

PhD értekezés (tervezet)

Bakos Tamás alezredes

- 2026 -

**NEMZETI KÖZSZOLGÁLATI EGYETEM
KATONAI MŰSZAKI DOKTORI ISKOLA**

Bakos Tamás

**Kritikus szervezetek és kritikus infrastruktúrák
rezilienciájának fejlesztése**

Doktori (PhD) értekezés

Témavezető: Dr. Kovács Ferenc PhD

Budapest, 2026.

TARTALOM

BEVEZETÉS.....	6
AZ ÉRTEKEZÉSBEN ALKALMAZOTT TERMINOLÓGIA.....	7
A TÉMA AKTUALITÁSA, A TÉMAVÁLASZTÁS INDOKLÁSA	7
TUDOMÁNYOS PROBLÉMA	9
KUTATÓI HIPOTÉZISEK, A KUTATÁS FŐBB CÉLKITŰZÉSEI	10
KUTATÁSI MÓDSZEREK.....	12
AZ ÉRTEKEZÉS SZERKEZETI FELÉPÍTÉSE.....	13
SZAKIRODALMI ÁTTEKINTÉS.....	14
KRITIKUS SZERVEZETEK – HAZAI PUBLIKÁCIÓK	14
KRITIKUS SZERVEZETEK – KÜLFÖLDI PUBLIKÁCIÓK	17
OBJEKTUMVÉDELEM – HAZAI PUBLIKÁCIÓK.....	18
1. FEJEZET	21
A KRITIKUS SZERVEZETEK ÉS INFRASTRUKTÚRÁK AZONOSÍTÁSÁNAK, KIJELÖLÉSÉNEK ÉS REZILIENCIÁJÁNAK SZABÁLYOZÓ RENDSZERE.....	21
1.1. AZ EURÓPAI UNIÓ KRITIKUS INFRASTRUKTÚRÁK VÉDELMEVEL KAPCSOLATOS FŐBB LÉPÉSEI ÉS DOKUMENTUMAI	21
1.1.1. Az Európai Unió korábbi szabályzói.....	21
1.1.2. Az Európai Unió hatályos szabályzói	29
1.2. MAGYARORSZÁG KRITIKUS INFRASTRUKTÚRÁK VÉDELMEVEL KAPCSOLATOS FŐBB LÉPÉSEI ÉS DOKUMENTUMAI	33
1.2.1. Magyarország korábbi szabályzói.....	34
1.2.2. Magyarország jelenleg hatályos szabályzói.....	43
1.3. ÖSSZEFOGLALÓ TÁBLÁZAT ÉS RÉSZKÖVETKEZTETÉSEK	54
2. FEJEZET A KRITIKUS SZERVEZETEK ÉS INFRASTRUKTÚRÁK AZONOSÍTÁSI ÉS KIJELÖLÉSI ELJÁRÁSÁNAK FOLYAMATA.....	60
2.1. A KRITIKUS ÉS JELENTŐS SZERVEZETEK ÉS INFRASTRUKTÚRÁK AZONOSÍTÁSÁNAK ÉS KIJELÖLÉSÉNEK RÉSZTVEVŐI.....	60
2.1.1. Üzemeltető/Tulajdonos/Felelős.....	61
2.1.2. Kijelölő hatóságok	62
2.1.3. Nyilvántartó hatóság	63
2.1.4. Ágazati szakhatóságok.....	64
2.1.5. Ellenőrzésbe bevont szervek	67
2.1.6. Ellenálló képességért felelős vezető.....	68
2.1.7. Szakmai tanácsadó szervezetek	70
2.2. A KRITIKUS ÉS JELENTŐS SZERVEZETEK ÉS INFRASTRUKTÚRÁK AZONOSÍTÁSÁNAK ÉS KIJELÖLÉSÉNEK ELVI FOLYAMATA	71

2.2.1. Kritikus és jelentős szervezetek, infrastruktúrák azonosítása és kijelölése	71
2.2.2. Kijelölt kritikus szervezetek feladatai	74
2.3. ELLENÁLLÓ KÉPESSÉGI TERV (EKT)	75
2.3.1. Az EKT felépítése	76
2.3.2. EKT kapcsolódó mellékletei, okmányai	79
2.4. KRITÉRIUMOKRA ÉPÜLŐ KOCKÁZATELEMZÉS.....	81
2.4.1. Az Ellenálló Képességi Mátrix (EKM)	82
2.4.2. Kockázatazonosítás és kockázatelemzés további lehetséges módszerei.....	85
2.4.3. Kockázatelemzés eredményeinek ágazati és horizontális kritériumokra épülő kezelése...	92
2.5. AZ INTERDEPENDENCIA VIZSGÁLAT	94
2.5.1. Az interdependencia dimenziói.....	94
2.5.2. Az interdependencia vizsgálatának lépései.....	100
2.6. RÉSZKÖVETKEZTETÉSEK.....	104
3. FEJEZET A KRITIKUS SZERVEZETEK ÉS INFRASTRUKTÚRÁK FIZIKAI VÉDELME	107
3.1. LÉTESÍTMÉNYEK FIZIKAI VÉDELMÉNEK ELVEI.....	107
3.1.1. A védelem fogalma.....	107
3.1.2. Létesítmények megközelíthetősége.....	109
3.1.3. Kritikus elemek létesítményeinek védelme	122
3.1.4. Élőerős őrzés-védelem	128
3.1.5. Átfogó védelem	130
3.1.6. Relatív védelem	133
3.2. LÉTESÍTMÉNY FIZIKAI VÉDELMÉNEK TERVE	134
3.2.1. Fizikai Védelmi Terv kialakítása, felépítése	135
3.2.2. Kapcsolódó védelmi tervek	142
3.3. RÉSZKÖVETKEZTETÉSEK.....	144
4. FEJEZET KRITIKUS SZERVEZETEK ÉS INFRASTRUKTÚRÁK REZILIENCIÁJÁNAK FEJLESZTÉSI LEHETŐSÉGEI.....	146
4.1. KRITIKUS SZERVEZETEK DOKUMENTÁCIÓ HIERARCHIÁJA.....	147
4.1.1. Kritikus szervezetek dokumentáció hierarchiájának kialakítása	147
4.1.2. Dokumentációk felülvizsgálata, fejlesztése.....	149
Dokumentáció hierarchia hatása a védelmi képességekre	150
4.2. KRITIKUS SZERVEZETEK SZEMÉLYI ÁLLOMÁNYÁNAK FELKÉSZÍTÉSE.....	151
4.2.1. Felkészítés célja, rendszere, alapelvei.....	152
4.2.2. Kritikus szervezetek személyi állománya felkészítésének jelenlegi helyzete.....	156
4.2.3. A kritikus szervezetek ellenálló képességével kapcsolatos belső képzés.....	160
4.3. KIJELÖLT KRITIKUS SZERVEZET BELSŐ FELKÉSZÍTÉSÉNEK ELLENŐRZÉSE	168

4.3.1. Szervezeti belső felkészítés vezetői szintű ellenőrzésének metodikája	169
4.4. RÉSZKÖVETKEZTETÉSEK.....	174
5. ÖSSZEGZÉS.....	176
ÚJ TUDOMÁNYOS EREDMÉNYEK.....	181
AJÁNLÁSOK, KUTATÁSI EREDMÉNYEK ALKALMAZÁSI LEHETŐSÉGEI	181
6. ALKALMAZOTT RÖVIDÍTÉSEK.....	183
7. ÁBRJEGYZÉK.....	184
8. FELHASZNÁLT IRODALOM	185
9. SZERZŐ PUBLIKÁCIÓS JEGYZÉKE	192
MELLÉKLETEK.....	194
1. SZÁMÚ MELLÉKLET.....	195
A magyarországi kritikus infrastruktúrákkal kapcsolatos korábbi, hatálytalan jogszabályok részletes összefoglalója	195
2. SZÁMÚ MELLÉKLET.....	223
Képzési program a kritikus szervezet fizikai védelmének oktatásához (MINTA)	223
3. SZÁMÚ MELLÉKLET.....	227
Kohéziós táblázat.....	227

BEVEZETÉS

„Bármely egyszerű probléma megoldhatatlanná fejleszthető, ha eleget töprengünk rajta.”

Woody Allen

Az infrastruktúra fogalmára számos meghatározást találhatunk, melyek több szempontból közelítik meg a fogalmat, de mindegyikük valamilyen műszaki tartalomként tekint rá.

Bakos Ferenc által szerkesztett Idegen szavak és kifejezések szótárában az infrastruktúra *„a gazdaság működésének üzemén kívüli előfeltételeit biztosító álló- és forgóeszközök; a lakásállomány és a legkülönbözőbb szolgáltatások (művelődésügy, közlekedés, közművek, hírközlés, egészségügy, kereskedelem stb.) állóeszközei, illetve ezek hálózataként”*¹ szerepel.

Dr. Kovács Ferenc munkáiban és előadásaiban pedig így fogalmaz: *„az infrastruktúra a termeléshez és a lakosság ellátásához kapcsolódó azon eszközök, intézmények és szolgáltatások összessége, amelyek nem részei közvetlenül a termelési folyamatnak, de annak nélkülözhetetlen feltételei”*².

A meghatározások rávilágítanak arra, hogy a civilizációk és az őket kiszolgáló infrastruktúrák milyen szoros kapcsolatban állnak egymással. Egy civilizáció fejlődése szorosan összefügg és nagyban függ az őt kiszolgáló infrastruktúra fejlődésével. Napjaink modern társadalma már olyan szorosan kapcsolódik a kiszolgáló infrastruktúrához, hogy egy komolyabb kiesést, szolgáltatás vagy eszköz hibát nehezen tud tolerálni, vagyis nincs felkészülve arra, hogy teljes vagy részleges infrastruktúra nélkül működjön.

Az a tény már régóta ismert, hogy az infrastruktúrák bizonyos pontjaira mért nagyon kis beavatkozással, nagy károkat lehet okozni a fejlett társadalmak infrastruktúráiban, melyek hálózati jellegüknél fogva további komoly, széles körű katasztrófához is vezethetnek. A filmiparban már külön kategóriát képeznek a *„katasztrófa filmek”*, mégis kormányzati szinten először csak az 1990-es években, az Amerikai Egyesült Államokban jelent meg az igény arra, hogy a fontos, kiemelt, kritikus rendszereket és elemeiket, hálózatokat, infrastruktúrákat elemezzék veszélyeztetettségi szempontból is.

¹ BAKOS Ferenc (szerk.) (1978): *Idegen szavak és kifejezések szótára* – Budapest, Akadémiai Kiadó.

² KOVÁCS Ferenc (2014): *A kritikus infrastruktúra védelme I.* – Budapest, KMDI PowerPoint előadás.

AZ ÉRTEKEZÉSBEN ALKALMAZOTT TERMINOLÓGIA

A nemzetközi használatban, mind a jogi, mind a szakmai, illetve a magyarázó szövegekben a „*critical infrastructure*” terminológia az általánosan elterjedt.

Magyarországon a „*kritikus infrastruktúra*”, mint fogalom az elmúlt évtizedben jelent meg a szakmai életben. Az Európai Unió hivatalos kiadványainak magyar nyelvű fordításai a „*létfontosságú infrastruktúra*” kifejezést használták, melyet az abban az időben készült több szakmai anyag is átvett. Az elmúlt 20 évben fogalomköre bővült és kialakításra kerültek a jogszabályi alapjai, melyekben „*létfontosságú rendszerekként*”, illetve azok részeit „*létfontosságú rendszerelemekként*” definiálták. A jelenleg hatályos jogszabályok az alapvető szolgáltatást nyújtó szervezeteket „*kritikus szervezetekként*” definiálják, a „*kritikus infrastruktúra*” kifejezést pedig ezen szervezetek eszközeként határozzák meg.

Értekezésem első fejezetében következetesen azt a terminológiát fogom alkalmazni, melyet az adott fejezetben tárgyalt jogszabály vagy szakmai szöveg eredetileg is használt. A további fejezetekben a törvényben megadott fogalomra építve, az ott meghatározott terminológiát használom.

A TÉMA AKTUALITÁSA, A TÉMAVÁLASZTÁS INDOKLÁSA

A modern társadalmak infrastruktúráról való függése és az infrastruktúrák sebezhetősége rámutat arra, hogy a társadalmak napi életéhez szükséges szolgáltatások, eszközök, módszerek védelmével kiemelten kell foglalkozni. Ez a terület az elmúlt 25 évben valóban kiemelt figyelmet kapott, megkezdődtek a kutatások, vizsgálatok a témában és a törvényhozók megalkották a szükséges alapszabályzókat.

