáltatottság csökkentésére. A Tanács egyúttal felkérte a tagállamok képviselőit, hogy sajátosságaiknak megfelelően kezdjék meg veszélyhelyzeti reagálóképességük hatékony fejlesztését, járuljanak hozzá a megfelelő szintű és tartalmú információcseréhez, valamint a felkészültség szinten tartása és a megelőzés érdekében szervezzenek önálló, komplex, nemzetközi gyakorlatokat is.

A fenti folyamatok eredményeként *2005 novemberében* a Bizottság kiadta a kritikus infrastruktúrák védelmére vonatkozó európai programról szóló *Zöld Könyv*ét,[2] amely a leendő EU-s programmal kapcsolatos alapvető elméleteket, célkitűzéseket, definíciókat és intézkedéseket rögzítette. A dokumentum elfogadása új fejezetet nyitott az európai program kialakításának folyamatában, tekintettel arra, hogy alapvetően egy vitaindító, konzultációs dokumentumként került nyilvánosságra. A *Zöld Könyv* elsődleges célja volt, hogy felhívja a figyelmet egy-egy terület megválaszolatlan kérdéseire, illetve aktív együttműködésre ösztönözze az egyes szektorok képviselőit. A dokumentum megjelenésével párhuzamosan meghatároztak egy úgynevezett *konzultációs időszakot* is. Az útmutató jellegű uniós *Zöld Könyv*re kifejezetten optimistán és pozitív hozzáállással reagáltak a tagállamok, annak ellenére, hogy az a tagállamokra nézve kötelező feladatkörök tervezetét is tartalmazta. Az egyéves konzultációs periódus során – akkor még 25 tagállamból – 22 ország adott hivatalos választ, valamint mintegy száz észrevétel és javaslat érkezett a magánszféra részéről. A vélemények összességében elismerték a *Zöld Könyv* tartalmát.

A dokumentumban megtalálhatók voltak azok az alapvető fogalmak, elvek, eljárások és végrehajtási módszerek, amelyek keretet adtak a későbbi európai program megvalósításához. A célkitűzés a kritikus infrastruktúrák folyamatos rendelkezésre állásának feltételeit garantáló védelem biztosítása, a sebezhető pontok csökkentése, valamint azonnali, bevált beavatkozási és hatékony helyreállítási eljárások rendszeresítése. Ennek megvalósítása érdekében időszakos felülvizsgálati ciklusokat terveztek be, hogy a változó kihívásoknak és igényeknek való megfelelés biztosítható legyen.

---

[2] A dokumentum pontos címe: Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról. COM (2005) 576 final.

A *Zöld Könyv*ben foglaltak szerint a kritikus infrastruktúrák védelme *három fő pilléren* (megelőzés, felkészülés, ellenálló képesség) támaszkodva törekszik az infrastruktúrák biztonságos működését elősegítő intézkedések megtételére. A *megelőzés* időszaka főként a különböző leállások, meghibásodások kockázatának lehető legkisebb mértékű szintre történő csökkentésére irányul. Ennek tükrében a megelőzési tevékenységek közé soroljuk:

– a veszélyeztető tényezők elemzését,
– a kockázatok feltérképezését és
– a legérzékenyebb pontok beazonosítását,

amelyek alapján meghatározható a szükséges védelmi szint is.

A *felkészülés* fázisa elsősorban a tulajdonosok, üzemeltetők, felügyeleti szervek és központi államigazgatási szervek felkészítését, valamint a lakosság általános értelemben vett felkészítését jelenti. A legfőbb cél az, hogy az érintettek között aktív kommunikáció és eredményes együttműködés alakuljon ki. Az *ellenálló képesség* kialakításához további három összetevő szükséges. Elsődleges ezek közül az alternatívák biztosítása a kieső szolgáltatás mielőbbi pótlásának érdekében. Ehhez kapcsolódik a bekövetkezett esemény utáni, minél rövidebb idő alatt történő visszaállítás képessége, végül pedig a sebezhető pontok számának csökkentése. Utóbbi eredményeként az infrastruktúra ellenálló képessége nő.

A *Zöld Könyv* stratégiai dokumentumként *három védelmi stratégiát kínált* a későbbi irányelv kidolgozásához, amelyekre az európai kritikus infrastruktúra védelmi tevékenység felépíthető:

– mindenfajta veszéllyel szembeni védelem: összetett megközelítés, amely számol a szándékos, ártó jellegű támadásokkal és a természeti katasztrófák veszélyeivel egyaránt, ellenben a terrorizmust nem kezeli kiemelt kihívásként;
– mindenfajta veszéllyel szembeni védelem, különös tekintettel a terrorizmusra: komplex és rugalmas megközelítés, amely tekintettel van az egyéb támadásokból származó fenyegetésekre és a természeti katasztrófák okozta veszélyekre, de középpontjában az ártó szándékú cselekmények általi veszélyeztetettség, vagyis a terrorizmus áll;
– a terrorveszélyekkel szembeni védelem: kifejezetten a terrorizmusra összpontosító megközelítés, amely nem tekint prioritásnak más egyéb veszélyeztető tényezőt.

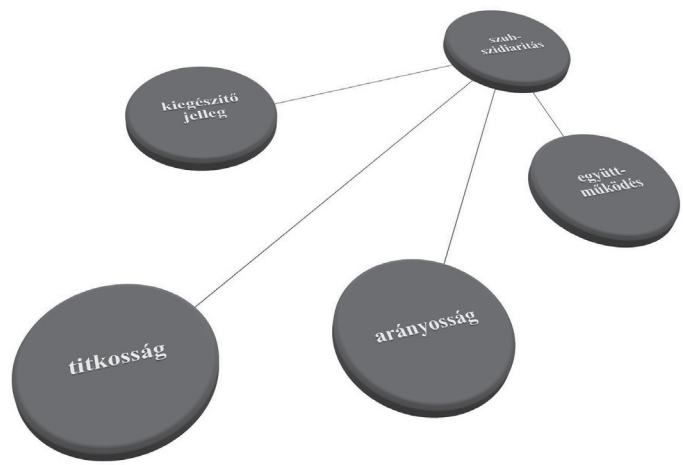
Ahhoz, hogy uniószerte megvalósulhasson a fentiek alapján kidolgozott védelmi tevékenység, különbséget kellett tenni európai és nemzeti kritikus infrastruktúrák között. A *Zöld Könyv* alapján az elsődleges és magasabb szintű kritikus infrastruktúrákat nevezzük *európai kritikus infrastruktúráknak* (European Critical Infrastructure, a továbbiakban: ECI). Olyan elemekre állapítható meg az európai szint, amelyeknél a létesítésből vagy a kialakuló helyzetekből fakadóan a határon átnyúló hatás lehetősége fennáll. Az ilyen infrastruktúra sérülése az adott tagállamon kívül más ország biztonságát is veszélyezteti, tehát akár regionális vagy globális szintű fenyegetésekhez vezethet. Tekintettel arra, hogy az EPCIP-kezdeményezéseket megelőzően a legtöbb tagállam két- vagy többoldalú megállapodások kötésével rendezte a határ menti veszélyeztetettségből fakadó feladatokat és felelősségeket egymás között, az EPCIP kiegészíti ezeket a már meglévő egyezményeket, vagyis európai szintre fejleszti őket.

A másodlagos, de a tagállamok szempontjából ugyanúgy kiemelt jelentőségű halmazt alkotják a *nemzeti kritikus infrastruktúrák* (National Critical Infrastructure, a továbbiakban: NCI). Az ilyen infrastruktúrák létesítésüket tekintve egy adott tagállam területén találhatók, és sérülésük, leállásuk, megsemmisülésük esetén hatásuk is kizárólag az ország határain belül érezhető.

Fentieken túl a *Zöld Könyv* felhívta a figyelmet az EU területén kívül található olyan infrastruktúrákra, amelyek esetleges üzemzavara vagy megsemmisülése hatással lehet az Európai Unió tagállamaira, azok infrastruktúráira, kormányzati, gazdasági, egyéb működésére. A 2006-os finn elnökség[3] ideje alatt kezdődött meg a kritikus infrastruktúrák védelme *külső dimenziójának* erősítése. Ennek keretében olyan harmadik országokkal kialakított együttműködések biztosítanak széles körű tapasztalatszerzési lehetőséget, mint az Amerikai Egyesült Államok, Kanada, Izrael, Japán, Oroszország és az Európai Környezetvédelmi Ügynökség[4] (European Environment Agency). Az együttműködési területeket négy fő célkitűzés mentén azonosították:

- meglévő tapasztalatok általános cseréje,
- együttműködés a kijelölt ECI-kel kapcsolatban,
- együttműködés harmadik országokbeli kritikus infrastruktúrákkal kapcsolatban,
- a kritikus infrastruktúrák kapacitásának növelése a partnerországokban.

A *Zöld Könyv*ben megfogalmazott öt fő alapelv körvonalazza a tagállami védelmi mechanizmusok kereteit, amelyek a következők:



1. ábra
KIV-alapelvek

Forrás: Bonnyai 2014, 47.

[3] Finnország 2006. július 1-től 2006. december 31-ig látta el az Európai Unió Tanácsának soros elnökségét.

[4] European Environment Agency (EEA), megalapozott és független tájékoztatást ad a környezetvédelmi és környezetbiztonsági kérdésekben, a környezet javításáról, a környezetvédelmi szempontokról és a fenntarthatósági tevékenységről. Az 1993 óta Koppenhágában működő ügynökség munkájában jelenleg – az Európai Unió tagállamain kívül – Izland, Liechtenstein, Norvégia, Svájc és Törökország vesz részt, míg Albánia, Bosznia-Hercegovina, Macedónia, Montenegró és Szerbia együttműködő országként szerepel.

A középpontba a *szubszidiaritás* került, amely szerint a kritikus infrastruktúrák védelme elsősorban nemzeti hatáskör, tehát az elsődleges felelősségi szintet a tagállamhoz kell delegálni. Szervesen kapcsolódik ehhez a *kiegészítő jelleg,* amely hangsúlyozza, hogy a meglévő tagállami együttműködések alapján, azok kiegészítésével alakul ki az uniós szintű *együttműködés* és koordináció a kritikus infrastruktúrák védelme területén. A Bizottság állásfoglalása szerint mindehhez a *titkosság* elvére van szükség annak érdekében, hogy a kritikus infrastruktúrákkal kapcsolatos információk illetéktelen kézbe kerülése elkerülhető legyen. Ezzel csökkenthető a váratlan, súlyos események száma, illetve az infrastruktúrák manipulálásának valószínűsége. Összességében pedig minden szabályozásnak kiemelt figyelemmel kell lennie arra, hogy a jogi háttér, az intézkedések és eljárások *arányosak* legyenek a megállapított fenyegetések által hordozott veszély tényleges szintjével.

Az alapelvek rendszerét két úgynevezett sarokpont teszi teljessé. A „rész-egész elv" és a „leggyengébb láncszem effektus" alapvetően meghatározza, hogy a kritikus infrastruktúrák jellemzőit, veszélyeztetettségét, kiszolgáltatottságát és ezeken alapuló védelmét csak komplexitásában lehet vizsgálni. Az első tényező értelmében az infrastruktúrákat önmagukban és egy rendszer részeként egyaránt értelmezhetjük, tehát a sebezhetőség szempontjából is figyelembe kell venni mindkét faktort. A második arra utal, hogy egy több elemből álló rendszer védelme mindig annyira zárt és hatékony, amennyire a leggyengébb pontja megfelel a biztonságos üzemelés kritériumainak.

Az első jogi aktus megtételét megelőzően a *Zöld Könyv* egyre szélesebb körben történő megismerése alapvetően pozitív visszhangot váltott ki az unión belül. Az Európai Unió Tanácsa egyetértését fejezte ki a tekintetben, hogy a kritikus infrastruktúrák védelme tagállami határokon belül nemzeti felelősség, míg határokon átterjedő esetekben európai szintű kezelést igényel. Kinyilatkozta továbbá, hogy a védelmi stratégiák közül az összveszély-megközelítési elv alkalmazásával (mindenfajta veszéllyel szembeni védelem, különös tekintettel a terrorizmusra) szándékozik megvalósítani a programot.

2.2. Az Európai Unió kritikus infrastruktúrák védelmére vonatkozó politikája

Az Európai Unióban a létfontosságú infrastruktúrákhoz azok a fizikai és információs technológiai berendezések és hálózatok, szolgáltatások és eszközök tartoznak, amelyek összeomlása vagy megsemmisítése súlyos következményekkel járhat a lakosság egészsége, védelme, biztonsága és gazdasági jóléte, illetve a tagállamok kormányainak hatékony működése szempontjából [Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról. COM (2005) 576 final].

A *Lisszaboni Szerződés* jelentős újításokat vezetett be az európai biztonsági stratégia és az európai biztonsági és védelmi politika területén, különösen a közös kül- és biztonságpolitika főképviselője hivatalának megerősítésével, az Európai Külügyi Cselekvési Szolgálat létrehozásával, egy kölcsönös védelmi segítségnyújtási cikk és szolidaritási záradék beiktatásával, valamint a védelmi területen kialakított strukturált együttműködés megteremtésével.

Az Európai Tanács által 2003. december 12-én *Egy biztonságos Európa egy jobb világban* címmel elfogadott *európai biztonsági stratégia* felszólította Európát, hogy járuljon

hozzá egy hatékonyabb, többoldalú világrendhez. A stratégia az Európai Unióra leselkedő legnagyobb veszélyeket és az előtte álló legnagyobb kihívásokat a következőkben látja:

- tömegpusztító fegyverek terjedése,
- terrorizmus és szervezett bűnözés,
- regionális konfliktusok,
- állam kudarca,
- tengeri kalózkodás,
- kézifegyverek és könnyű lőfegyverek, kazettás bombák és taposóaknák használata,
- energiabiztonság,
- éghajlatváltozás és a természeti katasztrófák következményei,
- informatikai biztonság,
- szegénység, éhínség.

A stratégia az EU biztonsági érdekeinek előmozdítására vonatkozó átfogó jellegű alapelveket fogalmazott meg, mint a megelőzés, fokozottabb képesség, nagyobb koherencia, együttműködés, és egyértelmű célokat határozott meg. A stratégiai célok közül a fenyegetésekre való válasz, a biztonságépítés kiemeltnek tekinthetők.[5]

Az Európai Tanács által 2004 decemberében elfogadott *A terrortámadások megelőzése, felkészültség és válaszadás* című következtetések, valamint *A terrorfenyegetések és -támadások következményeivel kapcsolatos EU szolidaritási program* támogatta a Bizottság szándékát, hogy javaslatot tegyen a létfontosságú infrastruktúrák védelmére vonatkozó európai programra (EPCIP), és jóváhagyta a létfontosságú infrastruktúrák figyelmeztető információs hálózatának (Critical Infrastructure Warning Information Network, a továbbiakban: CIWIN) Bizottság általi felállítását. Az EPCIP-re vonatkozó előterjesztést a Tanács 2004. decemberi ülésén, az EPCIP és a CIWIN felállítására vonatkozó tervezetet (az úgynevezett *Zöld Könyvet*) 2005 novemberében fogadták el.

Az Európai Bizottság közleménye (2006. december 12.) a létfontosságú infrastruktúrák védelmére vonatkozó európai programról[6] bemutatja az EPCIP végrehajtása érdekében javasolt elveket, eljárásokat és eszközöket. A fenyegetések, amelyekre a program reagálni kíván, nem korlátozódtak a terrorizmusra, hanem minden veszélyforrásra kiterjednek, beleértve a bűncselekményeket, természeti katasztrófákat, valamint a baleseteket okozó egyéb eseményeket is. Az EPCIP általános célkitűzése, hogy javítsa a létfontosságú infrastruktúrák védelmét az Európai Unióban. Az EPCIP jogi kerete a következőkből áll:

- az európai létfontosságú infrastruktúrák azonosítására és kijelölésére vonatkozó eljárás, valamint közös megközelítés annak értékeléséhez, hogy szükséges-e ezen infrastruktúrák védelmét javítani;
- az EPCIP végrehajtásának megkönnyítését célzó intézkedések, ideértve az EPCIP cselekvési tervet, a létfontosságú infrastruktúrák figyelmeztető információs hálózatát (CIWIN), uniós szintű, létfontosságú infrastruktúrák védelmét szolgáló szak-

[5] Lásd még a 2008. december 12-én *A biztonság megteremtése a változó világban* címmel az európai biztonsági stratégia végrehajtásáról elfogadott jelentést; az Európai Unió Tanácsa Elnökségének az európai biztonság- és védelempolitikáról szóló 2008. december 9-i és 2009. június 16-i jelentéseit; a Tanács által 2009. november 17-én elfogadott, a fentiekkel kapcsolatos következtetésekre és *Az európai biztonság- és védelempolitika tíz éve – Kihívások és lehetőségek* című nyilatkozatot.

[6] COM(2006) 786 végleges – Hivatalos Lap C 126., 2007.6.7.

értői csoportok létrehozását, a kapcsolódó információcsere-eljárásokat, valamint a kölcsönös függőségek azonosítását és elemzését;
– az EU-tagállamok számára az NCI-k kapcsán nyújtott támogatás, amelyet az egyes EU-tagállamok saját döntésük alapján vehetnek igénybe;
– külügyi dimenzió;
– kísérő pénzügyi intézkedések.

A Bizottság által 2006. december 12-én előterjesztett javaslatot két évvel később, az Európai Unió Tanácsának 2914. ülésén, 2008. december 8-án fogadták el mint az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelvet (a továbbiakban: Irányelv). Az Irányelv elfogadása az Európai Közösséget létrehozó római szerződés 308-as cikkelye alapján történt meg, amely kimondja, hogy „[h]a a *Közösség fellépése bizonyul szükségesnek ahhoz, hogy a közös piac működése során a Közösség valamely célkitűzése megvalósuljon, és e szerződés nem biztosítja a szükséges hatáskört, a Tanács, a Bizottság javaslata alapján és az Európai Parlamenttel folytatott konzultációt követően* egyhangúlag meghozza a megfelelő rendelkezéseket". (PRÉCSÉNYI–SOLYMOSI 2007)

Az Irányelv az Európai Unió egyéb politikai törekvéseivel és célkitűzéseivel harmonizálva határozta meg a kritikus infrastruktúrák azonosítására és kijelölésére vonatkozó eljárások, eszközök és elvek halmazát. Az Irányelv alkalmazhatóságának és értelmezhetőségének érdekében kiadtak egy nem kötelező iránymutatást,[7] amely a tagállami feladatok részletesebb levezetésével törekszik megkönnyíteni a kötelezettségek teljesítését.

Az Irányelv szerint a kihirdetéstől számított két éven belül a megvalósításhoz szükséges intézkedéseket a tagállamoknak végre kell hajtaniuk. Felkéri a tagállamokat, hogy évente készítsenek jelentést arról, hogy szektoronként hány olyan infrastruktúrát tartanak számon, amelyeknél az azonosítással és kijelöléssel kapcsolatban eljárást folytattak. Ehhez kapcsolódik a kétévente készítendő, általános adatokat tartalmazó összefoglaló jelentés kötelezettsége, amelyben ki kell térni a területükön található sebezhető pontokra és azok veszélyeztető tényezőire. A tagállamoknak tájékoztatniuk kell továbbá a Bizottságot a szektoronként kijelölt európai kritikus infrastruktúrák számáról, és az ezek miatt függőségbe kerülő tagállamokról egyaránt.

Az Irányelv szerint a végrehajtásban érintett ágazatok elsősorban az energia- és a közlekedési ágazat, tehát az ezekre vonatkozó ágazati kritériumokat kell előtérbe helyezni. A kritériumok meghatározása során a speciális tulajdonságoknak történő megfelelést, minimumkövetelményeket és küszöbértékeket vizsgálnak elsősorban. Fentiek mellett az Irányelvben meghatározott *horizontális kritériumok* szerint is értékelni szükséges az adott tagállamban található, lehetséges kritikus infrastruktúra elemeket. A veszteségek, a gazdasági hatás és a társadalmi hatás kritériumára vonatkozó küszöbértékeket a tagállamok eseti alapon, a sajátosságok figyelembevételével határozzák meg saját jogi szabályozásuk keretében.

Az Irányelv által körvonalazott azonosítási és kijelölési folyamat során, az ágazati és horizontális kritériumok definiálását követően a tagállamok felmérik azokat a potenci-

[7] Nem kötelező iránymutatás az európai kritikus infrastruktúrák meghatározásáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló Tanácsi Irányelv alkalmazásához (EUR 23665 EN – 2008).

ális infrastruktúrákat, amelyek az ágazati kritériumoknak való megfelelésükből fakadóan nemzeti kijelölésben érintettek lehetnek. Ezt követően azt kell vizsgálniuk, hogy a határon átnyúló hatás fennállhat-e az adott infrastruktúrára vonatkozóan, végül a horizontális kritériumok érvényesülésének alátámasztása következik. Amennyiben az infrastruktúra mindegyik feltételnek megfelel, úgy európai kritikus infrastruktúrává történő kijelölése is megkezdődhet. Tekintettel arra, hogy az európai kritikus infrastruktúra több tagállamra hatással van, az Irányelv kötelezi a kiindulási tagállamot arra, hogy tájékoztassa a lehetséges hatás alatt álló tagállamokat a beazonosítással kapcsolatos információkról, amelyekről az érintettekkel egyeztetéseket kell folytatni. A kijelölés csak akkor történhet meg, ha az érintett tagállamok arról megállapodás formájában egyetértő döntést hoztak. A kijelölést követően az adott tagállam informálja az infrastruktúra tulajdonosát/üzemeltetőjét a kijelölés tényéről, és a kijelölést rendszeresen felülvizsgálja. (Bonnyai 2014)

Az Irányelv felszólítja minden kijelölt kritikus infrastruktúra tulajdonosát/üzemeltetőjét, hogy a kijelölést követő egy éven belül dolgozzon ki *üzemeltetői biztonsági tervet* – amennyiben nem rendelkezik vele –, amelyet később rendszeresen felülvizsgál. Kötelezettség továbbá, hogy kijelölt kritikus infrastruktúra esetén *biztonsági összekötő tisztviselőt* kell alkalmazni – kivéve, ha már van ezzel egyenértékű munkakörrel rendelkező személy –, aki kapcsolattartó pontként funkcionál a tulajdonos/üzemeltető és az illetékes tagállami hatóságok között. Ezzel párhuzamosan az Irányelv kötelezi a tagállamokat a területükön elhelyezkedő európai kritikus infrastruktúrákkal kapcsolatos *kockázatértékelés* lefolytatására egyaránt.

A CIWIN mérföldkőnek tekinthető az uniós infrastruktúra védelmi közösség kialakításában. A jelenlegi rendszer vitafórum indítására és belső levelezésre alkalmas, de jelen formájában csak korlátozott terjesztésű adatok továbbítását teszi lehetővé. Fejlesztésével kapcsolatos középtávú cél a bizalmas minősítésű információk megosztási lehetőségének biztosítása. Az Európai Bizottság tulajdonában lévő védett, nyilvános, internetalapú információs és kommunikációs rendszerré fejlesztett CIWIN a regisztrált felhasználók részére biztosít lehetőséget a kritikus infrastruktúrákkal kapcsolatos információk cseréjére. Emellett tanulmányokat és jó gyakorlatokat kínál valamennyi tagállam részére. A CIWIN-portál a tesztidőszakokat követően, 2013 januárja óta rendeltetésszerűen működik. Az Európai Bizottság Belügyi Főigazgatósága *(Directorate-General for Home Affairs)* koordinálja az ezzel kapcsolatos tevékenységet, és rendszeresen konzultál a tagállamok kapcsolattartó pontjaival a stratégiai fejlesztési kérdések kapcsán. A tagállamok felelőssége kinevezni egy olyan közvetítő személyt *(executive and support officer),* aki közvetlenül közreműködik a CIWIN alkalmazásával és fejlesztésével kapcsolatos feladatokban.

A Görögországban 2004 márciusában létrejött *ENISA (European Network and Information Security Agency)* kulcsfontosságú szerepet tölt be európai szinten a kritikus információs infrastruktúrák védelme terén. Technikai szakértelmet nyújt a tagállamoknak és az Európai Unió intézményeinek, valamint jelentéseket és elemzéseket készít az információs rendszerek biztonságáról európai és globális szinten. Támogatja a nemzeti magánszektorok és az ENISA közötti szoros kapcsolatot és kölcsönhatást annak érdekében, hogy a nemzeti/kormányzati CERT-ek bekapcsolódjanak az európai információmegosztási és figyelmeztető rendszer fejlesztésébe. További feladata, hogy egy együttműködési keretet hozzon létre a hálózati és az informatikai biztonság fejlesztése érdekében. Célja, hogy megteremtse, növelje és koordinálja a közös európai biztonsági lépéseket a hálózat- és az információbiztonság területén.

Az Európai Parlament szorgalmazza, hogy az ENISA évente koordináljon és valósítson meg uniós szinten internetbiztonsági figyelemfelkeltő hónapot, hogy a tagállamok és az uniós állampolgárok különösen figyeljenek oda a kiberbiztonsággal kapcsolatos kérdésekre. Támogatja az ENISA-t – a digitális menetrend célkitűzéseinek megfelelően – a hálózati információbiztonsággal kapcsolatos feladatainak ellátásában, és különösen azáltal, hogy útmutatással és tanáccsal látja el a tagállamokat azzal kapcsolatban, hogy miként érjék el CERT-jeik tekintetében az alapvető képességeket, illetőleg hogyan támogassák a bevált gyakorlatok bizalmon alapuló környezet kialakítása révén történő cseréjét.

2.3. Külső dimenzió és tapasztalatok[8]

A kritikus infrastruktúrák védelmével kapcsolatos uniós tevékenység külső dimenziójának fejlesztése az elmúlt években jelentős mértékben felerősödött.

2.3.1. Európától a Távol-Keletig

A harmadik országokkal való együttműködés keretében az EGT-országok (az EU tagállamai, illetve Norvégia, Izland és Liechtenstein) több alkalommal vettek részt kritikus infrastruktúrák védelmével kapcsolatos EU-s találkozókon. Svájc 2008 óta tagja a D-A-CH összefogás keretében infrastruktúra-védelmi témákban is együttműködő platformnak, amelynek munkájában Németország és Ausztria az uniós közreműködő fél. 2010-ben a felsorolt három országhoz csatlakozott az Egyesült Királyság és Hollandia is, a kritikus információs infrastruktúrák védelme kapcsán. Németország ugyanakkor élen jár az eurázsiai partnerségek kialakításában és fenntartásában egyaránt. Oroszországgal olyan bilaterális együttműködést tart fenn, amelynek része a kritikus infrastruktúrák védelmére irányuló – különösen az energiaágazattal kapcsolatos – párbeszéd. Kínával – hasonlóan az Orosz Föderációhoz – szintén megalapozott kapcsolata van, amelynek keretében támogatja a kínai válságkezelési képességek fejlesztését és ezáltal a kritikus infrastruktúrák védelmének kialakítását is. Izraellel elsősorban a stratégiai tervezés és a polgári védelem kapcsán bonyolít időszakos tapasztalatcserét, amely a polgári védelem vonatkozásában kiterjed a kritikus infrastruktúrák védelmének kérdéskörére is [Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCI); European Commission SWD (2012) 190 final].

2.3.2. Transzatlanti együttműködés, új irányvonalak

Mindemellett az USA és Kanada felé történő nyitás és tapasztalatcsere került kifejezetten előtérbe az elmúlt néhány évben. 2010 márciusában, Spanyolországban rendezték meg az első úgynevezett EU–USA–Kanada Kritikus Infrastruktúra Védelmi Szakértői Konfe-

[8] BONNYAI Tünde (2014): *A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében.* Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem.

renciát, amelynek keretében a felülvizsgálati időszak szempontjaihoz is kapcsolódó célkitűzéseket nevesítettek:

- a kölcsönös függőség kockázatainak vizsgálata;
- az információmegosztás lehetőségeinek fejlesztése;
- a kritikus infrastruktúrák védelme hosszú távú stratégiájának kialakítása az EU-ban.

Mindezt átfogóan összegzi egy, a kritikus infrastruktúrák védelméről szóló jelentés is, amelyet az Európai Politikai Tanulmányok Központja *(Centre for European Policy Studies)* készített 2010-ben (*Protecting Critical Infrastructure in the EU 2010).* A tapasztalatok megosztása keretében és az Európai Bizottság ajánlása alapján, 2010 nyarán dolgozták fel uniós szinten a kritikus infrastruktúrák védelme érdekében kiadott Kanada–USA Közös Akciótervet, amelynek legfőbb célkitűzése volt az USA és Kanada közös, északi határterületeken lévő kritikus infrastruktúrái biztonságának erősítése. Az Akcióterv az információmegosztás, a partnerség és a kockázatértékelési tevékenységek fejlesztése mellett kötelezte el a feleket, amelyet közös projektek tervezésével és szervezésével valósítanak meg *(Canada-United States Action Plan for Critical Infrastructure; Homeland Security 2010).* A fentiek szerint megalapozott további együttműködés keretében 2011 júniusában, a magyar elnökség[9] alatt, Budapesten zajlott a II. EU–USA–Kanada Kritikus Infrastruktúra Védelmi Szakértői Konferencia, amely kifejezetten a tengerentúli kapcsolatok megerősítésére irányult. A fokozott együttműködés elsősorban a következő területekre vonatkozik:

- kritikus interdependenciák modellezése, függőség azonosításának módszerei,
- érintett hatóságok tapasztalatainak alkalmazása,
- információmegosztás elősegítése,
- ipari ellátási lánc biztonsága prioritásának hangsúlyozása,
- veszélyhelyzeti tervek kidolgozása,
- globális infrastruktúra-védelmi eszközrendszer önkéntes alapú kidolgozása (vizsgálatok és elemzések, kockázatkezelés, felkészülés és irányítás, információcsere).

A külső dimenzió szerepének jelentőségét támasztja alá a 2012-ben harmadik alkalommal megtartott III. EU–USA–Kanada Kritikus Infrastruktúra Védelmi Szakértői Konferencia, amelynek előremutató eredményei a tengerentúli kapcsolatok tényleges elmélyülése, közös szcenáriókban történő gondolkodás és az elméleti témakörök gyakorlati módszertanok irányába való elmozdítására irányuló szándék megjelenése voltak.

Mindez megjelenik az Európai Bizottság 2012 júniusában kiadott munkaanyagában az EPCIP felülvizsgálatáról. Ez volt az első olyan összefoglaló dokumentum, amely az Irányelv által meghatározott felülvizsgálati ciklus egyes eredményeit foglalta össze. Részletes áttekintést és elemzést adott a fejlesztés alatt álló kockázatértékelési módszertanról, a tagállamok által végrehajtott kötelezettségek vizsgálatáról és a harmadik országokkal való kapcsolattartás aktuális helyzetéről egyaránt. Az Irányelvben meghatározottaknak megfelelően – 2012 januárjában – megkezdődött az a felülvizsgálati folyamat, amely az Irányelv alkalmazását és lehetséges jövőbeli irányvonalait vizsgálta.

2012 első félévében tartották azokat a workshopokat, értekezleteket és konferenciákat, amelyek kifejezetten az elért eredmények kiértékelését, a jövőbeli lehetséges prioritások

[9] Magyarország 2011. január 1-től 2011. június 30-ig látta el az Európai Unió Tanácsának soros elnökségét.

megfogalmazását tűzték napirendre. Az Irányelv végrehajtásának felülvizsgálata kiterjedt a tagállamok szabályozási tevékenységére is. Megállapították, hogy a tagországok többsége teljesítette jogharmonizációs kötelezettségeit. Néhány ország esetében nem volt szükség jogszabályi változtatásokra, mert a meglévő nemzeti megközelítések és folyamatok ügyrendi módosítása kielégítette a végrehajtással kapcsolatos követelményeket (például: Ausztria, Észtország, Finnország, Egyesült Királyság). Ezekben az országokban, napjainkban is rendkívül magas szintű együttműködés jellemző a köz- és magánszféra között, amely jó példát állít a többi uniós tagállam elé. Az első megállapítások szerint alapvetően minden – akkor még 27 – tagállam rendelkezett valamilyen intézkedéssel a kritikus infrastruktúrák védelme vonatkozásában. A rendezvények, elemzések és értékelések hozzáadott értékei és eredményei alapján a felülvizsgálatról szóló összefoglaló előrevetítette a kritikus infrastruktúrák védelméről szóló új, átgondolt és átformált irányelvcsomag elfogadását 2012 novemberére [Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCI); European Commission SWD (2012) 190 final].

2013 májusában Washington látta vendégül a IV. EU–USA–Kanada Konferencia résztvevőit, amelynek keretében jelentős értelmezésbeli paradigmaváltás volt tapasztalható. A többoldalú elkötelezettség jegyében az információ- és tapasztalatcserén túl komplexebb témakörök is előtérbe kerültek, így az innovatív és előretekintő kezdeményezések között szerepelt:

- a klímaváltozás és annak hatásai a kritikus infrastruktúrák védelmére;
- a fizikai és információs infrastruktúrák közötti függőségek jelentősége és vizsgálata;
- az infrastruktúrák elavultságának lehetséges hatása a védelmi szint biztosítására. (DURKOVICH 2013)

A felülvizsgálat és a nemzetközi szintű együttműködések tapasztalatának felhasználásával 2013 augusztusában jelent meg az Európai Bizottság munkadokumentuma az EPCIP új megközelítéséről az európai kritikus infrastruktúrák biztonságosabbá tétele érdekében. Az új irányok az átdolgozott és praktikusabb végrehajtás felé mozdultak, amelyet a 2006–2012 közötti időszakban végrehajtott tevékenységek alapján, a tagállamok és az érintettek bevonásával nevesítettek. Az EPCIP végrehajtásának új megközelítése kifejezetten a megelőzésre, a készenlétre, valamint a rendkívüli eseményekre történő rugalmas és hatékony reagálásra irányul. Ennek érdekében az Európai Bizottság felkérte a tagállamokat, hogy tovább erősítsék a magas szintű védelmet, és fokozatosan növeljék a kritikus infrastruktúrák ellenálló képességét. A felülvizsgálat eredményeként az interdependenciák vizsgálatával kapcsolatos célkitűzéseket a következők szerint határozták meg:

- a kritikus infrastruktúra, az ipar és az államigazgatás közötti függőségek értékelése;
- az ágazatok közötti interdependencia elemzése;
- az ágazaton belüli, de országokon átívelő dependenciák feltérképezése.