Ha áttekintjük a nemzetközi és hazai jogszabályok által előírt feladatokat, és figyelembe vesszük a gyorsan változó biztonsági környezetet és technológiai fejlődést, könnyen belátható, hogy a kitűzött cél elérése, vagyis a kijelölt kritikus infrastruktúrák hatékony védelmének kialakítása még igen távoli jövőben valósulhat meg.

Az Európai Unió olyan irányelvet³ adott ki, mely a kritikus infrastruktúrák védelmének elsődleges és végső felelősségét a tagállamokra és az infrastruktúrák

³ Az Európai Unió Tanácsa. A Tanács 2008/114/EK irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. Brüsszel, 23.12.2008

tulajdonosaira/üzemeltetőire terheli. Cserében viszont, szinte szabad kezét ad a tagországoknak a nemzeti kritikus infrastruktúra védelemi programok kidolgozásában.

Fentiek alapján hazánkban már 2004-ben megkezdődött a kutatói munka, mely alapján, a Gazdasági és Közlekedési Minisztérium felkérésére 2005-ben elkészült „Az infrastruktúra kritikus elemeinek felmérése, védelmének és helyreállításának megszervezésére vonatkozó intézkedési javaslatok kidolgozása” c. tanulmány⁴, majd erre alapozva, több szakterület bevonásával a 2008-ban kiadott nemzeti „Zöld Könyv”⁵. Az európai és nemzeti irányelvek megjelenése, konzultációk és a több éves szakmai munka eredményeképpen 2012. november 12-én a Parlament megszavazta a létfontosságú rendszerek védelméről szóló törvényt⁶ (a továbbiakban: Lrtv.) és 2013-ban a végrehajtásához kapcsolódó kormányrendeletet⁷ (a továbbiakban: Lrtv.vr.). A törvény pontosította az alapfogalmakat, és meghatározza a nemzeti, illetve az európai létfontosságú rendszerelemekkel kapcsolatos kijelölés vagy visszavonás folyamatát és megadta azokat az ágazatokat, melyek szakterülete alá be kell sorolni egy adott eszközt, létesítményt vagy rendszerelemet.

2022. decemberében az Európai Unió új irányelvet⁸ adott ki a kritikus szervezetek rezilienciájáról, mely egyben hatályon kívül helyezte a korábbi tanácsi irányelvet. Az új irányelv megjelenése szükségessé tette a magyar jogszabályok modernizálását is, mely alapján megjelent a jelenleg hatályos, kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény (a továbbiakban: Kszetv.), illetve a törvény végrehajtásáról szóló 474/2024. (XII. 31.) Korm. rendelet (a továbbiakban: Kszetv.vr.), a korábbi Lrtv., Lrtv.vr., valamint a kapcsolódó ágazati kormányrendeletek pedig hatályukat veszítették.

A szabályozás az elmúlt 20 évben többször módosult, de közös bennük, hogy a kritikus szervezetekkel kapcsolatos teljes folyamat több résztvevős és a legnagyobb felelősség az adott szervezet vagy infrastruktúra üzemeltetőjére hárul. Az üzemeltetett szervezet, rendszer, létesítmény, infrastruktúra kritikusságának megállapítása, a folyamat elindítása, a védelmi intézkedések, fejlesztések megtervezése, végrehajtása és költségei is az üzemeltetőt terhelik.

⁴ KOVÁCS Ferenc (2005): *Az infrastruktúra kritikus elemeinek felmérése, védelmének és helyreállításának megszervezésére vonatkozó intézkedési javaslatok*. Gazdasági és Közlekedési Minisztérium (GKM), Budapest.

⁵ 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.

⁶ 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
⁷ 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

⁸ A Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről.

A szakterületen jártas szakemberek és a megfelelő jogosultságokkal rendelkező különböző hatóságok minden segítséget megadnak az üzemeltetők részére, a folyamat végrehajtásának minden fázisában részt is vesznek, mégis a kritikus szervezetté történő kijelölés és a kijelölt rendszerelemek valós védelmének kialakítása nagyon nehézkesen, lassan zajlik. A nehézségek oka a törvényi szabályozás üzemeltetők és a hatóságok szerinti eltérő értelmezése, a kritikusság nagyon szerteágazó, több esetben sok szakterületet érintő vizsgálatának nehézségei, valamint az ágazatok közötti, még feltáratlan interdependencia, vagyis függőségi viszony igen bonyolult hálója. Előzőkből és napjaink biztonsági környezetének ismeretében jól látható, hogy a társadalmak biztonságos működéséhez elengedhetetlenül szükséges a kapcsolódó infrastruktúrák megfelelő védelmének mielőbbi kialakítása. Napjaink geopolitikai eseményei a társadalmat – a kapcsolódó infrastruktúrán keresztül – egyre sebezhetőbbé teszik, így a *témához kapcsolódó infrastrukturális, védelmi kutatások, fejlesztések aktualitása megkérdőjelezhetetlen.*

A különböző létesítmények, rendszerek, eszközök magasabb szintű védelmének kialakítása a katonai szakterületek minden ágazatában alapfeladatként jelenik meg. A katonai műszaki szakterületen pedig kifejezetten fő feladatként jelentkeznek a láthatósággal, rejtéssel, megközelíthetőséggel, fizikai védelemmel kapcsolatos elvek, módszerek, eszközök. Műszaki katonaként és kiképzési szakemberként nagyobb rálátásom van katonai műszaki szakterületre, mely komoly inspirációt adott arra, hogy megvizsgáljam a katonai védelmi eljárások alkalmazhatóságát a „polgári élet” viszonyai között. Természetesen azonos módon nem alkalmazhatóak a katonai elvek, módszerek, de azokat alapul véve könnyebben ki lehet dolgozni a társadalmat kiszolgáló infrastruktúrák védelmét, műszaki megoldásait, módszereket, hatékonyabbá lehet tenni a védelmi eszközök alkalmazását, optimalizálva azokat a szükséges és megfelelő védelmi szintre.

TUDOMÁNYOS PROBLÉMA

A kutatás során megállapítottam, hogy a kritikus szervezetek és infrastruktúrák azonosítására, kijelölésére és védelmére vonatkozó jelenlegi szabályozási és gyakorlati rendszerek bár fejlett jogi keretek között működnek, végrehajtásuk mégsem tekinthető egységesnek és kellően hatékonyak. A nemzeti szabályozás meghatározza ugyan a kijelölési és védelmi folyamatok általános kereteit, azonban a gyakorlati végrehajtáshoz szükséges módszertani támogatás hiányos, amely a jogszabályok eltérő alkalmazását és az egyes szervezetek közötti jelentős végrehajtási különbségeket eredményezi.

A problémát tovább erősíti, hogy a jelenleg alkalmazott szabályzók, minták és eljárások nem vizsgálják kellő mélységben a kritikus szervezetek közötti, illetve az ágazatokon átívelő interdependenciát, így nem alkalmasak a komplex, többszintű függőségi rendszerek megfelelő elemzésére. A kölcsönös kapcsolati rendszerek összetettek és több jellemzővel bírnak. Az interdependencia vizsgálatának problémaköre abból ered, hogy ezen jellemzők feltárása eddig még nem történt meg és az elkülönített jellemzők elemzésére jelenleg nem áll rendelkezésre egységes, standardizált módszertan. Az ágazaton belüli és ágazatok közötti kölcsönhatások mélyebb elemzésének hiánya korlátozza a valós kockázatok feltárását, valamint akadályozza a rendszerszintű reziliencia kialakítását.

A jogszabályok szervezetenként eltérő értelmezése és a gyakorlati, módszertani támogatás hiánya a kritikus szervezetek védelmének eltérő színvonalában is megmutatkozhat. A fizikai védelem kialakítása számos esetben a szervezetek humán és anyagi erőforrásaitól függ, amelynek következtében a védelmi intézkedések gyakorlati megvalósítása nem minden esetben éri el a szükséges biztonsági szintet. A problémát fokozza, hogy a fizikai védelem tervezése sok esetben nem integrált módon történik, így a rendelkezésre álló erőforrások felhasználása sem tekinthető optimálisnak.

A kutatásaim és személyes tapasztalataim alapján a humán oldalon is azonosíthatók hiányosságok. A modern technológiai és műszaki védelmi megoldások fejlődése ellenére a kritikus szervezetek működésében továbbra is az emberi tényező jelenti az egyik legjelentősebb kockázatot. A nem megfelelő felkészültség, a hiányos védelmi tudatosság és a szervezeti folyamatok elégtelen ismerete jelentősen csökkentheti a kialakított védelmi rendszerek hatékonyságát, ezáltal gyengítheti a szervezetek ellenálló képességét. Bár ezt a problémát már több szervezet felismerte, de a humán erőforrás szervezeten belüli fejlesztési lehetőségei jelentős erőforrást igényelnek és a megfelelő támogató és ellenőrző mechanizmusok hiányában hosszú távon nem is biztosított a hatékonyságuk.

A feltárt problémák összességében arra mutatnak rá, hogy a kritikus szervezetek rezilienciájának fejlesztése nem kizárólag technikai vagy jogi kérdés, hanem olyan komplex, rendszerszintű kihívás, amely integrált megközelítést igényel.

KUTATÓI HIPOTÉZISEK, A KUTATÁS FŐBB CÉLKITŰZÉSEI

Természetesen a kritikus szervezetek azonosításával, kijelölésével és integrált védelmével kapcsolatos terület teljes vizsgálatát egy értekezéson belül nem lehet felvállalni.

Mivel az Európai Unió által kiadott irányelv szabad kezet ad a tagországoknak a nemzeti kritikus infrastruktúra védelmi programok kidolgozásában, így a nemzetek saját szabályozásaiban jelentős eltérések mutatkoznak. A nemzetek kritikus infrastruktúráinak védelmével kapcsolatos jogi szabályozók közötti összefüggéseket értekezésemben nem vizsgálom, csak a hazai szabályozást tekintem át.

Fentiek alapján az alábbi kutatói **hipotéziseket** fogalmaztam meg:

Feltételezem, hogy a jogi szabályozás megfelelő módosításával a kritikus szervezetek és infrastruktúrák azonosítási, kijelölési folyamatának és rezilienciájának hatékonysága növelhető.

Feltételezem, hogy az interdependencia, mint a kapcsolat egy bizonyos állapota rendelkezik olyan tulajdonságokkal, dimenziókkal, melyek elkülöníthetők egymástól, így a vizsgálatuk standardizálható és jól mérhető.

Feltételezem, hogy az interdependencia dimenzióinak meghatározását követően olyan egységes vizsgálati módszertan hozható létre, mely részletesebb és pontosabb függőségi elemzést eredményez, valamint alapja lehet az egységes országos interdependencia térkép kialakításának.

Feltételezem, hogy a fizikai védelem hatékonysága növelhető a minden részletre kiterjedő tervezéssel, a szükséges védelmi szint elérhető a humán és anyagi erőforrások előre tervezett optimalizálásával.

Feltételezem, hogy a kritikus szervezetek üzemeltetői nem rendelkeznek a megfelelő tudással az azonosítási és kijelölési folyamat, valamint a megfelelő védelmi intézkedések végrehajtásához.

Feltételezem, hogy támogató elemek nélkül a belső felkészítési rendszerek nem hatékonyak, eredményeik hasznosítása, a tapasztalatok visszaforgatása hosszabb távon nem történik meg, így erőforrást vonnak el, de a szervezet rezilienciáját nem növelik.

Az előzőekben felsorolt tények és indokok alapján jól látható, hogy egy potenciális kritikus szervezet folyamatos működését és üzembiztosságát megfelelően támogató reziliencia kialakításához a jogszabályi alapoktól kezdve, az azonosítás és kijelölési folyamaton keresztül, a fizikai védelem tervezése és megvalósítása időszakáig szükséges a folyamatot elemeznünk. Ennek érdekében az alábbi főbb **kutatási célokat** határoztam meg:

Olyan módosítási javaslatok megfogalmazása a nemzeti jogszabályok tartalmára, melyek a kritikus szervezetek és infrastruktúrák azonosítási és kijelölési folyamatának szabályait közelebb hozzák a gyakorlati végrehajtáshoz, törvény és kormányrendelet szintű szabályokkal támogatják a végrehajtás folyamatát.

Az interdependencia elkülöníthető dimenzióinak és jellemzőinek feltárása.

Javaslatot tenni az interdependencia vizsgálatának egységes gyakorlati módszerére.

Javaslatot tenni a kijelölt kritikus szervezetek és az infrastruktúrák üzemeltetői részére a megfelelő Fizikai Védelmi Terv elkészítéséhez, figyelemmel a kapcsolódó védelmi tervekkel való összhangjára.

Javaslatot tenni a kritikus szervezetek ellenálló képességének fejlesztésére, a szervezet vezetői és munkáltatói részére kialakított szervezeten belüli felkészítési rendszer kialakításával.

Kidolgozni a szervezetek belső felkészítési rendszerének főbb támogató elemeit.

KUTATÁSI MÓDSZEREK

A kitűzött kutatási céljaim elérése érdekében az alábbi főbb kutatási módszereket alkalmaztam:

1. tanulmányoztam a témával kapcsolatos hazai és külföldi szakirodalom vonatkozó részeit, tanulmányokat, a legújabb kutatások eredményeit és ajánlásait;
2. tanulmányoztam és elemeztem a témával kapcsolatos jogszabályokat, törvényeket, rendeleteket, határozatokat;
3. összegeztem a különböző szakterületek védelem, fizikai védelem és belső képzés témákban fellelhető dokumentumait, elemzéseit, melyek alapján kialakítottam saját következtetéseimet;
4. elemeztem adott kritikus szervezet⁹ azonosítási és kijelölési folyamatának végrehajtását, összehasonlítottam a jogszabályokban előírt végrehajtás folyamatával;¹⁰

⁹ Hozzáférést kaptam honvédelmi jelentős szervezet, nemzeti és európai pénzügyi kritikus szervezet, nemzeti biztonsági kritikus szervezet kijelölési és üzemeltetési dokumentumaihoz.

¹⁰ Honvédelmi Irányító Törzs vezetőjeként részt vettem európai kritikus szervezet veszélyhelyzetben történő reziliencia elemzésében.

5. részt vettem konkrét kritikus szervezet¹¹ előírt hatósági szakellenőrzésének folyamatában;
6. megvizsgáltam, megszereztem a katonai pályafutásom során eddig szerzett szakirányú ismereteimet, tapasztalataimat, a nem katonai védelmi feladatokba való átemelhetőség tekintetében;
7. konzultációt folytattam a témában érintett szakemberekkel mind a hatósági, mind az üzemeltetői oldalról;¹²
8. részt vettem a témához kapcsolódó konferenciák, workshopok szervezésében, végrehajtásában.

Kutatásaim részeredményeit a kutatás folyamán, azok előzetes megmértetése és a szakmával való megismertetése céljából, különböző szakmai kiadványokban megjelent publikációkban, tudományos konferenciákon, workshopokon elhangzott előadásaimban bemutattam.

AZ ÉRTEKEZÉS SZERKEZETI FELÉPÍTÉSE

A kitűzött kutatási céloknak megfelelően doktori értekezésemet négy fejezetre tagolom.

Az első fejezetben a hazánkban hatályos jogi szabályzókat tekintem át részletesen, kiemelve az elmúlt 20 évben történő módosításokat. Mivel célom elsősorban a kijelölési folyamat hatékonyságának, az interdependencia kezelésének, illetve a reziliencia hatékonyságnövelésének vizsgálata, ezért a hangsúlyt ezen témakörökre helyezem, a jogszabályok összehasonlító jellegű elemzésével.

A második fejezetben részletesen bemutatom a potenciális kritikus szervezetek azonosításának és kijelölésének elvi folyamatát, annak érdekében, hogy a valós végrehajtás tapasztalatai alapján konkrét javaslatokkal éljek a megfelelő pontokon történő módosításukra, illetve kiegészítő feladatokat javasoljak az előírt folyamat hatékonyabb végrehajtása érdekében.

A harmadik fejezetben az átfogó védelem rendszerét vizsgálva megállapítom a fizikai védelem helyét, szerepét a védelem rendszerében. A fizikai védelmi terv felépítésére adok részletes javaslatot, figyelembe véve az egyéb védelmi tervekkel való összhangot, mely növeli a védelem hatékonyságát. Több kritikus szervezet konkrét fizikai és egyéb védelmi terveinek vizsgálatával

¹¹ Részt vettem honvédelmi jelentős szervezet központi, illetve nemzeti és európai pénzügyi kritikus szervezet belső ellenőrzésén.

¹² Honvédelmi Irányító Törzs vezetőjeként részt vettem kritikus szervezetek veszélyhelyzetben történő felsőszintű támogatásában.

kialakítható egy egységes, részletes fizikai védelmi terv minta, mely igyekszik figyelembe venni az üzemeltető korlátait, lehetőségeit.

A *negyedik fejezetben* az előzőekben tárgyalt elvek és összegzett következtetések alapján, részletes magyarázattal kerül bemutatásra egy metodika, melyet követve kialakítható a kritikus szervezetek részére egy olyan belső felkészítési rendszer, mely a szervezet védelmi és üzembiztonsági képességeinek hatékonyságát az emberi tényező fejlesztésével éri el. A belső felkészítési rendszert támogató elemekként mutatom be a dokumentációs hierarchia és a képzésellenőrzés felépítését, szükségességét.

SZAKIRODALMI ÁTTEKINTÉS

A kritikus szervezetek azonosítása, kijelölése, illetve a létesítmények, infrastruktúrák fizikai védelmének kialakítása egymástól függetlenül kutatott területek, de fellelhető egymás közötti kapcsolatot taglaló szakirodalom is. Ezekről szeretnék egy rövid összegző áttekintést adni. A jogi szabályzó dokumentumok tartalmát, egymáshoz való viszonyukat nem vizsgálom a szakirodalmi áttekintésben, ezt a kérdést az I. fejezet tartalmazza.

Kifejezetten a kritikus szervezetek belső felkészítési rendszeréről, annak specialitásairól nem lelhető fel szakirodalom. A felnőttképzésről, szervezetek humán erőforrás fejlesztéséről, belső ellenőrzésről szóló publikációk, szakkönyvek információ tartalma viszont jól átültethető a kritikus szervezetek védelmi képességének fejlesztéséhez. Ezen dokumentumok elérhetőségét a *Felhasznált irodalom* jegyzéke tartalmazza

KRITIKUS SZERVEZETEK – HAZAI PUBLIKÁCIÓK

Magyarországon a legelső lépés a kritikus infrastruktúrák azonosításának és védelmének témakörében Kovács Ferenc, a Gazdasági és Közlekedési Minisztérium felkérésére 2005-ben készített tanulmánya az infrastruktúra kritikus elemeinek felmérése, védelmének és helyreállításának megszervezésére, melynek összefoglalója és eredményei¹³ a Hadmérnök 2006-os konferencia kiadványában is megjelentek.

¹³ KOVÁCS F.: Defence of the critical infrastructure. New Challenges in the Field of Military Sciences 2006 : 4th International Scientific Conference, Budapest, Magyarország, Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Főiskolai Kar (2006) 10 o.

Az első lépésekről ad összefoglalót, illetve a kritikus infrastruktúrák védelmének szabályozási nehézségeit tárják fel Précsényi Zoltán és Solymosi József 2007 és 2008-ban megjelent cikkei¹⁴
¹⁵. A 2008-ig megtett hazai első lépéseket Mógor Judit, Földi László és Solymosi József cikke mutatja be¹⁶. Ronyecz Lilla 2016-ban megjelent cikke¹⁷ a nemzetközi és a hazai veszélyeztetettségi tényezőkre világít rá.

A Zöld Könyv 2008-as megjelenése előtérbe helyezte a kritikus infrastruktúrák azonosításának és védelmének szükségességét. A kérdéskör bekerült az oktatási anyagok közé^{18,19}, illetve a Gazdasági és Közlekedési Minisztérium felkérésére további kutatásokkal egészült ki a biztonsági kérdések²⁰ és az európai közlekedési infrastruktúrák²¹ tekintetében.

A létfontosságú rendszerek védelmével kapcsolatos jogi alapok megjelenésével egyre több szakterületen kezdődik meg a kutatás, speciálisan az adott szakterület vonatkozásában. Sorra jelennek meg cikkek, tanulmányok, melyek a létfontosságú rendszerek védelmének egy adott szűkebb szegmensét veszik górcső alá.

Komoly lépés az infrastruktúrák védelmének terén az ENO Advisory Kft. 2009-ben megjelent könyve, melynek szerzői – Dr. Haig Zsolt, Hajnal Béla, Dr. Kovács László, Dr. Muha Lajos, Sik Zoltán Nándor – a kritikus információs infrastruktúrák meghatározására, addig még nem létező módszertant dolgoztak ki, és fejtették azt ki részletesen²².

Kovács Ferenc 2011-es cikkében, a repülőterek és a légiirányítás infrastruktúráinak vizsgálatából kiindulva a kritikus infrastruktúra fogalmi magyarázatát is érintette. A cikk halmazelméleti áttekintést adott a kritikus infrastruktúra elemek elhelyezésére a nemzeti, védelmi és katonai infrastruktúrák halmazában, és még a Lrtv. megjelenése előtt javaslatot tett

¹⁴ PRÉCSÉNYI Z., SOLYMOSI J.: Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé. *Hadmérnök*, II.1 (2007), 65-76 o.

¹⁵ PRÉCSÉNYI Z., SOLYMOSI J.: Kritikus infrastruktúrák azonosítása: körkép az EU-ban és az USA-ban tapasztalható nehézségekről. *Hadmérnök*, III.1 (2008), 59-69 o.

¹⁶ MÓGOR J., FÖLDI L., SOLYMOSI J.: Lépések a kritikus infrastruktúra védelmének magyarországi szabályozása felé. *Hadmérnök*, III évf. 4. szám (2008), 15-28 o.

¹⁷ RONYECZ L.: Létfontosságú rendszerek és létesítmények védelmével kapcsolatos nemzetközi tapasztalatok vizsgálata, azok integrálásának lehetőségei hazai rendszerbe. *Műszaki katonai Közlöny*, XXVI. évf. 2. szám (2016), 197-209 o.

¹⁸ KOVÁCS F.: Létfontosságú infrastruktúrák védelmének alapelvei. *MHTT Védelmi Infrastruktúra Szakosztály*, oktatási anyag, (2008)

¹⁹ KOVÁCS F.: A kritikus infrastruktúrák elméleti alapjai. *IVB Innovációs klubnap*, oktatási anyag, (2008)

²⁰ KOVÁCS F. (2008): *A kritikus infrastruktúra biztonsági kérdései*. Gazdasági és Közlekedési Minisztérium (GKM), Budapest.

²¹ KOVÁCS F. (2008): *Európai szempontból létfontosságú hazai közlekedési infrastruktúrák elemzése: tanulmány*. Gazdasági és Közlekedési Minisztérium (GKM), Budapest.

²² HAIG ZS., HAJNAL B., KOVÁCS L., MUHA L., SIK Z.: A kritikus információs infrastruktúrák meghatározásának módszertana. *ENO Advisory Kft.*, (2009)

a „kritikus infrastruktúra”, a „kritikus infrastruktúra védelme” és a „kritikus infrastruktúra képesség” fogalmára²³.

2013-ban, majd 2014-ben a kritikus infrastruktúrák közül kiemelten a közlekedési alrendszer vonatkozásában jelenik meg két tanulmány kötet, mely több írásban tárgyalja a közúti, vasúti, tengeri közlekedés biztonsági kérdéseit, illetve több szakterület – logisztika, média, informatika, társadalomtudományok – kapcsolódási pontjait elemzi^{24,25}.

2015-ben a Nemzeti Közszerológati Egyetem kiadásában jelenik meg Bognár Balázs, Bonnyai Tünde, Görög Katalin, Kátai-Urban Lajos, Vass Gyula könyve „Létfontosságú rendszerek és létesítmények védelme – Kézikönyv a katasztrófavédelmi feladatok ellátására” címmel, mely kifejezetten a katasztrófavédelem területére összpontosítva vizsgálja a létfontosságú rendszerek védelmének előzményeit, helyzetét, lehetőségeit.²⁶

Fontos mérföldkő volt a honvédelmi létfontosságú rendszeremekkel kapcsolatos szakterületen az első jelentősebb honvédelmi létesítmény azonosítási, kijelölési folyamatának végrehajtása. A végrehajtás tapasztalatait, javaslatait Ronyecz Lilla 2018-ban megjelent cikkében²⁷ publikálta.