Mindennek végrehajtásához bevezették a kritikus infrastruktúra védelmi tervezés definícióját, amely elsősorban a kölcsönös függőségeken kell alapuljon és kockázatként kell kezelje a kibertérrel kapcsolatos kihívásokat is. Az új megközelítés első lépéseként fókuszba került négy konkrét európai kritikus infrastruktúra (együttesen a Négy), amelyek egyértelműen

érzékeltetik a hálózatszerűséget, az interdependenciák jelentőségét, a kritikusság sajátos jegyeit, valamint a kiberbiztonság jelentőségét egyaránt:

- GALILEO, műholdas navigációs és helyzetmeghatározó rendszer az Európai Unió és az Európai Űrügynökség gondozásában. Célkitűzése az első olyan műholdalapú navigációs és helymeghatározó infrastruktúra létrehozása, amely kifejezetten polgári célokat szolgál.
- EUROCONTROL (Európai Szervezet a Légi Közlekedés Biztonságáért), a NATO javaslatára a légi közlekedés biztonságával kapcsolatos együttműködésre vonatkozó Egyezmény hozta létre 1961-ben, legfőbb célja az Egységes Európai Égbolt *(Single European Sky)* létrehozása, amelynek érdekében az európai légiforgalmi irányítás fejlesztésével és hatékonnyá tételével foglalkozik.
- Magasfeszültségű villamosenergia-hálózat és az azzal összeköttetésben álló ágazatok és alágazatok infrastruktúrái, amelyek az Európai Unió tagországai és más európai államok területén alkotnak összefüggő hálózatot.
- Páneurópai gázellátó hálózat és létesítményei, amelynek mind a tárolási, mind a szállítási, mind a felhasználási célú elemei létfontosságúak az európai uniós tagállamok szempontjából. (Bonnyai 2014)

2014. május 6–7-én került sor Athénban az V. EU–USA–Kanada Kritikus Infrastruktúra Védelmi Munkaműhelyre, amely során a résztvevők elmélyítették a párbeszédet a kritikus infrastruktúrák védelme és a rugalmasság elvének kulcsfontosságú kérdéseiben. A munkaműhely kiemelt célja volt a védelemre vonatkozó európai, amerikai és kanadai programok aktuális irányainak megismerése, a megváltozott fenyegetettségek, trendek és tapasztalatok megosztása. Érdemi véleménycsere zajlott a létfontosságú elemek azonosítása, a kijelölt infrastruktúrák biztonságának és ellenálló képességének fokozása, a klímaváltozás és a kiberbiztonság kapcsán. Ezen a találkozón kiemelt figyelmet szenteltek a hálózatbiztonság egyre markánsabb szerepének, az interdependenciák feltérképezésének, az alkalmazott kockázatelemzési módszereknek, valamint egyes rendkívüli időjárási eseményekkel kapcsolatos helyzetek kezelésének tapasztalatainak. Egyértelműen láthatóvá vált, hogy az Irányelv által korábban meghatározott terrorprioritás az összveszély-megközelítés felé mozdul el, a paradigmaváltás eredményeként a védelemről inkább a megelőzésre helyeződik a hangsúly. A kibervédelem vonatkozásában megállapították, hogy nem elég a védelem kialakítása során a fizikai biztonságra fókuszálni, az IT-biztonságra is kiemelt figyelmet kell fektetniük az üzemeltetőknek.

Mindezt megerősítette a 2014 júliusában, Brüsszelben tartott Kritikus Infrastruktúra Védelmi Kapcsolattartó Pontok (CIP POC) munkaműhelye, amely az EU-tagállamok előrehaladását vizsgálta, és a megszerzett tapasztalatok megosztását tűzte ki céljául. A tagállamok egyetértettek a kiberbiztonság fontosságával, a szektorokon átnyúló együttműködések (különösen az állami és magánszektor vonatkozásában) erősítésének szükségességével, a megelőző szemléletű kríziskezelés fejlesztésével kapcsolatban. A találkozón az Irányelv implementálásának aktuális helyzetét is bemutatta az Európai Bizottság, amellyel kapcsolatban felmerült, hogy a megjelölt két ágazat (energia, közlekedés) mellett további ágazatokat is bevonjanak európai szinten.

A 2014 novemberében tartott CIP POC munkaműhely két kiemelkedő témakörét a fentiekkel kapcsolatosan állapították meg. Az Európai Tanács Közös Kutató Központja (JRC)

a kiberfolyamatok modellezésével kapcsolatos fejlesztési irányokat mutatta be, valamint a kommunikációs rendszerek biztonságát, a kibertérből érkező fenyegetettségekre történő felkészülési lehetőségeket helyezte előtérbe. Emellett itt mutatták be a CIWIN rendszer béta verzióját is.

2014 decemberében a közlekedés prioritásával Európai Közlekedési Kritikus Infrastruktúra Védelmi Konferenciát tartottak az tagállamok Athénban. Az üzemeltetők szempontjait előtérbe helyező rendezvényen a tömegközlekedés kapcsán kiemelték, hogy a terror-, a kiber- és a katasztrófafenyegetettség mellett a legnagyobb problémát a kisebb bűncselekmények (például: rongálás, graffiti) okozzák, amelyek jelentős gazdasági károkkal és az utasok bizalomvesztésével járnak. A konferencián megállapították, hogy a nemzetközi sztenderdek a terror központú védelmi megközelítésről fokozatosan áttértek a hazánkban is alkalmazott összveszély-megközelítésre.

2015-ben Rigában tartották a VI. EU–USA–Kanada Konferenciát, ahol a szakértői szinten bevált gyakorlatok, eljárásrendek megosztása került a középpontba, külön hangsúlyt fektetve az együttműködések gyakorlatba történő átültetésére. A rendezvény keretében három fontos területre világítottak rá: krízishelyzetek kezelése, kiberfenyegetettség kihívásai, szervezett bűnözés elleni fellépés szükségessége. A részt vevő országok ennek jegyében a tagállamok közötti, valamint az EU–USA és EU–Kanada együttműködés további erősítése mellett kötelezték el magukat, különös tekintettel az energiaszektorra.

A 2013–2015-ös időszak erőfeszítéseinek egyik előremutató fejleménye a skót, olasz és holland kormányzat által alapított Miracle elnevezésű projekt, amelynek 2015. júniusi záró konferenciáján mutatták be az ellenálló képesség fokozását célzó kutatómunka eredményeit. A projekt keretében gyakorlati tapasztalatokra épülő stratégiák és elméletek kidolgozása zajlott, abból a célból, hogy a meglévő megelőzési, felkészülési és védelmi képességek fejleszthetők legyenek. A kutatótevékenység külön hangsúlyt fektetett a lakosság biztonságát fenyegető kockázatokra is – beleértve egy terrortámadás következményeit – annak érdekében, hogy az érintett szakemberek felkészültsége fokozható legyen. A projekt alaptézise az volt, hogy amennyiben a kritikus infrastruktúrákkal kapcsolatos rugalmassági stratégiákat helyi szinten sajátítják el és fejlesztik a szakemberek, az előmozdítja a nemzeti és az európai szintű kritikus infrastruktúrákkal kapcsolatos rugalmassági képességeket is.

A 2015 júliusában, Brüsszelben tartott CIP POC ülésen a tagállamok a 2015 áprilisában elfogadott *Európai Biztonság Rendje* alapján és az új fenyegetettségek okozta kihívások kezelésének érdekében a harmadik országok felé történő nyitásról értekeztek. Az EU célkitűzései közé bekerült a biztonsági kérdések vonatkozásában Ukrajna és Moldávia bevonása, amely a kritikus infrastruktúrák védelme kapcsán elsősorban az információ- és tapasztalatmegosztás vonatkozásában értelmezhető. A meglévő tapasztalatok és a „keleti nyitás" alapján kérdésként merült fel az Irányelv módosítása is. A tagállamok véleménye általánosságban különbözött ebben a kérdésben, de a szorosabb nemzetközi kapcsolatok építése (például: gyakorlatok tartása), valamint a meghatározó üzemeltetők EU-s rendezvényekre történő meghívása vonatkozásában az álláspontok megegyeztek.

Ezt a típusú együttműködést volt hivatott erősíteni a 2015 októberében, Zágrábban tartott RECIPE 2015 elnevezésű projekt keretében nemzetközi munkaműhely is. A projekt célja volt a hiányosságok feltárásával és megoldási javaslatok kidolgozásával megerősíteni a kritikus infrastruktúrák és az ezekkel kapcsolatos védelmi kapacitások alkalmazkodóképességét. A rendezvényen szakemberek és üzemeltetők oszthatták meg egymással

nemzeti szintű tapasztalataikat, amelyek összegzéséből zárt körben terjeszthető egységes iránymutatás készült. A célkitűzések alapján az alábbi területek vonatkozásában került sor kockázatkezelési és eljárási modellek kidolgozására:

– köz- és magánszektor közötti partnerség kialakítása és fejlesztése,
– érintett résztvevői kör tagjai közötti érzékeny adat- és információcsere,
– a kritikus infrastruktúrák védelmével foglalkozó nemzeti központok feltételrendszerének kialakítása.

Az együttműködés fejlesztése érdekében a holland CIP POC (Critical Infrastructure Protection National Point of Contact in the Neatherlands, azaz Hollandia hivatalos kritikus infrastruktúra-védelmi kapcsolattartó pontja) kezdeményezte 2015. II. félévében egy olyan munkacsoport létrehozását, amely a kritikus infrastruktúrák védelmével és a polgári védelemmel foglalkozó területek közötti együttműködés elősegítését célozza, illetve megfelelő felületet teremt a két szakterület közötti összeköttetés megteremtésére. A Kritikus Infrastruktúra Védelmi Kapcsolattartó Pontokat ebben a megközelítésben támogató első érdemi tanácskozásra 2016 januárjában, Hágában került sor, ahol a fő téma a kritikus infrastruktúrák ellenálló képességének fokozása[10] volt. Mindez jól tükrözte a holland elnökség[11] egyik főbb prioritását, hogy összekapcsolja a katasztrófák lehetséges dominóhatásainak jobb megértését a kritikus infrastruktúrák ellenálló képességének erősítésével. Mindez az új EU Polgári Védelmi Mechanizmusról[12] szóló határozatban (1313/2013/EU) már megjelent, tekintettel arra, hogy az a teljes katasztrófavédelmi ciklust felölelő, összveszélyalapú (természeti és ember által okozott katasztrófákat figyelembe vevő) megközelítést alkalmazott, és rendelkezései alapján kijelenthető, hogy a Bizottság egyre nagyobb hangsúlyt kíván a megelőzésre és a felkészülésre fektetni. A polgári védelmi és a kritikus infrastruktúrák védelmével foglalkozó szakterületek közeledését jelzi, hogy a Bizottság által koordinált, a nemzeti katasztrófakockázat-értékelésről szóló tájékoztatókban szinte minden ország vonatkozásában megjelenik a kritikus infrastruktúrák védelme mint érintett terület. Ugyanezt erősíti az ENSZ Sendai Katasztrófakockázat-csökkentési Keretterve,[13] amelynek hét célkitűzése közül az egyik a kritikus infrastruktúrák ellenálló képességének növelését tartalmazza 2030-ig. Ennek megfelelően a Bizottság törekszik arra, hogy bevonja a felkészülés területén a kritikus infrastruktúrák védelmének szektorait, elsősorban a gyakorlatok, képzések és pályázatok megvalósításába.

A CIP POC ülések következő állomása volt a 2016 februárjában, Brüsszelben tartott tanácskozás, amelyen első alkalommal nevesítették az egészségügyi ágazat jelentőségét, és az európai szintre emelésének lehetőségét. A tagállamok kiemelten fontosnak tartották az ágazat jogszabályi szintű megjelenítését, tekintettel arra, hogy az már az olasz és a magyar jogrendben is szerepel. Mindemellett továbbra is hangsúlyos témakörként jelent meg

[10] „Building bridges to enhance resilient infrastructures."

[11] Hollandia 2016. január 1-től 2016. június 30-ig látta el az Európai Unió Tanácsának soros elnökségét.

[12] A közösségi polgári védelmi mechanizmus célja, hogy elősegítse az emberek, a tulajdon, a környezet és a kulturális örökség védelme érdekében, a természeti és ember által okozott katasztrófák, terrorcselekmények, műszaki, radiológiai és környezeti balesetek esetében szükséges együttműködését, az EU-n belül, vagy egy harmadik országban egyaránt.

[13] Katasztrófakockázat-csökkentési Világkonferencia, 2015. március 14–18. Szendai (Japán). www.preventionweb.net/files/43291_sendaiframeworkfordrren.pdf (Letöltés ideje: 2018. 07. 24.)

az információbiztonság, tekintettel az akkor még készülő uniós *Hálózat- és Információbiztonsági Irányelv*ben foglalt jövőbeli feladatokra. A találkozón elhangzott tagállami hozzászólások alapján megállapítható, hogy a 2015. novemberi párizsi terrortámadás (és következményei) befolyást gyakoroltak a kritikus infrastruktúrák védelmének európai helyzetére és megítélésére egyaránt.

2016. május 10–12-én Hollandiában rendezték meg az első kritikus infrastruktúrák védelmének közösségi szintű fejlesztésére irányuló nemzetközi gyakorlatot. A VITEX 2016 elnevezésű gyakorlat – jellege és célkitűzései alapján – újszerű kezdeményezésnek tekinthető az EU szintjén, tekintettel arra, hogy a kritikus infrastruktúrák védelme nemzetközi gyakorlati tapasztalatainak összefoglalására egy kiválasztott és prioritásként kezelt ágazat vonatkozásában eddig még nem volt példa. Ahogy korábban már említettük, a holland elnökség egyik fő feladataként határozták meg a „nemzetközi biztonságot", amelynek szerves része a kritikus infrastruktúrák védelme, azok biztonságának nemzeti és közösségi szintű fokozása, a hatályos irányelv alkalmazásának dinamikus fejlesztése. Ehhez járult hozzá a gyakorlat, amelynek lényege az energiaágazatban a villamosenergia-ellátás lehetséges kihívásainak azonosítása, a működési problémák tagállami és európai szintű megoldása volt.

A Szlovák Elnökség[14] ideje alatt kiemelten nagy figyelmet szenteltek a biztonsági, biztonságpolitikai, belbiztonsági szakpolitikák tartalmi elemeinek fejlesztésére, azon belül a kritikus infrastruktúrák védelmével kapcsolatos megközelítések újragondolására. Az elnökség átvételét követően Pozsonyban tartottak egy szakértői találkozót, amelyen több mint 60 kritikus infrastruktúra védelmi és lakosságvédelmi (polgári védelmi) szakértő vett részt. A rendezvény egyik fő célkitűzése volt, hogy az EU polgári védelmi mechanizmusa és a létfontosságú rendszerek védelme kapcsán tett intézkedései közötti együttműködési lehetőségeket keressen, és a tagállamok által támogatott és elfogadott sarokpontok mentén közelítse egymáshoz a két tevékenységet. Legfontosabb területekként a kockázatkezelési és a veszélyhelyzet kezelésével kapcsolatos feladatokat azonosították. A holland elnökség által kezdeményezett megközelítések továbbfejlesztésének egyik lépése volt ez a találkozó, amelyen megfogalmazták a kritikus infrastruktúrák teljesítményalapú kockázatelemzési módszerének lehetőségeit is. Ez a módszer vizsgálja egy vagy több veszélyeztető tényező kölcsönhatását, a sebezhetőséget és mindezek együttes hatását a rendszer teljesítményére irányulóan (katasztrófaeseményt követően és a helyreállítás időszakában). A teljesítményalapú kockázatelemzés egyik fontos jellemzője, hogy a kritikus infrastruktúrák vonatkozásában figyelembe veszi az egymástól való függőséget és a dominóhatást, beleértve az összetett kockázatokat is. Mindehhez azonban a teljesítménycélok megállapítására van szükség, amelyeket a kormányzat, az üzemeltető és az érintett közösség szoros együttműködése keretében szükséges meghatározni. Ennek körülményei az egységes szemlélet ellenére tagállamonként jelentős mértékben eltérnek, alkalmazása tehát várhatóan esetleges lesz a nemzeti szintet vizsgálva.

A 2016 szeptemberében tartott VII. EU–USA–Kanada Kritikus Infrastruktúra Védelmi Szakértői Konferencia egyik legfontosabb megállapítása volt, hogy a kritikus infrastruktúrák tekintetében folyamatosan alkalmazkodni kell a változó körülmények adta lehetőségekhez és kihívásokhoz, amelyek a 21. században főként kibertámadások formájában nyilvánulhatnak meg. A tagállamok és a részt vevő országok egyetértettek abban, hogy

[14] Szlovákia 2016. július 1-től 2016. december 31-ig látta el az Európai Unió Tanácsának soros elnökségét.

a növekvő adatvagyon védelme fokozottan priorizált terület mind az állami, mind a magánszektor szereplőinek a számára, azok megfelelő védelmének kialakításához szükséges az együttműködés és a kommunikáció mellett az információk széles körű megosztása. A találkozó fontos eredményének kell tekinteni, hogy a tapasztalatok alapján megállapították, hogy a rendkívüli eseményekre készített modellezésekkel és a kritikus infrastruktúrákat érintő gyakorlatok tapasztalatainak felhasználásával a létfontosságú rendszerek védelme tovább erősíthető. A következő (nyolcadik) találkozóra a bolgár elnökség[15] alatt került sor, ahol a tagállami szakértők kifejezetten nagy hangsúlyt fektettek a kritikus infrastruktúrák információbiztonsággal és kibervédelemmel kapcsolatos felkészültségére. A tanácskozás fontos eredménye, hogy a résztvevők egyetértettek abban, hogy az IT-biztonság jelentőségének markáns növekedése hatást gyakorol a kritikus infrastruktúrák reagálóképességére. Felmerült az eredeti irányelv felülvizsgálatának igénye is, amelyet a szakértők a NIS-irányelv alkalmazási tapasztalatainak felhasználása útján tartottak megvalósíthatónak.

A kritikus infrastruktúrák védelme vonatkozásában is mérföldkőnek tekinthetjük a NATO 2014-es walesi csúcstalálkozóját, amelyen a szövetségesek meghirdették a NATO kibervédelmi képességeinek fejlesztési célkitűzéseit. A katonai rendeltetésű szövetség felismerte, hogy egy kibertámadás az egész NATO-ra hatással lehet, ezért deklarálta, hogy a kibertérben is érvényesnek tekinti a nemzetközi jogot, majd ezzel párhuzamosan a NATO kollektív védelmi stratégiájának legfontosabb elemei közé emelte a kibervédelmet. Ennek keretében a tagállamok elfogadták egy kibővített kibervédelmi politika kidolgozását, döntöttek arról, hogy életre hívnak egy úgynevezett virtuális gyakorlóteret *(NATO Cyber Range),* ahol a tagországok a kibervédelmi képességeiket tesztelhetik. Fontos azonban hangsúlyozni, hogy a szövetség számára prioritást jelent a NATO-hálózatok kibervédelmének biztosítása, illetve a hálózatokhoz kapcsolódó tagországok által üzemeltetett hálózatok kibervédelmére vonatkozó követelmények megfogalmazása és ellenőrzése, de kiberbiztonság vonatkozásában a NATO a defenzív (védelemorientált) álláspontot vallja magáénak, nem pedig a kollektív kibertámadási rendszerekét. A kibertér már a 2010-es lisszaboni NATO-csúcs megállapításai alapján azon globális közös terek részét képezte, amelyek nem köthetők egy-egy országhoz vagy régióhoz, de meghatározó szerepük van a szövetség biztonsága szempontjából. 2016-ban a NATO főtitkára bejelentette, hogy a tagállamok döntése értelmében hadszíntérré nyilvánítja a kiberteret.

***

Összességében megállapítható, hogy folyamatosan növelni kell az EU-n belüli és azon kívüli párbeszédek lehetőségeit. Ezzel párhuzamosan a hatékonyabb felkészülésre kell törekedni a potenciálisan bekövetkezhető események tekintetében, különös tekintettel a kibertérben jelentkező veszélyeztető tényezőkre. Az európai szintű kritikus infrastruktúrák azonosítása és kijelölése továbbra is prioritást élvez, ugyanakkor egyértelművé vált, hogy ennek alapfeltétele a nemzeti kijelölések megtörténte.

A kritikus infrastruktúrák védelmének területén egyértelmű célkitűzés az erősebb nemzetközi közösség, a jól működő nemzetközi intézmények és a szabályokon alapuló nemzetközi rendszer kialakítása. Napjaink technológiai, ipari, gazdasági fejlettsége, a társadalmi

[15] Bulgária 2018. január 1-től 2018. június 30-ig látta el az Európai Unió Tanácsának soros elnökségét.

rétegek között tapasztalható szakadéknyi különbségek, a szélsőséges vallási és politikai nézeteket valló csoportok elszaporodása és időszakos megerősödése, a világ terrorveszélyeztetettségének elmúlt években történő exponenciális növekedése mind okot szolgáltatnak arra, hogy a jövőre való tekintettel törekedjünk környezetünk fokozott megóvására.

Felhasznált irodalom

BONNYAI Tünde (2014): *A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében.* Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem.

DURKOVICH, Caitlin (2013): Working Together to Enhance Critical Infrastructure Resilience Around the Globe. *The CIP Report,* Vol. 11. No 11. (May). (Center for Infrastructure Protection and Homeland Security) 2–3.

PRÉCSÉNYI Zoltán – SOLYMOSI József (2007): Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé. *Hadmérnök,* 2. évf. 1. sz. 65–76.

Hivatkozott jogszabályok és dokumentumok

A Bizottság közleménye (2006. december 12.) a létfontosságú infrastruktúrák védelmére vonatkozó európai programról COM (2006) 786 final. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Al33260 (Letöltés ideje: 2018. 07. 24.)

Canada-United States Action Plan for Critical Infrastructure; Homeland Security (2010). Elérhető: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx (Letöltés ideje: 2018. 07. 24.)

Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCI); European Commission SWD (2012) 190 final, 2012, Brussels.

Green Paper on an European programme for critical infrastructure protection (Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról) – COM (2005) 576 final, Brussels, 17. 11. 2005. Elérhető: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=celex:52005DC0576 (Letöltés ideje: 2018. 07. 24.)

Protecting Critical Infrastructure in the EU – CEPS Task Force Report (2010). Brussels, Centre for European Policy Studies.

3. fejezet
A jogszabályi környezet összefüggéseinek és részletszabályainak bemutatása

Bognár Balázs

3.1. A nemzeti szabályozás keretei[1]

Az uniós folyamatok alapján egyértelmű volt, hogy a magyar nemzeti programnak meg kell felelnie a kormány és a tulajdonosok, üzemeltetők elvárásainak, miközben biztosítania szükséges az állami közreműködés és a jogi háttér meglétét egyaránt. Olyan struktúrát kellett kialakítani, amely napjaink új típusú biztonsági kihívásaira érdemben tud reagálni, alkalmas az állami és magánszféra összehangolására, illetve képes a kritikus infrastruktúrák működésében bekövetkező bármilyen változások következményeinek hatékony kezelésére.

Magyarország európai uniós tagállammá válását követően (2004) valamennyi közösségi szabályozással kapcsolatos kötelezettség, illetve az uniós jogalkotási folyamatokban történő részvétel automatizmussá[2] vált. Hazánk aktív szerepet vállalt a kritikus infrastruktúrák védelmére irányuló közösségi szintű szabályozási tevékenység formálásában, így az EU normaalkotási eljárásával párhuzamosan Magyarországon is megindult a jogi környezet kialakítása.

A 2007-ben megkezdett egyeztetéseken részt vevő szervezetek[3] egyetértettek abban, hogy az akkor még csak tervezet formájában létező uniós irányelv végrehajtásához saját jogi eszközök megalkotására van szükség. Első lépésként – az akkori Kormányzati Koordinációs Bizottság égisze alatt – elkészült a hivatásos katasztrófavédelmi szerv (a továbbiakban: katasztrófavédelem) beszámolója a hazai kritikus infrastruktúrák helyzetéről és védelméről, amelyben az addig végzett tevékenység összefoglalása mellett jövőbeli feladatokra irányuló javaslatok is szerepeltek. Ennek alapján rendelték el egy olyan munkacsoport felállítását, amely a magyar nemzeti program kidolgozásával foglalkozott. A közös munka keretében minden ágazat kinyilvánította álláspontját a kritikus infrastruktúrák védelmének rá vonatkozó szegmenseit illetően, majd hozzájárult a magyar *Zöld Könyv* elkészíté-

---

[1] Bonnyai Tünde – Bognár Balázs (2009): The process of critical infrastructure protection. *Academic and Applied Research in Military Science,* Vol. 8. Issue 3. 499–513.

[2] Értsd: jogharmonizációs kötelezettség.

[3] Egészségügyi Minisztérium, Földművelésügyi és Vidékfejlesztési Minisztérium, Gazdasági és Közlekedési Minisztérium, Honvédelmi Minisztérium, Igazságügyi és Rendészeti Minisztérium, Környezetvédelmi és Vízügyi Minisztérium, Miniszterelnöki Hivatal, Oktatási és Kulturális Minisztérium, Büntetés-végrehajtás Országos Parancsnoksága, Határőrség Országos Parancsnoksága, Országos Rendőr-főkapitányság, BM Országos Katasztrófavédelmi Főigazgatóság.

séhez és kiadásához. A hazai *Zöld Könyv* – összhangban az EU *Zöld Könyv*vel – célja, hogy az érintettek részére (állam – tulajdonos/üzemeltető – felhasználó) biztosítsa azokat az alapvető információkat, definíciókat, elveket és folyamatokat, amelyek a későbbi uniós irányelv értelmezése és megvalósítása során nélkülözhetetlenek. A *Zöld Könyv* alapján rugalmasabb és hatékonyabb, egységes nemzeti kritikus infrastruktúra védelmi programot fogalmaztak meg. A kidolgozás során a meglévő jogszabályi környezet felülvizsgálatára is sor került annak érdekében, hogy a kritikus infrastruktúrák védelmére vonatkozó hazai szabályozás teljes körű legyen.

A hazai *Zöld Könyv*ben megfogalmazott célkitűzések szerint a kritikus infrastruktúrák védelme a kockázatok azonosításán alapuló megelőzés, az érintettek bevonásával megvalósuló felkészülés és az ellenálló képesség fejlesztésének hármas rendszerében működő mechanizmus. Az EU iránymutatásának megfelelően nem irányul minden veszélyeztető tényező elleni védelemre, hanem elemzések és tapasztalatok alapján, célirányosan garantálja a megfelelő védelmi szintet. Az EPCIP-ben felsorolt alapelveket *(szubszidiaritás, kiegészítő jelleg, együttműködés, titkosság, arányosság)* a hazai adaptálás során kiegészítették. A *nemzetközi szerződésekből fakadó kötelezettségek teljesítésének* elvként történő meghatározását az indokolta, hogy Magyarországnak NATO szövetségesi feladatainak is eleget kell tennie. Így a hazai jogi környezet hat alapelvet nevesített.

3.1.1. A korábbi szabályozás

A magyar Nemzeti Kritikus Infrastruktúra Védelmi Program (a továbbiakban: NKIV Program) kiemelt figyelmet szentelt az érintettekre, annak érdekében, hogy növelje a fogyasztói bizalmat, eredményesebbé és gördülékennyé tegye a partneri együttműködést az üzemfolytonosság biztosításának jegyében.

A dokumentum egyik legfontosabb tartalmi eleme a feladatok és felelősségi körök meghatározása volt, amelyben jól elkülönültek az állami és a tulajdonosi/üzemeltetői vonatkozások. Az egyértelmű szétválasztás segítette az egyes intézkedések átláthatóságát, miközben egységet és kapcsolatot teremtett az érintettek között. Állami feladatként nevesítették

- a világos jogi és szervezeti háttér kidolgozását,
- az elvárt védelmi szintek meghatározását,
- az információáramoltatás biztosítását,
- a felelősségarányos finanszírozás megteremtését és
- a támogatások rendelkezésre bocsátását egyaránt.

Ezzel párhuzamosan a tulajdonosi/üzemeltetői kör lett felelős az adott infrastruktúra értékeléséért, a tervezési és védelmi programok tényleges fenyegetettségek alapján történő átdolgozásáért, valamint a biztonsági összekötő tisztviselő kinevezéséért és az üzemeltetői biztonsági terv kidolgozásáért. A NKIV Program végrehajtásához a hazai *Z*öld *K*önyv tartalmazta az uniós programban megjelölt szektorok magyar viszonyokra történő átdolgozását, vagyis a kritikus infrastruktúrák vonatkozásában megkülönböztetett hazai szektorok első listáját. (KÁTAI-URBÁN 2013)

Az NKIV Program végrehajtására vonatkozó jogi háttér biztosítása ekkor már elengedhetetlen volt. Egy évvel a hazai folyamatok tényleges megkezdését követően adták

ki a *2080/2008. (VI. 30.) kormányhatározatot a Kritikus Infrastruktúra Védelem Nemzeti Programjáról*.[4] A kormányhatározat kihirdette a nemzeti programról szóló *Zöld Könyv*et. Elrendelte a szükséges ágazati konzultációk lefolytatását, amelyhez ágazatonként minisztériumot vagy országos hatáskörű szervet rendelt felelősként. A különböző ágazati hatáskörbe tartozó tevékenységek összehangolása érdekében szabályozási koncepció kidolgozását írta elő. Mindezeken felül a Kormány meghatározta a CIWIN-hez történő csatlakozás lehetőségeinek vizsgálatát és az ezzel kapcsolatos jelentés Kormány részére történő felterjesztését is.

Az uniós Irányelv hatálybalépésével, illetve a fenti kormányhatározatban megállapított határidők közeledtével (2009. szeptember) és lejártával ismét előtérbe került a NKIV Program és vele együtt a feladatok megvalósításának szükségessége. A feladatok megosztása és a felelősségi körök tisztázása, illetve az EU-s kötelezettség teljesítése érdekében kiadták a *1249/2010. (XI. 19.) kormányhatározatot 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.*

Az új kormányhatározat a belügyminiszter hatáskörébe utalta:

– az európai kritikus infrastruktúrák védelmével kapcsolatos tevékenység koordinálását,
– a nemzeti kapcsolattartó pont feladatait, valamint
– az azonosítás és kijelölés folyamataihoz szükséges két- vagy többoldalú egyeztetések lebonyolítását.

A nemzeti fejlesztési miniszter feladataként nevesítette:

– a Magyarországon található európai kritikus infrastruktúrák kijelölését, valamint
– a kijelölés által érintett ágazati jogszabályok áttekintését és szükséges módosítását.

A honvédelmi miniszter feladatkörébe utalta:

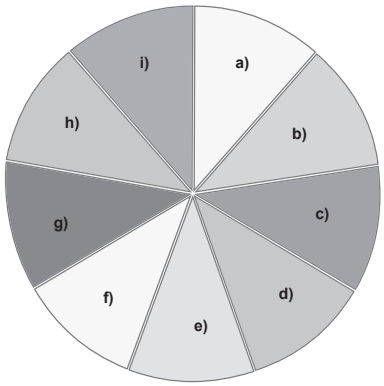
– a honvédelmi érdekből kritikusnak tekintendő infrastruktúrák védelmére vonatkozó intézmény- és követelményrendszer kialakítását.

A Kormányra az Európai Bizottság felé történő éves jelentési kötelezettséget ruházta az alábbi tartalommal:

– a kritikus infrastruktúrák védelmével kapcsolatos feladatok végrehajtásának összefoglalása,
– a kijelölt európai kritikus infrastruktúrák nevesítése,
– az érintett tagállamok száma, illetve
– az alkalmazott kritériumok részletes kifejtése.

Ezenfelül az Irányelvben meghatározottak szerint ágazatonként jelentést kellett készíteni azon sebezhető pontok, fenyegető veszélyek és kockázatok típusairól, amelyek a kijelölt európai kritikus infrastruktúrára vonatkoznak [1249/2010. (XI. 19.) kormányhatározat]. A legfontosabb tevékenységet akkoriban a 2010 novemberében létrehozott, alábbi összetételű szakmai munkacsoport végezte, amelynek felállítását szintén a kormányhatározat rendelte el.

[4] Hatályon kívül helyezve: 2014. március 5.



a) **Honvédelmi miniszter**
b) Alkotmányvédelmi Hivatal
c) Országos Katasztrófavédelmi Főigazgatóság
d) Terrorelharítási Központ
e) Országos Rendőr-főkapitányság
Belügyminiszter
f) Nemzeti Biztonsági Felügyelet — **Közigazgatási és igazságügyi miniszter**
g) Magyar Kereskedelmi és Engedélyezési Hivatal — **Nemzetgazdasági miniszter**
h) Nemzeti Közlekedési Hatóság
i) Magyar Energia Hivatal
Nemzeti fejlesztési miniszter

1. ábra

A KIV-munkacsoport összetétele

Forrás: BONNYAI 2011, 53.

A delegált szakértők munkája eredményeként 2011 januárjában elkészült az EU felé küldendő első jelentés tervezete. Ezt követően a horizontális kritériumok rendszerének átültetése következett, amelyet a Kormány még a következő hónapban megtárgyalt és elfogadott. 2011 tavaszán megtörtént az EU által kijelölt ágazatok (közlekedés és energetika) potenciális európai kritikus infrastruktúráinak felmérése, amely alapján Magyarország nem tett javaslatot kijelölésre.

A fenti kormányhatározat feladatszabása alapján, a Nemzeti Fejlesztési Minisztérium vezetésével 2011 áprilisában megalakult a Kritikus Infrastruktúra Védelmi Konzultációs Fórum (a továbbiakban: KIV KF), azzal a céllal, hogy

– a kritikus infrastruktúrák védelmére magas szintű módszertant alakítson ki,
– a szabályozási feladatokat tudományos igényességgel készítse elő és
– döntés-előkészítő fórumként működjön.

A fórum munkájában részt vettek az érintett minisztériumok, intézmények, az energetikai, hírközlési és közlekedési szektor érintett hatóságai és szolgáltatói, illetve tudományos testületek képviselői. A KIV KF feladataként határozták meg, hogy

– elemezze és értékelje hazánk és harmadik országok együttműködéseit, függőségeit;
– aktív és személyes kapcsolatot alakítson ki a szolgáltatókkal, amely alapján a közös tevékenységek gördülékenyebben, az állami szempontok megértetése útján rugalmasabban végezhetők;
– az infokommunikációs technológiák szektorának hangsúlyozása érdekében a hazai energetikai, közlekedési, kormányzati informatikai és hírközlési szolgáltatók által biztosított szolgáltatások vizsgálata útján értékelje a fenti szolgáltatások kiesésének hatásait;
– azonosítsa a kapcsolódó hazai és nemzetközi legjobb gyakorlatokat;
– a meglévő tapasztalatok alkalmazásával javaslatokat tegyen a kritikus infrastruktúrák ellenálló képességének növelésére, illetve a kritikus infrastruktúrák védelmével kapcsolatos jogszabálytervezetek megalkotására egyaránt. [1249/2010. (XI. 19.) kormányhatározat]

3.1.2. A hatályos szabályozás

Az európai uniós folyamatok felülvizsgálata, az új megközelítések térnyerése Magyarországon is jótékonyan járult hozzá a kritikus infrastruktúrák védelmi rendszerének kialakításához. 2011. második félévében a már említett munkacsoport, valamint a KIV KF tevékenysége nyomán megkezdődött a hazai jogharmonizáció, amelynek eredménye a 2013. március 1-jén hatályba lépett 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Fontos hangsúlyozni, hogy a törvény az EU Irányelv által meghatározott tagállami kötelezettségeken túl (biztonsági összekötő személy és üzemeltetői biztonsági terv) több nemzeti sajátosságot is alapul vesz. A kritikus infrastruktúrák védelmével kapcsolatos feladatkört a hatósági felügyelet alatt tartás irányába tereli, ezáltal szigorúbb, de alapvetően együttműködésre ösztönző nemzeti keretszabályozást valósít meg. Európai uniós szinten is példaértékű a rendkívüli események kezelésével kapcsolatos állami beavatkozás kötelezettsége, a hálózatbiztonság prioritása, valamint a biztonsági összekötő személy kapcsán megállapított követelmények tudatos és szakmai jellege. (Bognár 2012)

*A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény*t (a továbbiakban: Lrtv.) az Országgyűlés 2012 novemberében tárgyalta meg és fogadta el. Célja elsősorban a kritikus infrastruktúrák azonosítása, másodsorban a kijelölést követően a megfelelő szintű védelem biztosítása. Az Lrtv. az értelmező rendelkezésekben található alapvető fogalmak meghatározásán túl körvonalazza a nemzeti és az európai kritikus infrastruktúrák kijelölésének rendjét, rendelkezik az üzemeltetői biztonsági terv készítésének kötelezettségéről, a biztonsági összekötő személy kijelöléséről, a nyilvántartás és ellenőrzés szabályairól, valamint a szankcionálás lehetőségeiről. Előírja továbbá az Európai Bizottság irányába történő éves jelentési kötelezettséget is. (Bognár et al. 2014)

Az Lrtv. felhatalmazást adott az alábbiakkal kapcsolatos részletszabályok kidolgozására:

- ágazati rendeletek,
- horizontális kritériumok,
- együttműködési alapelvek,
- közigazgatási bírság összegei,
- biztonsági összekötő személlyel kapcsolatos követelmények,
- üzemeltetői biztonsági tervvel kapcsolatos követelmények, valamint
- részletes hálózatbiztonsági speciális szabályok.

A felhatalmazó rendelkezések által a keretszabályozás alappillére lett a *65/2013. (III. 8.) Korm. rendelet* (a továbbiakban: Lrtv. vhr.), amelyet az Lrtv. végrehajtási rendeleteként tartunk számon. A kormányrendelet részletesen szabályozza:

- az azonosítási jelentés készítését,
- az azonosítási folyamat és kijelölési eljárás általános rendjét,
- az ágazati kijelölő és javaslattevő hatóságok szerepét, valamint
- a szakhatósági közreműködést egyaránt.

Fentieken túl külön rendelkezik:
- az ECI-k kijelölési eljárásáról,
- a biztonsági összekötő személy általános képesítési követelményeiről, amelyeket az ágazati kormányrendeletek további, szakmai feltételekkel egészítenek ki.

A részletszabályok nevesítik az üzemeltetői biztonsági terv készítésének körülményeit, részletesen meghatározzák a hatóságok, szakhatóságok és véleménynyilvánító szervek együttműködésének rendjét a szakhatósági eljárásra, az ellenőrzésekre és a rendkívüli események kezelésére vonatkozóan. A kormányrendelet melléklete tartalmazza az európai uniós mintán alapuló, kiegészített horizontális kritériumok rendszerét is.

A törvény és a végrehajtási rendelet szakmai kiegészítését képezik az úgynevezett ágazati rendeletek. Az ágazati kormányrendeletek az Lrtv. mellékleteiben felsorolt ágazatok és alágazatok vonatkozásában eltérő vagy kiegészítő rendelkezéseket tartalmaznak az azonosítási és kijelölési eljárás kapcsán, valamint megállapítják az ágazati kritériumokat és a biztonsági összekötő személlyel kapcsolatban meghatározott egyéb követelményeket. A meghatározott tíz ágazat vonatkozásában – eddig – nyolc ágazati kormányrendelet lépett hatályba, amelyek a következők:
- 360/2013. (X. 11.) Korm. rendelet az *energetikai* létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről;
- 512/2013. (XII. 29.) Korm. rendelet egyes *rendvédelmi szervek* létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) kormányrendelet módosításáról;
- 540/2013. (XII. 30.) Korm. rendelet a létfontosságú *agrárgazdasági* rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről;
- 541/2013. (XII. 30.) Korm. rendelet a létfontosságú *vízgazdálkodási* rendszerelemek és vízi létesítmények azonosításáról, kijelöléséről és védelméről;
- 246/2015. (IX. 8.) Korm. rendelet az *egészségügyi* létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről;
- 330/2015. (XI. 10.) Korm. rendelet a *pénzügyi* ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről;
- 359/2015. (XII. 2.) Korm. rendelet a *honvédelmi* létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről,
- 249/2017. (IX. 5.) Korm. rendelet az *infokommunikációs technológiák* ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

Az azonosítással és a kijelölési eljárással kapcsolatos definíciós környezet értelmezése (az Lrtv. alapján):

Ágazati kritériumok: azok a szempontok, küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy rendszerelem megzavarása vagy megsemmisítése által kiváltott hatásra vonatkoznak. Az ágazati kritériumok teljesülése esetén az eszköz, létesítmény, rendszer vagy azok egy része létfontosságú rendszerelemmé jelölhető ki abban az ágazatban, amelybe tartozik.

Horizontális kritériumok: azok a szempontok, amelyek egy rendszerelem megzavarása vagy megsemmisítése által kiváltott, a bekövetkező veszteségekre (emberélet, sérülés), az egészségre, a gazdasági és társadalmi következményekre, a természetre és az épített környezetre gyakorolt hatásra vonatkoznak.

Ágazati kijelölő hatóság: az ágazati és horizontális kritériumok vizsgálata alapján, a közigazgatási hatósági eljárás szabályainak megfelelően, határozatban dönt a nemzeti létfontosságú rendszerelem kijelöléséről vagy a kijelölés visszavonásáról. Kijelölés esetén meghatározza az üzemeltetői biztonsági terv kidolgozásának határidejét, valamint a létfontosságú rendszerelem védelmével összefüggő, a rendszerelem működését befolyásoló veszélyeztető tényezőkhöz igazodó védelmi/biztonsági feltételeket szab az üzemeltető részére.

Azonosítási jelentés: olyan dokumentum, amely az adott infrastruktúra tevékenységét, fizikai és informatikai biztonsági körülményeit és veszélyeztetettségét mutatja be a vizsgált időpontban. Célja, hogy igazolja vagy cáfolja a kritikus infrastruktúrává történő kijelölés feltételeinek teljesülését.

Biztonsági összekötő személy: feladata a kapcsolattartás az üzemeltető és a kijelölési eljárásban részt vevő hatóságok között. Biztonsági összekötőnek az a büntetlen előéletű személy jelölhető ki, aki kormányrendeletben meghatározott képzettséggel rendelkezik.

Üzemeltetői biztonsági terv: tartalmazza a létfontosságú rendszerelemeket és azt a szervezeti és eszközrendszert, amely biztosítja azok védelmét. Az üzemeltetői biztonsági tervben kell megjelölni azokat a biztonsági intézkedéseket, amelyek kialakítása és működtetése biztosítja a létfontosságú rendszerelem védelmét, beleértve azokat az ideiglenes intézkedéseket, amelyeket a különböző kockázati és veszélyszinteknek megfelelően foganatosítani kell.

A kritikus infrastruktúrák védelmével kapcsolatos tevékenység különleges jogrendbeli kapcsolódásai:

A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. CXXVIII. törvény (a továbbiakban: Kat.)

- 43. § (1) bekezdése szerint a kritikus infrastruktúrák védelme érdekében a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF) főigazgatója katasztrófaveszélyt állapíthat meg;
- 44. § cd) pontja szerint a Kormány veszélyhelyzetet hirdethet a kritikus infrastruktúrák olyan mértékű működési zavara esetén, amelynek következtében a lakosság alapvető ellátása több napon keresztül, vagy több megyét érintően akadályozott.

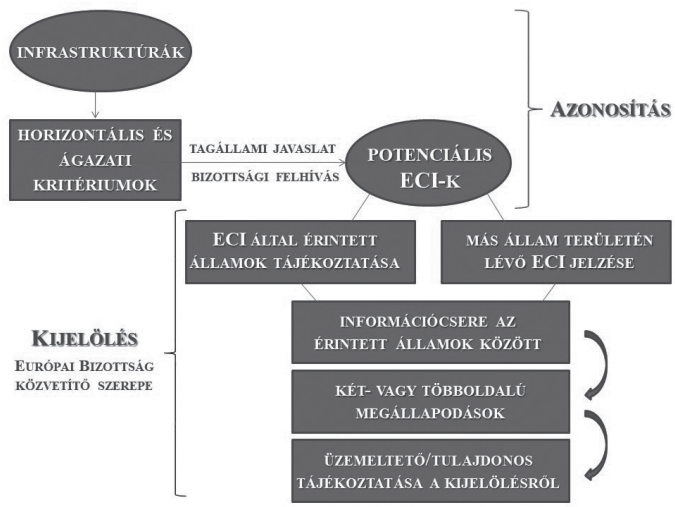
A Kat. végrehajtásáról szóló 234/2011. (XI. 10.) Korm. rendelet 31. § (2) bekezdés b) pontjában tételesen szerepel, hogy a központi veszélyelhárítási terv tartalmazza a kritikus infrastruktúra elemek katasztrófák elleni védelmére irányuló feladatokat, amely alapján a BM OKF főigazgatója megelőző és beavatkozói tevékenységet folytathat.

3.2. Az európai létfontosságú infrastruktúrák kijelölésének/kijelölés visszavonásának folyamata

Az Európai Unió *Zöld Könyve* szerint a határon átnyúló hatás lehetőségének fokozott fennállása esetén egyes infrastruktúrák sérülése nemcsak az adott tagállamban, hanem azon

kívül is veszélyeztetheti az élet- és vagyonbiztonságot. Az ilyen veszélyeztetettség regionális vagy globális szintű kockázati szintet jelenthet, ezért a fentieknek megfelelő potenciális létfontosságú rendszerelemeket európai kritikus infrastruktúraként (ECI) szükséges kijelölni.

Tekintettel arra, hogy az ECI működése, zavara vagy megsemmisülése több tagállamra hatással lehet, az Irányelv kötelezi a kiindulási tagállamot arra, hogy tájékoztassa a lehetséges hatás alatt álló tagállamokat a beazonosítással kapcsolatos információkról, amelyekről nemzetközi egyeztetéseket kell folytatni. A kijelölés csak akkor történhet meg, ha az érintett tagállamok arról megállapodás formájában döntést hoztak. A kijelölést követően az adott tagállam informálja az érintett infrastruktúra tulajdonosát/üzemeltetőjét a kijelölés tényéről, és a kijelölést rendszeresen felülvizsgálja. Az Irányelv szerinti, általános kijelölési folyamatot a következő ábra szemlélteti:



2. ábra

ECI-kijelölés általános folyamata az Irányelv alapján

Forrás: BONNYAI 2014

A hazai jogi szabályozás alapján európai kritikus infrastruktúrává történő kijelölést, illetve a kijelölés visszavonását kezdeményezheti:

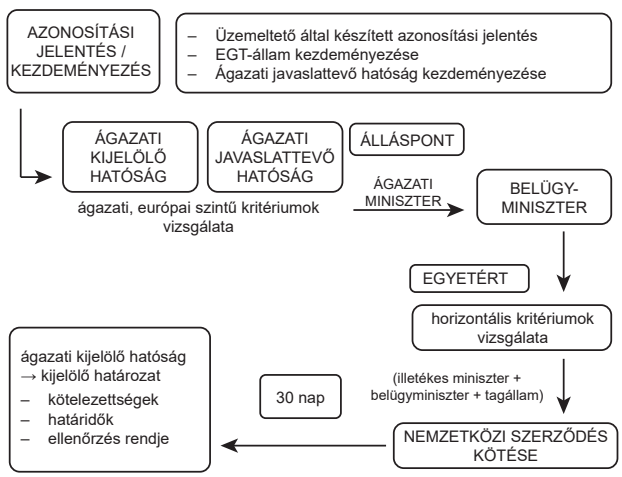
- *az érintett üzemeltető,* illetve a kormányrendeletben megállapított ágazati javaslattevő hatóság;
- az *Európai Unió tagállama* és az Európai Gazdasági Térségről szóló megállapodásban részes más állam *(EGT-tagállam).*

Az illetékes ágazati kijelölő hatóság – hivatalból indított eljárás keretében – megvizsgálja a kijelölésre/kijelölés visszavonására irányuló kezdeményezést, és a vizsgálat alapján kialakított álláspontjáról tájékoztatja az ágazatért felelős miniszter útján a katasztrófák elleni védekezésért felelős minisztert.

Az *európai létfontosságú rendszerelemmé nyilvánítással* kapcsolatban *nemzetközi szerződést kell kötni,* amelyet a katasztrófák elleni védekezésért felelős miniszter – egyetértése

esetén – az ágazati hatáskörrel rendelkező miniszterrel együtt kezdeményez az érintett tagállam irányába. Abban az esetben, ha az európai létfontosságú rendszerelem kijelöléséről/kijelölés visszavonásáról az ágazati miniszter és a katasztrófák elleni védekezésért felelős miniszter *ellentétes álláspontot* képvisel, a végleges döntést a Kormány hozza meg.

A nemzetközi szerződés hatálybalépésétől számított 30 napon belül az ágazati kijelölő hatóság *határozatot hoz* a kijelölésről. Az eljárás során a horizontális kritériumok teljesülésének vizsgálatát a katasztrófák elleni védekezésért felelős miniszter végzi. Az ágazati kijelölő hatóság kijelölő határozatában nevesíti az üzemeltető kötelezettségeit és az ellenőrzés rendjét, amelynek a nemzetközi szerződéssel összhangban kell lennie.



3. ábra
Az ECI kijelölésének eljárása hazánkban

Forrás: Bonnyai 2014

Kijelölés visszavonására irányuló kezdeményezés kapcsán (amennyiben a kezdeményezéssel a katasztrófák elleni védekezésért felelős miniszter egyetért) a kijelölés visszavonása a nemzetközi szerződésben foglaltaknak megfelelő közigazgatási eljárás keretében történik. A kijelölés visszavonását követően az ágazati kijelölő hatóság megvizsgálja a *nemzeti szintű kritériumok teljesülését, és szükség esetén határozatot hoz a nemzeti létfontosságú rendszerelem kijelöléséről.*

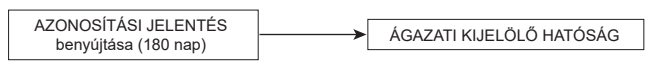
Amennyiben a katasztrófák elleni védekezésért felelős miniszter:

– az üzemeltető/ágazati javaslattevő hatóság európai kijelölésre irányuló *kezdeményezésével nem ért egyet,* az ágazati kijelölő hatóság köteles megvizsgálni a nemzeti kijelölés kérdését, és a kormányrendeletben meghatározott feltételek fennállása esetén dönt a kijelölésről;
– az üzemeltető/ágazati javaslattevő hatóság *európai kijelölés visszavonására irányuló kezdeményezésével nem ért egyet,* az ágazati kijelölő hatóság tájékoztatja az érintetteket a kijelölés fenntartásáról.

3.3. A nemzeti létfontosságú infrastruktúrák kijelölésének/kijelölés visszavonásának folyamata[5]

A potenciális nemzeti létfontosságú infrastruktúrák azonosítása keretében történik az infrastruktúrák kockázatbecslés-alapú meghatározása, amelynek elsődleges célja, hogy az egyes ágazatokra meghatározott kritériumok alapján, az üzemeltetők által működtetett infrastruktúrákat értékeljék és rangsorolják (megfelelnek-e az ágazati kritériumoknak). Az ágazati kormányrendeletek határozzák meg, hogy mely üzemeltetők kötelezettek azonosítás lefolytatására, annak keretében *azonosítási jelentés* készítésére, amely:

- a vizsgált rendszerelemre vonatkozó kockázatelemzést és annak eredményét,
- a kijelölésre irányuló javaslatot (vagy a kijelölés indokolatlanságát),
- a teljességére vonatkozó üzemeltetői nyilatkozatot, valamint
- az azonosítási eljárás kezdő- és zárónapját tartalmazza.



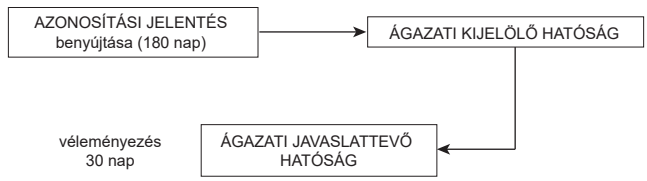
Az azonosítási jelentések benyújtási határideje az adott ágazati kormányrendelet hatálybalépését követő 180 nap.[6] A benyújtás az ágazati kijelölő hatóság részére történik, amelyet minden egyes ágazat esetében az ágazati kormányrendelet nevesít. Amennyiben egy potenciális kritikus infrastruktúra üzemeltetője nem tartja be a benyújtási határidőt, úgy az illetékes kijelölő hatóság – határidő megadásával – felszólítja a pótlásra. A benyújtást követően az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény. (a továbbiakban: Ákr.) szerinti *közigazgatási hatósági eljárás indul* az adott infrastruktúra nemzeti kritikus infrastruktúrává történő kijelölésének vizsgálatára. Az ágazati kijelölő hatóság által lefolytatott, az ágazati és horizontális kritériumok teljesülésének vizsgálatára irányuló *hatósági eljárás 70 napos*.

Ennek keretében az ágazati kormányrendeletek szerinti ágazati javaslattevő hatóság(ok) véleményezi(k) az azonosítási jelentést, amire a jogszabály *30 napot* biztosít. A véleményezés alapvetően az azonosítási jelentésben foglalt szakmai megállapításokra vonatkozik, az ágazati kritérium(ok) teljesülésére irányul. Az ennek során megalkotott, kockázatelemzéssel kapcsolatos javaslataikat az ágazati javaslattevő hatóságok megküldik az illetékes kijelölő hatóság részére. A javaslattevő hatóságoknak lehetősége van továbbá jelezni a kijelölő hatóság felé egyes üzemeltetők azonosítási jelentésre történő felszólításának szükségességét is, tehát kezdeményezhetnek kijelölési eljárást.

---

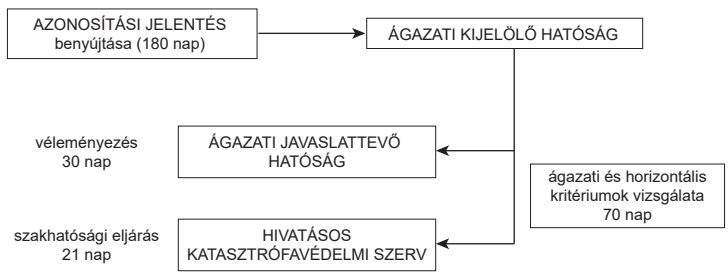
[5] Lásd: 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról; A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény.

[6] Hatályban lévő kormányrendeletek esetében a benyújtás határidejét az ágazati kijelölő hatóság külön állapítja meg.



A megindított kijelölési eljárás további fontos részcselekménye a *horizontális kritériumok*[7] *teljesülésének vizsgálata.* Ennek érdekében az ágazati kijelölő hatóság szakhatóságként bevonja (első fokon) a területileg illetékes hivatásos katasztrófavédelmi szerv helyi szervét.[8]

Azoknál az ágazatoknál, amelyeknél a katasztrófavédelem az eljárás során kijelölő hatósági feladatokat lát el, a szakhatósági megkeresésnek nincs helye, vagyis a horizontális kritériumok vizsgálata a kijelölő hatóság tevékenységében történik.



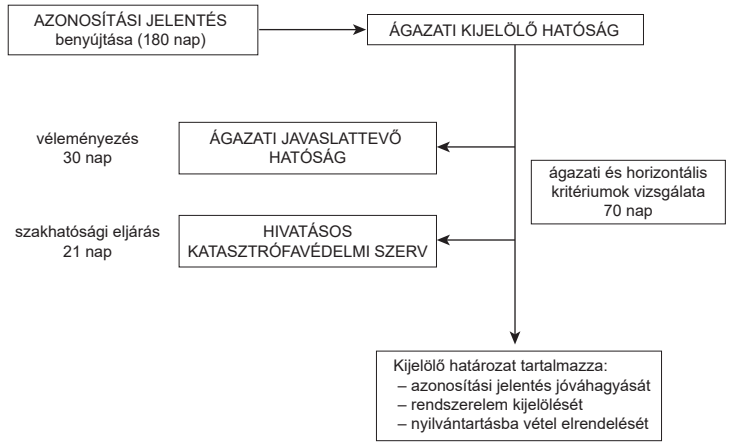
Az ágazati javaslattevő hatóság véleménye, a szakhatósági állásfoglalás, valamint az ágazati kijelölő hatóság szakmai vizsgálata és véleménye alapján, a fentiek szerint lefolytatott eljárás *határozathozatallal* zárul, amelyben az ágazati kijelölő hatóság az alábbi döntéseket hozhatja:

– a kritikus infrastruktúra kijelölése és nyilvántartásba vétele, amennyiben legalább egy ágazati és egy horizontális kritérium teljesülése fennáll;
– a korábbi kijelölés visszavonása és a nyilvántartásból való törlése;
– a kijelölési dokumentáció alapján a kijelölésre vagy a visszavonásra irányuló javaslat elutasítása, vagy
– legfeljebb 90 napos határidő kitűzésével a feltárt hibák, hiányosságok megjelölése mellett új azonosítási jelentés benyújtására kötelezés.

A kijelölésre irányuló, a kijelölést elfogadó hatósági eljárást a következő ábra foglalja össze:

[7] A horizontális kritériumok vizsgálatának részletes leírását az 4. fejezet tartalmazza.

[8] Az egyes közérdeken alapuló kényszerítő indok alapján eljáró szakhatóságok kijelöléséről szóló 531/2017. (XII. 29.) Korm. rend. 1. melléklet 19. táblázat (Egyéb ügyek) 9. sor.



4. ábra

A kijelölési eljárás főbb mozzanatai

Forrás: a szerző szerkesztése

Amennyiben kijelölő határozat kiadására kerül sor, annak tartalmaznia kell:

- az üzemeltető azonosítási jelentésének jóváhagyását,
- a létfontosságú rendszerelem nyilvántartásba vételét,
- az üzemeltetői biztonsági terv kidolgozásának határidejét, valamint
- a kijelölt infrastruktúra védelmével összefüggő, annak egyedi sajátosságaihoz, környezetéhez és az általa potenciálisan előidézhető veszélyek mértékéhez igazodó további kötelezettségeket.

3.4. A biztonsági összekötő szerepe és hazai követelményei

Az európai uniós Irányelv, valamint a hatályos jogszabályok alapján az európai és a nemzeti létfontosságú rendszerelem üzemeltetőjének feladata, hogy gondoskodjon a biztonsági összekötő személy (nemzetközi rövidítése: SLO, security liaison officer) foglalkoztatásáról, és folyamatosan biztosítsa a tevékenységéhez szükséges feltételeket. Amennyiben az üzemeltető a követelményeknek megfelelő személyt már foglalkoztat, az a személy biztonsági összekötőnek kinevezhető *(= mentesülési kivételszabály).*

A biztonsági összekötő személy *elsődleges feladata* az üzemeltető és a kijelölési eljárásban részt vevő hatóságok (ágazati kijelölő hatóság, javaslattevő hatóságok, katasztrófavédelem, véleménynyilvánító szervek) közötti *kapcsolattartás,* és *felelős az együttműködésre vonatkozó kötelezettségek betartásáért.* A legtöbb biztonsági összekötő személy már a kijelölési eljárás során (tehát a kijelölés előtt, vagyis a biztonsági összekötő személyként történő kinevezését megelőzően!) aktívan részt vesz az azonosítási jelentés elkészítésében, az azzal kapcsolatosan felmerült kérdések megválaszolásában (például: hiánypótlás, helyszíni ellenőrzés).

A kijelölt létfontosságú rendszerelemként történő működés során fontos szerepe lehet a kijelölés visszavonására irányuló azonosítási jelentés [Lrtv. vhr. 2. § (2) a) pont szerint] elkészítésében, illetve *felelős* az *5 évente* készítendő *azonosítási jelentés* [Lrtv. vhr. 2. § (8) bekezdés szerint] összeállításáért, vagyis a kijelölés fenntartására vonatkozó eljárás lefolytatásában történő részvételért. Mindezek ellátása keretében *kockázatelemzést* végez a veszélyeztető tényezők vizsgálata, a potenciális sebezhetőségek feltárása, a folyamatos rendelkezésre állást akadályozó körülmények által okozott következmények értékelése céljából.

Ennek területei a *működés vonatkozásában* legfőképpen
- a természeti és épített környezet, földrajzi elhelyezkedés vizsgálata,
- a működési feltételek (például: energiaellátás) összefoglalása,
- a működési sajátosságok megállapítása.

A *működés zavara tekintetében* pedig elsősorban
- a működési zavarok hatása a rendszerelemen belül,
- a működési zavarok hatása a rendszerelemen kívül (például: környezet, lakosság, szolgáltatási lánc, dominóelv, nemzetgazdaság, közbiztonság, államigazgatás működése).

Az *együttműködési kötelezettség* tekintetében kiemelt szerepe van a folyamatban lévő hatósági eljárások során az illetékes *hatóságok munkájának támogatás*ában, az *ellenőrzések* szervezésében és lebonyolításában, a *gyakorlatok* előkészítésében és végrehajtásában. Az üzemeltetővel kötött munkaszerződésében (és munkaköri leírásában) célszerű rögzíteni, hogy felelős az üzemeltető adatszolgáltatási kötelezettségének teljesítéséért, illetve a rendkívüli események kezelésében történő aktív részvételért. *Rendkívüli eseményeket* követően az Lrtv. vhr. 11. § (6) e) pontja szerint közreműködik a következtetések megállapításában, amelyeket kötelessége beépíteni a biztonsági folyamatokba és dokumentációkba (üzemeltetői biztonsági terv) egyaránt.

Biztonsági összekötőnek az a *büntetlen előéletű személy* jelölhető ki, aki a végrehajtási és ágazati kormányrendeletekben *meghatározott képzettséggel rendelkezik.* A büntetlen előéletre és a végzettségre vonatkozó követelmény teljesülését a biztonsági összekötőnek kell igazolnia, amelyet az ellenőrzések során a katasztrófavédelem és az illetékes hatóságok ellenőrizhetnek (Lrtv.). A 2017. január 1-jén hatályba lépett módosítások következtében a biztonsági összekötő személyeknek az ágazatnak megfelelő szakirányú végzettség mellett rendelkezniük kell

a) védelmi igazgatási, katasztrófavédelmi vagy rendészeti igazgatási szakon szerzett felsőfokú végzettséggel,
b) tűzvédelmi, iparbiztonsági, polgári védelmi szakmai irányú rendészeti szervezői szakképesítéssel, vagy ezzel egyenértékű végzettséggel,
c) iparbiztonsági szaktanfolyami végzettséggel,
d) iparbiztonsági szakon szerzett felsőfokú végzettséggel, vagy
e) a katasztrófavédelem hivatásos szerveinél legalább 5 év iparbiztonsági szakterületen szerzett gyakorlattal.

Ezek a rendelkezések alapvetően a szakmaiságot, a tudatosságot és a tervezhetőséget hivatottak erősíteni (Lrtv. vhr.).

3.5. Az üzemeltetői biztonsági terv készítésének célja és alapvető módszere

Az üzemeltetői biztonsági terv (nemzetközi rövidítése: OSP, Operator Security Plan) készítése az üzemeltető kijelölő határozatban előírt törvényi kötelezettsége, amelynek határideje nem lehet rövidebb a kijelölő határozat közlésétől számított 60 napnál. Amennyiben a kijelöléskor a rendszerelem rendelkezik olyan biztonsági dokumentummal, amely az üzemeltetői biztonsági terv tartalmi elemeit magában foglalja, akkor a kijelölő hatóság rendelkezhet úgy a határozatban, hogy a meglévő dokumentumot elfogadja a kötelezettség teljesítéseként *(= mentesülési kivételszabály).*

A létfontosságú rendszerelem védelmét és folyamatos rendelkezésre állását az üzemeltetői biztonsági tervvel összhangban kell megszervezni. A dokumentáció tartalmi és formai követelményeit – az Lrtv. vhr. 2. sz. melléklete alapján – a kijelölő határozat részletezi, de mindenképpen tartalmazza:

- a kritikus infrastruktúra pontos megnevezését;
- azt a szervezeti eszközrendszert, amely biztosítja annak védelmét;
- azokat az ideiglenes intézkedéseket, amelyeket a különböző kockázati és veszélyszinteknek megfelelően foganatosítani kell;
- meglévő vagy kialakítás alatt álló biztonsági megoldásokkal kapcsolatos eljárást,
- potenciálisan bekövetkezhető rendkívüli eseményeket.[9]

Az Lrtv. vhr. 2. sz. melléklete alapján elkészített üzemeltetői biztonsági tervet (a továbbiakban: ÜBT), az ágazati kijelölő hatóság a határozatában meghatározott követelmények teljesülése érdekében a nyilvántartásba vételt megelőzően formailag és tartalmilag ellenőrzi, hiányosság esetén az üzemeltetőt hiánypótlásra szólítja fel. Az ágazati kijelölő hatóság az ellenőrzött („elfogadott") üzemeltetői biztonsági tervet küldi meg a nyilvántartó hatóságnak és az üzemeltetőnek. A rendkívüli események kezelése e szerint a terv szerint kezdődhet meg. Tekintettel arra, hogy a nyilvántartó hatóság egyben a rendkívüli események koordinációjáért is felel, rendelkeznie kell a terv egy példányával.

Az ÜBT üzemeltető általi, önálló módosítása *jelentős működésbeli* változások esetén vagy a *kétévente esedékes rendszeres felülvizsgálat* eredményeinek függvényében válhat szükségessé. A módosításokról minden esetben jegyzőkönyvet kell készíteni, azt a kijelölő és nyilvántartó hatóságnak meg kell küldeni. A módosított üzemeltetői biztonsági tervet a benyújtás rendje szerint kell az illetékes hatóságok részére eljuttatni.

Soron kívüli felülvizsgálatot kezdeményezhet az ágazati kijelölő hatóság vagy az ágazati kijelölő hatóságon keresztül a BM OKF, amelyet az üzemeltető köteles 45 napon belül elvégezni. A felülvizsgálatról jegyzőkönyv készül, amelyet az üzemeltető – ha a felülvizsgálat eredményeként a tervet nem szükséges módosítani – megküld az ágazati kijelölő hatóság és a BM OKF részére.

Az európai létfontosságú rendszerelem vagy a nemzeti létfontosságú rendszerelem működésének védelmét és folyamatosságát az üzemeltetői biztonsági tervvel összhangban kell megszervezni, ezért annak *tartalma nem nyilvános*.

---

[9] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.

Az üzemeltető alábbi *kötelezettségei* a működés folyamatos nyomon követését biztosítják a hatóságok részére:

– az azonosításkor fennálló körülményeket érintő változásokról 8 napon belül tájékoztatja az illetékes ágazati kijelölő hatóságot;
– a nyilvántartott adatokat érintő változásokról 3 napon belül tájékoztatja a nyilvántartó hatóságot;
– rendkívüli esemény bekövetkezésekor haladéktalanul értesíti az illetékes ágazati kijelölő hatóságot és a hivatásos katasztrófavédelmi szerv területi szervének ügyeleti szolgálatát egyaránt.[10]

Felhasznált irodalom

Bognár Balázs (2012): A létfontosságú rendszerek és létesítmények védelme. *Katasztrófavédelmi Szemle,* 19. évf. 4. sz. 13–17.

Bognár Balázs – Kátai-Urbán Lajos – Vass Gyula (2014): A létfontosságú rendszerek és létesítmények védelméről szóló szabályozás végrehajtása Magyarországon. *Bolyai Szemle,* 23. évf. 2. sz. 105–112.