Terék Tamás 2019-ben megjelent cikke a létfontosságú rendszeremek azonosítási, kijelölési folyamatát vizsgálva arra keresi a választ, hogy egy Veszélyes Katonai Objektumok státuszába tartozó létesítmény miért nem került kijelölésre honvédelmi létfontosságú rendszeremmé.²⁸

Megkerülhetetlen témára, a mesterséges intelligencia és az új generációs informatikai és internetes hálózatok kritikus infrastruktúrákban való megjelenésére hívja fel a figyelmet Pál Anita 2024-ben megjelent cikke, mely pár gondolatban kiemeli a kritikus infrastruktúrák védelmében és sebezhetőségében megnyíló új ablakot, felvetve a kibereszközök alkalmazásának lehetőségét és etikai kérdéseit is.²⁹

²³ KOVÁCS F. (2011): Repülőterek és légiirányítás a kritikus infrastruktúra részeként. Repüléstudományi közlemények. *Ludovika Egyetemi Kiadó*, XXIII:2. online konferencia kiadvány, 15 o.

²⁴ HORVÁTH A. (szerk.): Fejezetek a kritikus infrastruktúra védelemből. Kiemelten a közlekedési alrendszer. Budapest: *Magyar Hadtudományi Társaság*, 2013. (Tanulmánykötet)

²⁵ HORVÁTH A., BÁNYÁSZ P., ORBÓK Á. (szerk.): Fejezetek a létfontosságú közlekedési rendszeremek védelmének aktuális kérdéseiről. Budapest, *Nemzeti Közszerológati Egyetem*, 2014. (Tanulmánykötet)

²⁶ BOGNÁR B., BONNYAI T., GÖRÖG K., KATAI-URBÁN L., VASS GY.: Létfontosságú rendszerek és létesítmények védelme, Kézikönyv a katasztrófavédelmi feladatok ellátására. Budapest, *Nemzeti Közszerológati Egyetem*, 2015.

²⁷ RONYECZ L.: A létfontosságú rendszeremek kijelölési eljárásának tapasztalatai. *Műszaki Katonai Közöny* XXVIII : 2, pp. 81-91., 10 p. (2018)

²⁸ TERÉK T.: A létfontosságú veszélyes katonai objektum definiálása, elhelyezése a Magyar Honvédség rendszerében. *Katonai Logisztika*, 3, pp. 5-23., 19 p. (2019)

²⁹ PÁL A.: A jövőbiztos kritikus infrastruktúra. *Biztonságtudományi Szemle*, 6:2, pp 79-90, 12p (2024)

A kritikus infrastruktúrák védelmének fontosságára és napjaink biztonsági környezetének komoly változásaira mutat rá Kovács Ferenc 2024-ben megjelent cikke, mely részletesen bemutatja az kritikus infrastruktúrák stratégiai szerepét és sérülésének hatásait, következményeit az orosz-ukrán háborúban.³⁰

KRITIKUS SZERVEZETEK – KÜLFÖLDI PUBLIKÁCIÓK

2001. szeptember 11-i tragikus események bizonyították a fejlett országok sebezhetőségét a terrorizmussal szemben. Több nemzet ekkor kezdett el foglalkozni a veszélyeztetettség újbóli felmérésével, a különböző veszélyhelyzetek hatásainak vizsgálatával.

Míg a világ országai elkezdtek a kritikus infrastruktúrák védelmével kapcsolatos legalapvetőbb fogalomrendszerük felállítását, az USA már egy lépéssel tovább haladt és 2003-ra elkészített egy nemzeti stratégiát a kritikus infrastruktúrák fizikai védelmének kialakításához. Munkacsoportot hoztak létre, mely munkacsoport a 2006-ban kiadott jelentésében ajánlásokat fogalmazott meg a kritikus infrastruktúra védelmi programok létrehozására, és az aktuális nemzeti infrastruktúra védelmi terv végrehajtásának támogatására³¹.

2010-ben, a Brüsszelben működő Centre for European Policy Studies (CEPS) kutatóintézet jelentést adott ki a kritikus infrastruktúrák védelmének aktuális helyzetéről, kiemelten az európai kritikus infrastruktúra politikát vizsgálva³².

Az USA jelenleg aktuális, 2013. évben kiadott Nemzeti Infrastruktúra Védelmi Terve (National Infrastructure Protection Plan – NIPP 2013³³) kiemelten a résztvevők – állami és ipari szereplők, magán szektor – együttműködésének erősítése érdekében, a védelem fokozásának elősegítésére készült. Összefoglalja az elmúlt időszak eredményeit, célokat fogalmaz meg, elemzés található benne az új kockázati tényezőkről.

A kritikus infrastruktúrák interdependencia kérdésével kapcsolatban jelentősen kevesebb irodalmat találni. Az interdependencia vizsgálatával, jellemzőivel *Steven M. Rinaldi*, *James P. Peerenboom* és *Terrence K. Kelly* már 2002-ben megjelent cikkükben foglalkoztak. Feltárták

³⁰ KOVÁCS F.: A kritikus infrastruktúra stratégiai szerepe az orosz-ukrán háborúban. *Hadtudomány*, 34:3, pp 29-39. 11p (2024)

³¹ *The national strategy for The Physical Protection of Critical Infrastructures and Key Assets*. USA, 02.2003

³² HAMMERLI, BERNHARD (chair): *Protecting critical infrastructure in the EU*, Centre for European Policy Studies, Brussels, 2010.

³³ NIPP 2013 - Partnering for Critical Infrastructure Security and Resilience. *Homeland Security*, USA, 2013.

az interdependencia összetevőit, tényezőit, ezen tényezők tulajdonságait, melyek nagyon jó alapot adnak az interdependencia vizsgálati módszereinek kidolgozására.

Érdekes cikk jelent meg 2018-ban az *International Journal of Disaster Risk Reduction* lapban, melyben C. PURSIAINEN az északi országokat vizsgálva megállapította, hogy az egyes infrastruktúrák védelme helyett a „létfontosságú társadalmi funkciók” biztosítására kell fókuszálni, vagyis előrevetítette a reziliencia fontosságának kérdését.³⁴

A külföldi publikációk között is számos olyat találhatunk, melyek a létfontosságú rendszerek védelmével kapcsolatos egy-egy szektort, részterületet emelnek ki és azt vizsgálják behatóbban, mint például az infokommunikáció, tömegközlekedés, vasúti és közúti szállítás.

OBJEKTUMVÉDELEM – HAZAI PUBLIKÁCIÓK

Mind a nemzetközi, mind a hazai jelentősebb tudományos folyóiratokban nagy számban jelennek meg létesítmények védelmével kapcsolatos publikációk. Véleményem szerint a legkiterjedtebb és nagyfokú védelmi intézkedéseket a bűnös célú robbanások elleni védelem igényli, ezért a nagymennyiségű publikáció szelektálása során az ehhez a témakörhöz kapcsolódó, hazai publikációkra helyeztem a hangsúlyt. Ezek közül emelnék ki pár közlést.

BALOGH Zsuzsanna kettő 2008-ban megjelent cikkében^{35,36} is elemzi a robbanások hatását és az ellenük való védelem lehetőségeit, kifejezetten az építészeti tervezés és technikai kivitelezés szempontjából, illetve 2010-ben megjelent cikkében³⁷ speciálisan a üvegre mint építőanyagra koncentrált.

Hazai szerzőket tekintve a legtöbb robbantásokkal és azok hatásaival foglalkozó publikáció LUKÁCS László nevéhez köthető. Megjelent cikkei igen részletesen, gyakran a történelmi előzményeket is figyelembe véve elemzi a robbanóanyagok fejlődését, a robbantások

³⁴ C.PURSIAINEN: Critical infrastructure resilience: A Nordic model in the making? , *International Journal of Disaster Risk Reduction*, 27. (2018)

³⁵ BALOGH Zs.: Építészeti tervezés robbantásos cselekmények ellen. *Műszaki Katonai Közlöny*, XVIII : 1-4 pp. 53-59., 7 p. (2008)

³⁶ BALOGH Zs.: Épületek robbantásos cselekmények elleni védelmének technikai lehetőségei. *Műszaki Katonai Közlöny*, XVIII : 1-4 pp. 105-117., 13 p. (2008)

³⁷ BALOGH Zs.: Üveg az építészetben, a terrorista robbantások tükrében. *Műszaki Katonai Közlöny*, XX : 1-4 pp. 257-271., 14 p. (2010)

cselekmények végrehajtását, hatásait. Ezen részletes elemzésekre épül a robbantásos cselekmények elleni védelem lehetőségeinek leírása^{38 39 40 41 42 43 44 45 46}.

LUKÁCS László vezetésével 2012-ben kutatócsoport alakult a „Kritikus infrastruktúra védelmi kutatások” című, TÁMOP-4.2.1.B-11/2/KMR-2011-0001 pályázat, 4. alprogram, „Robbantásos építményvédelem” kiemelt kutatási terület keretében. A kutatócsoport szakemberei a terrorizmus kialakulásának hátterét, a robbantásos cselekmények eszközrendszerét, fizikai, társadalmi hatásait, a kockázatok elemzését, az építmények védelmét vizsgálták alapos részletességgel. Kutatásaik alapján 2013-ban került kiadásra az „Állandó épületek robbantásos cselekményekkel szembeni védelme fokozásának módszerei, lehetőségei, eszközei” c. tervezési segédlet SZABÓ Sándor és TÓTH Rudolf szerkesztésében.

A terrorizmus általi fenyegetettség stratégiai szintű kezelésének elemzésétől, a robbanóanyagok és hatásuk bemutatásán keresztül fejt ki részletesen az objektumok védelmének lehetőségeit BALOGH Zsuzsanna 2013-ban írt értekezésében. Az értekezés – fentiekén kívül – kiemeli még a robbantásos cselekmények elleni fontosabb szabályzó dokumentumokat.

Az improvizált robbanóeszközök elleni védekezés katonai oldalról való megközelítéséről olvashatunk DARUKA Norbert 2013-ban megjelent értekezésében, melyben kiemelten foglalkozik az improvizált robbanóeszközök ismertetésével, az ellenük való védekezés katonai stratégiájával, valamint az eszközök semlegesítésének és a robbanások hatásai csökkentésének lehetőségeivel.

³⁸ LUKÁCS L.: Robbantásos merényletek elkövetésének lehetősége Magyarországon. *Hadtudomány*, 3., pp. 82-90. , 9 p. (1994)

³⁹ LUKÁCS L.: Robbantásos merényletek elkövetésének lehetőségei Magyarországon. In: Mueller, Othmár (szerk.) *ÉTE Robbantástechnikai szakbizottságának 6. Nemzetközi Robbantástechnikai Kollokvium : előadás kötet*, Budapest, Magyarország (1995) pp. 1-4. , 4 p.

⁴⁰ LUKÁCS L.: A terrorcselekmények megelőzésének korszerű eszközei, különös tekintettel a robbantásos fenyegetésekre. In: Mueller, Othmár (szerk.) *Az ÉTE Robbantástechnikai szakbizottságának 7. Nemzetközi Robbantástechnikai Kollokviuma : előadás kötet*, Budapest, Magyarország (1997) pp. 1-4. , 4 p.

⁴¹ LUKÁCS L. (2009): A terrorista robbantás és a repülés. *Repüléstudományi Közlemények*, 2009 : 2 p. online , 9 o

⁴² LUKÁCS L.: Épületek elleni robbantásos cselekmények és jellemzőik. *Műszaki Katonai Közlöny*, XXII : Különszám pp. 4-13. , 10 p. (2012)

⁴³ LUKÁCS L., Balogh Zs.: Bombatámadás az USA nagy követség ellen – Nairobi, 1998. augusztus 07. *Műszaki Katonai Közlöny*, XXIII : 2 pp. 159-178. , 20 p. (2013)

⁴⁴ LUKÁCS L.: Építmények robbantásos cselekmények elleni védelme. *Műszaki Katonai Közlöny*, 24 : 3 pp. 65-74. , 10 p. (2014)

⁴⁵ LUKÁCS L., BALOGH Zs.: Turisztikai létesítmények, események robbantásos fenyegetettsége. *Műszaki Katonai Közlöny*, XXVIII : 2 pp. 238-251. , 14 p. (2018)

⁴⁶ LUKÁCS L., BALOGH Zs.: A kritikus infrastruktúra létesítményeinek robbantásos cselekmények elleni védelméről. *Honvédségi Szemle*, 2019:3 pp. 85-102. , 18 p.