Bonnyai Tünde (2011): *A kritikus infrastruktúra védelem fogalmi rendszere, hazai és nemzetközi szabályozása.* Pályázati anyag a Katasztrófavédelmi Tudományos Tanács pályázatára.

Bonnyai Tünde (2014): *A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében.* Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem.

Bonnyai Tünde – Bognár Balázs (2009): The process of critical infrastructure protection. *Academic and Applied Research in Military Science,* Vol. 8. Issue 3. 499–513.

Kátai-Urbán Lajos szerk. (2013): *Iparbiztonságtan I. Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához*. Budapest, Nemzeti Közszolgálati Egyetem.

Hivatkozott jogszabályok és dokumentumok

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.

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.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény.

[10] 65/2013. (III. 8.) Korm. rend.

Vákát oldal

4. fejezet
A hivatásos katasztrófavédelmi szerv feladat- és hatásköre

Bognár Balázs

4.1. Feladat- és hatáskörök áttekintése

A katasztrófavédelem az Lrtv. és az Lrtv. vhr. rendelkezéseiben deklarált koordinatív és hatósági szerepet kapott, a kritikus infrastruktúrák védelméhez kapcsolódó tevékenysége elsősorban a rendeltetéséből és a vonatkozó jogszabályi háttér alapján vezethető le. *A katasztrófák elleni védekezés rendszerében – a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény* (Kat.) különleges jogrendre vonatkozó rendelkezései alapján [44. § cd) pont] – a kritikus infrastruktúrák meghibásodása, kiesése vagy megsemmisülése lehetőséget ad arra, hogy a Kormány veszélyhelyzetet hirdessen, amelyet a BM OKF főigazgatója által megállapított katasztrófaveszély időszaka [43. § (1) bekezdés] előz meg. A fentiek maradéktalan végrehajtása érdekében a katasztrófavédelmi törvény 12. § c) pontja szerint a védekezésre való felkészülés és a megelőzés keretében a BM OKF főigazgatója kapcsolatot tart a kiemelt informatikai és távközlési szolgáltatókkal, a kritikus infrastruktúra elemek üzemeltetőivel, valamint az országos médiaszolgáltatókkal egyaránt.

Ezt a felhatalmazást egészíti ki *a katasztrófák elleni védekezés egyes szabályairól szóló 62/2011. (XII. 29.) BM rendelet* 13. §-ában rögzített, a katasztrófavédelmi igazgatókat feljogosító feladatkör, amely szerint

- ellátják a kritikus infrastruktúrák védelmével kapcsolatos feladatokat;
- közreműködnek a kritikus infrastruktúra elemek beazonosítási, kijelölési folyamatában;
- irányítják az illetékességi területükön található európai vagy nemzeti kritikus infrastruktúra elemek védelmének erősítését célzó területi katasztrófavédelmi gyakorlatok tervezését és végrehajtását;
- összesítik, a tervezés során felhasználják az illetékességi területükön található európai vagy nemzeti kritikus infrastruktúra elemek védelmét ellátó szervezetek, valamint az érintett hálózat üzemeltetőjének tapasztalatait és igényeit;
- kapcsolatot tartanak az illetékességi területükön található európai vagy nemzeti kritikus infrastruktúra elemek tulajdonosaival, üzemeltetőivel, az azok védelmét ellátó szervezetekkel, valamint az érintett hálózatok üzemeltetőivel.

A kifejezetten szakmai alapokon nyugvó, hatósági formában érvényesíthető tevékenységi köröket az Lrtv. és az Lrtv. vhr. rendelte a szervezethez, amelyeket együttesen értelmezve

határozható meg a *hivatásos katasztrófavédelmi szerv markáns – de nem privilegizált – szerepe* a kritikus infrastruktúrák védelmének hazai rendszerében.

Fontos hangsúlyozni, hogy az a tevékenység, amelyet a katasztrófavédelem és a további – eljárásban részt vevő – szervek végeznek az alapvető szükségleteket biztosító rendszerek *folyamatos rendelkezésre állása érdekében,* rendkívül *magas szintű együttműködési hajlandóságot,* az állam részéről biztosítandó, a *szolgáltató hatósági szemlélet szerinti működést* és a *reagálóképesség folyamatos fejlesztésének igényét* feltételezi mind az üzemeltető, mind a hatóságok részéről.

Az ellátott feladatok jellegét és a katasztrófavédelem hatáskörrel felruházott szervezeti szintjeit tekintve a kritikus infrastruktúrák védelméhez köthető feladatok az alábbiak szerint jelentkeznek a szervezetben:

- hivatásos katasztrófavédelmi szerv helyi szerve *(katasztrófavédelmi kirendeltség)*
  - elsőfokú szakhatóság – horizontális kritériumok vizsgálata
- hivatásos katasztrófavédelmi szerv területi szerve *(katasztrófavédelmi igazgatóság)*
  - ágazati kijelölő hatóság – meghatározott ágazatokban
- hivatásos katasztrófavédelmi szerv központi szerve *(BM OKF)*
  - nyilvántartó hatóság,
  - ellenőrzéseket koordináló szerv,
  - általános javaslattevő hatóság,
  - rendkívüli események kezelése,
  - Európai Kritikus Infrastruktúra Védelmi Kapcsolattartási Pont (CIP POC),
  - információbiztonsági hatóság.

A 4.2.–4.6. alfejezetek a BM OKF, vagyis a központi szerv feladat- és hatásköreit mutatják be, a 4.7. alfejezet a területi szervek, míg a 4.8. a helyi szervek feladatait foglalja össze.

4.2. Nyilvántartási szabályok – a nyilvántartó hatóság

Az Lrtv. vhr. 10. § (1) bekezdésében a Kormány – a honvédelmi kritikus infrastruktúrák kivételével[1] – az európai és nemzeti kritikus infrastruktúrák nyilvántartó hatóságaként jelöli ki a BM OKF-et, amely ennek keretében jogosult a jogszabályi felhatalmazásnak megfelelő adatok nyilvántartására és kezelésére. A hatósági eljárás keretében hozott véglegessé vált határozatot az ágazati kijelölő hatóság haladéktalanul megküldi a BM OKF részére, amelyet a kijelölési eljárás, illetve a kijelölés visszavonására vonatkozó eljárás lefolytatásának, valamint a hatósági ellenőrzések lebonyolításának biztosítása érdekében nyilvántartásba vesz. A nyilvántartási jogkör kiterjed:

- az üzemeltető adataira (név, székhely/lakcím, levelezési cím, cégjegyzékszám/egyéni vállalkozói nyilvántartási szám, adószám, képviselő neve, telefonszám, e-mail-cím);
- *biztonsági összekötő személy* személyazonosító adataira (telefonszám, e-mail-cím, szakirányú végzettség, végzettséget igazoló okirat sorszáma);

[1] Honvédelmi létfontosságú rendszerelemek tekintetében külön kormányrendeletben meghatározott nyilvántartó hatóság jár el. Lásd 6. fejezet.

– nemzeti létfontosságú rendszerelemek és olyan európai *létfontosságú rendszerelemek megnevezésére,* amelyek hazai érintettségűek;
– az üzemeltetői biztonsági tervre (és módosításaira);
– az ágazati kijelölő hatóság létfontosságú rendszerelem kijelölésére, illetve a kijelölés visszavonására irányuló *határozatára.*

Az üzemeltető és a biztonsági összekötő személy adatai tekintetében az érintett felelőssége és kötelezettsége, hogy az adataiban bekövetkező változásról 72 órán belül tájékoztassa a BM OKF-et.

Az eljárások és ellenőrzések lefolytatása érdekében a nyilvántartó hatóság kérésre *adatot továbbíthat* a kijelölési/kijelölés visszavonására irányuló eljárásban részt vevő ágazati javaslattevő és kijelölő hatóságok, valamint a szakhatósági állásfoglalás kiadásában érintett szervezetek részére:

– az ellenőrzések előzetes koordinációjának lebonyolításához;
– a helyszíni ellenőrzések lefolytatása céljából;
– a jogszabály alapján feladat- és hatáskörrel rendelkező hatóságok részére a hatósági ellenőrzések lefolytatása céljából;
– rendkívüli esemény bekövetkezése esetén az eseménykezelésben és a helyreállításban részt vevő szervek tevékenységének támogatása céljából;
– saját területi és helyi szervei részére hatósági, megelőzési, kapcsolattartási és tájékoztatási feladatai elvégzése, illetve rendkívüli esemény kezelése céljából.

A jogosult szervek írásban, az adatigénylés céljának és az átvenni kívánt adatok körének pontos megjelölésével kérhetnek adatszolgáltatást, amelyet a nyilvántartó hatóságnak 15 napon belül teljesítenie kell.

A BM OKF a kijelölés *visszavonásáról szóló határozat véglegessé válása után egy évvel,* illetve a kijelölést elutasító határozat véglegessé válásakor *törli az adatokat* a nyilvántartásból, és erről értesíti az érintett üzemeltetőt is.[2]

Az ágazatok szakértőivel folytatott egyeztetések és a korábbi fejlesztési tapasztalatok alapján a BM OKF-nél rendelkezésre álló Microsoft SharePoint csoportmunka-alkalmazás jelentette a megfelelő fejlesztési platformot a nyilvántartási rendszer kialakítására, így 2014 júliusában megkezdődött a létfontosságú rendszerek és létesítmények SharePoint-alapú nyilvántartásának tervezése, majd fejlesztése. A fejlesztés, tesztelés és éles használat során folyamatosan változnak, nőnek a nyilvántartással kapcsolatos igények, amelyek mind komplexebbé és hatékonyabbá tették és teszik az alkalmazást.

A SharePoint alkalmazásának előnyei:

– központilag menedzselt szervereken fut, a katasztrófavédelem hálózatából bárhonnan elérhető, tehát biztosított a magas rendelkezésre állás,
– felhasználói szintű azonosítás,
– a jogosultsági szint személyre szólóan, illetve csoportszinten szabályozható,
– több felhasználós adatrögzítés, valós idejű adatlekérdezés,

[2] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény; A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet.

- az adatrögzítés naplózott (létrehozás és utolsó módosítás időpontja és felhasználója),
- nincs különleges szoftverigénye (Internet Explorerben fut),
- könnyen elsajátítható, intuitív módon tanulható a használata,
- mindenkinek egységes, naprakész információt biztosít, valós idejű frissítéssel,
- összekapcsolható a Microsoft Office programokkal (Word, Excel, Access, Outlook),
- automatikus, valós idejű, e-mail-alapú változáskövetés,
- nyilvános és egyéni lekérdezések, kimutatások készítése statikus és dinamikus feltételekkel.

A kritikus infrastruktúrák jelenlegi nyilvántartása alkalmas:
- az Lrtv.-ben felsorolt adatok nyilvántartására,
- kijelölő és kijelölést visszavonó határozatok nyilvántartására,
- határozatok szkennelt példányának tárolására,
- a nyilvántartott adatok visszanyerésére (keresés, szűrés, csoportosítás, összesítés),
- a nyilvántartott adatok alapján listák, kimutatások, grafikonok készítésére valós idejű adatok felhasználásával.

A nyilvántartás elkülönített listákban tárolja a kijelölt rendszerelemek adatait, az üzemeltetői adatokat, a biztonsági összekötő személyek adatait, illetve a határozatok szkennelt példányait. A listák között kapcsolódási pontokat alakítottak ki; az egyes listák a következők szerint épülnek fel:

Kijelölt rendszerelemek lista adattartalma:
- üzemeltető (és képviselő),
- kijelölt rendszerelem megnevezése,
- ágazat, alágazat,
- kijelölő hatóság,
- státusz, státusz dátuma,
- biztonsági összekötő személy,
- ÜBT iktatószáma, dátuma, kezelési utasítása/minősítése, minősítés érvényessége,
- állami vagy önkormányzati szervként működik-e az üzemeltető,
- létesítmény címe,
- ellenőrzés dátuma, ellenőrök neve,
- tájékoztató körlevelek kiküldésének aktuális állapota.

Biztonsági összekötők lista adattartalma:
- név, születési név,
- születési hely, idő,
- anyja neve,
- telefon, fax, e-mail,
- szakirányú végzettség megnevezése,
- végzettséget igazoló okirat sorszáma,
- biztonsági összekötő személyek részére szervezett tanfolyamon részt vett-e.

Üzemeltetői adatok lista adattartalma:

– üzemeltető neve,
– székhely címe, megye,
– levelezési cím,
– cégjegyzékszám,
– képviselő neve,
– telefon, fax, e-mail,
– információbiztonsági szempontú státusza (állami vagy önkormányzati szerv-e).

Dokumentumtár adattartalma:
– dokumentum típusa, a feltöltött dokumentum,
– iktatószám,
– kiadmányozás dátuma,
– kijelölt rendszerelem megnevezése,
– adatkezelő személy megnevezése, felvitel-módosítás dátuma.

Az adatok nyilvántartásba vétele több lépcsőben, több dokumentum felhasználásával történik. A kijelölt rendszerelem alapadatait a nyilvántartó hatóságnak megküldött kijelölő határozat alapján rögzítik. Az üzemeltető képviselőjére és a biztonsági összekötő személyre vonatkozó adatok bekérésére a hatóság formanyomtatványt készített, amelyet az érintettek írásban, postai úton juttatnak el a BM OKF részére. Az üzemeltetői biztonsági tervre vonatkozó adatok a megküldött ÜBT alapján kerülnek az adatbázisba. Tekintettel arra, hogy a nyilvántartó hatóság nem vesz részt a kijelölési eljárásokban, így közvetlen információval a kijelölés folyamatáról, annak pillanatnyi állásáról nem rendelkezik. A nyilvántartásban rögzítendő adatokról a BM OKF részben a kijelölő hatóság, részben az üzemeltető, részben a biztonsági összekötő személy által – jogkövető módon – megküldött dokumentumok beérkezése alkalmával szerez tudomást.

A papír alapon érkező dokumentumok iktatását követően a kapott adatokat a nyilvántartó rendszerben rögzítik. A feldolgozott dokumentumok tárolása zárt, elkülönített lemezszekrényben történik. A nyilvántartáshoz kapcsolódó irattár elkülönített körletben került kialakításra, a helyiségbe való bejutás csak többszintű elektronikus beléptetést követően lehetséges.

4.3. Ellenőrzések rendje – az ellenőrzést koordináló szerv[3]

Az Lrtv. 8. § (1) bekezdése az ellenőrzéseket koordináló szervként nevesíti a BM OKF-et, amely a kijelölt európai és nemzeti rendszerelemeket – a honvédelmi kritikus infrastruktúrák kivételével[4] – rendszeresen, legalább 5 évente ellenőrzi.

A koordinált ellenőrzések elsődleges célja a jogszabályszerű működés és az ÜBT-ben foglaltak valószerűségének vizsgálata, a nyilvántartott adatok megfelelőségéről való meg-

[3] Vonatkozó jogszabályok: A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény; A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet

[4] Honvédelmi létfontosságú rendszerelemek tekintetében külön kormányrendeletben meghatározott ellenőrzést koordináló szerv jár el. Lásd 6. fejezet.

győződés, valamint a fizikai, humán és informatikai biztonsági feltételek meglétének vizsgálata.

Ezen feladatkörében:

– *koordinálja* a hatósági ellenőrzéseket, amelyek végrehajtására tárgyévet megelőző év november 30-ig éves ellenőrzési tervet készít az érintett hatóságok javaslatai alapján;
– *javaslatot tesz* a jogszabály alapján feladat- és hatáskörrel rendelkező hatóságok részére ellenőrzés lefolytatására;
– több társhatóság bevonásával *együttes hatósági ellenőrzéseket szervez,* amelyekben a hatóságok kötelesek együttműködni;
– az eljárások kimeneteléről, a megállapított hiányosságok pótlásáról *tájékoztatást kérhet* mind az összehangolt, mind a saját hatáskörben lefolytatott ellenőrzéseket végző szervektől.

A hatóságok az együttműködés keretében minden évet megelőző év október 15-ig megküldik az ellenőrzési tervre vonatkozó javaslataikat a BM OKF részére, együttműködésüket az Lrtv. szerinti kötelezettség garantálja. Ugyanez alapján a részt vevő hatóságok tájékoztatják a BM OKF-et az ellenőrzések tapasztalatairól és eredményeiről egyaránt. Az adott évben végrehajtott ellenőrzésekről a BM OKF a következő év március 1-jéig összefoglaló jelentést készít.

A kritikus infrastruktúrák védelme vonatkozásában az ellenőrzés mint hatósági eszköz elsősorban az üzemeltetővel történő hatékony és eredményes együttműködést erősíti, amelyben a szolgáltató hatóság szupportív szerepet tölt be. A védelmi tevékenység alapvető céljának – az üzemfolytonosság, a folyamatos rendelkezésre állás biztosítása – teljesülése érdekében végzett ellenőrzések lehetőséget teremtenek azon hiányosságok feltárására, amelyek rendkívüli események bekövetkezése során a szolgáltatás visszaállításának idejére vagy a szolgáltatással érintettek körének kiterjedésére lehet hatással.

Amennyiben bármely típusú ellenőrzés során megállapítják, hogy az üzemeltető nem tesz eleget a jogszabályokban foglalt kötelezettségeinek, úgy a *részt vevő hatóságok kezdeményezésére, illetve önállóan* az ágazati kijelölő hatóságnak joga van:

– felszólítani az üzemeltetőt a kötelezettségei betartására – ennek megtörténtét ellenőrizni;
– kötelezni az üzemeltetőt az üzemeltetői biztonsági terv módosítására, vagy új terv készítésére;
– bírságot kiszabni, amelynek mértéke 100 000 Ft-tól 3 000 000 Ft-ig terjedhet, és a jogerőre emelkedéstől számított 15 napon belül kell megfizetni.

Fontos hangsúlyozni, hogy a hivatásos katasztrófavédelmi szerv központi szerve (BM OKF) önállóan nem tehet szankcionálási intézkedést, arra kizárólag az ágazati kijelölő hatóságot hatalmazza fel az Lrtv. vhr.

4.4. Általános javaslattevő hatósági feladatkör[5]

Az Lrtv. vhr. 3. § szerint a Kormány a BM OKF-et a közrend, a közbiztonság, a lakosságvédelem, az alkotmányvédelem, a nemzetbiztonság és a terrorelhárítás kiemelt szempontjaira tekintettel általános *javaslattevő hatósággá* jelöli ki. Ennek keretében külön kötelezettsége, hogy az egyes ágazatok vonatkozásában figyelemmel legyen a potenciális kritikus infrastruktúrákra. Amennyiben megállapítja, hogy egy infrastruktúra-elem sérülése, kiesése vagy megsemmisülése

- hatást gyakorolhat a *közbiztonság* fenntartására,
- befolyásolhatja a *lakosság és az anyagi javak védelmét vagy a nemzetgazdaság működését,*
- *alkotmányvédelmi, nemzetbiztonsági vagy terrorelhárítási* szempontból meghatározó érdekeket és alapelveket sért,

javasolnia kell az illetékes ágazati kijelölő hatóság felé a nemzeti kritikus infrastruktúrává történő kijelölési eljárás megindítását. Az illetékes ágazati kijelölő hatóság – a javaslat mérlegelését követően – rendelkezik az üzemeltető irányába az azonosítási jelentés elkészítésére.

A BM OKF ezt az ágazatokon átívelő jogkörét a *Közbiztonság-védelem* ágazat (vagyis a rendvédelmi szervek) vonatkozásában *nem gyakorolhatja.*

4.5. Rendkívüli események – központi koordináló szerv[6]

Figyelemmel arra, hogy a BM OKF nyilvántartó hatóságként rendelkezik a kritikus infrastruktúrák alapvető adataival és az ÜBT-k által ismeri a megelőzés érdekében tett, illetve a védekezés során foganatosítandó intézkedéseket, a bekövetkezett rendkívüli eseményre történő reagálás, mentésszervezés, irányítás, valamint a lakosság tájékoztatása, a károk felmérése és a helyreállítás a BM OKF koordinálásával történik.

Az üzemeltető elsődleges felelőssége rendkívüli esemény bekövetkezésekor a területi katasztrófavédelmi igazgatóság ügyeleti szolgálatának értesítése, amely szükség esetén gondoskodik az elsődleges beavatkozó szervek helyszínre irányításáról, majd az értesítési rendnek megfelelően tájékoztatja a BM OKF-et.

Az Lrtv. vhr. 11. § (6) bekezdése alapján rendkívüli esemény bekövetkeztekor a BM OKF jogosult az érintett hatóságoktól további adatokat kérni a beavatkozás és kárelhárítás eredményes végrehajtása érdekében, amely adatszolgáltatást az érintett hatóság köteles soron kívül teljesíteni. A mindezekhez szükséges erők-eszközök bevonására az érintett ágazati kijelölő hatóság tesz javaslatot.

---

[5] Vonatkozó jogszabály: A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet.

[6] Vonatkozó jogszabály: A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet.

A BM OKF ezen szerepkörében elsődlegesen operatív irányítást végez, a helyszínre érkező beavatkozó állomány, az üzemeltető saját állománya, valamint az ágazat részéről rendelkezésre bocsátható erők, eszközök vonatkozásában, annak érdekében, hogy az üzemmenet folytonossága a lehető legrövidebb időn belül visszaállítható legyen.

A rendkívüli eseményt kiváltó okok azonosítását, a megtett intézkedések értékelését az érintett ágazati kijelölő hatóság, a beavatkozó szervek és a biztonsági összekötő személy együttesen végzik. Ha a vizsgálat során bebizonyosodik, hogy a bekövetkezett rendkívüli eseménnyel összefüggő kockázatot az ÜBT-ben korábban nem vizsgálták, akkor az üzemeltető soron kívül módosítja azt, és a megfelelő eljárásrendet követve megküldi az illetékes ágazati kijelölő hatóságnak.

A rendkívüli események azonosítása, megelőzése, valamint hatékony kezelése érdekében a katasztrófavédelem gyakorlatokat szervez a kritikus infrastruktúrák üzemeltetőinek közreműködésével, ami szintén mutatja, hogy a hatóság és az ügyfél közötti aktív és tartalmas kapcsolattartás és az együttműködés nélkülözhetetlen eleme a kritikus infrastruktúrák védelmének.

4.6. Európai Kritikus Infrastruktúra Védelmi Kapcsolattartási Pont

A Kat. vhr. 1. § 9. pontja megállapítja, hogy az *„Európai Kritikus Infrastruktúra Védelmi Kapcsolattartási Pont”* feladatait „az európai kritikus infrastruktúrák védelmével kapcsolatos információk kezelésével megbízott központi államigazgatási szerv kijelölt szervezeti egysége” látja el, amelyet a belügyminiszter felelősségi köreinek felsorolásánál a hivatásos katasztrófavédelmi szerv központi szerveként nevesít. Ennek megfelelően a kapcsolattartási feladatokat a BM OKF Kritikus Infrastruktúra Koordinációs Főosztálya látja el.

A jogi környezet folyamatos változása, a nemzetközi események rendszeres nyomon követése, a külföldi tapasztalatok hatékony és eredményes felhasználása érdekében a kapcsolattartási tevékenység egyre nagyobb hangsúlyt kap. Ennek keretében a BM OKF rendszeresen részt vesz az úgynevezett CIP POC *(Critical Infrastructure Protection Point of Contact)* üléseken, amelyek féléves rendszerességgel uniós szinten tekintik át a létfontosságú rendszerekkel kapcsolatos tagállami tevékenységet.

Kapcsolatot tart az unió Közös Kutatóközpontjával *(Joint Research Centre – EU JRC),* tagja az európai kritikus infrastruktúrák védelmét célzó program hatékony megvalósítása érdekében létrehozott referensi hálózatnak *(European Reference Network for Critical Infrastructure Protection – ERNCIP).* A nemzetközi tevékenység keretében képviseli Magyarországot az EU által szervezett, valamint a kritikus infrastruktúrák védelme külső dimenziójának erősítése keretében megtartott konferenciákon, továbbképzéseken és gyakorlatokon egyaránt.

4.7. Kijelölő hatósági tevékenység – közbiztonság-védelem, illetve víz ágazat vonatkozásában[7]

A fenti feladatok ellátásán túl a *közbiztonság-védelem ágazatban* történő kijelölési eljárásokban a katasztrófavédelem területi szerve vagy a rendőrség területi szerve jár el első fokon mint *kijelölő hatóság.* Az ágazati kormányrendelet

- az Alkotmányvédelmi Hivatal (a továbbiakban: AH),
- a Büntetés-végrehajtás Országos Parancsnoksága (a továbbiakban: BVOP) és szervei,
- a Nemzetbiztonsági Szakszolgálat (a továbbiakban: NBSZ),
- a Nemzeti Védelmi Szolgálat (a továbbiakban: NVSZ),
- a Terrorelhárítási Információs és Bűnügyi Elemző Központ (a továbbiakban: TIBEK),
- az Országos Rendőr-főkapitányság (a továbbiakban: ORFK) és szervei, illetve
- a Terrorelhárítási Központ (a továbbiakban: TEK)

vonatkozásában helyezi a hatósági jogkört a *katasztrófavédelemhez,* míg

- a BM OKF és szervei kijelölése esetén
- az általános *rendőrségi feladatok ellátására létrehozott szerv* megfelelő illetékességű szerve jár el kijelölő hatóságként.

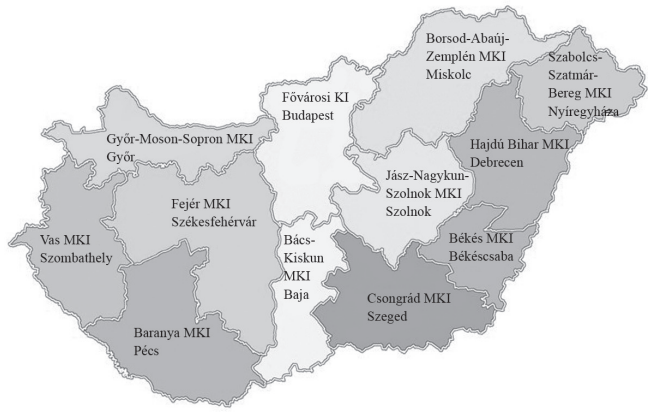
Az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) kormányrendelet módosításáról szóló 512/2013. (XII. 29.) kormányrendelet hatálybalépésével a katasztrófavédelemnél is szükséges volt elkészíteni a kijelölési eljárások alapjául szolgáló azonosítási jelentéseket, amelyek mind az igazgatóságok, mind a BM OKF vonatkozásában tartalmazzák:

- a rendszerelem átfogó leíró meghatározását, jellemzését;
- a vizsgált rendszerelem funkciójának helyettesíthetőségét;
- az informatikai rendszereket, azok védelmét;
- a folyamatos feladatellátás súlyos fennakadását okozó veszélyeztető forrásokat;
- a külső erőszakos beavatkozások mint veszélyeztető hatások vizsgálatát és valószínűségének becslését;
- a rendszerelemet veszélyeztető informatikai kibertámadások kockázatainak vizsgálatát és valószínűségének becslését;
- a folyamatos feladatellátásban történő súlyos fennakadás következményeinek értékelését;
- a rendszerelem horizontális kritériumainak vizsgálatát;
- a fentiek alapján megfogalmazott kijelölési javaslatot.

[7] Az ágazatok részletes kifejtését a 4. fejezet tartalmazza.

A *vízügyi és vízvédelmi hatósági feladatokat* 2014 szeptembere óta a katasztrófavédelem látja el az alábbiak szerint:

– *I. fokú hatóság* – 12 katasztrófavédelmi igazgatóság:



1. ábra

Vízügyi hatósági illetékesség

Forrás: BM OKF

Bács-Kiskun Megyei Katasztrófavédelmi Igazgatóság,
Baranya Megyei Katasztrófavédelmi Igazgatóság,
Békés Megyei Katasztrófavédelmi Igazgatóság,
Borsod-Abaúj-Zemplén Megyei Katasztrófavédelmi Igazgatóság,
Csongrád Megyei Katasztrófavédelmi Igazgatóság,
Fejér Megyei Katasztrófavédelmi Igazgatóság,
Fővárosi Katasztrófavédelmi Igazgatóság,
Győr-Moson-Sopron Megyei Katasztrófavédelmi Igazgatóság,
Hajdú-Bihar Megyei Katasztrófavédelmi Igazgatóság,
Jász-Nagykun-Szolnok Megyei Katasztrófavédelmi Igazgatóság,
Szabolcs-Szatmár-Bereg Megyei Katasztrófavédelmi Igazgatóság,
Vas Megyei Katasztrófavédelmi Igazgatóság.

– *II. fokú hatóság* – BM OKF

Ebből adódóan a *Víz ágazatban* történő kijelölési eljárásokban a katasztrófavédelem 12 vízügyi hatáskörrel és illetékességgel rendelkező területi szerve jár el *kijelölő hatóságként*.

Fenti két ágazatban kapott hatáskörében végzi a kijelölési eljárással kapcsolatos hatósági tevékenységet, vizsgálja az azonosítási jelentést, bevonja az ágazati javaslattevő hatóságo(ka)t, és az Lrtv. vhr. 4. § (2) bekezdése értelmében – kijelölő hatóságként – vizsgálja a horizontális kritériumok teljesülésével kapcsolatos szakkérdéseket is, tekintettel arra, hogy szakhatósági megkeresésnek ez esetben nincs helye.

4.8. Horizontális kritériumok vizsgálata – szakhatósági feladatok[8]

A katasztrófavédelem minden egyes nemzeti létfontosságú rendszer kijelölésére irányuló eljárásban – kivéve a katasztrófavédelemmel kapcsolatos kijelöléseket – *szakhatósági feladatokat* lát el. A kijelölési eljárás bemutatása során már említésre került, hogy a katasztrófavédelem a horizontális kritériumok teljesülésének vizsgálata érdekében vesz részt az eljárásban, mint szakhatóság. Hatáskör tekintetében első fokon az üzemeltető telephelye szerint illetékes katasztrófavédelmi kirendeltség, tehát a hivatásos katasztrófavédelmi szerv helyi szerve, míg másodfokon az üzemeltető telephelye szerint illetékes fővárosi/megyei katasztrófavédelmi igazgatóság, vagyis a hivatásos katasztrófavédelmi szerv területi szerve jár el.

A szakhatóság – a horizontális kritériumrendszer teljes körű vizsgálatának biztosítása érdekében – véleménynyilvánítás céljából a következő szerveket vonja be az állásfoglalás kialakításába:

- *pénz- és adóügyi biztonság* vonatkozásában a Nemzeti Adó- és Vámhivatal illetékes szervét;
- *közrend, közbiztonság, lakosságvédelem, alkotmányvédelem, nemzetbiztonság, terrorelhárítás* vonatkozásában a Rendőrség, az AH, valamint a TEK illetékes szervét;
- *politikai hatás* kritériuma vonatkozásában az illetékes kormánymegbízottat;
- *környezeti hatás* kérdésében területi környezetvédelmi hatóságot,[9] a területi vízügyi és vízvédelmi hatóságot, valamint az országos természetvédelmi és környezetvédelmi hatóságot.

A szakkérdések tekintetében a véleményt nyilvánító szerveknek és a szakhatóságnak együttesen 21 napja van a szakhatósági állásfoglalás elkészítésére, amelyben döntenie kell a horizontális kritériumok teljesülésének fennállásáról.

A horizontális kritériumok teljesülését a vizsgált potenciális kritikus infrastruktúra vonatkozásában az azonosítási jelentésben bemutatott veszélyeztetettség, a rendelkezésre álló biztonsági (fizikai-humán-IT) intézkedések, valamint a helyi sajátosságok alapján szükséges felmérni. Horizontális kritérium teljesülése nélkül a rendszerelem nem jelölhető ki létfontosságúvá.

A szakhatósági feladatok ellátása új típusú jogkör a katasztrófavédelmi szervek állományának, amelyhez központi szintű eljárásrendet és iratmintákat dolgozott ki az illetékes szakterület. A horizontális kritériumok vizsgálata ugyanis nehezen körvonalazható, rendkívül összetett feladat, amellyel kapcsolatban az objektivitásnak különösen nagy szerepe kell legyen. A horizontális kritériumok elsődlegesen a lakossági, gazdasági, környezeti és politikai körülményeket körvonalazzák, összetételük – a vizsgált hatás összefüggésében – a következő:

---

[8] Az alfejezet Bonnyai alapján készült.

[9] Kormányhivatalok Környezetvédelmi és Természetvédelmi osztályai.

1. táblázat

Horizontális kritériumok és a vizsgált hatás összefüggései

KRITÉRIUMTÍPUS	FELTÉTELRENDSZER	HATÁS
veszteségek kritériuma	24 óra leforgása alatt a halálos áldozatok száma a 20 főt meghaladja, vagy a súlyos sérültek száma legalább 75 fő	lakossági
	72 óra leforgása alatt a halálos áldozatok száma a 40 főt meghaladja, vagy a súlyos sérültek száma legalább 150 fő	
gazdasági hatás kritériuma	a gazdasági veszteség mértéke, vagy a termékek és szolgáltatások romlásának mértéke, amelyek ötvenezer fő vonatkozásában meghaladják az egy főre eső bruttó nemzeti jövedelem (GNI) bármely 30 napos időszakra vetített mértékének 25%-át	nemzetgazdasági/államigazgatási
társadalmi hatás kritériuma	300 fő/km2-nél sűrűbben lakott területen a köznyugalom súlyos megzavarása, beleértve a lakosságot érő káros pszichológiai és közegészségügyi hatásokat is	lakossági/államigazgatási
környezeti hatás kritériuma	az ország tájegységeiben, kiemelkedő földrajzi területeiben visszafordíthatatlan, negatív változás következik be	lakossági/nemzetgazdasági
	az infrastruktúrában bekövetkező sérülés vagy zavar, az épített vagy természetes környezet oly mértékű rongálódását idézi elő, amelynek következtében:	
	• 10 000 fő kimenekítése/kitelepítése válik szükségessé • legalább 100 km^2 nagyságú terület tartósan szennyeződik • a folyóvizek/tavak medre/élővilága szenved tartós károsodást	

Forrás: BONNYAI 2014

A katasztrófavédelem egyik legmeghatározóbb feladata a kritikus infrastruktúrák védelmének rendszerében, hogy a horizontális kritériumok vizsgálata alapján elsődlegesen vegye figyelembe a kijelölésre javasolt kritikus infrastruktúra elem által potenciálisan veszélyeztetett lakosság körülményeit, függőségeit, és a valószínűsíthetően okozott hatásokat egyaránt. Ahogy a fenti táblázatban is látható, az öt horizontális kritérium közül egyedül a gazdasági hatás kritériumánál nem állapítható meg elsődleges hatás a lakosság vonatkozásában, miközben a további négy kritérium közvetlenül a lakossággal áll összefüggésben.