Az infrastruktúrák és erre építve a kritikus infrastruktúrák fogalomrendszerét elemezve indítja BONNYAI Tünde 2014-ben megjelent értekezését, vizsgálva a kritikus infrastruktúrák veszélyeztetettségi tényezőit. Az értekezés rávilágít arra, hogy a kritikus infrastruktúrák védelmében milyen komoly szerepe van a lakosság tájékoztatásának, előzetes felkészítésének.

ANTAL Örs 2014-ben megjelent cikke⁴⁷ jó összefoglalót ad az épületek rögtönzött robbanóeszközök elleni fizikai védelmének technikai kialakításához. Összefoglalja a rögtönzött robbanószerkezetek főbb típusait, tulajdonságait, illetve technikai példákat, berendezéseket mutat a fizikai védelem kiépítéséhez.

Az infrastruktúra veszélyeztetettségéről, a mérnöki gyakorlatban alkalmazott infrastruktúravédelmi szabályozásokról, szabványokról ad kritikus összefoglalót ROMÁN Zsolt és KOVÁCS Ferenc 2016-ban megjelent cikke⁴⁸. Napjaink mérnöki gyakorlatát is figyelembe véve fogalmaznak meg javaslatokat mind a központi igazgatási szervek gondolkodásmódjának szükséges változtatásához, mind a tervezői munkát segítő, védelmi témájú szabványok létrehozásának tekintetében.

PETHŐ Richárd 2017-ben készült értekezésében a tömegtartózkodású objektumok improvizált robbanóeszközökkel történő támadásainak hatásait vizsgálja. Kiemelt hangsúlyt fektet a „LÁTNIK” rendszer bemutatására, mely a bűnös célú robbantásos cselekmények kárbecslésének és az ellenük történő védekezés munkafolyamatainak tervezésekor igen hatékonyan alkalmazható.

SZABÓ Lajos 2021-ben megjelent értekezése az objektumok fogalmi meghatározásának elemzésétől indul, részletesen vizsgálva az objektum, az objektumvédelem definícióinak pontos jelentését, elméleti háttérét, majd rendszerként vizsgálja a védelem elemeit és elveit. Ezen fogalmi elemzésekre és elvekre építve mutatja be a megelőző védelmi zóna fontosságát, felépítését, eszközeit.

Értekezésem elkészítéséhez az előbbieken kiemelt dokumentumokon kívül számos írást áttekintettem, melyek egy-egy gondolattal, egy új megközelítéssel támogatták kutatásomat. Ezen dokumentumok előtalálási helyeit a Felhasznált irodalom jegyzéke tartalmazza.

⁴⁷ ANTAL Ö.: Az épületek védelmének korszerű lehetőségei házi készítésű robbanóeszközök ellen. *Műszaki Katonai Közlöny*, 24 : 1 pp. 107-119. , 13 p. (2014)

⁴⁸ ROMÁN Zs., KOVÁCS F.: Épületek robbantás elleni védelmének szabályozási kérdései. *Műszaki Katonai Közlöny*, XXVI : 3. pp. 93-104., 11 p. (2016)

1. FEJEZET

A KRITIKUS SZERVEZETEK ÉS INFRASTRUKTÚRÁK AZONOSÍTÁSÁNAK, KIJELÖLÉSÉNEK ÉS REZILIENCIÁJÁNAK SZABÁLYOZÓ RENDSZERE

A kritikus szervezetek témakörében készült legfontosabb szabályzó dokumentumokat, tartalmukat, egymáshoz való viszonyukat vizsgálom ebben a fejezetben. A kritikus szervezetekkel és infrastruktúrákkal foglalkozó hazai szabályzók részletes vizsgálata előtt fontos röviden áttekintenünk az Európai Unió által korábban kiadott és aktuális közleményeket, hiszen a hazai rendszer alapjait e közlemények adják.

Az EU tagországait, illetve az EU-n kívül eső országokat érintő kritikus infrastruktúrák kérdése önmagában is hatalmas terület, értekezésemben ezt a témakört nem tárgyalom részletesen, csak abban az esetben érintem, amennyiben a nemzeti kritikus szervezetek és infrastruktúrák témaköréhez szorosan kapcsolódik.

1.1. AZ EURÓPAI UNIÓ KRITIKUS INFRASTRUKTÚRÁK VÉDELMEVEL KAPCSOLATOS FŐBB LÉPÉSEI ÉS DOKUMENTUMAI

Az Európai Unió számára a kritikus infrastruktúrák védelme kiemelt feladat kell, hogy legyen, hiszen a közös politika, védelem és piac alapjait a tagországok által egymás rendelkezésére bocsátott infrastruktúrái képezik, amelyekre a tagállamok az elmúlt évtizedekben egyre jobban támaszkodtak.

A biztonsági kockázatok elemzése, több tudományos és politikai fórum után, első lépésként az európai állam- és kormányfők Tanácsa 2003-ban fogadta el az Európai Biztonsági Stratégia című határozatát, melyben az EU közbiztonságára leselkedő belső és külső eredetű veszélyekkel szembeni közös fellépés jelentőségét emelték ki⁴⁹. Ennek tükrében az Európai Tanács 2004. júniusi ülése felkérte az Európai Közösségek Bizottságát, hogy készítsenek egy átfogó stratégiát a létfontosságú infrastruktúrák védelmére, így elindult a folyamat.

1.1.1. Az Európai Unió korábbi szabályzói

1.1.1.1. Az Európai Közösségek Bizottságának COM(2004) 702 számú közleménye

⁴⁹ *A secure europe in a better world, European Security Strategy*, Brussels, 12.12.2003.

„A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben” c. közleményt 2004.10.20-án adták ki a Tanács és az Európai Parlament részére, azzal a céllal, hogy összegezze a létfontosságú rendszerek védelmével kapcsolatos addigi intézkedéseket és javaslatokat fogalmazzanak meg a további feladatok tekintetében.

A közlemény elsősorban és kiemelten a katasztrófális terrortámadásokat emeli ki fő veszélyként, melyre különböző – sérültekkel és károkkal járó – példákat is hoz.

Fontos része, hogy elsőként fogalmazta meg a létfontosságú infrastruktúrák körét:

„A létfontosságú infrastruktúrákhoz azok a fizikai és információs technológiai berendezések és hálózatok, szolgáltatások és eszközök tartoznak, amelyek összeomlása vagy megsemmisítése súlyos következményekkel járhat a polgárok egészsége, védelme, biztonsága és gazdasági jóléte, illetve a tagállamok kormányainak hatékony működése szempontjából.”

Gazdasági ágazatokra és kulcsfontosságú szolgáltatásokra osztja a létfontosságú infrastruktúrák körét, melyek az energiaipar, kommunikáció és információs technológia, pénzügy, egészségügy, élelmiszer, vízellátás, veszélyes anyagokkal kapcsolatos tevékenységek és az állami infrastruktúrák. Kiemeli, hogy ezek az infrastruktúrák az interdependencia miatt sokkal kiszolgáltatottabbak az összeomlás vagy megsemmisülés szempontjából. Határidőként 2005 végét jelöli meg egy tagállami és európai szintű létfontosságú infrastruktúra jegyzék összeállítására.

A kritikusság megállapítása vonatkozásában első feladatként egy kritérium rendszer felállítását szorgalmazza, melyhez három tényező vizsgálatát adja meg útmutatóként:

Hatókör: veszteségekkel érintett földrajzi terület nagysága alapján, mely lehet nemzetközi, nemzeti, tartományi/területi vagy helyi.

Nagyságrend: a hatás mértéke alapján értékel az alábbi szempontok alapján:

nincs – minimális – mérsékelt – jelentős hatása van:

- a lakosságra (áldozatok, megbetegedések száma, evakuálás);
- a gazdaságra (GDP-hatás, gazdasági veszteség, szolgáltatásromlás);
- a környezetre (környezetkárosító hatás);
- az interdependencia vonatkozásában;
- az állam iránti bizalomra (politikai hatás).

Időbeli hatás: egy adott infrastrukturális elemmel kapcsolatos veszteség mennyi idő elteltével fejthet ki komoly hatást (pl. azonnali, 24-48 óra, egy hét, egyéb)

A közlemény kidolgozásának időpontjáig elért eredmények közül a nukleáris anyagok kezeléséből adódó veszélyekre, a nemzetközi közlekedés biztonságos biztosítására, a tájékoztatás biztonságára, információvédelemre vonatkozó intézkedéseket emeli ki.

A dokumentum kardinális pontja a szubszidiaritás elvének bevezetése a létfontosságú infrastruktúrák védelmével kapcsolatban, mely szerint csak az országhatárokon áttérjedő hatással rendelkező infrastruktúrák esetében kell európai szinten foglalkozni a védelemmel. A többi esetben a létfontosságú infrastruktúrák védelmének kialakítása a tagállamok feladata, de közös keretben. Ez a közös keret a létfontosságú infrastruktúrák védelmére vonatkozó európai program, az un. EPCIP⁵⁰.

Az EPCIP célja a szakterület és a tagállamok kormányainak támogatása ágazatonkénti elemzések, védelmi technikák, kockázatfelmérések kiadásával, folyamatban lévő vagy tervezett jogi intézkedések közre adásával, a sebezhető pontok és interdependencia elemzésével. A közlemény kiemeli, hogy az EPCIP legfontosabb támogató eleme a létfontosságú infrastruktúrákkal kapcsolatos figyelmeztető információs hálózat, az un. CIWIN⁵¹.

1.1.1.2. Az európai Zöld Könyv és a végleges EPCIP

Az Európai Közösségek Bizottságának COM(2005) 576. és COM(2006) 786. számú kiadványa a Zöld Könyvet és a végleges közleményt a létfontosságú infrastruktúrák védelmére vonatkozó európai programról.

A témával kapcsolatos konzultációs eljárás második lépéseként 2005-ben az Európai Nemzetek Bizottsága *zöld könyvet* adott ki, melynek célja az EPCIP és CIWIN felállítására vonatkozó lehetséges megközelítési irányok elemzése, nagy létszámú résztvevő bevonásával. A zöld könyv eredményeképpen 2006-ban a Bizottság kiadta a létfontosságú infrastruktúrák védelmére vonatkozó európai programról szóló közleményét, melyben bemutatja a végrehajtás érdekében javasolt elveket, eljárásokat és eszközöket.

A *zöld könyv* kérdéseket fogalmazott meg és lehetséges irányokra adott javaslatot az EPCIP általános célja és alapelvei, valamint a kialakítandó védelem szintjével kapcsolatban. Kiemelte a tagállamok, az ágazatok és gazdasági szereplők együttműködésének fontosságát és javasolta

⁵⁰ European Programme for Critical Infrastructure Protection

⁵¹ Critical Infrastructure Warning Information Network

egy szoros EPCIP keret megalkotását annak érdekében, hogy a lehető leghatékonyabb védelmi szintet lehessen elérni a tagországok és gazdasági szereplők hátrányos érintettsége nélkül.

Javaslatot fogalmazott meg a létfontosságú EU-infrastruktúra fogalmára, melynek alapja a határokon átnyúló hatás. Kiemelte, hogy e hatások vizsgálatánál és az európai kritikus infrastruktúrák kijelölésénél fokozottan figyelembe kell venni az interdependenciát, de módszertani ajánlást nem adott.

Mivel sok európai vállalat határokon átnyúló tevékenységet folytat, felmerült, hogy a tagországok nemzeti kritikus infrastruktúrái nem hagyhatók figyelmen kívül az európai kritikus infrastruktúrák vizsgálatánál. A kérdés az volt, hogy a nemzeti kritikus infrastruktúrák teljes mértékben, vagy részben legyenek e integrálva az európai kritikus infrastruktúrák rendszerébe, vagy az ezzel kapcsolatos döntéseket a tagország saját hatáskörben hozza meg.