***

A feladatkörök áttekintése alapján is egyértelműen látható, hogy *a létfontosságú rendszerek és létesítmények védelmének rendszerében kiemelkedő szerepet tölt be a hivatásos katasztrófavédelmi szerv.* Az elmúlt évek tapasztalatai azt mutatják, hogy a jogkövető magatartás a szolgáltató hatósági mentalitás által ténylegesen elérhető az egyre szélesedő üzemeltetői

körben. A kijelölt elemek üzemeltetői bizalommal fordulnak a katasztrófavédelemhez mint hatósághoz, amit a 2018-ban újonnan hatályba lépő jogszabályok tovább erősíthetnek.

Felhasznált irodalom

Bognár Balázs (2012): A létfontosságú rendszerek és létesítmények védelme. *Katasztrófavédelmi Szemle,* 19. évf. 4. sz. 13–17.

Bonnyai Tünde (2014): *A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében.* Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem.

Hivatkozott jogszabályok és dokumentumok

A katasztrófák elleni védekezés egyes szabályairól szóló 62/2011. (XII. 29.) BM rendelet

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

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet

Vákát oldal

5. fejezet
Információbiztonsági feladatellátás a kritikus infrastruktúrák védelme kapcsán

Bognár Balázs

5.1. Jogszabályi háttér

Napjainkban a számítógépes rendszerek, kommunikációs eszközök működése rendkívül nagy hatást gyakorol a társadalom egészére, nélkülük az állam és gazdaság biztonságos üzemeltetése sem képzelhető el. Ezek az eszközök, rendszerek olyan mélyen beépültek a létfontosságú infrastruktúrákba, hogy kiesésük ellehetetleníthetné a különböző szolgáltatások igénybevételét, ami akár teljes szolgáltatások leállását, katasztrófahelyzetet is előidézhetne.

A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti adatvagyon részét képező valamennyi adat, az ezeket kezelő információs rendszerek, illetve a létfontosságú rendszerek és rendszerelemek elektronikus információs rendszereinek biztonsága.

Az elektronikus információs rendszerek biztonsága alatt a bennük kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt (az egész rendszerre vonatkozó), teljes körű (minden veszélyeztető tényezőt figyelembe vevő), folytonos (megszakítás nélkül rendelkezésre álló) és a kockázatokkal arányos védelmét értjük. A bizalmasság alatt azt kell érteni, hogy egy rendszerben tárolt adatot, információt kizárólag az arra jogosult személy, a jogosultsága mértékéig ismerheti meg, használhatja fel, vagy rendelkezhet felhasználásáról. A sértetlenség az adat tulajdonsága, amely arra vonatkozik, hogy a tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. A rendelkezésre állás azt hivatott biztosítani, hogy az adott informatikai rendszer, a benne tárolt adat vagy információ az arra jogosult személyeknek a szükséges időben és időtartamban elérhető és használható legyen.

A nemzeti adatvagyon, valamint a kapcsolódó létfontosságú rendszerek és létesítmények információbiztonságának megteremtése érdekében 2013 márciusában a magyar Kormány 1139/2013. számú határozatával elfogadta Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló dokumentumot. A Stratégia célja, hogy az Alaptörvény elveivel összhangban, a kibertér biztonsági környezetének elemzése alapján meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján

Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is. Mindezt egészíti ki a 1838/2018. (XII. 28.) kormányhatározattal elfogadott Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiája.

A kibertérből érkező fenyegetéseket már a 2001-es budapesti konvenció (Számítástechnikai Bűnözésről szóló Egyezmény) megfogalmazásakor felismerték a tagországok, de ezt követően, egy évtized elteltével került sor valódi védelmi célok megfogalmazására. A stratégiáink igazodnak az Európai Parlament által 2012. november 22-én elfogadott, *A kiberbiztonságról és védelemről szóló,* 2012/2096(INI) számú határozatában a tagállamok felé megfogalmazott ajánlásokhoz, valamint az Európai Bizottság és az Európai Unió közös kül- és biztonságpolitikájának főképviselője által 2013. február 7-én *Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér* címmel közzétett közös közleményhez. A hazai stratégiák illeszkednek továbbá a NATO 2010 novemberében elfogadott Stratégiai Koncepciójához, a Szövetség 2011 júniusában elfogadott Kibervédelmi Politikájához és ennek végrehajtási tervéhez, valamint a 2010. november 19–20-i lisszaboni és a 2012. május 20–21-i chicagói NATO-csúcs dokumentumaiban megfogalmazott szövetségi kibervédelmi elvekhez és célokhoz.

Az első igazán jelentős szakmai előrelépést az Európai Parlament, a Tanács és a Bizottság által 2016 júliusában elfogadott első, az egész Európai Unióra kiterjedő kiberbiztonsági direktíva jelentette. Az irányelv elfogadását hosszú tárgyalási szakasz előzte meg, ugyanis a Bizottság már 2013-ban előterjesztette a hálózat- és információbiztonságra vonatkozó javaslatát. Aktualitását a 21. század teremtette kihívások adják. Mai viszonyok között az egyre sűrűbben fellépő üzemzavarok és az informatikai sérülékenységek, károkozók, vírusok (együttesen fenyegetések) elleni küzdelem egységes válaszlépéseket követel meg a biztonság fokozásának érdekében.

A NIS-irányelvként megismert direktíva minden uniós tagállam számára előírja a biztonságos és megbízható digitális környezete kiberbiztonsági szempontú fejlesztését. Célja, hogy minden tagállam rendelkezzen minimális képességekkel, szükséges intézményekkel, szabályokkal, valamint a hálózat- és információbiztonság magas szintjét biztosító nemzeti szintű stratégiával. Első lépésként a tagállamok ennek érdekében azonosítják a területükön alapvető szolgáltatásokat nyújtó gazdasági szereplőket, illetve ha a tagállami szabályozás előírja, a kiemelt szerepet játszó ún. digitális szolgáltatóikat, tekintettel arra, hogy az irányelv különböző megfelelési kritériumokat, valamint incidensbejelentési kötelezettséget fogalmaz meg rájuk vonatkozóan.

Az incidens bejelentése mint kötelezettség azért fontos, mert előfordulhat olyan biztonsági esemény vagy súlyos biztonsági esemény, amelyre egyedül nem képes egy szolgáltatásokat nyújtó üzemeltető reagálni, IT vagy egyéb biztonsági szakember vagy eszköz és technológia hiányában. Az ún. eseménykezelő központok azonban segítséget nyújthatnak a probléma elhárításában, legyen az akár technikai, akár humán jellegű.

Az irányelv 2016. augusztus 8-i hatálybalépését követően a tagállamoknak 21 hónapjuk volt (2018. május 8.) a szükséges nemzeti intézkedések megtételére, jogszabályok megalkotására, és további 6 hónapot kaptak az alapvető szolgáltatásokat nyújtó szereplők azonosítására. Ennek megvalósítása érdekében:

- ki kellett dolgozni a nemzeti hálózat- és információbiztonsági stratégiát,
- ki kellett jelölni a nemzeti hatóságot, amely felügyeli az átültetést és a végrehajtást,

- ki kellett jelölni egy vagy több „gyors reagálású kibervédelmi csoportot” (CSIRT/CERT),
- meg kellett határozni, hogy mely kritériumok alapján esik egy-egy szervezet az irányelv hatálya alá, és azonosítani kell a konkrét érintetteket.

A NIS-ben megfogalmazott alapelvek és értékek mentén dolgozták ki és fogadták el az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) jelenleg is hatályos verzióját. Célja az állami és önkormányzati szervek, illetve a nemzeti elektronikus adatvagyon és az azt kezelő elektronikus információs rendszerek, valamint a létfontosságú rendszerek elektronikus információs rendszerei megfelelő szintű védelmének biztosítása. A törvény alapján az elektronikus információs rendszereket – a kockázatarányos védelem megvalósítása érdekében – biztonsági osztályba, míg magát a szervezetet – a védelmi felkészültségük alapján – biztonsági szintbe kell sorolni. Az Ibtv. rendelkezik többek között a közvetlenül vagy közvetetten a hatálya alá tartozó szervezetek feladatairól és kötelezettségeiről, az elektronikus információs rendszer biztonsági osztályba sorolásáról és a megfelelés felméréséről, a szervezet biztonsági szintbe sorolásáról és a megfelelés felméréséről, cselekvési terv készítéséről, informatikai biztonsági incidensek bejelentéséről, illetve az elektronikus információs rendszer biztonságáért felelős személy feladatairól egyaránt.

Az információbiztonság témakörében jelenleg hatályos releváns jogszabályok a következők:

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról;
- 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól;
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról;
- 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről;
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről;
- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról.

Az Ibtv. 2. § (2) bekezdés c) pontja alapján a törvény (és végrehajtási rendeletei) előírásait kell alkalmazni az Lrtv. alapján kijelölt szervezetek elektronikus információs rendszereire is.

Annak érdekében, hogy az e törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából, kockázatelemzés alapján. A kockázatelemzés ki kell hogy terjedjen az elektronikus információs rendszerek vagyonelemeinek felmérésére, hogy meghatározható legyen a védelem tárgya (adatok). A különböző vagyonelemek tekintetében meg kell határozni, hogy milyen sebezhetőség jellemző rájuk, milyen fenyegetéseknek vannak kitéve IT, infrastrukturális, környezeti, humán, társadalmi, politikai, gazdasági stb. szempontból. Ezt követően meg kell határozni, hogy melyek az elfogadható kockázatok, amelyekkel a rendszer „együtt tud élni", működését jelentős mértékben nem képesek befolyásolni, illetve melyek azok, amelyek nem elfogadhatók a szervezet számára, és intézkedéseket kell foganatosítani az adott kockázat csökkentésére. Ezen kockázatok mérséklésére alternatívákat kell felállítani, illetve fel kell tárni a maradványkockázatokat is, amelyek további értékelésre szorulnak.

Az elektronikus információs rendszerek osztályba sorolása a fenti szempontok alapján, ötfokozatú skálán történik, a rendszerben kezelt adatoktól és az elektronikus információs rendszer funkcióitól függően. Például minél több személyes vagy különleges (politikai hovatartozás, egészségügyi adat, szexuális beállítottság stb.) adatot, esetleg minősített adatot kezel az adott rendszerben egy szervezet, annál magasabb osztályba kell hogy kerüljön, mivel a kockázatok is magasabbak. Minél több érintettje van egy biztonsági eseménynek, vagy minél szenzitívebb adat, annál magasabb szintű védelmet kell biztosítani a rendszer működése során. Kritikus infrastruktúrák tekintetében – rendeltetésükből és létfontosságú jellegükből adódóan – a szabályozás a rendelkezésre állást követeli meg elsődlegesen a bizalmasság – sértetlenség – rendelkezésre állás hármas szempontrendszerét nézve, de természetesen nem zárható ki, hogy bizonyos – például az egészségügy ágazatba tartozó, nagy mennyiségű személyes adatot kezelő – rendszerek tekintetében hangsúlyosabb lesz a sértetlenség és a bizalmasság követelménye is.

Az egyes biztonsági osztályokhoz meghatározott követelményrendszer társul, amelyet az adminisztratív, a fizikai és a logikai védelem terén kell a rendszereknek teljesíteniük. Az adminisztratív védelem körébe tartoznak például a szabályzatok, a biztonságért felelős személyek kinevezése, nyilvántartások, kockázatelemzés, dokumentációk, eljárásrendek megléte, üzletmenet-folytonosság tervezése, oktatás, képzés stb. A fizikai védelmi intézkedések között említhetők a rendszerhez és az eszközökhöz történő hozzáférés szabályozása, ellenőrzése, felügyelete, az áramellátás biztosítása, tűz-, víz-, egyéb károk elleni védelem, karbantartás. A logikai védelmi intézkedések közé tartoznak többek között a biztonsági elemzések, tesztelések, konfigurációkezelés, frissítések, naplózások, az adathordozók védelme, azonosítás, hitelesítés, vagy a kommunikáció védelme. A jogszabályok alapján meghatározható az egyes rendszerek irányadó biztonsági osztálya, amelynek meg kell felelni, és amelyhez társított követelményeket teljesíteni szükséges.

A biztonsági osztályba sorolást a kockázatelemzés elvégzését követően a szerv vezetője hagyja jóvá. A biztonsági osztályba sorolást háromévenként, vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni. A rendszer teljes életciklusában (működése minden időszakában és formájában) alapvető kötelezettség az irányadó osztálynak megfelelő biztonsági követelmények megvalósítása és fenntartása.

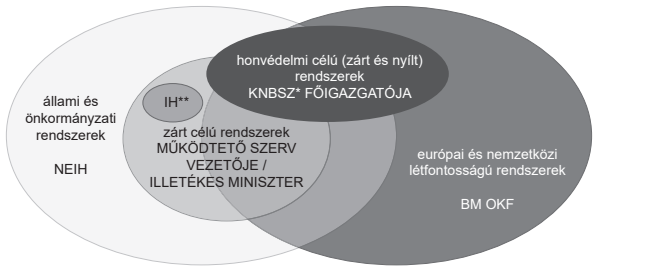
A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet vagy szervezeti egységeket az elektronikus információs rendszerek védelmére való felkészültségük (biztonsági menedzsmentjük) alapján biztonsági szintbe kell sorolni a jogszabályban meghatározott szempontok szerint. Az elektronikus információs rendszerrel rendelkező szervezet/szervezeti egység biztonsági szintje a szervezet biztonsági menedzsmentjének fejlettségét, érettségét méri. A szintén ötfokozatú rendszerben a leggyengébb szint (1-es) azt jelenti, hogy a szervezetnél vannak az információbiztonságot érintő szabályozók, de a folyamatok ad hoc jellegűek, nem ellenőrzöttek. A szintek emelkedésével párhuzamosan a folyamatok szabályozottabbak, ellenőrzöttek, számon kérhetők, oktatottak, teszteltek, mérhetők, auditáltak lesznek. A rendszerek biztonsági osztálya és a használó szervezet biztonsági szintje között erős összefüggés van, hiszen szigorú védelmi intézkedéseket csak fejlett biztonsági kultúrával rendelkező szervezet tud biztosítható módon végrehajtatni.

A létfontosságú rendszerek, létesítmények elektronikus információs rendszereinek biztonsági osztályba sorolásához a 41/2015. (VII. 15.) BM rendelet ad segítséget. Az osztályba sorolásnál a rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint a rendszer sértetlenségének és rendelkezésre állásának követelményeit kell a funkciónak megfelelően érvényesíteni. A rendelet 1. melléklete nem kötelező érvényű iránymutatást nyújt a biztonsági osztály megállapításához. Az egyes osztályoknál azt mérlegeli, hogy az elektronikus információs rendszereket érintő sérülés okozta kár milyen nagyságrendű a kezelt adatok, az üzlet-, ügymenet akadályozása, valamint a további társadalmi, politikai hatások, esetleges személyi sérülések tekintetében.

A biztonsági osztályokhoz és szintekhez tartozó követelményeket nem kell rögtön teljesíteni, a jogszabály lehetőséget ad a fokozatos elérésre. Amennyiben a szervezet vagy szervezeti egység nem éri el az 1-es biztonsági szintet, abban az esetben a vizsgálatot követően 6 év áll rendelkezésre, hogy az 1-es szinthez tartozó előírásoknak megfeleljen. Ezt követően minden egyes szintet érintően, a következő magasabb szintre lépéshez 2 év áll rendelkezésre *(fokozatos elérés elve),* egészen addig, amíg el nem éri az irányadó fokozatot. A biztonsági osztályok tekintetében a vizsgálat elvégzését követően, minden egyes következő biztonsági osztály eléréséhez szintén 2 év áll rendelkezésre.

További kötelezettség a szervezetre nézve, hogy elektronikus információs rendszer biztonságáért felelős személyt nevezzen ki, a rendszer védelmével kapcsolatos felelősöket, feladatokat, hatásköröket az informatikai biztonsági szabályzatban vagy egyéb, az információbiztonságot érintő belső szabályozóban szabályozza.

Az elektronikus információs rendszerek biztonságának hatósági felügyelete több szervezet felelősségi körébe tartozik. A hatósági tevékenység két fő oszlopa a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) és a BM OKF mint információbiztonsági hatóság, de egyes speciális rendszerek tekintetében egyedi felelősségek lépnek érvénybe. A különböző típusú elektronikus információs rendszerek hatósági felügyeletének megoszlása a következő ábrán látható:



1. ábra

Elektronikus információs rendszerek hatósági felügyelete

Forrás: BM OKF

A katasztrófavédelem szervezeti rendszerében kiemelt területként jelentkezik a *létfontosságú rendszerek és létesítmények* védelmével kapcsolatos feladatok ellátása, a potenciális kritikus infrastruktúra elemek beazonosítása, valamint a kijelölt elemek hatósági felügyelet alatt tartása, ez által az ezekhez tartozó *információbiztonsági hatósági tevékenység hatékonyságának fokozása.*

5.2. Információbiztonsági hatósági tevékenység[1]

Az Ibtv., illetve az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet alapján az *európai vagy nemzeti létfontosságú létesítmények, rendszerek elektronikus információs rendszerei* esetében a *BM OKF*-et nevesítették eljáró hatóságként.

Ugyanezen Korm. rendelet az információbiztonsági hatósági feladatellátás másik legmeghatározóbb szerepet játszó hatóságaként (NEIH) a *Nemzetbiztonsági Szakszolgálatot* jelölte ki, amely *valamennyi állami és önkormányzati szerv* vonatkozásában eljárhat, a *nevesített kivételeken kívül* (például: polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei; honvédelmi célú elektronikus információs rendszerek; kritikus infrastruktúrák – amelyek üzemeltetője nem állami/önkormányzati szerv).

A BM OKF az Lrtv. alapján kijelölt létesítmények, rendszerek elektronikus információs rendszerei esetében látja el a hatósági feladatokat és a biztonsági felügyeletet a következő táblázatban ismertetett kivételekkel:

[1] Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról 187/2015. (VII. 13.) Korm. rendelet.

kivétel	eljáró hatóság
a rendészetért felelős miniszter alá tartozó szerveknél működő zárt célú elektronikus információs rendszer	rendszert működtető szerv vezetője
a honvédelmi célú elektronikus információs rendszerek és a honvédelemért felelős miniszter alá tartozó szervek, gazdasági társaságok zárt célú elektronikus információs rendszerei	Katonai Nemzetbiztonsági Szolgálat főigazgatója
a külpolitikáért felelős miniszter alá tartozó szerveknél működő zárt célú elektronikus információs rendszer	külpolitikáért felelős miniszter
polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei	rendszert működtető szerv vezetője

A katasztrófavédelem *információbiztonsági hatóságának* feladatkörébe a következő feladatok és jogosultságok tartoznak:

1. Biztonsági osztályba és szintbe sorolással, biztonsági események vizsgálatával kapcsolatos tevékenység során:
   - végzi az osztályba sorolás és a biztonsági szint megállapításának ellenőrzését és az ellenőrzés eredménye alapján *döntés* meghozatalát,
   - az osztályba sorolásra és – ehhez kapcsolódóan – a rendszert működtető szervek biztonsági szintjeire vonatkozó, jogszabályban meghatározott követelmények teljesülésének *ellenőrzését,*
   - az ellenőrzés során a feltárt vagy tudomására jutott *biztonsági hiányosságok elhárításának elrendelését* és eredményességének ellenőrzését,
   - a rendelkezésre álló információk alapján *kockázatelemzés* elvégzését,
   - a hozzá érkező biztonsági eseményekkel kapcsolatos bejelentések kivizsgálására irányuló *hatósági eljárás* megindítását (eljárás határideje 30 nap, logikai védelmi intézkedés teljesülésének vizsgálatára indított eljárás határideje 120 nap).
2. Nyilvántartás vezetésével kapcsolatos tevékenysége keretében kezeli:
   - a szervezet *azonosítás*ához szükséges adatokat (megküldés 60 napon belül),
   - a szervezet elektronikus információs rendszereinek *megnevezés*ét, *besorolás*ait, technikai adatait,
   - a szervezet elektronikus információs rendszereinek *biztonsági felelős*ére vonatkozó adatokat (megküldés 60 napon belül),
   - a szervezet *informatikai biztonsági szabályzat*át (megküldés 90 napon belül),
   - a biztonsági eseményekkel kapcsolatos, a kormányzati eseménykezelő központtól kapott *értesítések*et.
   - A nyilvántartásból adattovábbítás kizárólag az eseménykezelő központok részére történhet.
   - Az adatokat a tevékenység befejezésének bejelentését követő 5 év elteltével kell törölni.

3. Ellenőrzésekkel kapcsolatos tevékenység és szankcionálás:
   - a jogszabályokban foglalt *biztonsági követelmények* és az ezekhez kapcsolódó *eljárási szabályok* teljesülésének ellenőrzése,
   - a *követelményeknek való megfelelőség* alátámasztásához szükséges dokumentumok bekérése,
   - a központi költségvetési és az európai uniós forrásból megvalósuló *fejlesztési projektek* tervezési szakaszában az információbiztonsági követelmények megtartásának ellenőrzése, azokra ajánlások tétele,
   - a *fejlesztési projektek* tervezési szakaszában szakmai részvétel biztosítása és a biztonsági követelmények beépülésének ellenőrzésére irányuló tevékenység folytatása,
   - a sérülékenység megszüntetésére vonatkozó *intézkedési terv* készítése,
   - amennyiben a rendszert működtető szervezet a biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, vagy nem tartja be, akkor az érintett felszólítása a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére, vagy a körülmények mérlegelésével *bírság kiszabása*, amely további nem teljesülés esetén megismételhető.
4. Egyéb tevékenység:
   - az információs társadalom *biztonságtudatosság*ának *elősegítése* és támogatása,
   - a hazai és nemzetközi információbiztonsági, kibervédelmi, létfontosságú információs infrastruktúra védelmével kapcsolatos *gyakorlatok*on történő részvétel,
   - *kapcsolattartás és együttműködés* a hatóságokkal, valamint az eseménykezelő központokkal.

5.3. Informatikai biztonsági eseménykezelés[2]

Az informatikai biztonsági események kezelésének egyre növekvő jelentőségét az a tény világítja meg leginkább, hogy a *kritikus infrastruktúraként működő szolgáltatások egyre inkább informatikai rendszerek támogatásával, vagy egyenesen informatikai rendszereken keresztül valósulnak meg, ezért az informatikai rendszerekkel kapcsolatos kockázatok,* fenyegetettségek közvetlenül transzformálódnak a kapcsolódó infrastruktúrákra is. A létfontosságú rendszerelemek vizsgálata esetén látható, hogy a magyar gazdaság szinte minden szektora érintett valamilyen formában. Egy nem megfelelően kezelt informatikai incidens a továbbgyűrűző hatás (dominóhatás) miatt beláthatatlan károkat okozhat mind a termelésben, mind a szolgáltatások működésében, jelentős hatást gyakorolva a lakosság életére is. Gondoljunk bele, mi történne, ha egy hackercsoport átvenné az irányítást a magyar bankok vagy a víztisztító telepek informatikai rendszerei felett.

A jogszabály hatálya alá tartozó szervezet elektronikus információs rendszereit érintő súlyos biztonsági eseményekről tájékoztatnia kell a megfelelő eseménykezelő központot (GovCERT, MilCERT, IntCERT), ahol szükség esetén segítséget kap az esemény keze-

[2] Az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet.

lésében, és együtt kell működnie az incidens kivizsgálásában. Az Ibtv. és végrehajtási rendeletei a kijelölt létfontosságú rendszerek és létesítmények elektronikus információs rendszerei tekintetében a kiberincidensek kezelését, vagyis az informatikai biztonsági eseménykezelő központ működtetését a Nemzetbiztonsági Szakszolgálat – azon belül a kormányzati eseménykezelő központ (GovCERT) feladatkörébe helyezte. Az eseménykezelő központ részletes feladatait, hatáskörét az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet szabályozza a következők szerint:

1. Biztonsági eseményekkel kapcsolatosan:
   - biztonsági események és kockázatok kezelésére vonatkozó *eljárások* meghatározása,
   - biztonsági események megelőzése céljából *tájékoztatási és tudatosítási tevékenység* végzése,
   - a biztonsági események nemzeti szintű *nyomon követése,*
   - a tudomására jutott biztonsági eseményekről az *érintettek haladéktalan értesítése,*
   - *reagálás* a biztonsági eseményekre,
   - kockázatokkal és biztonsági eseményekkel kapcsolatos *tájékoztatás,* korai előrejelzés, riasztás, bejelentéstétel és *információterjesztés* az érdekeltek számára,
   - *sérülékenységvizsgálat* lefolytatása,
   - a biztonsági eseményekről *nyilvántartás* vezetése (megtett intézkedések és azok eredménye beleértendő).
2. Sérülékenységekkel és fenyegető kockázatokkal kapcsolatosan:
   - az elektronikus információs rendszerek biztonságáért felelős személyek *tájékoztatása,*
   - a hatóságok és más eseménykezelő központok tájékoztatása,
   - a sérülékenységekről és fenyegetésekről, valamint a hozzájuk kapcsolódó, javasolt biztonsági intézkedésekről a honlapján rendszeres tájékoztatás biztosítása.
3. Nemzeti szintű, egyéb feladatai:
   - *elemzések, jelentések* készítése a magyar és a nemzetközi információbiztonsági irányokról,
   - *évente jelentés* készítése a tevékenységéről a polgári nemzetbiztonsági szolgálatokért felelős miniszter részére.
   - nem kötelező érvényű *állásfoglalások, ajánlások* kiadása,
   - a biztonsági események kezelésére irányuló *tájékoztatók* tartása, tudatosítási programokban, szakértői-oktatói tevékenységben részvétel,
   - kormányzati információtechnológiai és biztonságiesemény-kezelési *együttműködési fórum* működtetése,
   - részvétel az infokommunikációs biztonságra vonatkozó stratégiák és *szabályozások* előkészítésében.

5.4. Az alapvető és a bejelentés-köteles szolgáltatást nyújtókkal kapcsolatos feladatok[3]

A 2017. év egyik kiemelt feladata volt a tagállamok számára a NIS-irányelv nemzeti jogrendbe történő teljes körű átültetése, különös tekintettel az alapvető szolgáltatást nyújtó szereplőkkel, valamint a magyar terminológiában bejelentés-köteles szolgáltatókkal (az irányelvben digitális szolgáltatók) kapcsolatos feladat- és intézményrendszer kialakítása. A jogharmonizáció során elsődleges cél volt, hogy az új feladatrendszer ellátása a már meglévő, információbiztonsági területen hatáskörrel rendelkező szervek tapasztalataira és képességeire építve, azokat kiegészítve valósuljon meg.

A NIS-irányelv két szolgáltatói kört nevesít, az alapvető és a bejelentés-köteles szolgáltatást nyújtókat, és az általuk nyújtott szolgáltatások folyamatosságának biztosítása, illetve az általuk kezelt adatok védelme érdekében biztonsági követelmények és bejelentési kötelezettség előírását várja el a tagállamoktól.

Az új szabályozás értelmében *alapvető szolgáltatást nyújtó szereplőnek minősül* a kritikus infrastruktúrák azon köre, amelyeket az irányelv által meghatározott – az Lrtv.-hez képest szűkített – ágazatokban (energia, pénzügy, egészségügy, ivóvízellátás, közlekedés, digitális infrastruktúrák) már kijelöltek létfontosságú rendszerré, létesítménnyé, valamint a működésük hálózati és információs rendszerektől függ, és az ezeket érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában. Ezen szolgáltatók beazonosítása a már meglévő jogszabályi háttér alapján, az abban foglalt kritériumrendszer kiegészítésével történik. Az új kijelölési eljárásokban a szokásos ágazati és horizontális kritériumokon túl a jövőben az alapvető szolgáltatásokra vonatkozó kritériumokat is vizsgálni kell. Az új szabályozás hatálybalépésekor már létfontosságúnak kijelölt rendszerelemek tekintetében az üzemeltetőnek 60 napon belül kiegészítést kellett benyújtania az azonosítási jelentéséhez a fenti kritériumoknak történő megfelelésről. Mivel az irányelv szerinti alapvető szolgáltatást nyújtó szereplők a nemzeti szabályozás alapján létfontosságú rendszernek, létesítménynek kijelöltek egy szűkebb köre, így az elektronikus információbiztonsággal kapcsolatos felügyeletük, kötelezettségeik nem változnak.

A *bejelentés-köteles szolgáltatást nyújtókkal* (online piacterek, keresőprogramok, felhőalapú számítástechnikai szolgáltatások) kapcsolatos hatósági és eseménykezelési feladatok meghatározása és végrehajtása a hatályos információbiztonsági jogszabályok mintájára, de teljesen új, különálló jogszabály alapján valósul meg, amely a Nemzetbiztonsági Szakszolgálathoz telepíti a kapcsolódó hatósági hatáskört és eseménykezelési feladatkört, ami által az eddigi információbiztonsági feladatrendszer kibővült.

A bejelentés-köteles szolgáltatásokkal kapcsolatosan az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény is módosult, ugyanis értelmező rendelkezései

[3] Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény; a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény; az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Korm. rendelet.

között határozták meg magát a *bejelentés-köteles szolgáltatást,* amely alatt olyan információs társadalommal összefüggő szolgáltatást értünk, amely:

- lehetővé teszi, hogy az online piactér weboldalán online adásvételi vagy szolgáltatási szerződéseket kössenek (= online piacterek, webáruházak);
- információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (= online keresőszolgáltatások),
- távoli hozzáférést tesz lehetővé a többek között hálózati funkciókat, adattárolást, alkalmazások, szolgáltatások futtatását biztosító számítástechnikai megoldásokhoz (= felhőalapú számítástechnikai szolgáltatások).

A fenti szolgáltatásokat nyújtó, *magyarországi székhellyel rendelkező* gazdasági társaságok körét a *NIS-irányelv III. melléklete szerint* kell *szűkíteni,* tehát azokra a szolgáltatókra terjed ki az új szabályozás személyi hatálya, amelyek a mellékletben meghatározott digitális szolgáltatást nyújtanak, és *nem tartoznak a mikro- és kisvállalkozások körébe*.[4]

Az így kialakuló ügyfélkörnek (bejelentés-köteles szolgáltatók) regisztrálnia kell magát a hatóságnál, amely nyilvántartásba veszi. A szabályozás hatálya alá tartozó szolgáltatóknak kockázatokkal arányos biztonsági intézkedéseket kell bevezetniük és alkalmazniuk. A működés során bekövetkező azon biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általa az Európai Unión belül kínált bejelentés-köteles szolgáltatás nyújtására, haladéktalanul be kell jelenteni az eseménykezelő központ részére. A szolgáltató mind a biztonsági események kezelése, mind a hatósági eljárások lebonyolítása tekintetében köteles a hatósággal együttműködni.

A szolgáltatók által bejelentett biztonsági események kezelése, kivizsgálása, az üzletmenet-folytonosság mielőbbi visszaállítása érdekében a *GovCERT* szintén eseménykezelési-feladatkörében jár el.

Információbiztonsági hatáskörében a Nemzetbiztonsági Szakszolgálat a következő feladatok ellátására kötelezett.

1. Biztonsági események megelőzése/kivizsgálása/felszámolása és terjedésének korlátozása érdekében végezett tevékenysége keretében
   - regisztráció alapján nyilvántartást vezet,
   - tájékoztató kampányt szervez és végez;
   - kapcsolatot tart az érintett szolgáltatókkal, a bűnüldöző hatóságokkal, más tagállamok illetékes ágazati hatóságaival, az adatvédelmi hatósággal,
   - a nyilvánosságot szükség szerint tájékoztatja az egyes biztonsági eseményekről;
   - szükség szerint kötelezi a bejelentésköteles szolgáltatást nyújtót a nyilvánosság tájékoztatására;
   - hatósági ellenőrzést végez a bejelentés-köteles szolgáltatást nyújtók kötelezettségeinek teljesítése céljából.
2. Bekövetkezett biztonsági eseménynél a GovCERT jelentése alapján *hivatalból indított hatósági eljárása* keretében vizsgálja
   - a szolgáltató által megtett megelőző és az adott eseményt kezelő tevékenységét,

[4] A kis- és középvállalkozásokról, fejlődésük támogatásáról szóló a 2004. évi XXXIV. törvény 3. § (2)–(3) bekezdések alapján.

– a szolgáltató részére meghatározott követelmények teljesülését,
– a biztonsági intézkedések megfelelőségét.
– Helyszíni ellenőrzést folytathat és műszaki vizsgálatot végezhet.

A vizsgálat eredményeként hatósági döntést hoz, amelynek tartalma:
– a biztonsági esemény bekövetkezése tényének megállapítása,
– az elhárításra javasolt intézkedések,
– a további károkozások megelőzése érdekében javasolt intézkedések.

***

Magyarországon, azzal, hogy a hivatásos katasztrófavédelem szervezetrendszerében alakították ki a kritikus infrastruktúrák védelmének átfogó felügyeletét, egy szervezetnél összpontosul a bekövetkező rendkívüli események kezelése, illetve a létfontosságú rendszerek és létesítmények hálózatbiztonsági szempontú, hatósági feladatrendszere is.

Mindez szerves része annak a nemzeti rendszernek, amelyben a hazánk kiberterének biztonságára irányuló, védelmi célú, a kockázatok csökkentésére törekvő és az incidensek kezelésével kapcsolatos tevékenységek megvalósulnak. Magyarország kiberbiztonságának letéteményeseiként a BM OKF és a GovCERT folyamatos és szerteágazó együttműködése nélkülözhetetlen, feladatellátásukat érdemben és szakmai támogatás szempontjából a hatósági munka teszi teljessé.