A *zöld könyv* a létfontosságú infrastruktúrák üzemeltetői és tulajdonosai részére is javasol feladatszabást, melynek elmulasztása bírság kiszabását vonhatná maga után. Ilyen feladatai lehetnek az adott infrastruktúra kritikusságának vizsgálata, biztonsági összekötő tisztviselő kijelölése, szükség szerint Üzemeltetői Biztonsági Terv és Vészhelyzeti Intézkedési Terv elkészítése.

A CIWIN kialakítása nem volt kérdéses, hiszen a gyors információáramlás az egységes, összefogott európai kritikus infrastruktúra védelem alapja lehet. A javaslat szerint a CIWIN lehetne egy témával kapcsolatos vélemények és gyakorlatok cseréjének szakmai fóruma, vagy egy sürgősségi riasztó rendszer, illetve akár egy olyan többszintű rendszer mely mindkét lehetőséget magában foglalja és ellátni képes.

Mivel a létfontosságú rendszerek védelme egyértelműen feladatokat ró a tagországokra, a létfontosságú infrastruktúrák tulajdonosaira és üzemeltetőire, felmerült kérdésként a rendszer különböző elemeinek finanszírozása, értékelése és ellenőrzése is.

A Zöld Könyv alapján beérkező javaslatokat az Európai Bizottság feldolgozta, és 2006-ban kiadta a létfontosságú infrastruktúrák védelmére vonatkozó európai programról szóló közleményét, mely már konkrét javaslatokat tartalmaz az európai létfontosságú infrastruktúrák védelmének kialakítására. Végül a következő fogalom került be a közleménybe:

„Az EPCIP általános célkitűzése, hogy javítsa a létfontosságú infrastruktúrák védelmét az EU-ban.”

Az EPCIP által kezelendő fenyegetések típusainál – bár a terrorveszélyt prioritásként ismerték el – összveszély-megközelítést határoztak meg, illetve a közlemény kiemelte, hogy minden esetben arra a veszélyre kell összpontosítani, melyre az adott infrastruktúra a legsebezhetőbb.

Az EPCIP végrehajtására vonatkozó alapelvek, a szubszidiaritás, a kiegészítő jelleg, a titkosság, az arányosság, az együttműködés és az ágazati megközelítés is bekerültek a végleges közleménybe.

A közlemény azt a keretet igyekszik megadni, melyet Az EPCIP kialakításához és működtetéséhez szükségesnek lát. Ezt a keretet a következő pontokban foglalja össze:

1. Szükséges kidolgozni az európai létfontosságú infrastruktúrák (ECI-k) azonosítására és kijelölésére vonatkozó eljárást.
2. Az EPCIP végrehajtására és fenntartására vonatkozó intézkedések kidolgozása.
3. Tagállamok támogatása a nemzeti létfontosságú infrastruktúrák azonosításának, kijelölésének folyamatában és védelmének kialakításában.
4. Az európai létfontosságú infrastruktúrák védelmének kialakítására.
5. A nemzetközi határoktól független, a rendszerek közötti interdependencia figyelembe vétele.
6. 2007-2013-as időszakra tervezett kísérő pénzügyi intézkedések, támogató pénzügyi programok indítása.

A Közlemény mellékletében részletezi az EPCIP végrehajtási tervét, melyet három fő munkafolyamatra és azokon belül több szakaszra bont:

1-es munkafolyamat: EPCIP stratégiák kidolgozása.

2-es munkafolyamat: az európai létfontosságú infrastruktúrák védelme.

3-as munkafolyamat: a nemzeti létfontosságú infrastruktúrák támogatása.

1.1.1.3. A létfontosságú infrastruktúrák figyelmeztető információs hálózata (CIWIN⁵²)

Az Európai Közösségek Bizottságának COM(2008) 676. javaslata a létfontosságú infrastruktúrák figyelmeztető információs hálózatának létrehozásáról szól.

Az Európai Unió tagállamaiban elindult a létfontosságú infrastruktúrák védelmét célzó intézkedések kidolgozása. A tagországok önálló munkája azt eredményezte, hogy több ország

⁵² Critical Infrastructures Warning Information Network - CIWIN

lemaradt ezzel a tevékenységgel, így hamar belátták, hogy a CIWIN létrehozása jelentős előnnyel járna a megszerzett tapasztalatok, bevált gyakorlatok megosztásával, mellyel időt és kutatási, fejlesztési költségeket is meg lehet spórolni. A tagállamok közötti információcsere azonban bonyolult folyamat, természetes, hogy az érdekelt felek tartanak az érzékeny információk cseréjétől. Az információk hatékony cseréjéhez bizalom és rugalmasság kialakítására van szükség.

A CIWIN rendszer kialakítása érdekében az érdekelt felekkel több szintű konzultációk és hatásvizsgálatok sorát folytatták le. A COM(2008) 676. javaslat így foglalta össze a szakpolitikai alternatívákat:

1. alternatíva: Nem kerül sor szakpolitikai alternatíva kidolgozására, a tagországoknak egyedül kell megoldaniuk a kérdést.
2. alternatíva: A CIWIN az Európai Unió meglévő riasztórendszerei (polgárvédelem⁵³, a radiológia⁵⁴, az állat és növénybetegségek⁵⁵, emberi fertőző betegségek⁵⁶, illetve általános termék⁵⁷ és élelmiszerbiztonság⁵⁸) továbbfejlesztésével kerül kialakításra.
3. alternatíva: A CIP-pel kapcsolatos információk cseréjének nyílt platformja.
4. alternatíva: egy önkéntes, biztonságos riasztó/kommunikációs rendszer kialakítása.
5. alternatíva: az előzőhöz hasonló kialakítású biztonságos riasztó/kommunikációs rendszer kialakítása, két elkülönített riasztó és információs feladattal.

A Bizottság az elvégzett hatásvizsgálatok alapján a 4. alternatívát találta a legelőnyösebbnek.

A Bizottság által összeállított javaslatot a Tanács elfogadta és 2009. január 01-i hatállyal határozatot adott ki a CIWIN létrehozására. A prototípus kísérleti szakaszát követően a CIWIN 2013. január 15-e óta működik.

1.1.1.4. Az európai kritikus infrastruktúrák azonosítása, kijelölése és védelme⁵⁹

Az Európai Unió Tanácsának 2008/114/EK irányelve részletesen összefoglalta az Európai Létfontosságú Infrastruktúrák azonosításában, kijelölésében és védelmében eddig végzett

⁵³ 2007/779/EK, Euratom tanácsi határozat

⁵⁴ 87/600/Euratom tanácsi határozat

⁵⁵ 82/894/EGK és a 2000/29/EK tanácsi irányelvek

⁵⁶ 2119/98/EK európai parlamenti és tanácsi határozat

⁵⁷ 2001/95/EK európai parlamenti és tanácsi irányelv

⁵⁸ 178/2002/EK európai parlamenti és tanácsi rendelet

⁵⁹ Az Európai Unió Tanácsának 2008/114/EK irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről

tevékenységeket. Ismételten kiemelte, hogy a ECI-k védelmének elsődleges és végső felelőssége a tagállamokat és az infrastruktúrák tulajdonosait/üzemeltetőit terheli, viszont a kölcsönös függőségi viszony miatt minden munkafolyamatnak európai szinten egységes eljárásokat, szabályokat kell követniük.

Az irányelv:

- figyelembe veszi az ágazati sajátosságokat;
- a speciális jogszabályok és szerződések miatt a nukleáris energiára területére nem vonatkozik;
- kiegészíti, támogatja a tagországok eddig meghozott szabályzóit;
- előírja a kijelölt Európai Létfontosságú Infrastruktúrák számára egy Üzemeltetői Biztonsági Terv⁶⁰ elkészítését;
- előírja a Biztonsági Összekötő Tisztviselő kijelölését a nemzetközi hatóságokkal való együttműködés érdekében;
- előírja, hogy a tagállamok szolgáltatassanak általános információkat az ágazatok sebezhetőségéről, annak érdekében, hogy a későbbiekben konkrét javaslatok kidolgozását és egységesítését segítsék az ECI-k védelmének fokozását illetően;
- előírja a tagországok részére az európai kritikus infrastruktúrák védelmével foglalkozó kapcsolattartó pont⁶¹ létrehozását.

A kiadott irányelv a következő módon határozza meg a „kritikus infrastruktúra” fogalmát:

„a tagállamokban található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna valamely tagállamban.”

és az „európai kritikus infrastruktúra” fogalmát:

„a tagállamokban található olyan kritikus infrastruktúra, amelynek megzavarása vagy megsemmisítése jelentős hatással lenne legalább két tagállamra.”

⁶⁰ Operator Security Plan - OSP

⁶¹ European Critical Infrastructure Protection Contact Point – ECIP CP

A kiadott irányelv mindössze két ágazatot – az energia- és a közlekedési ágazatot – érinti, illetve a horizontális kritériumokként a veszteségek, a gazdasági és a társadalmi hatás kritériumait határozza meg.

Az irányelv nagyon tág keretet ad a tagországok részére az európai kritikus infrastruktúrák azonosítása és kijelölése vonatkozásában. Az ágazati kritériumok megadását teljesen az ágazati szakterületekre bízza, a horizontális kritériumok hozzávetőleges küszöbértékeinek követését pedig a tagállamok önállóan dönthetik el. Kiemeli, hogy amennyiben egy potenciális kritikus infrastruktúra nem elégíti ki az európai horizontális kritériumokat, akkor nem jelölhető ki Európai Kritikus Infrastruktúrává.

A kijelölés folyamatára nem ad meg konkrét lépéseket, a végrehajtást azokra a tagországokra bízza, amelyekre az adott ECI jelentős hatással lehet.

1.1.1.5. A NIS irányelv⁶²

A 2010-es évek gyors információtechnológiai fejlődése – mely napjainkban sem lassult – és a biztonsági események számának és hatásának növekedése szükségessé tette a jogi szabályozás széleskörű kiterjesztését és egységesítését.

A NIS értelmében a tagállamoknak egy hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát kell kidolgozniuk, amely meghatározza a stratégiai célokat és prioritásokat, a szükséges szakpolitikai és szabályozási kereteket. Az irányelv bevezeti az „*alapvető szolgáltatást nyújtó szereplő*” definícióját és meghatározza az azonosításukra vonatkozó kritériumokat. Mindezek mellett meghatározza a kötelezően figyelembe veendő ágazatokat (*energia, közlekedés, banki szolgáltatások, pénzügyi piaci infrastruktúrák, egészségügy, ivóvízellátás és elosztás, digitális infrastruktúra*) és szolgáltatásokat is (*online piactér, online keresőprogram, felhőalapú számítástechnikai szolgáltatás*), de nem korlátozza a tagországokat abban, ha egyéb ágazatot vagy szolgáltatást vennének fel a nemzeti stratégiájukba.

A nemzeti stratégiának ki kell terjednie a felkészültségre, reagálásra és helyreállításra, az oktatásra, kutatás-fejlesztésre, kockázatelemzésre vonatkozó intézkedések kidolgozására is. Ezen túlmenően minden tagállamnak ki kell jelölnie illetékes nemzeti hatóságot vagy hatóságokat az irányelv alkalmazásának irányítására és ellenőrzésére, egy kapcsolattartó pontot

⁶² Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (NIS)

a határokon átnyúló koordinációra, illetve számítógép-biztonsági eseményekre reagáló csoportokat (CSIRT⁶³) az események kezelésére.

Uniós szinten az irányelv létrehoz egy együttműködési csoportot a stratégiai kérdések megvitatására és a bevált gyakorlatok megosztására, melynek tagjai a tagállamok, a Bizottság és az ENISA⁶⁴ képviselői közül kerül ki. A továbbiakban erre a csoportra bízta a nemzeti CSIRT-ek közötti együttműködés koordinálását, munkájuk támogatását.

Fontos kivétel, hogy a digitális szolgáltatókra vonatkozó előírások nem alkalmazandók a mikro- és kisvállalkozásokra.

1.1.2. Az Európai Unió hatályos szabályzói

1.1.2.1. A NIS2 irányelv⁶⁵

A 2020-ban elterjedt COVID19 világjárvány alapjaiban változtatta meg az emberek életvitelét. A járványügyi korlátozások időszakában a társadalmi és gazdasági tevékenységek igen jelentős része áttért a digitális világba, az infokommunikációs technológiák és ezen belül az Internet megléte és stabilitása elengedhetetlenné vált. Nem csak az emberek közötti kapcsolat alapját jelentette, de a szélessávú hálózatok ugrásszerű fejlődést jelentettek a tanulás, munka, kutatás-fejlesztés és a kormányzati, közszolgálati területeken is.⁶⁶

A megnövekedett digitalizáció a kiberfenyegetések számát is megemelte, mely szükségessé tette a NIS felülvizsgálatát. Míg a NIS irányelv elsősorban a kiberbiztonsági együttműködés minimumfeltételeinek megteremtésére és a tagállamok képességeinek kialakítására, harmonizációjára törekedett, a NIS2 már egy szigorúbb, egységesebb szabályozási keretet hozott létre. A NIS2 hatálya kibővült több kiemelten kritikus ágazattal (*szennyvíz, Információs és Kommunikációs Technológia (IKT) szolgáltatások irányítása*), illetve a NIS-ben meglévő ágazatok bővültek új alágazatokkal (*Energia ágazat: távfűtés, hidrogén; Digitális*

⁶³ Computer Security Incident Response Team - CSIRT

⁶⁴ European Network and Information Security Agency – Európai Hálózat és Információbiztonsági Ügynökség. 2004-es alakulása óta feladatköre bővült, modernizálódott, neve 2019. óta European Union Agency of Cybersecurity – Európai Unió Kiberbiztonsági Ügynökség. <https://www.enisa.europa.eu/>

⁶⁵ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályaon kívül helyezéséről (NIS 2 irányelv)

⁶⁶ Digitális megoldások a világjárvány idején. https://commission.europa.eu/strategy-and-policy/coronavirus-response/digital-solutions-during-pandemic_hu (letöltés: 2026. 01. 20.)

infrastruktúra: felhőszolgáltatók, adatközpontok, tartalomszolgáltatók, bizalmi szolgáltatók, nyilvános hírközlés). A NIS2 külön mellékletben nevezi meg az egyéb kritikus ágazatokat is (*Postai és futárszolgáltatások, Hulladékgazdálkodás, Vegyszerek gyártása és forgalmazása, Élelmiszertermelés -feldolgozás – forgalmazás, Gyártás, Kutatás*)

Az egyik jelentős változás, hogy a korábban „*alapvető szolgáltatást nyújtó szereplő*” fogalma kikerült az irányelvből, mivel nehézkes volt az alapvető szolgáltatásokat nyújtó szereplők és digitális szolgáltatók közötti különbségek meghatározása, illetve jelentős eltérések mutatkoztak a tagállamokban a szervezetek azonosítása között. Annak érdekében, hogy az alkalmazási kört jobban ki lehessen terjeszteni a gazdaság nagyobb részére és egységesebb legyen az azonosítás, az irányelv hatálya alá tartozó szervezeteket „*alapvető szervezetek*” és „*fontos szervezetek*” közé sorolja. A NIS2 részletesen megadja, hogy mely szervezeteket kell vizsgálni és az alapvető szervezetté minősíteni. Külön pontban kiemeli, hogy az (EU) 2022/2557 irányelv szerint kritikus szervezetnek minősített szervezetek alapvető szervezetek is egyben.

A NIS irányelv általános jelleggel írta elő a „*megfelelő technikai és szervezési intézkedések*” alkalmazását konkrét tartalom nélkül, a NIS2 viszont részletesen előírja a minimumkövetelményeket mind a kijelölt alapvető szervezetek, mind a CSIRT-ek részére. Külön kiemeli a kockázatelemzést, az incidenskezelést, az üzletmenet-folytonosság biztosítását, az ellátási lánc biztonságát, a hitelesítési megoldások alkalmazását, valamint a rendszeres képzéseket.

Az incidensek bejelentési kötelezettsége is szigorúbbá vált. A NIS általános megfogalmazásában a jelentős biztonsági eseményeket indokolatlan késedelem nélkül kell jelenteni a nemzeti CSIRT részére. Ennek értelmezése tagországonként változott. A NIS2 külön fejezetben részletezi a jelentéstételi kötelezettséget, többlépcsős bejelentési és visszaellenőrzési rendszert vezet be, pontosan megadva a jelentés tartalmát és határidejét.

Össességében tehát, a NIS irányelv a kiberbiztonsági együttműködés és a minimális harmonizáció alapjait teremtette meg, a NIS2 pedig egy átfogó, szigorúbb kiberbiztonsági szabályozás.

1.1.2.2. Az európai kritikus szervezetek rezilienciájáról⁶⁷

⁶⁷ Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről

Az infrastruktúrák és a kibertér napjainkra jellemző magas szintű összefonódását is jól mutatja, hogy az (EU) 2022/2557 és a NIS2 irányelvek nem csak egy időben jelentek meg, de az elkészítésük is teljes összhangban zajlott. Mindkét irányelv több pontja is hivatkozik a másikra és alapelveként fogalmazza meg a két irányelv együttes alkalmazását.

Az (EU) 2022/2557 irányelv kifejezetten a 2008/114/EK irányelv felülvizsgálatának eredményei alapján, annak leváltása és terület szabályzásának modernizálása céljából készült. Ennek egyik legszembetűnőbb példája az irányelv hatályának kiterjesztése, mely már magában foglalja – az energia és a közlekedés ágazatok mellett – a banki szolgáltatások, pénzügyi piaci infrastruktúra, egészségügy, ivóvíz, szennyvíz, digitális infrastruktúra, közigazgatás, valamint az ürtevékenységek ágazatait is. Gondolkodásmód váltást jelez, hogy az irányelv a kritikus infrastruktúrák védelme helyett a kritikus infrastruktúrákat üzemeltető szervezetek rezilienciáját fogalmazza meg:

„reziliencia: valamely kritikus szervezet azon képessége, hogy megelőzzön egy eseményt, azzal szemben védekezzen, arra reagáljon, annak ellenálljon, azt enyhítse, tompítsa, ahhoz alkalmazkodjon, és abból helyreálljon;”

Az irányelv előírja, hogy a tagállamoknak nemzeti reziliencia-stratégiát kell elfogadniuk 2026. január 17-ig, melynek feladata, hogy kijelölje a célokat, kijelölje vagy megalakítsa a nemzeti illetékes hatóságokat és az egyedüli kapcsolattartó pontot, valamint a kritikus szervezetek együttműködésének, támogatásának kereteit.

Az új irányelv is a tagországok kezébe adja a stratégia kialakítását, de már sokkal konkrétabb célokat, feladatokat határoz meg. A tagállamoknak átfogó kockázatértékelést kell készíteniük, amelynek figyelembe kell vennie a természeti katasztrófákat, baleseteket, népegészségügyi szükséghelyzeteket, hibrid fenyegetéseket, valamint ellenséges cselekményeket, ideértve a terrorizmust is. A tagállami kockázatértékelésnek ki kell terjednie a több ágazatot érintő, illetve határokon átnyúló hatásokra és a kritikus szervezetek közötti függőségekre, vagyis az interdependencia vizsgálatára is.

Az irányelv előírja, hogy a tagállamoknak 2026. július 17-ig azonosítani kell a kritikus szervezeteiket, melyek az irányelv mellékletében felsorolt ágazatok és alágazatok valamelyikébe sorolhatók, valamint a következő kritériumoknak is megfelelnek:

- a) az adott szervezet egy vagy több alapvető szolgáltatást nyújt;
- b) az említett tagállam területén működik és ott található a kritikus infrastruktúrája is;

- c) egy esemény jelentős zavart kelt a szervezet egy vagy több alapvető szolgáltatásnak biztosításában, vagy egyéb olyan alapvető szolgáltatásokban, amelyek az említett alapvető szolgáltatástól függenek.

Az irányelv pontosítja a zavart keltő hatások feltárásához szükséges követelményeket is, külön kiemelve az alapvető szolgáltatástól függők számának, a kapcsolódó ágazatok interdependencia hatásainak vizsgálatát, a gazdasági és társadalmi, környezeti és egészségügyi hatások figyelembevételét és a földrajzi sebezhetőséget. Külön kiemeli, hogy a tagállamoknak biztosítaniuk kell a kritikus szervezetek megfelelő támogatását, mely kiterjedhet módszertani útmutatásra, képzésekre, információmegosztásra, valamint az érintett szereplők közötti koordinációra.

Az európai kritikus infrastruktúrák tekintetében is új megfogalmazást ad az irányelv. Bevezeti a „különös európai jelentőségű kritikus szervezet” fogalmát, melyek hat vagy több tagállam számára nyújtanak alapvető szolgáltatásokat, ezért uniós szintű egyedi támogatásban részesülhetnek és külön szabályok szerinti tanácsadó missziók segítik őket.

A tagállamok közötti koordinációt és értesítési rendszer kialakítását is előírja abban az esetben, ha egy szervezet:

- a) olyan kritikus infrastruktúrát vesz igénybe, amely két vagy több tagállam között fizikailag össze van kötve;
- b) olyan vállalati struktúra részét képezi, amely más tagállamokban lévő kritikus szervezetekkel kapcsolatban áll;
- c) alapvető szolgáltatásokat nyújt más tagállamnak.

Az irányelvben újdonság, hogy részletesebb iránymutatást ad az azonosított kritikus szervezetek részére a saját kockázatértékelésük végrehajtására és reziliencia-intézkedéseik kidolgozására. Pontonként említi nem csak a védelmi intézkedések típusait (fizikai, üzemfolytonossági, adminisztratív, információvédelmi), hanem a rezilienciát tágabb körben érintő eszközöket is, úgymint: alkalmazkodást célzó intézkedések, következménykezelési eljárások, protokollok, kritikus funkciók és személyzet kezelése és ellenőrzése, képzések, gyakorlatok.

Az irányelv alapján az Európai Bizottság több módon is támogatja a tagországok kritikus szervezetekkel kapcsolatos munkáját.

Szervezhet *Bizottsági tanácsadó missziót*, mely segítséget nyújt az azonosítás és a reziliencia követelményei teljesítésének értékelésében, a különös európai kritikus szervezetek azonosításában, véleményezi a hozott intézkedéseket.

Létrehozta a kritikus szervezetek rezilienciájával foglalkozó csoportot, mely támogatja az Európai Bizottságot és elősegíti a tagállamok közötti együttműködést és információcserét, elemzi a tagországok stratégiáit, interdependencia vizsgálatokat hajt végre, dokumentumokat dolgoz ki és elemez.

Az Európai Bizottság támogatja a kritikus szervezeteket azzal, hogy iránymutatásokat és módszertanokat, valamint határokon átnyúló képzési tevékenységeket és a kritikus szervezetek rezilienciájának tesztelését szolgáló legjobb gyakorlatokat dolgoz ki, valamint szükség esetén uniós pénzügyi forrásokat nyithat meg.

1.2. MAGYARORSZÁG KRITIKUS INFRASTRUKTÚRÁK VÉDELMEVEL KAPCSOLATOS FŐBB LÉPÉSEI ÉS DOKUMENTUMAI

Magyarországon már a 90-es években is jelentek meg tanulmányok, szakmai írások a fontosabb létesítmények védelmének témájában. Katonai oldalról a robbantásos merényletek elleni, katasztrófavédelmi oldalról az ipari vagy természeti katasztrófák elleni védelem lehetőségeit is többen vizsgálták.

A katasztrófavédelmi szervek jogelőd szervezetei, illetve későbbiekben a Katasztrófavédelmi Koordinációs Tárcaközi Bizottság kiemelten kezelte a veszélyhelyzet kezelés, megelőzés, valamint a beavatkozás és helyreállítás feladatait és megállapították, hogy a szerteágazó felelősségi körök miatt a szakterületek önállóan nem, csak egymással együttműködve képesek ezt a tevékenységet végezni⁶⁸.

2004. május 1-jén az Európai Unió teljes jogú tagjává vált Magyarország, így már tagállamként az európai Zöld Könyv és az EU 2008/114/EK irányelve alapján megkezdődhetett a kritikus infrastruktúrák azonosításával, kijelölésével és védelmével kapcsolatos jogi háttér kidolgozása.

⁶⁸ 1150/2012. (V. 15.) Korm. határozat a Katasztrófavédelmi Koordinációs Tárcaközi Bizottság létrehozásáról, valamint szervezeti és működési rendjének meghatározásáról

2005-ben a Gazdasági és Közlekedési Minisztérium felkérésére készített tanulmány⁶⁹ alapján, majd 2007-ben a minisztériumok és az országos hatáskörű szervek együttműködésével, kezdetét vette a magyar nemzeti kritikus infrastruktúra védelmi program kidolgozása. Első jelentős jogi lépés a terrorizmus elleni küzdelem aktuális feladatairól szóló kormányhatározat⁷⁰ módosítása volt, mely előírja a „*Kritikus Infrastruktúra Védelem Európai Programjának megközelítését tükröző, a különböző ágazati feladat- és hatáskörbe tartozó kritikus infrastruktúra védelmi tevékenységek közös keretrendszerbe foglalásáról és ágazatközi összehangolásáról*” szóló előterjesztés elkészítését.