Ez a komplexitás garantálja a kiberbiztonság és az információbiztonság új, modern megközelítését, a kibertérből érkező veszélyek és a természeti és civilizációs katasztrófák egységes kezelését, amely nagymértékben hozzájárul a magyar lakosság közbiztonsági szintjének, a nemzeti biztonságkultúrának az emeléséhez.

Hivatkozott jogszabályok és dokumentumok

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény

Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény

Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról 187/2015. (VII. 13.) Korm. rendelet

Az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet

Az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről 270/2018. (XII. 20.) Korm. rendelet

6. fejezet
Ágazati sajátosságok

Bonnyai Tünde

6.1. Energetikai létfontosságú rendszerek és létesítmények kijelölési eljárása[1]

Az Lrtv. vhr. rendelkezéseit az energetikai létesítmények tekintetében (az energetikai létesítmény elemének kell tekinteni a technológiai hírközlési és informatikai rendszert is) az *energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 360/2013. (X. 11.) Korm. rendeletben* (a továbbiakban: energetikai Korm. rend.) foglalt eltérésekkel kell alkalmazni. Ide tartoznak a villamosenergia-rendszer létesítményei;[2] a kőolaj és cseppfolyós szénhidrogén termék szállítóvezetékek és tárolók, a kőolajtermelés és -feldolgozás létesítményei; az együttműködő földgázrendszer, a célvezetékek, a földgáztermelésben, -előkészítésben, -feldolgozásban használt vezetékek; a bányászati, tároló és gázüzemi létesítmények, valamint a cseppfolyósföldgáz-terminálok. [Az Lrtv. rendelkezésein túl az energetikai Korm. rend. 3. § a–c) alpontjai további három kritériumot határoznak meg az európai létfontosságú rendszerelemek azonosításával és kijelölésével kapcsolatban.]

Az energia ágazatban nevesített ágazati kijelölő hatóságok:

– villamosenergia-rendszer → *Magyar Energetikai és Közmű-szabályozási Hivatal;*
– kőolaj-, földgázipar, bányafelügyelet → *bányafelügyelet* (kormányhivatal illetékes főosztályaként);
– kőolajfeldolgozás és -tárolás → *kormányhivatal mérésügyi feladatkörében eljáró megyeszékhely szerinti járási* (fővárosi kerületi) *hivatala.*

Az energia ágazatban kijelölhető nemzeti létfontosságú rendszerelemek ágazati kritériumai:

– *villamosenergia-rendszerirányítás* tekintetében → olyan elem, amelynek kiesése esetén az ellátásbiztonság nem tartható fenn, és amely 30 percen belül nem helyettesíthető;
– *villamosenergia-termelés* tekintetében → olyan elem, amelynek importtal vagy más módon sem helyettesíthető kiesése legalább 24 órán át, az előző 3 év csúcsidei bruttó energiafelhasználás átlagának legalább 10%-át elérő teljesítménycsökkenést okoz a teljes belföldi villamosenergia-termelésben;

[1] Az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 360/2013. (X. 11.) Korm. rendelet.

[2] Kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek.

- átviteli hálózat tekintetében → olyan elem, amelynek kiesése eredményeként bármely további elem (meghatározott) feszültségszinttől való eltérése a 24 órát meghaladja, és más módon nem pótolható;
- *elosztó hálózat* tekintetében → olyan 1 kV-osnál nagyobb, de legfeljebb 132 kV-os elem, amely kiesésének időtartama (x)
  a) 24 < x < 48 óra, és legalább 10 000 felhasználót érint;
  b) 48 < x < 72 óra, és legalább 5 000 felhasználót érint;
  c) x > 72 óra, és legalább 2 000 felhasználót zár ki az ellátásból;
- *kőolajipar* tekintetében → olyan elem, amelynek más módon nem pótolható kiesése ahhoz vezet, hogy a belföldi késztermékigény 55 napon túl legalább 70%-ban nem kielégíthető;
- *földgázszállítás és rendszerirányítás* tekintetében → olyan elem, amelynek kiesése esetén a hazai földgázellátás kapacitásának legfeljebb 85%-a áll rendelkezésre, és más módon nem pótolható;
- *földgáztermelés* tekintetében → olyan elem, amelynek legalább 72 órás kiesése esetén a lekötött kitermelési kapacitás rendelkezésre állása legfeljebb 40%, és más módon nem pótolható;
- *földgáztárolás* tekintetében → olyan elem, amelynek kiesése esetén a lekötött kitárolási kapacitás rendelkezésre állása legfeljebb 40%, és más módon nem pótolható;
- *földgázelosztás* tekintetében → olyan elem, amely kiesésének időtartama (x):
  a) 24 < x < 48 óra, és legalább 10 000 felhasználót érint;
  b) 48 < x < 72 óra, és legalább 5 000 felhasználót érint;
  c) x > 72 óra, és legalább 2 000 felhasználót zár ki az ellátásból.

Az Lrtv. és az Lrtv. vhr. általános és speciális, valamint az energetikai Korm. rend. rendelkezései alapján az energia ágazat azonosítási, minősítési és kijelölési eljárása az alábbiak szerint zajlik.

6.1.1. Azonosítás és minősítés

Azonosítási tevékenységet folytat (ágazaton belüli *saját rendszerű azonosítás*):

- a villamosenergia-rendszer létesítményeinek a villamos energiáról szóló törvény szerinti engedélyese;
- kőolaj és cseppfolyós szénhidrogén termék szállítóvezeték és tároló üzemeltetője;
- kőolajtermelésben és -feldolgozásban használt létesítmény üzemeltetője;
- földgázellátásról szóló törvény szerinti rendszerüzemeltető;
- földgázellátó célvezeték üzemeltetője;
- normál légköri nyomáson és szobahőmérsékleten gáz halmazállapotú szénhidrogén bányászatához szükséges létesítmény üzemeltetője.

Azonosítási folyamat lépései:

(cél: egyes rendszerelemek normál üzemállapotban, külön-külön történő vizsgálata a külső erőszakos beavatkozás következtében történő kiesésre és a tevékenység pótlásának lehetőségeire való különös tekintettel)

a) az üzemeltető a vizsgálat végrehajtásához az ágazati kritériumok és a vizsgálat célja alapján *módszertant* készít;
b) felméri a rendszer egészét, majd azt energetikai létesítményekre, a létesítményeket pedig rendszerelemekre bontja *(ezt a folyamatot nevezzük elemlehatárolásnak);*
c) az elemlehatárolás alapján azonosított rendszerelemek mindegyikére lefolytatja a saját módszertana szerinti vizsgálatot;
d) a vizsgálat eredményéről – rendszerelemenként – *nyilatkozatot tesz;*
e) az általa létfontosságúként azonosított rendszerelemekről összefoglaló táblázatot készít, amely tartalmazza az egyes rendszerelemek aktuális védelmét, valamint a kiesésük esetén érintett minősített felhasználók számát és körét;
f) a vizsgálat eredményéről jelentést készít és nyújt be az ágazati kijelölő hatóság részére (ezt tekintjük *azonosítási jelentésnek*), amely tartalmazza az azonosított rendszerelemek darabszámát, a vizsgálat kezdő- és zárónapját, valamint a vizsgálat teljességéről szóló üzemeltetői nyilatkozatot.

Speciális szabályok az azonosítási jelentés vonatkozásában:
– Ha a rendszer új energetikai létesítménnyel bővül, arról az üzemeltető 30 napon belül tájékoztatja az ágazati kijelölő hatóságot, amelyben nyilatkozik arról, hogy a bővülés hatással lehet-e az általa lefolytatott legutolsó azonosítás eredményére.
– Amennyiben az ágazati kijelölő hatóság megállapítja, hogy az új létesítmény hatást gyakorol a legutolsó azonosítás eredményére, kötelezi az üzemeltetőt, hogy 180 napon belül új azonosítási jelentést nyújtson be *(soron kívüli azonosítás)* az új energetikai létesítmény rendszerelemeire vonatkozóan.
– Ha az üzemeltető szerint az új létesítmény jelentősége vagy a kockázati tényezők változása indokolja, a rendszer egészére vonatkozóan új azonosítást végez *(előre hozott azonosítás).*
– *Európai létfontosságú rendszerelem* vonatkozásában – amennyiben az azonosítás óta semmiféle változás nem történt az üzemeltető rendszerében – az üzemeltető nyilatkozhat úgy, hogy nem indokolt „ciklikus” azonosítási jelentés készítése.
– Amennyiben a fenti nyilatkozatot az ágazati kijelölő hatóság megalapozatlannak tartja, vagy az európai létfontosságú rendszerelemre az Európai Bizottság hívja fel a figyelmet, az ágazati kijelölő hatóság *120 napos határidővel* azonosítási jelentés benyújtására kötelezi az üzemeltetőt.

Ágazati minősítés lépései (ágazaton belüli *saját rendszerű minősítés*):
a) az ágazati kijelölő hatóság a minősítési döntés előtt az azonosítási eljárás jogszerűségének és teljességének ellenőrzése érdekében megtekinti az azonosítási dokumentációt, és vizsgálja az elemlehatárolás célszerűségét;
b) az ágazati kijelölő hatóság az azonosítási jelentés vizsgálatát követően döntésében
   – a rendszerelemet *nemzeti* létfontosságú rendszerelemnek minősítheti, illetve
   – az összefoglaló táblázatra utalással az ágazati kijelölő hatóság lehetséges *európai* létfontosságú rendszerelemnek minősítheti a vizsgált elemet, vagy
   – új, legfeljebb 90 napon belül elkészítendő azonosítási jelentés benyújtására kötelezi az üzemeltetőt a feltárt hibák és hiányosságok tételes megjelölésével.

6.1.2. Kijelölés

A kijelölési eljárás lépései:

a) az azonosítási jelentést jóváhagyó, nemzeti létfontosságú rendszerelemnek minősítő döntés véglegessé válását követő 30 napon belül az ágazati kijelölő hatóság megindítja a *horizontális kijelölési eljárást;*
b) nemzeti célú kijelölés esetén az ágazati kijelölő hatóság beszerzi a szakhatósági állásfoglalást, amelynek elkészítéséhez *a szakhatóság*[3] *csak az összefoglaló táblázatot tekintheti meg, amelyről másolatot nem készíthet;*
c) ha a szakhatósági állásfoglalás alapján felmerül a vizsgált rendszerelem európai szintű kijelölése, úgy az ágazati kijelölő hatóság felfüggeszti az eljárást, és ennek tényét jelzi a katasztrófák elleni védekezésért felelős miniszter felé;
d) ha az eljárás során a minősített rendszerelemre legalább egy horizontális és egy ágazati kritérium fennáll, az ágazati kijelölő hatóság létfontosságú rendszerelemnek jelöli ki, amelyről tájékoztatja az energiapolitikáért felelős (innovációs és technológiai) minisztert.

(A kijelölő határozat nem tartalmazhat olyan adatot, amely önmagában elegendő a kijelölt rendszerelem felismerésére.)

Speciális szabályok az EGT-állam kijelölésre irányuló kezdeményezésére vonatkozóan:

– ha az üzemeltető, az ágazati kijelölő hatóság vagy az innovációs és technológiai miniszter szerint más EGT-államban az energetikai ágazatba tartozó, Magyarországot érintő lehetséges létfontosságú rendszerelem van, erről a katasztrófák elleni védekezésért felelős minisztert értesíti;
– ha az EGT-állam európai létfontosságú rendszerelem kijelölését kezdeményezi, azt az ágazati kijelölő hatóság megvizsgálja, és álláspontjáról a katasztrófák elleni védekezésért felelős minisztert és az innovációs és technológiai minisztert tájékoztatja;
– nemzetközi szerződés megkötése előtt az innovációs és technológiai miniszter egyeztet az érintett üzemeltetővel.

Az energetikai Korm. rend. a biztonsági összekötő személyre vonatkozóan szakirányú műszaki végzettséget ír elő. 2018. július 1-től az általános képesítési követelményeken túl a biztonsági összekötő személynek szakirányú műszaki szakon szerzett felsőfokú végzettséggel kell rendelkeznie.

Az energia ágazattal kapcsolatosan fontos kiemelni, hogy a Magyar Energetikai és Közmű-szabályozási Hivatal (a továbbiakban: MEKH) megalkotta a *Rotációs Kikapcsolási Rendre* (a továbbiakban: RKR) vonatkozó eljárásrendjét.[4] Az RKR az alapja egy esetleges forráshiány esetén, előre tervezett módon elrendelt felhasználói korlátozás megvalósításának. Az RKR alkalmazásakor alapelv, hogy a felhasználói kikapcsolásokra csak a legszükségesebb mértékben és a lehető legrövidebb időtartamra hozható intézkedés úgy,

[3] Szakhatóságként az 531/2017. (XII. 29.) Korm. rendelet alapján a katasztrófavédelem helyi szerve jár el.
[4] A villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről szóló 280/2016. (IX. 21.) Korm. rendelet.

hogy társadalmi szinten minél kisebb kár következzen be. A villamosenergia-felhasználói kikapcsolások csak akkor alkalmazhatók, ha a közvetlenül fenyegető energiaellátási krízis a klasszikus piacszabályzó eszközökkel vagy a már bekövetkezett krízis az ellátási szabályzatokban előírt eszközökkel nem hárítható el. Az RKR a villamosenergia-felhasználók különböző csoportjainak a villamos energia forrásoldala (~ szolgáltatói oldal) és a fogyasztás (~ felhasználói oldal) egyensúlyának megőrzése céljából a villamosenergia-hiánnyal arányos kikapcsolását és kikapcsolásának gyakoriságát, fokozatait határozza meg. Az RKR-ben a rotációs elv alapján – a károk legkisebb mértékre történő csökkentése érdekében – az egyes ellátási területeken 3 órát meg nem haladó kikapcsolási csoportok szerepelnek. Az így kialakított csoportok között körforgásszerűen hajtják végre a korlátozásokat.

A villamosenergia-ellátás vonatkozásában 3 szintű rendellenességről beszélhetünk:

– *jelentős zavar:* válsághelyzetet el nem érő mértékű üzemi hiba, amelynek során a villamosenergia-rendszer erőműveiben vagy közcélú hálózatain olyan, a villamosenergia-ellátási szabályzatokban meghatározott esemény következik be, amely a villamos energia termelését, termelési készségét, átvitelét, elosztását, szolgáltatását vagy felhasználását jelentősen korlátozza vagy megszünteti, illetőleg a villamosenergia-rendszer üzembiztonságát, szabályozhatóságát vagy együttműködő képességét súlyosan veszélyezteti,
– *válsághelyzet veszélye:*
  • válsághelyzet veszélye *I. fokozatának* minősül, ha a folyamatos villamosenergia-ellátást veszélyeztető olyan tartós erőművi és import teljesítményhiány jelentkezik, hogy a villamosenergia-rendszer erőművi tartaléka 10%-ra csökken, vagy országos szinten a tüzelőanyag-készlet olyan mértékben csökken, hogy a villamosenergia-ellátás folyamatossága 3 napon belül veszélybe kerülhet.
  • válsághelyzet veszélye *II. fokozatának* minősül, ha a villamosenergia-rendszer erőművi tartaléka 7%-ra csökken, vagy országos szinten a villamosenergia-ellátás folyamatossága 2 napon belül veszélybe kerülhet.
– *válsághelyzet:* külön törvényben meghatározott szükséghelyzetet, illetve veszélyhelyzetet el nem érő mértékű, a személyeket, vagyontárgyaikat, a természetet, a környezetet, illetőleg a felhasználók jelentős részének ellátását közvetlenül veszélyeztető villamosenergia-ellátási zavar (a védekezés irányításáért a Kormány felelős).

Ha a villamosenergia-ellátási válsághelyzet a 6 órás időtartamot meghaladja, a Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zrt. (a továbbiakban: MAVIR) elrendeli az RKR alkalmazását. A rendszerirányító és az elosztói engedélyesek felkészülnek az RKR alkalmazására annak érdekében, hogy elkerülhető legyen a villamosenergia-rendszer összeomlása, és a társadalom a legkisebb veszteséget szenvedje el. A rendszerirányító határozza meg az alkalmazandó kikapcsolási fokozatot a hiány nagyságától függően. A szükséges kikapcsolásokat és visszakapcsolásokat az elosztó hálózati engedélyes végzi el, figyelembe véve a rendszerirányító utasításait és a kapcsolás helyén fennálló aktuális üzemállapotot.

Az RKR működése vonatkozásában a hatósági feladatokért elsődlegesen a MEKH felelős, a kapcsolódó eljárásokban *alapvető felhasználókat* jelöl ki, amelyek az RKR alkalmazásakor sem korlátozhatók. A kijelölések hatósági eljárásban zajlanak, a kijelölt alapvető felhasználók körét *háromévente kell felülvizsgálni*. A MEKH a kijelölési eljárások során a katasztrófavédelem területi szerve, a MAVIR, illetve a területileg illetékes elosztó

véleményét is kikérheti. A vonatkozó kormányrendelet szerint az alábbi, a társadalom működéséhez szükséges tevékenységet ellátó, a villamosenergia-ellátásukban nem korlátozható felhasználók jelölhetők ki:

- villamosenergia-rendszer irányítását, üzemzavar-elhárítását végző létesítmények;
- földgázszállítási rendszer irányítását, üzemzavar-elhárítását végző létesítmények;
- kiemelt jelentőségű honvédelmi létesítmények;
- katasztrófavédelmi irányító központok;
- megyei (fővárosi) védelmi bizottságok működési helyei;
- rendvédelmi szervek különleges jogrend időszaki üzemanyagigényét biztosító, ill. nemzeti stratégiai tartalékot kezelő társaság töltőállomásai közül katasztrófavédelmi kirendeltségenként egy töltőállomás;
- országos közszolgálati televízió- és rádióállomás, és hírközlési eszközei, rendvédelmi szervek hírforgalmazását biztosító hálózati berendezések;
- Lrtv. szerinti egészségügyi ágazatban kijelölt szolgáltatók;
- közforgalmi repülőterek, repülésirányító berendezések;
- radioaktív hulladéktároló;
- kényszeráramú szennyvízszállítást és szennyvíztisztítást biztosító létesítmények;
- árvíz és belvízvédekezés idején belvízmentesítést szolgáló szivattyútelepek.[5]

6.2. Víz ágazati létfontosságú rendszerek és létesítmények kijelölési eljárása[6]

Az Lrtv. vhr. rendelkezéseit a vízgazdálkodási létesítmények tekintetében a *létfontosságú vízgazdálkodási rendszerelemek és vízi létesítmények azonosításáról, kijelöléséről és védelméről szóló 541/2013. (XII. 30.) Korm. rendeletben* (a továbbiakban: víz ágazati Korm. rend.) foglalt kiegészítésekkel kell alkalmazni.

(Az Lrtv. rendelkezésein túl a víz ágazati Korm. rend. 4. § a–c) alpontok további 3 kritériumot határoznak meg az európai létfontosságú rendszerelemek azonosításával és kijelölésével kapcsolatban.)

A víz ágazatban – ivóvíz-szolgáltatás, szennyvízelvezetés és –tisztítás, árvízvédelmi létesítmény esetén – ágazati *javaslattevő hatóságként* jár el valamennyi *területi vízügyi igazgatóság* [223/2014. (IX. 4.) Korm. rendelet 1. melléklet].

A víz ágazatban nevesített ágazati kijelölő hatóság az illetékes vízügyi hatóság. A 223/2014. (IX. 4.) Korm. rendelet szerint területi vízügyi hatóságként és szakhatóságként első fokon a hivatásos katasztrófavédelmi igazgatóság jár el.[7] Szintén az illetékes vízügyi hatóság feladata a *helyszíni ellenőrzést lefolytató szerv* által végrehajtandó tevékenységek maradéktalan ellátása. Az Lrtv. vhr. 4. § (2) bekezdése alapján külön szakhatósági megkeresésnek nincs helye, a horizontális kritériumok vizsgálatát a kijelölő hatóság végzi.

A víz ágazatban kijelölhető nemzeti létfontosságú rendszerelemek ágazati kritériumai:

---

[5] A villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről szóló 280/2016. (IX. 21.) Korm. rendelet.

[6] A létfontosságú vízgazdálkodási rendszerelemek és vízi létesítmények azonosításáról, kijelöléséről és védelméről szóló 541/2013. (XII. 30.) Korm. rendelet.

[7] Lásd térképen 4. fejezet 4.7. Kijelölő hatósági tevékenység alfejezet 1. ábra.

– *ivóvíz-szolgáltatás* tekintetében → például olyan felszíni víztisztító mű, amelynek kapacitása meghaladja a 25 000 m^3/d szolgáltatott ivóvízmennyiséget, és olyan ivóvíztároló medence, amelynek tárolókapacitása meghaladja a 25 000 m^3-t;
– *szennyvízelvezetés és -tisztítás* tekintetében → például olyan telep, amelynek kapacitása meghaladja a 250 000 lakosegyenérték szennyezőanyag-terhelést, és amelynek működésképtelenné válása a felszíni víz jelentősen kedvezőtlen állapotát eredményezi;
– *vízkárelhárítás* tekintetében → például olyan vízi létesítmény, amelynek kiesése töltésszakadás veszélyével járó rendkívüli árhullámot indíthat / térségi vízellátást veszélyeztetheti / természeti értékek károsodásával jár / mezőgazdasági vízszolgáltatást veszélyeztetheti;
– árvízi védekezés tekintetében → például olyan elsőrendű árvízvédelmi vízilétesítmény, amely olyan öblözetet véd, amelyben a kitört víz lokalizálására nincs lehetőség.

A víz ágazati Korm. rend. a biztonsági összekötő személyre vonatkozóan területi vagy szakági irányító munkakör betöltéséhez előírt mérnöki végzettséget állapít meg (a rendelkezés 2018. július 1-jén lépett hatályba).

6.3. Rendvédelmi létfontosságú rendszerek és létesítmények kijelölési eljárása (Közbiztonság-védelem ágazat)[8]

Az Lrtv. vhr. rendelkezéseit a rendvédelmi létesítmények tekintetében az *egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról szóló 512/2013. (XII. 29.) Korm. rendeletben* (a továbbiakban: rendvédelmi Korm. rend.) foglalt eltérésekkel és kiegészítésekkel kell alkalmazni.

Fontos kiemelni, hogy a rendvédelmi ágazatban több tekintetben is eltérések mutatkoznak a kijelölési eljárás lefolytatása során. Minden érintett rendvédelmi szervezet azonosítást végez a potenciális létfontosságú rendszerelemei vonatkozásában, amelynek végén a hivatásos katasztrófavédelmi szerv döntése alapján jelölik ki a rendvédelmi ágazat nemzeti létfontosságú rendszerelemeit. Kivételt képez ez alól a katasztrófavédelem, amelynek szervei vonatkozásában a Rendőrség illetékes szerve végzi a kijelölő hatósági feladatokat. Ennek megfelelően *a kijelölési eljárásban érintett szervek a következők:*

– ágazati javaslattevő hatóság – a BM OKF, a BVOP és szervei, az ORFK azon saját rendszerei és létesítményei vonatkozásában, amelyek üzemeltetőjét irányítja/felügyeli;

[8] Egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról szóló 512/2013. (XII. 29.) Korm. rendelet.

– ágazati kijelölő hatóság – az AH, a BVOP, az NBSZ, az NVSZ, a TIBEK, az ORFK és területi szervei, valamint a TEK vonatkozásában a telephely szerint illetékes *katasztrófavédelmi igazgatóság;*
– ágazati kijelölő hatóság – a BM OKF és szervei vonatkozásában a telephely szerint illetékes *rendőr-főkapitányság.*

Speciális szabályok a kijelölési eljárás során:
– a kijelölési eljárás során az ágazati kijelölő hatóság dönt a horizontális kritériumok teljesüléséről, így az Lrtv. vhr. szerinti *szakhatósági megkeresésnek nincs helye;*
– az ágazati kijelölő hatóság az azonosítási jelentés tartalma, az ágazati, valamint a horizontális kritériumok együttes vizsgálata alapján dönt a kijelölésről;
– a BM OKF és szervei vonatkozásában az *ellenőrzést koordináló szerv* a katasztrófák elleni védekezésért felelős miniszter, aki az általa kijelölt szervezeti egység közreműködésével látja el a feladatot;
– a hatósági eljárás során véleményezés céljából – a horizontális kritériumok teljesülésének vizsgálata keretében – az Lrtv. vhr.-ben megjelölt véleménynyilvánító szervek ugyanúgy megkereshetők, mint más ágazatoknál.

Az ágazat kapcsán a BM OKF *nem gyakorolhatja* általános javaslattevő hatósági jogkörét.

A közbiztonság-védelem ágazatban kijelölhető nemzeti létfontosságú rendszerelemek ágazati kritériumai:
– olyan elem, amely a kiesés miatt az Alaptörvényben, valamint az adott rendvédelmi szerv jogállásáról szóló törvényben meghatározott *feladatai közül legalább kettőt nem tud ellátni,* és 12 órán belül nem helyettesíthető;
– olyan elem, amely az érintett rendvédelmi szerv *legalább kettő* alapfeladata ellátásában részt vevő *szervezeti egység működését biztosítja,* és kiesése 48 órán belül sem pótolható;
– olyan elem, amely az érintett rendvédelmi szerv alapfeladatának ellátását biztosító *informatikai és infokommunikációs rendszerek működését garantálja,* és kiesése 8 órán belül sem pótolható.

A rendvédelmi Korm. rend. a biztonsági összekötő személyre vonatkozóan felsőfokú szakirányú végzettséget ír elő.

6.4. Honvédelmi létfontosságú rendszerek és létesítmények kijelölési eljárása[9]

Az Lrtv. vhr. rendelkezéseit a honvédelmi létesítmények tekintetében *a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről* szóló *359/2015. (XII. 2.) Korm. rendeletben* (a továbbiakban: honvédelmi Korm. rend.) foglalt eltérésekkel és kiegészítésekkel kell alkalmazni, figyelembe véve a honvédelmi létfontosságú rendszerelemek

[9] A honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről szóló 359/2015. (XII. 2.) Korm. rendelet.

azonosításáról, kijelöléséről, ellenőrzéséről, valamint az ezzel összefüggő adatok nyilvántartásáról szóló 46/2016. (VIII. 25.) HM utasítás (a továbbiakban: HM utasítás) tartalmát.

(Az Lrtv. rendelkezésein túl a honvédelmi Korm. rend. nem határoz meg egyéb kritériumot az európai létfontosságú rendszerelemek azonosításával és kijelölésével kapcsolatban.)

A honvédelmi ágazatban az Lrtv. és az Lrtv. vhr. által meghatározott kivételszabályok (például: nyilvántartó hatósági jogkör, ellenőrzés koordinációja) alkalmazására is figyelemmel kell lenni.

A honvédelmi létfontosságú rendszerek vonatkozásában a *javaslattevő, a nyilvántartó, a kijelölő hatósági feladatokat ellátó és az ellenőrzések koordinációját végző szerv a Honvédelmi Minisztérium*. A vonatkozó HM utasítás szerint a feladatokat az alábbi szervezeti egységek végzik:

- ágazati javaslattevő hatóság: HM Védelmi Igazgatási Főosztály,
- ágazati kijelölő hatóság: HM Hatósági Főosztály,
- ágazati nyilvántartó hatóság (a hadiipari rendszerek kivételével): HM Védelmi Igazgatási Főosztály,
  (a hadiipari rendszerekkel kapcsolatos nyilvántartó hatósági feladatokat a Magyar Honvédség Logisztikai Központ látja el)
- ágazati ellenőrzést koordináló szerv: HM Védelmi Igazgatási Főosztály.

A honvédelem ágazatban kijelölhető nemzeti létfontosságú rendszerelemek ágazati kritériumai:

Az a létesítmény/infrastruktúra/eszköz/szolgáltatás jelölhető ki,

- amelynek kiesése a *honvédelmi ágazat működésképtelenségét* vagy *súlyos zavarát* okozza, és nem, vagy csak a *honvédelmi érdek aránytalanul nagy sérelmével helyettesíthető,*
- amely *szerepel az ország védelmével kapcsolatban kidolgozott tervekben,* és amelynek kiesése – a műveleti tervek rugalmasságán belül – nem, vagy csak a honvédelmi érdek aránytalanul nagy sérülésével helyettesíthető,
- amelynek *kiesése a Befogadó Nemzeti Támogatás*[10] *keretében vállalt honvédségi feladatok végrehajthatóságát jelentősen veszélyezteti,* vagy abban súlyos zavart okoz, és nem, vagy csak az érintett felek érdekeinek aránytalanul nagy sérelmével helyettesíthető,
- amelynek *leállása vagy meghibásodás miatt történő kiváltása vagy helyettesítése hosszabb ideig tart,* mint amennyit a honvédelmi ágazat súlyos képességvesztés nélkül el tud viselni,
- amely *stratégiai fontosságú honvédségi gyártó, javító, tároló vagy elosztó kapacitást képvisel,* és nem helyettesíthető a készenlétfokozás rendszerét szabályozó tervekben meghatározott időn belül,
- amely a *NATO szövetségi rendszer Magyarországon lévő rendszereleme,* és védettségének sérülése, teljesítőképességének vagy más jellemzőjének negatív változása

[10] Egy befogadó nemzet által békeidőszakban, szükségállapotok, válság, vagy konfliktus esetén a fogadó nemzet területén elhelyezkedő, működő, illetve átvonuló szövetséges erők és szervezetek számára nyújtott polgári és katonai segítség. Az ilyen segítségnyújtás alapját a fogadó nemzetek, a küldő nemzetek és/vagy a NATO illetékes szervei között megkötött megállapodások képezik. [MC 334/1. A Fogadó Nemzeti Támogatás (HNS) NATO alap- és irányelvei 2000, 7.]

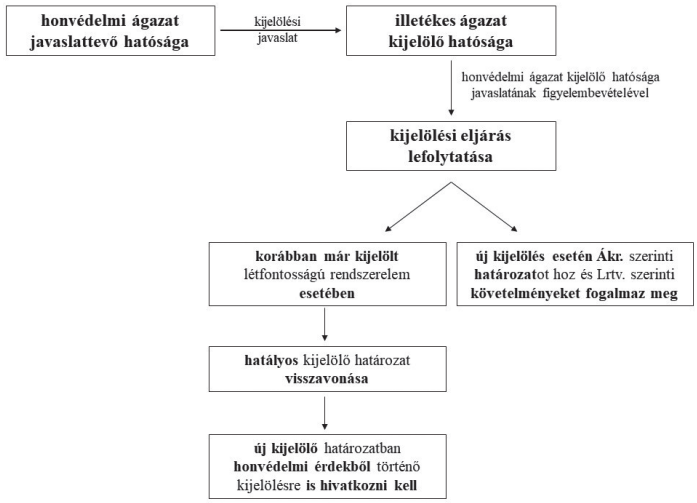
a szövetségi rendszer működésében, biztonságában súlyos zavart vagy működésképtelenséget okoz,
- amely a *NATO Válságreagálási Rendszerrel összhangban álló Nemzeti Intézkedési Rendszerben meghatározott rendszabályok végrehajtásához elengedhetetlenül szükséges,* vagy
- amely *speciális honvédelmi igényeket elégít ki,* nincs helyettesítője, és kiesése a honvédelmi igazgatás működésképtelenségét vagy súlyos zavarát okozza.

A honvédelmi Korm. rendelet meghatároz ágazaton belüli és ágazaton kívüli honvédelmi létfontosságú rendszerelemeket, amelyekre a fenti ágazati kritériumok valamelyike érvényes lehet*:*
- Ágazaton belüli rendszerelemeknek tekintjük a Honvédelmi Minisztérium, a honvédelemért felelős miniszter közvetlen alárendeltségébe tartozó szervezetek, a Katonai Nemzetbiztonsági Szolgálat, valamint a Magyar Honvédség katonai szervezetei által működtetett rendszerelemeket és létesítményeket.
- Ágazaton kívüli rendszerelemeknek tekintjük a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény 18. §-ában felsorolt honvédelemben közreműködő szerveket vagy az irányításuk, felügyeletük vagy tulajdonosi joggyakorlásuk alá tartozó szerv, szervezet, intézmény által működtetett rendszerelemet és létesítményt.

Az ágazaton belüli honvédelmi létfontosságú rendszerelemek kijelölési eljárása azonos az Lrtv. és az Lrtv. vhr. által meghatározott kijelölési eljárással. Az azonosítási jelentés benyújtását követően – a kijelölési eljárás részeként – a kijelölő hatóság szakhatósági eljárás keretében bevonja a katasztrófavédelmet a horizontális kritériumok vizsgálata érdekében, majd az eljárás végén határozatot hoz.

A honvédelmi Korm. rendelet meghatározza az ágazaton kívüli honvédelmi létfontosságú rendszerelemek azonosításának és kijelölésének szabályait. Ágazaton kívüli honvédelmi létfontosságú rendszerelemmé az a rendszerelem vagy létesítmény jelölhető ki:
- amelyet az illetékes ágazat kijelölő hatósága az adott ágazat kritériumai alapján nem jelölt ki létfontosságú rendszerelemmé, *azonban a honvédelmi ágazati kritériumok alapján honvédelmi létfontosságú rendszerelemmé kijelölése feltétlenül indokolt,* vagy
- amely esetében az *illetékes ágazat kritériumai szerinti kijelölés* az adott rendszerelem vagy létesítmény működése vonatkozásában *nem biztosítja a honvédelmi érdek maradéktalan érvényesülését.*

Ágazaton kívüli honvédelmi rendszerelemmé történő kijelölés esetén *javaslattevő hatóságként a HM Védelmi Igazgatási Főosztály jár el,* amelynek javaslata alapján az illetékes ágazat kijelölő hatósága, a honvédelmi ágazat kijelölő hatóságának állásfoglalását is figyelembe véve, lefolytatja a kijelölési eljárást, és annak eredményéről a javaslattevő hatóságot tájékoztatja. Amennyiben az illetékes ágazati kijelölő hatóság egy létfontosságúnak már kijelölt rendszerelemet honvédelmi létfontosságú rendszerelemnek jelöl ki, ezzel egyidejűleg a korábbi kijelölő határozatát visszavonja, és az új kijelölő határozatában a honvédelmi érdekből történő kijelölésre is hivatkozik. A folyamatot az alábbi ábra szemlélteti.



1. ábra

Az ágazaton kívüli kijelölés folyamata

Forrás: a szerző szerkesztése

Az ágazaton kívüli kijelölés szabályait tartalmazó rendelkezéseket az *energia ágazat létesítményeire nem kell alkalmazni*.

A honvédelmi Korm. rend. az ágazaton belüli honvédelmi létfontosságú rendszerelem tekintetében a biztonsági összekötő személynek katonai felsőfokú végzettséget és az adott rendszerelem működtetésében legalább 2 éves szakmai tapasztalattal való rendelkezést ír elő.

Az Lrtv. rendelkezései szerint a honvédelmi ágazat tekintetében a *honvédelmi Korm. rendelet határozza meg az ellenőrzések koordinálásáért felelős szervet* (HM Védelmi Igazgatási Főosztály), az ellenőrzés kiegészítő szabályait, valamint az ellenőrzés résztvevőinek körét az alábbiak szerint:

– az ellenőrzést ütemezett módon, éves ellenőrzési terv alapján kell végrehajtani oly módon, hogy a rendszerelemet legalább kétévente ellenőrizzék;
– az *ellenőrzésbe bevonható*: az ágazati kijelölő hatóság, a HM vagyonfelügyeletért felelős szervezeti egysége, a Honvéd Vezérkar csoportfőnökségei, a HM Védelemgazdasági Hivatal, az illetékes védelmi igazgatási szervek, hadiipari rendszerelem esetében a Magyar Kereskedelmi Engedélyezési Hivatal, valamint a hivatásos katasztrófavédelmi szerv központi szerve;
– az ellenőrzésekről, a megállapított hiányosságokról, valamint a hiányosságok megszüntetésére irányuló javaslatokról összefoglaló jelentést készül;
– az ellenőrzött rendszerelem üzemeltetője az ellenőrzés során megállapított hiányosságok megszüntetésére irányuló intézkedéseiről 90 napon belül tájékoztatja az ágazati ellenőrzést koordináló szervet.

6.5. Agrárgazdasági létfontosságú rendszerek és létesítmények kijelölési eljárása[11]

Az Lrtv. vhr. rendelkezéseit az agrárgazdasági létesítmények tekintetében *a létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 540/2013. (XII. 30.) Korm. rendeletben* (a továbbiakban: agrár Korm. rend.) foglalt eltérésekkel és kiegészítésekkel kell alkalmazni.

(Az Lrtv. rendelkezésein túl az agrár Korm. rend. 6. § további 2 kritériumot határoz meg az európai létfontosságú rendszerelemek azonosításával és kijelölésével kapcsolatban.)

Az agrár ágazat vonatkozásában

- ágazati javaslattevő hatóságként jár el a *fővárosi és megyei kormányhivatal élelmiszerlánc-biztonsági és állategészségügyi igazgatósága,* valamint *növény- és talajvédelmi igazgatósága*
- ágazati kijelölő hatóságként jár el a *Nemzeti Élelmiszerlánc-biztonsági Hivatal (NÉBIH).*

Az agárágazatban kijelölhető nemzeti létfontosságú rendszerelemek ágazati kritériumai:

- *növényi genetikai* erőforrásokat megőrző *génbank* → ha legalább ezer megőrzött tétellel rendelkezik;
- *vetőmag-előállító létesítmény* → ha a kukorica és a búza vonatkozásában a tárgyévet megelőző tíz év átlagos vetésterülete tíz-tíz százalékának vetőmagszükségletét képes ellátni;
- *állati oltóanyag előállítását biztosító létesítmény*
  - ha az állatbetegségek bejelentésének rendjéről szóló miniszteri rendeletben meghatározott bejelentési kötelezettség alá tartozó állatbetegségek elleni oltóanyagot állít elő,
  - ha az oltóanyag-előállítás nélkülözhetetlen komponensének beszállítója, s ezen tevékenységének nettó árbevétele eléri az évi 1 milliárd forintot;
- *élelmiszer-előállítást biztosító létesítmény*
  - ha *emlősállatok vágását* és vágóhídi darabolását végzi meghatározott napi kapacitás szerint,
  - ha *baromfihús feldolgozását,* tartósítását végzi meghatározott napi kapacitás szerint,
  - ha *hús-, baromfihúskészítmény-gyártást* végez meghatározott napi kapacitás szerint,
  - ha egyéb *gyümölcs-, zöldségfeldolgozást, tartósítást* végez meghatározott éves kapacitás szerint,
  - ha *tejfeldolgozást* végez meghatározott napi kapacitás szerint,
  - ha *malomipari termékek gyártását* végzi, és az előző évi termelési átlaga elérte a 60 000 tonnát, továbbá
  - ha *kenyér, friss pékáru gyártását* végzi, és az előző évi termelési átlaga elérte a 100 000 tonnát.

[11] A létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 540/2013. (XII. 30.) Korm. rendelet.

– egy *vállalkozás termelést és elosztást végző létesítménye,* ha a vállalkozásnak vonatkozó jogszabály szerinti élelmiszerlánc-felügyeleti díjköteles nettó árbevétele eléri vagy meghaladja a 40 milliárd forintot;
– élelmiszer-kereskedelmi tevékenységet végző *vállalkozás élelmiszer tárolását, elosztását végző logisztikai létesítménye* meghatározott nettó árbevétel vagy meghatározott ellátóképesség szerint;
– napi 10 000 adag fölötti kapacitással rendelkező *főzőkonyha;*
– nemzeti vagy európai létfontosságú rendszerelemként *kijelölt kórház ellátását biztosító főzőkonyha;*
– állati eredetű melléktermék-feldolgozó *létesítmény* meghatározott kategóriájú melléktermék-feldolgozó kapacitással;
– *állami tartalékok vonatkozásában működő létesítmény,* ha tároló létesítménye tekintetében együttesen 500 millió forintot meghaladó értékben Gazdaságbiztonsági Tartalékban[12] vagy Állami Céltartalékban lévő készletek tárolását végzi.

Az agrár Korm. rend. 8. § a–d) pontjai a biztonsági összekötő személyre vonatkozóan, az egyes nemzeti létfontosságú rendszerelemek ágazati kritériumaihoz kötődően írnak elő végzettségi követelményeket.

6.6. Egészségügyi létfontosságú rendszerek és létesítmények kijelölési eljárása[13]

Az Lrtv. vhr. rendelkezéseit *az egészségügyi létesítmények tekintetében az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendeletben* (a továbbiakban: egészségügyi Korm. rend.) foglalt kiegészítésekkel kell alkalmazni.

(Az Lrtv. rendelkezésein túl az egészségügyi Korm. rend. 11. § további kritériumokat határoz meg az európai létfontosságú rendszerelemek azonosításával és kijelölésével kapcsolatban.)

Az egészségügy ágazatban az ágazati kijelölő hatósági feladatokat az *egészségügyért felelős miniszter* (jelenleg az emberi erőforrások minisztere) *látja el.* A minisztert *feladatai ellátásában egy döntés-előkészítő bizottság* (a továbbiakban: Bizottság) *segíti.* A Bizottság elnökből és tíz, az alágazatoktól és az Emberi Erőforrások Minisztériumából delegált tagból áll. A Bizottság feladata az ágazati kritériumok vizsgálata (európai, nemzeti vonatkozásban egyaránt) a javaslattevő hatóságok bevonásával. A bizottsági tagság feltétele, hogy a tagok már elvégezték, vagy a felkérés elfogadását követő egy éven belül elvégezzék a biztonsági

[12] Az egész nemzetgazdaság vagy egy egész ágazat folyó és különleges jogrendi működését, a mozgósított gazdaság feladatai végrehajtását jelentősen befolyásoló, alapvetően fontos energiahordozókat, import alapanyagokat, valamint a lakosság védelmét szolgáló és ellátásában keletkező jelentős kihatású piaci zavarok elhárítására kiszabott kohászati, vegyipari, papír- és nyomdaipari, egyéb ipari és élelmiszeripari termékeket tartalmaz. (Tóth 2007, 2.)

[13] Az egészségügyi létesítmények tekintetében az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet.

összekötői tanfolyamot. Az alágazatokat képviselő tagok esetében további elvárás legalább 5 éves szakmai gyakorlat. A delegált tagok megbízatása három évre szól.

Ágazati javaslattevő hatóságok:

– aktív fekvőbeteg-ellátás alágazat: Állami Egészségügyi Ellátó Központ;
– mentésirányítás alágazat: Országos Mentőszolgálat;
– egészségügyi tartalékok alágazat: Állami Egészségügyi Ellátó Központ;
– vérkészletek alágazat: Országos Vérellátó Szolgálat;
– magas biztonsági szintű biológiai laboratóriumok alágazat: országos tisztifőorvosi feladatokért felelős helyettes államtitkárság (EMMI);
– gyógyszer-nagykereskedelem alágazat: Országos Gyógyszerészeti és Élelmezés-egészségügyi Intézet.

Az egészségügy ágazatban kijelölhető nemzeti létfontosságú rendszerelemek ágazati kritériumai:

– azok az *aktív fekvőbeteg-ellátók (kórházak),* amelyek
  • legalább 400 aktív ággyal rendelkeznek, vagy a területi ellátási kötelezettségükbe tartozók létszáma eléri vagy meghaladja az 1,5 millió főt,
  • kiesése esetén a legközelebbi kórház közúton 45 percen belül nem közelíthető meg az ellátottak által, vagy a kórház működésének folyamatos fenntartásához egészségpolitikai érdek fűződik.
– azok a *mentésirányítási központok,* ahonnan legalább egy megyére vagy a Fővárosra kiterjedően irányítják a mentési tevékenységet.
– az Állami Egészségügyi Tartalék (a továbbiakban: ÁEüT) tekintetében
  • az a nyilvántartási rendszer, amelynek kiesése a normál működési rendet legalább 24 óráig lehetetlenné teszi, vagy helyreállítása legalább 48 óráig tart,
  • minden olyan raktár vagy tárolókapacitás, ahol az ÁEüT összértékének legalább 10%-a található,
  • az Állami Egészségügyi Tartalékkal való gazdálkodás szabályairól szóló rendeletben meghatározott orvostechnikai eszköz- és gyógyszernormák egyes tételei készletmennyiségének 50%-át meghaladó mennyiséget tartalmazó raktárak,
– a *vérkészletek* tekintetében
  • az országos vér- és transzfuziológiai készletek nyilvántartási rendszere,
  • a tároláshoz, illetve a véradáshoz szükséges infrastruktúraelemek, ha ezek megsérülése 3 napos vagy annál hosszabb ideig tartó fennakadást jelentene az országos vérellátó rendszerben.
– azon *laboratóriumok,* amelyekben rendszeresen tárolnak, feldolgoznak vagy vizsgálnak közepes biztonsági szintű vagy magas biztonsági szintű mikrobiológiai vagy egyéb biológiai anyagot, valamint toxint, vagy ehhez a tevékenységhez műszaki-technológiai támogatást nyújtanak,
– az egészségügyi szolgáltatások nyújtásához szükséges szakmai minimumfeltételekről szóló rendelet szerint kijelölt *referencialaboratóriumok,*
– azon *gyógyszer-nagykereskedelmi tevékenységet végző gazdálkodó szervezet,* amely
  • gyógyszerforgalmazásra vonatkozó piaci részesedése az éves árbevétel alapján Magyarországon meghaladja
    • a gyógyszertári kiszállítások esetében a 15%-ot vagy

- fekvőbeteg-szakellátást végző gyógyintézet esetében a 15%-ot,
- országos lefedettséget biztosító logisztikával rendelkezik, és
- forgalmazási területén a felhasználók igényének megfelelő teljes gyógyszerkört forgalmazza.

Helyszíni ellenőrző szervként a kijelölt kórházak és laboratóriumok vonatkozásában a népegészségügyi feladatkörében eljáró *fővárosi és megyei kormányhivatalt,* egyebekben a minisztert jelölték ki, aki a minisztérium ellenőrzési feladatokat ellátó szervezeti egysége közreműködésével látja el ezt a feladatot.

Az egészségügyi Korm. rendelet tételesen meghatározza azon üzemeltetők körét, amelyek azonosítási jelentés benyújtására kötelezettek (például: kórházak, a mentésirányítást végző szervezet, az állami vérkészletek kezelője, az egészségbiztosítás informatikai rendszerei üzemeltetője, vagy a gyógyszer-nagykereskedelmi tevékenységet végző szervezetek).

Részletesen szabályozza továbbá, hogy az Lrtv. vhr.-ben előírtakon túl az azonosítási jelentésnek, valamint az üzemeltetői biztonsági tervnek milyen tartalmi követelményeknek kell megfelelniük. Ilyen eltérés például az azonosítási jelentés esetében az, hogy

– az azonosítási jelentésben szereplő kockázatelemzésnek tartalmaznia kell az aktuális védelmi szintről, valamint az esetleges kiesés következményeiről szóló elemzést is,
– a laboratóriumok esetében az azonosítási jelentésben fel kell tüntetni a bejelentési kötelezettség alapjául szolgáló anyagok nevét, mennyiségét, helyét, továbbá az ezekkel kapcsolatos műszaki-technológiai támogatási szolgáltatást, a laboratórium méretét, a dolgozók számát és végzettségét is,
– tevékenységváltozás esetén új azonosítást kell végezni, és a működési engedély módosítását elrendelő határozat véglegessé válásától számított 90 napon belül új azonosítási jelentést kell benyújtani.

Az egészségügy ágazatban kijelölt létfontosságú rendszerelemek által készített üzemeltetői biztonsági terveknek az Lrtv. vhr.-ben előírt tartalmi követelményeken túl az alábbi részterveket is tartalmazniuk kell:

– közművek kiváltására, alternatív működtetésére vonatkozó terv,
– szükséges, elengedhetetlen szolgáltatások biztosítására vonatkozó terv,
– élelmezési terv,
– gyógyszerek, egészségügyi fogyóeszközök, vér- és vérkészítmények pótlási terve és
– kommunikációs terv.

Az egészségügyi Korm. rendelet meghatározza az egészségügyi ágazatban biztonsági összekötő személyként foglalkoztatottak képesítési követelményeit. Az általános képesítési követelményeken túl a laboratóriumokban, valamint a gyógyszer-nagykereskedelemben történő foglalkoztatás esetén az általánostól eltérő követelményt ír elő a jogszabály.

2017. november 1-jén az egészségügy ágazatból kivált a *Társadalombiztosítás* mint önálló ágazat, és a hozzá tartozó társadalombiztosítási ellátások igénybevételéhez kapcsolódó informatikai rendszerek és nyilvántartások alágazat. Az új ágazat szabályozása még nem készült el, az egészségügyi Korm. rend. vonatkozó rendelkezései hatályban vannak, így potenciális létfontosságú rendszerelemekként idesorolhatók

– az *egészségbiztosítás azon informatikai rendszerei,* amelyek kiesése során a rendszer egészének bizalmassága, sértetlensége vagy rendelkezésre állása sérül, és ez olyan mértékű üzemzavart eredményez,
  • amelynek az elhárítása legalább 48 órát vesz igénybe, vagy
  • amely következményeinek az elhárítása és az üzemszerű működés helyreállítása legalább 48 órát vesz igénybe, függetlenül attól, hogy az üzemzavar mennyi ideig állt fenn.

6.7. A pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények kijelölési eljárása[14]

Az Lrtv. vhr. rendelkezéseit a *pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 330/2015. (XI.10.) Korm. rendeletben* (a továbbiakban: pénzügy Korm. rend.) foglalt eltérésekkel és kiegészítésekkel kell alkalmazni.

Pénzügy ágazatban
– az ágazati javaslattevő hatósági hatáskört a pénzügyi közvetítőrendszer felügyeletével kapcsolatos feladatkörben eljáró *Magyar Nemzeti Bank* (a továbbiakban: MNB) kapta meg, és a *helyszíni ellenőrzés lefolytatására is jogosult.*
– Ágazati kijelölő hatóságként a pénz-, tőke- és biztosítási piac szabályozásáért felelős *miniszter* (jelenleg a pénzügyminiszter) *jár el.* A minisztert ez irányú feladatai elvégzésében egy *döntés-előkészítő bizottság* (a továbbiakban: Bizottság) *segíti.* A Bizottság az elnökből és további hat tagból áll. Bizottság összetételéről a miniszter dönt, de a delegálás feltétele a legalább 2 éves szakirányú szakmai tapasztalat. A delegált tagok mandátuma három évre szól.

A kijelölési eljárás döntési mechanizmusa szerint a bizottsági döntéshozatal szavazattöbbséggel történik, szavazategyenlőség esetében az elnök szavazata döntő (a Bizottság határozatképes, amennyiben az elnökön, vagy távollétében az ügyrendben meghatározott helyettesítési rend szerint illetékes személyen kívül további három tag jelen van). Az elbírálás körültekintő végrehajtása érdekében a Bizottság adatokat igényelhet az MNB-től, illetve az érintett üzemeltetőtől egyaránt.

A pénzügyi Korm. rendelet alapján *egy pénzügyi ágazati létesítmény akkor jelölhető ki* nemzeti létfontosságú rendszerelemmé, *ha a gazdasági, társadalmi vagy politikai hatás, mint horizontális kritériumok közül egy,* és egy ágazati kritérium teljesül. *A többi ágazattól eltérően a pénzügyi ágazat kijelölési eljárásában a szakhatóság a veszteségek és a környezeti hatás kritériumát nem vizsgálja.*

A pénzügy ágazatban kijelölhető nemzeti létfontosságú rendszerelemek ágazati kritériumai:

[14] A pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 330/2015. (XI. 10.) Korm. rendelet.

– olyan, a gazdaság finanszírozását támogató *hitelintézet,* amely magyar állami tulajdonban van;
– magyarországi székhellyel rendelkező *betétbiztosítási vagy befektetésbiztosítási rendszer,* amely kártalanítási funkciót tölt be a pénzügyi vagy befektetési szolgáltatást ellátó intézmény esetleges fizetésképtelenségének bekövetkezésekor;
– magyarországi székhellyel rendelkező *vállalkozás, amely a készpénzellátás folyamatosságát segíti;*
– olyan magyarországi székhellyel rendelkező *hitelintézet,* amely – a mérlegfőösszeg alapján[15] – legalább 10%-os piaci részesedésű;
– azon magyarországi székhellyel rendelkező *vállalkozás, amely tőzsdei tevékenységet végez.*

A pénzügyi szektor esetében a biztonsági összekötő személynek szakirányú jogi vagy közgazdasági felsőfokú végzettséggel rendelkező szakembernek kell lennie.

6.8. Az infokommunikációs technológiák ágazathoz tartozó létfontosságú rendszerek és létesítmények kijelölési eljárása[16]

Az Lrtv. vhr. rendelkezéseit *az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 249/2017. (IX. 5.) Korm. rendeletben* (a továbbiakban: IT Korm. rend.) foglalt eltérésekkel és kiegészítésekkel kell alkalmazni.

(Az Lrtv. rendelkezésein túl az IT Korm. rend. 14. § további 2 kritériumot határoz meg az európai létfontosságú rendszerelemek azonosításával és kijelölésével kapcsolatban.)

Az ágazat vonatkozásában az egyes alágazatokhoz rendelve határozták meg az eljáró hatóságokat, a következők szerint:
– az internet-infrastruktúra és internet-hozzáférés szolgáltatása,
– a vezetékes és vezeték nélküli elektronikus hírközlési szolgáltatások, vezetékes és vezeték nélküli hírközlő hálózatok,
– a rádiós távközlés,
– az űrtávközlés,
– a műsorszórás és
– a postai szolgáltatások alágazatok vonatkozásában ágazati kijelölő hatóságként jár el a *Nemzeti Média- és Hírközlési Hatóság Hivatala* (a továbbiakban: NMHH Hivatala), amelynek munkáját *döntés-előkészítő bizottság segíti.* A bizottság szervezeti és működési szabályait az NMHH SZMSZ-ben rögzítik.
– *a kormányzati informatikai, elektronikus hálózatok alágazat* vonatkozásában ágazati kijelölő hatósági feladatokat lát el a közigazgatási informatika infrastrukturális

[15] A vállalat teljes vagyonát mutató mérlegének utolsó sora, amely az egyik legjobb mérőszáma egy pénzügyi vállalkozás méretének, illetve befolyásának a gazdasági életben. A feltüntetett összeg tartalmazza a pénzügyi vállalkozás teljes hitelállományát, illetve az elhelyezett összes betétet és a saját tőkét is.

[16] Az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 249/2017. (IX. 5.) Korm. rendelet.

megvalósíthatóságának biztosításáért felelős *miniszter* (jelenleg a belügyminiszter), akinek munkáját *döntés-előkészítő bizottság segíti.* A Bizottság az elnökből és további hat tagból áll. A Bizottság összetételéről a miniszter dönt.
– a *postai szolgáltatások alágazat* tekintetében ágazati javaslattevő hatóságként jár el a postaügyért felelős *miniszter* (jelenleg a nemzeti vagyon kezeléséért felelős tárca nélküli miniszter).

Az ágazatban kijelölt létfontosságú rendszerelemeknél helyszíni ellenőrzést – a kormányzati informatikai, elektronikus hálózatok kivételével – az NMHH Hivatala végezhet. A kormányzati informatikai, elektronikus hálózatok információbiztonsági szempontú helyszíni ellenőrzését a Nemzetbiztonsági Szakszolgálat végzi.

Az IT-ágazatban kijelölhető potenciális nemzeti létfontosságú rendszerelemek például:
– olyan elektronikus *hírközlési szolgáltató,* amely Magyarország területén vezetékes és vezeték nélküli elektronikus hírközlési szolgáltatást biztosít, és amelynek *kiesése összesen több mint ötvenezer természetes vagy jogi személyt érinthet;*
– olyan elektronikus hírközlési szolgáltató, amely *egyetemes hírközlési szolgáltatást nyújt;*
– olyan *műsorszóró* átviteli rendszer*,* amelynek kiesése más rendszerelemmel nem váltható ki, és *Magyarország területének legalább 95%-án elérhető,*
– olyan meghatározott *kormányzati célú hálózat,* amely az emberéletet is fenyegető *veszélyhelyzet előrejelzését, jelzését vagy az emberéletet is fenyegető katasztrófa elhárítását támogatja*.

Az IT Korm. rend. tételesen meghatározza, hogy az ágazat tekintetében milyen végzettségeket lehet szakirányúnak tekinteni.

Felhasznált irodalom

TÓTH József (2007): A védelmi célú tartalékolás rendszere és strukturális változása napjainkban. *Szolnoki Tudományos Közlemények,* 11. sz.

Hivatkozott jogszabályok és dokumentumok

Az egészségügyi létesítmények tekintetében az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet

Egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról szóló 512/2013. (XII. 29.) Korm. rendelet

Az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 360/2013. (X. 11.) Korm. rendelet

A honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről szóló 359/2015. (XII. 2.) Korm. rendelet

Az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 249/2017. (IX. 5.) Korm. rendelet

A létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 540/2013. (XII. 30.) Korm. rendelet

A létfontosságú vízgazdálkodási rendszerelemek és vízi létesítmények azonosításáról, kijelöléséről és védelméről szóló 541/2013. (XII. 30.) Korm. rendelet

MC 334/1. A Fogadó Nemzeti Támogatás (HNS) NATO alap- és irányelvei (2000)

A pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 330/2015. (XI. 10.) Korm. rendelet

A villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről szóló 280/2016. (IX. 21.) Korm. rendelet

Vákát oldal

Összegzés

NATO- és európai uniós tagállammá válásunkból adódóan gyakorlatilag a kezdetektől részesei lehettünk a kritikus infrastruktúrák védelmére irányuló nemzetközi szintű kezdeményezéseknek, amelyek alapján 2008-ban az EU-tagállamok közül az elsők között alakítottuk ki Nemzeti Programunkat.

A 2012-ben elfogadott és 2013-ban hatályba lépett törvény, majd a részletszabályozást tartalmazó végrehajtási kormányrendelet adta azt a keretet, amely biztosítja, hogy a létfontosságú rendszerek és rendszerelemek azonosítása és kijelölése rendszerben történjen meg. *Mindezek ágazatspecifikus kiegészítései az egyes szektorokat szabályozó kormányrendeletek, amelyek kivételekkel, pontosításokkal és ágazati sajátosságokkal teszik teljessé a keretszabályozást.*

Fontos hangsúlyozni, hogy az EU által meghatározott kötelezettségek vonatkozásában hazánk szigorúbb szabályrendszert állított fel, amelyben a biztonsági összekötő személlyel és az üzemeltetői biztonsági tervvel kapcsolatos elvárások kifejezetten előrelátó szemléletet mutatnak.

A kritikus infrastruktúrák védelme komplex rendszerének áttekintése alapján egyértelműen látható, hogy *a létfontosságú rendszerek és létesítmények védelmével kapcsolatos feladatok tekintetében markáns szerepet lát el a hivatásos katasztrófavédelmi szerv.*

Tekintettel arra, hogy ez a típusú védelmi feladatkör rendkívül szerteágazó tevékenység, a katasztrófavédelemhez delegált feladat- és hatáskörök is különös jelentőségűek. A jog- és szakszerű feladatellátás érdekében fontos, hogy kellő hangsúly kerüljön a továbbképzések végrehajtására és az aktualitások folyamatos nyomon követésére. Ennek érdekében rendszeressé válik a katasztrófavédelmen belüli, célirányos, ágazati sajátosságokhoz köthető felkészítések szervezése.

A jövőben különös figyelmet kell szentelni a létfontosságú rendszerek és rendszerelemek védelmére létrehozott rendszer folyamatos fejlesztésének, időszakos felülvizsgálatának, annak érdekében, hogy a veszélyeztető tényezőkkel arányos válaszok, az együttműködés jegyében biztosított folyamatos működés és a rendelkezésre álló tapasztalatok rendszeres feldolgozása megvalósítható legyen.

Vákát oldal

MELLÉKLETEK

Rövidítések jegyzéke

ÁEüT	Állami Egészségügyi Tartalék
Agrár Korm. rend.	A létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 540/2013. (XII. 30.) Korm. rendelet
Ákr.	Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény
AH	Alkotmányvédelmi Hivatal
BM OKF	BM Országos Katasztrófavédelmi Főigazgatóság
BRICS-államok	Brazília, Oroszország, India, Kína és Dél-Afrika
BSI	Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de), Német Szövetségi Köztársaság Szövetségi Információs Technológiai Biztonsági Hivatal
BVOP	Büntetés-végrehajtás Országos Parancsnoksága
CBRN események	Chemical, biological, radiological and nuclear incident, kémiai, biológiai, radiológiai és nukleáris esemény
CERT	Computer Emergency Response Team, számítástechnikai sürgősségi reagáló egység
CIMIC	Civil-Military Co-operation, Civil-katonai együttműködés képessége
CIP POC	Critical Infrastructure Protection Point of Contact, Kritikus infrastruktúra védelmi kapcsolattartó pont
CIRC	NATO Computer Incident Response Capability, NATO Számítógépes Biztonsági Események Kezelése
CIWIN	Critical Infrastructure Warning Information Network, Kritikus Infrastruktúrák Figyelmeztető Információs Hálózata
CPNI	Centre for the Protection of National Infratructure (www.cpni.gov.uk), Nemzeti Infrastruktúra Védelmi Központ (Nagy-Britannia és Észak-Írország Egyesült Királysága)
D-A-CH	Germany (D) – Austria (A) – Switzerland (CH) Németország–Ausztria–Svájc együttműködés
ECI	European Critical Infrastructure, európai kritikus infrastruktúra
EEA	European Environment Agency (www.eea.europa.eu), Európai Környezetvédelmi Ügynökség
EGC	European Government CERTs, Európai Kormányzati CERT-ek
Egészségügyi Korm. rend.	Az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet
EGT	Európai Gazdasági Térség

Energetikai Korm. rend.	Az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 360/2013. (X. 11.) Korm. rendelet
ENISA	European Network and Information Security Agency, Európai Unió Információs és Hálózatbizonsági Ügynöksége
ENSZ [UN]	Egyesült Nemzetek Szervezete, United Nations Organisation
ENSZ EGB	Egyesült Nemzetek Szervezete Európai Gazdasági Bizottsága
EPCIP	European Programme for Critical Infrastructure Protection, Európai Program a Kritikus Infrastruktúrák Védelmére
ERNCIP	European Reference Network for Critical Infrastructure Protection (www.erncip-project.jrc.ec.europa.eu), Referencia Hálózat a Kritikus Infrastruktúrák Védelmére
EU JRC	Joint Resource Center (www.ec.europa.eu/jrc/ EU Közös Kutatási Központ
GovCERT	Kormányzati Eseménykezelő Központ
Honvédelmi Korm. rend.	A honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről szóló a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről szóló 359/2015. (XII. 2.) Korm. rendelet
Ibtv.	Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
IKT	infokommunikációs technológiák
IPCC	Intergovernmental Panel on Climate Change (www.ipcc.ch), Éghajlat-változási Kormányközi Testület
ISIS	Iraki és Levantei Iszlám Állam
IT	információs technológiák
IT Korm. rend.	Az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 249/2017. (IX. 5.) Korm. rendelet
Kat.	A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény
Kat. vhr.	A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról szóló 234/2011. (XI. 10.) Korm. rendelet
KIV	kritikus infrastruktúrák védelme
KIV KF	Kritikus Infrastruktúra Védelmi Konzultációs Fórum
KNBSZ	Katonai Nemzetbiztonsági Szolgálat
Lrtv.	Létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény
Lrtv. vhr.	A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet
MAVIR	Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zrt.
MEKH	Magyar Energetikai és Közmű-szabályozási Hivatal
MILcert	Military Computer Emergency Readiness Team, Katonai Eseménykezelő Központ
MNB	Magyar Nemzeti Bank

NATO	North Atlantic Treaty Organisation, Észak-Atlanti Szerződés Szervezete Tagországok: Amerikai Egyesült Államok, Belgium, Bulgária, Cseh Köztársaság, Dánia, Egyesült Királyság, Észtország, Franciaország, Görögország, Hollandia, Izland, Kanada, Lengyelország, Lettország, Litvánia, Luxemburg, Magyarország, Norvégia, Olaszország, Portugália, Románia, Spanyolország, Szlovákia, Szlovénia, Törökország.
NBSZ	Nemzetbiztonsági Szakszolgálat
NCI	National Critical Infrastructure, nemzeti kritikus infrastruktúra
NÉBIH	Nemzeti Élelmiszerlánc-biztonsági Hivatal
NEIH	Nemzeti Elektronikus Információbiztonsági Hatóság
NICC	National Infrastructure Coordinating Center (www.dhs.gov/national-infrastructure-coordinating-center), Nemzeti Infrastruktúra-koordinációs Központ
NIPC	National Infrastructure Protection Center, Nemzeti Infrastruktúra Védelmi Központ (USA)
NIS	Az Európai Parlament és a Tanács 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
NKIV Program	Nemzeti Kritikus Infrastruktúra Védelmi Program
NVSZ	Nemzeti Védelmi Szolgálat
OECD	Organisation for Economic Co-operation and Development (www.oecd.org), Gazdasági Együttműködési és Fejlesztési Szervezet
ORFK	Országos Rendőr-főkapitányság
OSP	Operator Security Plan, üzemeltetői biztonsági terv
Pénzügy Korm. rend.	A pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 330/2015. (XI. 10.) Korm. rendelet
RKR	Rotációs Kikapcsolási Rend
Rendvédelmi Korm. rend	Az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról szóló 512/2013. (XII. 29.) Korm. rendelet
SCEPC	Senior Civil Emergency Planning Committee, NATO Felsőszintű Polgári Veszélyhelyzet Tervezési Bizottsága
SLO	security liaison officer, biztonsági összekötő személy
TEK	Terrorelhárítási Központ
TIBEK	Terrorelhárítási Információs és Bűnügyi Elemző Központ
USA	United States of America, Amerikai Egyesült Államok
ÜBT	üzemeltetői biztonsági terv
Víz ágazati Korm. rend.	A létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről szóló 541/2013. (XII. 30.) Korm. rendelet

Fogalomtár

Azonosítás (Lrtv. vhr.)	Az a folyamat, amely során a lehetséges létfontosságú rendszerelemeket kockázatelemzés, valamint az ágazati és horizontális kritériumok alapján meghatározzák.
Azonosítási jelentés	A kijelölő hatóság részére benyújtandó dokumentum, amely tartalmazza a vizsgált lehetséges létfontosságú rendszerelem megnevezését, a kockázatelemzést, valamint annak eredményét és a nemzeti/európai létfontosságú rendszerelemmé történő kijelölésre irányuló javaslatot, amely alapján a kijelölési eljárás lefolytatható.
Ágazati kritérium (Lrtv.)	Azok a szempontok, az azokhoz tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy eszköz, létesítmény rendszerelemének megzavarása vagy megsemmisítése által kiváltott hatásra vonatkoznak, és amelyek teljesülése esetén az eszköz, létesítmény, rendszer vagy azok része létfontosságú rendszerelemmé jelölhető ki azzal szoros összefüggésben, hogy melyik ágazatba tartozik.
Ágazati javaslattevő hatóság	Az adott ágazatra irányadó kormányrendeletben meghatározott hatóság, amelynek lehetősége van az ágazaton belül fellelhető potenciális kritikus infrastruktúra nemzeti létfontosságú rendszerelemmé történő kijelölésének/kijelölés visszavonásának kezdeményezésére, illetve feladata a kijelölési eljárás során az azonosítási jelentés véleményezése.
Ágazati kijelölő hatóság	Az adott ágazatra irányadó kormányrendeletben meghatározott hatóság, amelynek feladata az azonosítási jelentés alapján döntést hozni egy potenciális kritikus infrastruktúra nemzeti/európai szintű létfontosságú rendszerelemmé történő kijelöléséről.
Biztonsági összekötő személy	Büntetlen előéletű, megfelelő képesítéssel rendelkező, az üzemeltető által alkalmazott személy, akinek elsődleges feladata az üzemeltető és a kijelölési eljárásban részt vevő hatóságok, szakhatóságok közötti kapcsolattartás.
CIPedia©	A Wikipedia mintájára kialakított online közösségi szolgáltatás, amely a kritikus infrastruktúrák védelmére és az ellenálló képesség – rugalmasság kettős követelményéhez kapcsolódó témakörökre (szójegyzék, rendezvények, szervezetek, rövidítések) fókuszál (www.cipedia.eu).
CIMIC	A művelet érdekében végzett koordináció és együttműködés a parancsnok és a polgári oldal között, beleértve a nemzeti és helyi hatóságokat, valamint a nemzetközi, nemzeti kormányzati és nem kormányzati szerveket, ügynökségeket és a lakosságot.
Dominóelv	Az infrastruktúrák kölcsönös függőségéből adódó lehetséges összhatás, amelyet egy esemény vált ki, de láncolatként valamennyi összekapcsolódó infrastruktúrát érinthet.
EGT-állam (Lrtv.)	Az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam.
Európai létfontosságú rendszerelem (Lrtv.)	Az Lrtv. alapján kijelölt olyan létfontosságú rendszerelem, amelynek megzavarása vagy megsemmisítése jelentős hatással lenne – az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve – legalább két EGT-államra.
G-20	A G-20 a világ 19 legnagyobb gazdaságát és az Európai Uniót tömörítő szervezet, amely felöleli a világ bruttó nemzeti összterméken 90 és a világkereskedelem 80 százalékát (tartalmazza az EU belső kereskedelemét is).
Globalizáció	A globalizáció összetett társadalmi és gazdasági folyamat, melynek többek között gazdasági, politikai és kulturális vonatkozásai vannak, és amely egymás után éri el a világ országait.

Horizontális kritérium (Lrtv.)	Azok a szempontok, az azokhoz tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy eszköz, létesítmény rendszerelemének kiesése által kiváltott hatásra vonatkoznak, és amelyek teljesülése esetén – figyelemmel a bekövetkező emberiélet-veszteségekre, az egészségre gyakorolt hatásra, a gazdasági és társadalmi hatásokra, a természetre és az épített környezetre gyakorolt hatásra – az eszköz, létesítmény, rendszer vagy azok része létfontosságú rendszerelemmé jelölhető ki attól függetlenül, hogy mely ágazatba tartozik.
Infrastruktúra	Ember alkotta rendszerek és eljárások hálózata, amelyek szinergikusan együttműködve arra törekszenek, hogy folyamatosan alapvető termékeket és szolgáltatásokat állítsanak elő és terjesszenek. (Cecei–Mórocz 2004)
Interdependencia	Kölcsönös, egymástól való függőség.
Katasztrófa (Kat.)	A szükséghelyzet vagy a veszélyhelyzet kihirdetésére alkalmas, illetőleg a minősített helyzetek kihirdetését el nem érő mértékű olyan állapot vagy helyzet (például természeti, biológiai eredetű, tűz okozta), amely emberek életét, egészségét, anyagi értékeiket, a lakosság alapvető ellátását, a természeti környezetet, a természeti értékeket olyan módon vagy mértékben veszélyezteti, károsítja, hogy a kár megelőzése, elhárítása vagy a következmények felszámolása meghaladja az erre rendelt szervezetek előírt együttműködési rendben történő védekezési lehetőségeit, és különleges intézkedések bevezetését, valamint az önkormányzatok és az állami szervek folyamatos és szigorúan összehangolt együttműködését, illetve nemzetközi segítség igénybevételét igényli.
Kockázatelemzés (Lrtv. vhr.)	Fenyegetettségi és kockázati tényezők vizsgálata a rendszerelemek sebezhetőségének, valamint a megzavarásuk vagy megsemmisítésük által okozott következmények értékelése céljából.
Létfontosságú információs rendszer és létesítmény (Lrtv. vhr.)	A társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek.
Létfontosságú rendszerelem (Lrtv.)	Az Lrtv. 1–3. mellékletben meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.
Létfontosságú rendszerelem védelme (Lrtv.)	A létfontosságú rendszerelem funkciójának, folyamatos működésének és sértetlenségének biztosítását célzó, a fenyegetettség, a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányuló valamennyi tevékenység.
Nemzeti létfontosságú rendszerelem (Lrtv.)	E törvény alapján kijelölt olyan létfontosságú rendszerelem, amelynek megzavarásának vagy megsemmisítésének a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt jelentős hatása lenne Magyarországon.
Ökológiai lábnyom	A társadalomtervezésben használt érték, ami kifejezi, hogy adott technológiai fejlettségi szinten a társadalomnak milyen mennyiségű földre és vízre van szüksége önmaga fenntartásához, illetve a megtermelt hulladék elnyeléséhez. Ez az érték kiszámítható egyes emberekre, csoportokra, régiókra, országokra vagy vállalkozásokra is. A kifejezés William Rees és Mathis Wackernagel kanadai ökológusoktól származik.
Pandémia	Több országra vagy egész kontinensre kiterjedő járvány.
Proliferáció	Jelentése: burjánzás, terjedés; biztonságpolitikai értelmezésben a tömegpusztító fegyverek ellenőrizetlen terjedésére használt kifejezés.

Szubszidiaritás	Célja az EU és az uniós országok megosztott hatásköreibe tartozó területeken történő beavatkozás legmegfelelőbb szintjének meghatározása. Európai, nemzeti vagy helyi szintű fellépést érinthet. Valamennyi esetben az Európai Unió csak akkor és annyiban jár el, amikor és amennyiben hatékonyabban tud fellépni, mint az uniós országok a maguk megfelelő nemzeti vagy helyi szintjén.
Üzemeltető (Lrtv.)	Az a természetes, jogi személy vagy jogi személyiség nélküli szervezet, aki az eszköz, létesítmény, rendszer rendszerelemének tulajdonosa, engedélyese, rendelkezésre jogosultja vagy napi működéséért felelős.
Üzemeltetői biztonsági terv	A létfontosságú rendszerek működése során felmerülő zavar kialakulásának megelőzését, a bekövetkezett esemény elhárítását, következményeinek mérséklését szolgáló intézkedéseket tartalmazó üzemeltetői dokumentáció, amely a kockázatelemzés alapján kialakított eljárásrendek alkalmazásával biztosítja a létfontosságú rendszerek működésének teljes körű személyi, fizikai, adminisztratív és elektronikus védelmét.
Véleménynyilvánító szervek	A kijelölési eljárás során a szakhatóság a horizontális kritériumok vizsgálatába, véleménynyilvánítás céljából bevonja a Nemzeti Adó- és Vámhivatal illetékes szervét, a Rendőrséget, az Alkotmányvédelmi Hivatalt, a Terrorelhárítási Központot, valamint az illetékes kormányhivatalt.

Jogszabályok jegyzéke

EU-jogszabályok

A bizottság közleménye a Tanács és az Európai Parlament részére a létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben. Brüsszel, 2004. 10. 20. COM(2004) 702 végleges;
Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról. Brüsszel, 2005. 11. 17. COM(2005) 576 végleges;
A Bizottság közleménye a létfontosságú infrastruktúrák védelmére vonatkozó európai programról. Brüsszel, 2006. 12. 12. COM(2006) 786 végleges;
A Tanács 2008/114/EK Irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről;
Európai Biztonsági Stratégia 2003, Európai Belbiztonsági Stratégia 2010, Európai Biztonsági Stratégia megvalósításának menetrendje (COM(2015) 185 final, Strasbourg, 2015. 04. 28.;
A kiberbiztonságról és védelemről szóló EP határozat, 2012/2096(INI) 2012. 11. 22;
Az Európai Parlament és a Tanács 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

Fontosabb hazai jogszabályok

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről;
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról;
2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról;
2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről;
2016. évi CL. törvény. az általános közigazgatási rendtartásról;
2012. évi C. törvény a Büntető Törvénykönyvről;
2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról;
2009. évi CLV. törvény a minősített adat védelméről;
2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről;
65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról;
360/2013. (X. 11.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről;
512/2013. (XII. 29.) Korm. rendelet az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról;
540/2013. (XII. 30.) Korm. rendelet a létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről;
541/2013. (XII. 30.) Korm. rendelet a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről;

246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről;
330/2015. (XI. 10.) Korm. rendelet a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről;
359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről;
249/2017. (IX. 5.) Korm. rendelet az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről;
186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről;
187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról;
270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről;
234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról;
223/2014. (IX. 4.) Korm. rendelet a vízügyi igazgatási és a vízügyi, valamint a vízvédelmi hatósági feladatokat ellátó szervek kijelöléséről;
280/2016. (IX. 21.) Korm. rendelet a villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről;
94/2018. (V. 22.) Korm. rendelet a Kormány tagjainak feladat- és hatásköréről;
290/2011. (XII. 22.) Korm. rendelet a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény egyes rendelkezéseinek végrehajtásáról;
531/2017. (XII. 29.) Korm. rendelet az egyes közérdeken alapuló kényszerítő indok alapján eljáró szakhatóságok kijelöléséről;
1249/2010. (XI. 19.) Korm. határozat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról;
1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról;
1139/2013. (III. 21.) kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról;
1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról;
41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről;
62/2011. (XII. 29.) BM rendelet a katasztrófák elleni védekezés egyes szabályairól;

Hatályát vesztett, de fontos jogszabály:

2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról – hatályon kívül helyezve: 2014. 03. 05.

Ágazatok és alágazatok Magyarországon – Lrtv. 1–3. melléklet

ÁGAZAT	ALÁGAZAT
Energia	villamosenergia-rendszer létesítményei (kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek)
	kőolajipar
	földgázipar
Közlekedés	közúti közlekedés
	vasúti közlekedés
	légi közlekedés
	vízi közlekedés
	logisztikai központok
Agrárgazdaság	mezőgazdaság
	élelmiszeripar
	elosztó hálózatok
Egészségügy	aktív fekvőbeteg-ellátás
	mentésirányítás
	egészségügyi tartalékok és vérkészletek
	magas biztonsági szintű biológiai laboratóriumok
	gyógyszer-nagykereskedelem
Társadalombiztosítás	társadalombiztosítási ellátások igénybevételéhez kapcsolódó informatikai rendszerek és nyilvántartások
Pénzügy	pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei
	bank- és hitelintézeti biztonság
	készpénzellátás
Infokommunikációs technológiák	internet-infrastruktúra és internet hozzáférés szolgáltatás
	vezetékes és vezeték nélküli elektronikus hírközlési szolgáltatások, vezetékes és vezeték nélküli hírközlő hálózatok
	rádiós távközlés
	űrtávközlés
	műsorszórás
	postai szolgáltatások
	kormányzati informatikai, elektronikus hálózatok
Víz	ivóvíz-szolgáltatás
	felszíni és felszín alatti vizek minőségének ellenőrzése
	szennyvízelvezetés és -tisztítás
	vízbázisok védelme
	árvízi védművek, gátak
Közbiztonság – Védelem	rendvédelmi szervek infrastruktúrái
Honvédelem	honvédelmi rendszerek és létesítmények

A horizontális kritériumok értelmezése

(Lrtv. vhr. 1. sz. melléklet alapján)

Veszteségek kritériuma:

- *24 óra* leforgása alatt az *áldozatok* száma *meghaladja a 20 főt,* vagy a *súlyos sérültek* száma *legalább 75 fő,* vagy
- *72 óra* leforgása alatt az *áldozatok* száma *meghaladja a 40 főt,* vagy a *súlyos sérültek* száma *legalább 150 fő.*

A kritérium kifejezetten az emberélet vonatkozásában keletkező veszteséget hivatott vizsgálni. A kritérium teljesülésének megállapítását segíti az alábbi skála:

Fokozat	Leírás
1	Nincs áldozat és súlyos sérült
2	Az áldozatok (x), súlyos sérültek (y) száma nem éri el a 10 főt x;y < 10
3	A 24/72 óra leforgása alatt az áldozatok száma (x) a 10/20 főt meghaladja, vagy a súlyos sérültek száma (y) legalább 36/75 fő, de a 4-es szintet nem éri el. 24h esetén 10 < x < 20 vagy 36 < y < 75 72h esetén 20 < x < 40 vagy 75 < y < 150
4	A 24/72 óra leforgása alatt az áldozatok száma a 20/40 főt meghaladja, vagy a súlyos sérültek száma legalább 75/150 fő, de az 5-ös szintet nem éri el. 24h esetén 20 < x vagy 75 < y 72h esetén x > 40 vagy y > 150
5	A 12/36 óra leforgása alatt az áldozatok száma a 40/80 főt meghaladja, vagy a súlyos sérültek száma legalább 150/300 fő. 12h esetén 40 < x vagy 150 < y 36h esetén x > 80 vagy y > 300

Gazdasági hatás kritériuma:

- a gazdasági veszteség mértéke, vagy termékek és szolgáltatások romlásának mértéke,
- a rendszer és létesítmény fizikai sérüléséből, elvesztéséből fakadó közvetlen vagy közvetett károk, amelyek

50 000 fő vonatkozásában meghaladják az *egy főre jutó bruttó nemzeti jövedelem* (GNI) *bármely 30 napos időszakra vetített mértékének 25%-át.*

A kritérium kifejezetten a gazdasági/anyagi veszteség bruttó értékét hivatott vizsgálni. A kritérium teljesülésének megállapítását segíti az alábbi skála:

Fokozat	Leírás
1	A gazdasági hatása nem számottevő.
2	A közvetlen vagy közvetett károk 50 000 fő vonatkozásában az 1 főre eső GNI bármely 30 napos időszakra vetített mértékének (GNI mérték) legfeljebb 15%-át érik el. x < GNI mérték*15%
3	A közvetlen vagy közvetett károk 50 000 fő vonatkozásában, az 1 főre eső GNI bármely 30 napos időszakra vetített mértékének 15%-át elérik, de nem haladják meg annak 25%-át. GNI mérték*15% < x < GNI mérték*25%
4	A közvetlen vagy közvetett károk 50 000 fő vonatkozásában meghaladják az 1 főre eső GNI bármely 30 napos időszakra vetített mértékének 25%-át. x > GNI mérték*25%
5	A közvetlen vagy közvetett károk 50 000 fő vonatkozásában meghaladják az 1 főre eső GNI bármely 30 napos időszakra vetített mértékének 50%-át. x > GNI mérték*50%

Társadalmi hatás kritériuma:

– 300 fő/km^2-nél sűrűbben lakott területen a köznyugalom súlyos megzavarása, beleértve a lakosságot érő káros pszichológiai és közegészségügyi hatásokat is.

A köznyugalom: olyan társadalmi légkör, amelyben a törvényes rend iránti tisztelet, kölcsönös megbecsülés, az állampolgárok jogos érdekeinek elismertsége az uralkodó. A köznyugalmat elsősorban nemzetiségi és vallási előítéletekből, önzésből fakadó antiszociális viselkedési formák zavarják meg. Az e csoportba tartozó bűncselekmények hatása elsősorban a közvéleményben észlelhető nyugtalanság, zavar.

A Büntető Törvénykönyv (2012. évi C. törvény, Btk.) Különös Rész XXXII. fejezete részletesen meghatározza a *köznyugalom elleni bűncselekményeket*:

a) háborús uszítás;
b) közösség elleni izgatás;
c) a nemzetiszocialista vagy kommunista rendszerek bűneinek nyilvános tagadása;
d) nemzeti jelkép megsértése;
e) önkényuralmi jelkép használata;
f) hatósági rendelkezés elleni uszítás;
g) rémhírterjesztés;
h) közveszéllyel fenyegetés;
i) garázdaság;
j) rendbontás.

Az érintett lakott terület népsűrűsége meghatározásakor a Központi Statisztikai Hivatal elérhető legfrissebb adatait kell alapul venni.[17]

Köznyugalom súlyos megzavarása ebben az esetben: olyan esemény vagy eseménysor, amely legalább 72 órán keresztül, a lakosság egészét vagy a lakosság egyes csoportjait (az érintett területen élők legalább 25%-át) olyan mértékben érinti, hogy a lakosság egészsége, élete, tulajdona vagy környezete folyamatos közvetlen veszélynek van kitéve.

[17] www.ksh.hu/Helysegnevtar

A kritérium a lakosság mindennapos életének megzavarására gyakorolt hatásokat vizsgálja. A kritérium teljesülésének megállapítását segíti az alábbi skála:

Fokozat	Leírás
1	A népsűrűség nem éri el a 300 fő/km^2-t, vagy az eseménynek a köznyugalomra nincs hatása.
2	A 300 fő/km^2-nél sűrűbben lakott területen a köznyugalom mérsékelt megzavarása, beleértve a lakosságot érő káros pszichológiai és közegészségügyi hatásokat is. Az adott terület mindenkori lakosságának legfeljebb 10%-át érinti.
3	A 300 fő/km^2-nél sűrűbben lakott területen a köznyugalom oly mértékű megzavarása, (beleértve a lakosságot érő káros pszichológiai és közegészségügyi hatásokat is), amely esetén okszerűen lehet számolni a társadalom viselkedéskultúrájának negatív változásával, de a köznyugalom súlyos megzavarását nem éri el. Az adott terület mindenkori lakosságának legfeljebb 45%-át érinti.
4	A 300 fő/km^2-nél sűrűbben lakott területen a köznyugalom súlyos megzavarása, beleértve a lakosságot érő káros pszichológiai és közegészségügyi hatásokat is.
5	A 300 fő/km^2-nél sűrűbben lakott területen a köznyugalom megszűnése, beleértve a lakosságot érő káros pszichológiai és közegészségügyi hatásokat is.

Politikai hatás kritériuma:

– az állam és intézményei iránti közbizalom megszűnése, valamely állami szerv működésképtelenné válása miatt a lakosság biztonságérzete kritikus szint alá csökken.

Kritikus szint ebben az esetben: a hatályos Btk. Különös Részének XXIV. fejezetében *(Állam Elleni Bűncselekmények)* meghatározott bűncselekmény vagy bűncselekmények elkövetésével kialakuló olyan helyzet, amelynek eredményeként az Alaptörvényben foglaltakon nyugvó társadalmi viszonyok, különösen az állami, önkormányzati szervek működése legalább 72 órára leáll, vagy olyan szint alá csökken, ami a jogszabályokban meghatározott feladatellátás minimális szintjét is lehetetlenné teszi. Ilyen *tényállások:*

a) az alkotmányos rend erőszakos megváltoztatása;
b) az alkotmányos rend elleni szervezkedés;
c) lázadás;
d) rombolás;
e) hazaárulás;
f) hűtlenség;
g) az ellenség támogatása;
h) kémkedés;
i) kémkedés az Európai Unió intézményei ellen;
j) a szövetséges fegyveres erő ellen elkövetett kémkedés;
k) állam elleni bűncselekmény feljelentésének elmulasztása.

A kritérium a lakosság biztonságérzetére gyakorolt hatásokat az államba vetett bizalom vonatkozásában vizsgálja. A kritérium teljesülésének megállapítását segíti az alábbi skála, amelyben a kritikus szint jelentése: a közrend, közbiztonság sérelmének súlyos és közvet-

len veszélye áll fenn, de a lakosság élet- és vagyonbiztonságát jelentős mértékben még nem veszélyezteti.

Fokozat	Leírás
1	A politikai hatás nem veszélyezteti a lakosság biztonságérzetét.
2	Az állam és intézményei iránti közbizalom megszűnése, valamely állami szerv működésképtelenné válása miatt a lakosság biztonságérzete meginog.
3	Az állam és intézményei iránti közbizalom megszűnése, valamely állami szerv működésképtelenné válása miatt a lakosság biztonságérzete normál szint alá csökken, de nem éri el a kritikus szintet.
4	Az állam és intézményei iránti közbizalom megszűnése, valamely állami szerv működésképtelenné válása miatt a lakosság biztonságérzete kritikus szint alá csökken.
5	Az állam és intézményei iránti közbizalom hiánya, valamely állami szerv működésképtelenné válása miatt a lakosság biztonságérzete megszűnik.

Környezeti hatás kritériuma:

– az esemény vagy folyamat, amely miatt a természeti vagy épített környezetben, különösen:
  • az infrastruktúrában bekövetkező sérülés vagy zavar az épített vagy természetes környezet oly mértékű rongálódását idézi elő, amelynek következtében 10 000 fő kimenekítése vagy kitelepítése válik szükségessé, vagy legalább 100 km^2 nagyságú terület tartósan szennyeződik, vagy a felszín alatti vizek, vagy azok természetes víztartó képződményei, a folyóvizek és természetes tavak, valamint ezek medre vagy élővilága szenved tartós károsodást;
  • az ország tájegységeiben, kiemelkedő földrajzi területeiben visszafordíthatatlan negatív változás következik be.

A kritérium a lakosság környezetére gyakorolt hatásokat vizsgálja. A kritérium teljesülésének megállapítását segíti az alábbi skála:

Fokozat	Leírás
1	Nincs környezeti hatása.
2	A környezeti hatás oly mértékű rongálódáshoz vezet, hogy legalább 1 000 ember kimenekítése vagy kitelepítése válik szükségessé, legfeljebb 10 km^2 nagyságú terület tartósan szennyeződik, vagy a felszín alatti vizek, vagy azok természetes víztartó képződményei, vagy a felszíni vizek, azok medre vagy élővilága szenved tartós károsodást, vagy az ország tájegységeiben, kiemelkedő földrajzi területeiben (például: természetvédelmi területek) visszafordíthatatlan negatív változás következik be.
3	A környezeti hatás oly mértékű rongálódáshoz vezet, hogy legalább 5 000, de kevesebb mint 10 000 ember kimenekítése vagy kitelepítése válik szükségessé, 100 km^2-t el nem érő nagyságú terület tartósan szennyeződik, vagy a felszín alatti vizek, vagy azok természetes víztartó képződményei, vagy a felszíni vizek, azok medre vagy élővilága szenved tartós károsodást, vagy az ország tájegységeiben, kiemelkedő földrajzi területeiben (például: természetvédelmi területek) visszafordíthatatlan negatív változás következik be.
4	A környezeti hatás oly mértékű rongálódáshoz vezet, hogy 10 000 ember kimenekítése vagy kitelepítése válik szükségessé, legalább 100 km^2 nagyságú terület tartósan szennyeződik, vagy a felszín alatti vizek, vagy azok természetes víztartó képződményei, vagy a felszíni vizek, azok medre vagy élővilága szenved tartós károsodást, vagy az ország tájegységeiben, kiemelkedő földrajzi területeiben (például: természetvédelmi területek) visszafordíthatatlan negatív változás következik be.
5	A környezeti hatás oly mértékű rongálódáshoz vezet, hogy 100 000 ember kimenekítése vagy kitelepítése válik szükségessé, legalább 500 km^2 nagyságú terület tartósan szennyeződik, vagy a felszín alatti vizek, vagy azok természetes víztartó képződményei, vagy a felszíni vizek, azok medre vagy élővilága szenved tartós károsodást, vagy az ország tájegységeiben, kiemelkedő földrajzi területeiben (például: természetvédelmi területek) visszafordíthatatlan negatív változás következik be.

Az üzemeltetői biztonsági terv felépítése

(Lrtv. vhr. 2. sz. melléklet alapján)

I. Tartalmi követelmények

1. Általános bemutatás

Az üzemeltető megadja a kijelölt rendszerelem adatait:

a) megnevezése;
b) üzemeltető neve, székhelye, lakcíme, levelezési címe;
c) cégjegyzékszám vagy egyéni vállalkozói nyilvántartási szám;
d) adóazonosító szám;
e) képviselő neve, telefon- és telefaxszám, e-mail-cím;
f) pontos adat hiányában a kijelölt rendszerelem elhelyezkedésére vonatkozó más azonosító adat és földrajzi koordináta;
g) biztonsági összekötő neve, elérhetőségei.

Az üzemeltető általánosságban bemutatja a szervezetét, tevékenységét, irányítási rendszerét, a kijelölt rendszerelem védelmével kapcsolatos fő célkitűzéseit, a horizontális és ágazati kritériumok teljesülését, indokoltságát:

a) szervezeti struktúra és üzemvezetés;
b) személyzet (saját munkavállalók, külső, szerződéses munkavállalók);
c) kijelölt rendszerelem tevékenységének/működésének általános bemutatása, az elvárt, normális működés paraméterei;
d) kijelölt rendszerelem elemeinek azonosítása és értékelése a teljesült ágazati és horizontális kritériumok alapján;
e) belső audit és vezetőségi átvizsgálás;
f) a változtatások kezelése és annak követése.

2. A kijelölt rendszerelemek környezetének bemutatása

a) a környező területek jellemzése;
b) a működést biztosító közműszolgáltatások, szolgáltatók bemutatása:
   ba) elektromos áramellátás biztosítása,
   bb) vezetékes gázellátás biztosítása,
   bc) közüzemi ivóvízellátás, közüzemi szennyvízelvezetés és -tisztítás biztosítása,
   bd) infokommunikációs hálózati ellátás,
   be) egyéb;
c) a kijelölt rendszerelem környezetében található, a működésére befolyással bíró veszélyes üzemek, gyárak, erőművek megnevezése, címe, tevékenységi köre;
d) a természeti környezetre vonatkozó legfontosabb információk:
   da) a területre jellemző, a kijelölt rendszerelem sérülését eredményező és a következmények alakulására hatást gyakorló meteorológiai jellemzők,
   db) a helyszínt jellemző, a kijelölt rendszerelem biztonságos tevékenységére, üzemeltetésére, működésére hatást gyakorló legfontosabb geológiai és hidrológiai jellemzők.

3. A kijelölt rendszerelem bemutatása

Az üzemeltető ismerteti a kijelölt rendszerelem felépítését, elemeit, azok részletes tevékenységi körét, továbbá ezen részekről mellékel:

a) egy méretarányos ábrát,
b) helyszínrajzot, valamint
c) hozzátartozó útmutatót, magyarázatot.

A bemutatás kiemelten tartalmazza a kijelölt rendszerelem működését releváns módon befolyásoló informatikai rendszerek, eszközök, hálózatok ismertetését és a működésben betöltött szerepük leírását.

A kijelölt rendszerelem felépítésének, elemeinek, részletes tevékenységének, termelési, működési folyamatainak bemutatását az alábbi szempontok alapján kell elvégezni:

a) a kijelölt rendszerelem felépítése, elemei (helyszínrajz, amely bemutatja az elemeket, és vázlatosan feltünteti a létfontosságú elemet a hozzá tartozó útmutatóval, magyarázattal);
b) kiszolgáló infrastruktúra (közműhálózatok, technikai berendezések, szolgáltatást végző partnerek);
c) részletes tevékenység, a tevékenységekre vonatkozó legfontosabb technológiai és karbantartási folyamatok, műveletek;
d) tartalék rendszerelemek;
e) a lehetséges veszélyt jelentő anyagok, berendezések megjelölése, mennyisége, tárolási adatai;
f) a működésben releváns informatikai rendszerek, alkalmazások, hálózatok, azok funkciója;
g) a normál működési rend során a kijelölt rendszerelem működését garantáló eszközök, berendezések, technológiai és karbantartási folyamatok, műveletek menete, naplózása, ütemezése;
h) belső és külső tájékoztatási rendszerek;
i) felügyeleti és biztonsági szervezetek, eszközrendszerük, működésük (biztonsági szolgálat, elsősegélynyújtó és mentőszervezetek, munka-, tűz- és környezetvédelmi szolgálat, műszaki biztonsági szolgálat, katasztrófaelhárítási szervezet, távfelügyeleti és monitoringhálózatok, laboratóriumi hálózat, beléptető és az idegen behatolást érzékelő rendszerek stb.).

4. Kockázatok azonosítása, értékelése

Az üzemeltető azonosítja és értékeli a kijelölt rendszerelemmel összefüggő kockázatokat a következők szerint:

– kockázati lista [milyen releváns belső, külső kockázatok veszélyeztetik a kijelölt rendszerelem működését: gazdasági, technológiai, infrastrukturális (közműszolgáltatások kiesése, belső infrastruktúrák kiesése), humán, fizikai, információs technológiai, természeti, civilizációs katasztrófák, terrorizmus, egészségügyi, környezeti, társadalmi, logikai, földrajzi stb.];
– a kijelölt rendszerelem kölcsönösen függő (interdependens) kapcsolódásai és az azokból adódó kockázatok felmérése (a kijelölt rendszerelem kiesése milyen más ágazatokra, szervezetekre, személyekre van hatással);
– a kockázatok valószínűsíthető okainak feltárása, a bekövetkezéskor prognosztizálható negatív hatások meghatározása;
– a felmerült kockázatok értékelése a bekövetkezési valószínűség és az okozott káros hatások meghatározásával.

5. Kockázatkezelés

Az üzemeltető meghatározza a szükséges beavatkozás szintjeit a kockázati értékek szerint. Az üzemeltető bemutatja a feltárt kockázatok kezelésére vonatkozó szabványok, intézkedések, belső utasítások, eljárások, szabályok rendszerét, szükség szerint röviden ismerteti tartalmát.

6. A kijelölt rendszerelem védelmének eszközrendszere

Az üzemeltető megjelöli azokat a biztonsági intézkedéseket, amelyek kialakítása és működtetése biztosítja a kijelölt rendszerelem védelmét, továbbá meghatározza azokat az ideiglenes intézkedéseket, amelyeket a rendkívüli esemény okozta veszélyhelyzeti működés során a különböző kockázati és veszélyszinteknek megfelelően foganatosít. Ezen belül meghatározza a veszélyhelyzeti működés, rendkívüli esemény kritériumait (a normális működéssel történő összevetésben).

Rendkívüli eseménynek tekintendő az olyan külső vagy belső behatás, amely a kijelölt rendszerelem rendeltetésszerű működését jelentős mértékben veszélyezteti, akadályozza. Jelentősnek minősül az az esemény, melyet az üzemeltető saját erőforrásaival, külső segítség nélkül nem képes kezelni, elhárítani.

Az üzemeltető bemutatja a kijelölt rendszerelem elemeinek és egészének védelmére rendszeresített felszereléseket és a vezetéshez, a döntés-előkészítéshez szükséges infrastruktúrát a következők szerint:

- a veszélyhelyzeti vezetési létesítmények;
- a vezetői állomány veszélyhelyzeti értesítésének eszközrendszere;
- a dolgozók veszélyhelyzeti riasztásának eszközrendszere;
- a veszélyhelyzeti híradás eszközei és rendszerei;
- a veszélyhelyzet értékelését és a döntések előkészítését segítő informatikai rendszerek;
- a veszélyhelyzet kezelésének eljárásrendje;
- a riasztást, a védekezést és a következmények csökkentését végző végrehajtó szervezetek rendszeresített egyéni védőeszközei és szaktechnikai eszközei;
- a védekezésbe bevonható (nem közvetlenül erre a célra létrehozott) belső és a külső erők és eszközök;
- a kijelölt rendszerelem kiesése következtében alkalmazható vagy rendelkezésre álló alternatív megoldások;
- rendkívüli eseménykor értesítendők köre.

7. Az üzemeltetői biztonsági terv elkészítésébe bevont személyek, szervezetek megjelölése

Az üzemeltető megjelöli az üzemeltetői biztonsági terv elkészítésébe bevont személyeket, szervezeteket.

II. Formai követelmények

Az üzemeltetői biztonsági tervet írásban kell elkészíteni, és a nyilvántartó, valamint a kijelölő hatóság részére egy-egy eredeti – az üzemeltető és a biztonsági összekötő személy által aláírt – példányban papíralapon, továbbá elektronikus adathordozón is be kell nyújtani. A térképeket, a rajtuk szereplő méretaránynak megfelelően, nyomtatott formában is be lehet nyújtani. A térképvázlat vagy helyszínrajz tartalmazza a kijelölt rendszerelem egészét, és olyan méretarányú legyen, amely a megfelelő eligazodást biztosítja.

Vákát oldal

A Dialóg Campus Kiadó a Nemzeti Közszolgálati Egyetem könyvkiadója.

Nordex Nonprofit Kft. – Dialóg Campus Kiadó
www.dialogcampus.hu
www.uni-nke.hu
1083 Budapest, Ludovika tér 2
Telefon: (30) 426 6116
E-mail: kiado@uni-nke.hu

A kiadásért felel: Petró Ildikó ügyvezető
Felelős szerkesztő: Inzsöl Kata
Olvasószerkesztő: Szabó Ilse
Tördelőszerkesztő: Fehér Angéla
Nyomdai kivitelezés: Nordex Nonprofit Kft.

ISBN 978-615-5920-36-3 (nyomtatott)
ISBN 978-615-5945-28-1 (PDF)
ISBN978-615-5945-29-8 (EPUB)

A 21. század új típusú biztonságpolitikai kihívásokat hozott, amelyek jelentős mértékben befolyásolni képesek a mindennapi élet gördülékenységét, az államapparátus működőképességét, valamint a gazdasági mechanizmusok folyamatosságát biztosító kritikus infrastruktúrák rendelkezésre állását. Kiemelt szerepe van mindennek a védelmi tervezésben, a biztonságpolitikai irányvonalakban nemzetközi és hazai szinten egyaránt.

Jelen jegyzetben a szerzők az infrastruktúra kialakulásától egészen a létfontosságú rendszerek és rendszerelemek információbiztonsági vetületének bemutatásáig teljes körű képet adnak arról, hogy hazánkban milyen formában valósul meg az ehhez kapcsolódó, lakosságot veszélyeztető kockázatok csökkentése, hogyan működnek a hatóságok közötti és az üzemeltetőkkel kialakított együttműködési platformok, illetve milyen szerepe van mindebben a tudatos felkészülésnek, a megelőző szemléletnek és a rendkívüli események eredményes felszámolásán alapuló tapasztalatoknak.