1.2.1. Magyarország korábbi szabályzói

1.2.1.1. A Kritikus Infrastruktúra Védelem Nemzeti Programja – Zöld könyv⁷¹

2008-ban került kiadásra a 2080/2008. (VI. 30.) kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról, mely fontos mérföldkőként tartalmazta a Kritikus Infrastruktúra Nemzeti Programjáról szóló Zöld Könyvet. A kormányhatározat példa értékűen teszi meg az Európai Unió Tanácsának 2008/114/EK irányelve alapján meghatározott lépéseket. Legfelső szinteken határozza meg a felelősöket, többszereplős konzultációkat rendel el az ágazatok részére, elrendeli a hazai infrastruktúra létfontosságú elemeinek védelméről szóló részletes szabályozási koncepció összeállítását, figyelembe véve a hazai, az európai és a NATO szabályzókat, az üzemeltetők és tulajdonosok alkotmányos kötelezettségeit és kiemelten a honvédelem szempontjából fontos, kritikus infrastruktúra védelmére vonatkozó követelményeket.

A kormányhatározat 1. melléklete – maga a Zöld Könyv – alapként szolgált a további konzultációk és feladatok végrehajtásához. Fő célkitűzése, hogy biztosítsa a nemzeti kritikus infrastruktúrák védelméről szóló nemzeti program megvalósítását, a jogszabályi környezet megalkotását, összegezze a kormányzati szereplők nemzeti kritikus infrastruktúrák védelmére vonatkozó álláspontját. Fontos eleme, hogy először definiálja a kritikus infrastruktúrák fogalmát és határozza meg a lehetséges ágazatok körét.

⁶⁹ KOVÁCS Ferenc (2005): *Az infrastruktúra kritikus elemeinek felmérése, védelmének és helyreállításának megszervezésére vonatkozó intézkedési javaslatok*. Gazdasági és Közlekedési Minisztérium (GKM), Budapest.

⁷⁰ 2112/2004. (V. 7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól

⁷¹ Magyarország Kormányának 2080/2008. (VI. 30.) Korm. határozata a Kritikus Infrastruktúra Védelem Nemzeti Programjáról – Zöld könyv

A Kritikus Infrastruktúra fogalma a Zöld Könyv szerint:

„Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.

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.”

A nemzeti kritikus infrastruktúrák védelmében három főbb szintet céloztak meg:

1. *Megelőzés és védelem*, a legnagyobb kockázatú elemek beazonosításával, a kockázatok csökkenthetőségének elemzésével és védelmi intézkedések alkalmazásával;
2. *Felkészülés és jelzés*, az infrastruktúra tulajdonosok és üzemeltetők, valamint az állami szervek megfelelő felkészítésével;
3. *Üzemfolytonosság és ellenálló képesség biztosítása*, a működés visszaállíthatóságára, helyettesíthetőségre vonatkozó képességek, intézkedések tervezésével, fejlesztésével, bevezetésével.

A „következmény alapú kritikusság” megközelítés alapját a következmények elfogadható mértékének meghatározása képezi (*kis hatású, komoly zavar, válsághelyzet*), amely a következő kategóriák szerint elemezhető:

- **kiterjedés szerint:** a veszteség földrajzi terület szerint értelmezhető;
- **súlyosság:** nincs hatás, minimális, mérsékelt vagy jelentős hatással járó zavar. A súlyosság meghatározásánál az is fontos tényező, hogy mely területet érinti a zavar.

Ezek alapján a Zöld Könyv megkülönböztet:

- Társadalmi hatást: érintett lakosság száma;
- Gazdasági hatást: a gazdasági veszteség jelentősége;

- Környezeti hatás: a környezetre gyakorolt zavar, kár mértéke;
 - Politikai hatást: állam és intézményei iránti bizalom csökkenése;
 - Közegészségügyi hatást: áldozatok, betegségek, súlyos sérülések száma;
 - Pszichológiai hatást: pl. vásárlói magatartás, általános viselkedés megváltozása;
 - Kölcsönös függőségi hatást: az interdependenciák erőssége, száma;
 - Alternatívák vizsgálatát: adott infrastruktúra elem nem, vagy csak nehezen helyettesíthető.
- **időbeli hatás:** arra vonatkozik, hogy egy adott infrastrukturális elemmel kapcsolatos veszteség mennyi idő elteltével fejthet ki jelentős hatást, illetve a zavar mennyi ideig kezelhető komoly hatás nélkül.

A Zöld Könyv a kritikus infrastruktúrákat veszélyeztető tényezők körét három főbb csoportba osztotta:

- szándékos cselekmények,
- természeti eredetű veszélyek,
- civilizációs, technológiai veszélyek,

valamint kiemeli, hogy támogatja az EPCIP megközelítését, vagyis alapelveként kezeli a minden fajta veszéllyel szembeni védelemre való felkészítést terrorizmus prioritással. Emellett a nemzeti Kritikus Infrastruktúra Védelem (a továbbiakban: KIV) Programjának kidolgozása és végrehajtása során a következő alapelveket határozta meg:

- *szubszidiaritás:* a tulajdonosok és az üzemeltetők felelőssége, hogy saját létesítményeik védelmét megtervezzék és arra vonatkozóan döntéseket hozzanak. a Kormányzatnak elemző, szabályozó, ellenőrző és támogató szerepe van;
- *kiegészítő jelleg:* a KIV kiegészíti a fennálló ágazati biztonsági intézkedéseket, szabályozási struktúrákat, nem azonos a fennálló veszélyhelyzet kezelés és beavatkozás rendszerével;
- *rugalmasság:* folyamatos felülvizsgálatot igénylő program, a mindenkori változásokra és kihívásokra gyorsan reagálni képes;
- *arányosság:* a védekezési stratégiák és intézkedések arányosak a mindenkori veszéllyel, melyet megfelelő kockázatkezelési módszerekkel lehet elérni. Így – ideális esetben – a védelem nem ró aránytalanul nagy terheket a szereplőkre;
- *finanszírozás:* a védelemmel kapcsolatos intézkedések finanszírozása a közreműködő szereplők felelőségi és érdekeltségi szintjéhez igazodik, figyelemmel a megállapított kockázati prioritásokra, ugyanakkor arányban áll a szereplők pénzügyi lehetőségeivel;

- *titkosság*: a kritikus infrastruktúrák védelmére vonatkozó információk cseréjének alapja a bizalom és a titkosság, mivel bizonyos információk felhasználhatók a létesítmények működésének megzavarására;
- *horizontális és ágazati megközelítés*: minden miniszter a hatáskörébe tartozó ágazat tekintetében önállóan felel az Nemzeti KIV-ben foglalt feladatai ellátásért, az ágazati feladatok végrehajtásának koordinációjáért;
- *szereplők közötti együttműködés*: valamennyi jogszabályban megszólított szereplő részt vesz a kritikus infrastruktúrák védelmében. Meghatározott feladataival és felelősségével összhangban valamennyi szereplőnek együtt kell működnie, és hozzá kell járulnia a Nemzeti KIV kidolgozásához és végrehajtásához.

A Zöld Könyv egycsatornás koordinációs és döntéshozatali mechanizmust javasolt, melyhez meghatározta a különböző szereplők főbb feladatait. Így a Kormány, a későbbiekben kijelölésre kerülő központi NKIV koordináló szerv, az államigazgatási szervek, valamint a tulajdonosok és üzemeltetők legfőbb feladatait, a teljes kritikus infrastruktúra azonosítási, kijelölési folyamat végrehajtása érdekében, valamint a kijelölt kritikus infrastruktúra elemek védelmének fejlesztésében, illetve a folyamatos kapcsolattartás érdekében. Ezek a feladatok a végrehajtás sorrendjében:

1. fogalmak tisztázása, a keretrendszer alapjainak lefektetése, mely nem eredményezhet párhuzamos szabályozást, ütközést a hatályos jogszabályokkal;
2. szektorelemzés, ágazati fogalmak, kritériumok meghatározása;
3. interdependencia elemzés;
4. kockázatelemzés, veszélyanalízis;
5. védelmi intézkedések tervezése, bevezetése;
6. a végrehajtás ellenőrzése, értékelése.

Mindezeken felül a határozat elrendeli a CIWIN-hez történő csatlakozás lehetőségeinek vizsgálatát is. A Zöld Könyv felveti a lehetőségét egy CIWIN hálózathoz kapcsolható, de önálló nemzeti, bizalmas információkezelésre alkalmas, fokozott védelmet élvező informatikai és hírközlési rendszer működtetését.

1.2.1.2. Az európai szabályzóknak való megfeleltetés⁷²

Az előző pontban tárgyalt kormányhatározat és a Zöld Könyv alapján a nemzeti kritikus infrastruktúrák védelmével kapcsolatos szakértői munka megkezdődött. Az Európai Unió Tanácsának 2008/114/EK tanácsi irányelve alapján az európai kritikus infrastruktúrák védelmével kapcsolatos ügyekben kapcsolattartó pont kijelölése volt szükséges, így a kormányhatározat a belügyminisztert jelölte ki az európai kritikus infrastruktúra védelem nemzeti kapcsolattartójaként és annak koordinációjára, valamint az Európai Bizottság részére évente küldendő jelentés elkészítésére.

Ennek érdekében felhatalmazta, hogy az ágazatok felelős minisztereivel együtt megbeszéléseket, egyeztetéseket folytasson más tagállamok kapcsolattartóival és az Európai Bizottsággal.

Emellett elrendelte egy szakmai munkacsoport létrehozását, az európai és a nemzeti kritikus infrastruktúrák azonosításához szükséges kritériumrendszert kidolgozása, valamint a potenciális európai kritikus infrastruktúrák azonosításának és kijelölésének felülvizsgálata érdekében.

A kormányhatározat külön pontban rendelte el a honvédelmi érdekből kritikus infrastruktúrák védelmére vonatkozó intézmény- és követelményrendszer kidolgozását, melyért a honvédelmi minisztert tette felelőssé.

1.2.1.3. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény⁷³

Az előző pontban említett munkacsoport a nemzeti „Zöld Könyv”, az európai és nemzeti irányelvek, valamint konzultációk és több éves szakmai munka eredményeképpen megalkotta a Lrtv.-t, mely 2013. március elsején lépett hatályba.

A törvény pontosítja az alapfogalmakat, és meghatározza az ágazatokat, a nemzeti, illetve az európai létfontosságú rendszerelemekkel kapcsolatos kijelölés vagy visszavonás folyamatát, az általános javaslattevő hatóság feladatát, valamint a folyamathoz kapcsolódó feltételeket.

⁷² 1249/2010. (XI. 19.) számú, „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” szóló határozat

⁷³ a továbbiakban: Lrtv.

A törvény – többek között – meghatározta az ágazati és horizontális kritérium, a létfontosságú rendszerelem, az üzemeltető fogalmát.

A későbbiekben, az EU NIS irányelv megjelentését követően, többször is módosításra, pontosításra kerültek az alapfogalmak, illetve újként az „*alapvető szolgáltatás*”, az „*alapvető szolgáltatást nyújtó szereplő*” fogalmak kerültek a törvény értelmező rendelkezései közé⁷⁴. A későbbiekben még bővült a „*helyszíni ellenőrzést lefolytató szerv*”, „*rendkívüli esemény*” és az „*európai létfontosságú rendszerelem*” fogalmakkal⁷⁵.

A törvény részletesen tárgyalja a nemzeti létfontosságú rendszerelemek azonosításának és kijelölésének, valamint az azonosítás vagy kijelölés visszavonásának teljes folyamatát, megadva a lépéseket és a különböző lépések és feladatok egymáshoz viszonyított határidejét.

2020-tól kezdődően új paragrafusokként kerültek be a törvénybe – illetve több alkalommal módosultak is – a nemzeti létfontosságú rendszerelemek körén belül kiemelt védelmet igénylő „*alapvető szolgáltatásokat nyújtó szereplők*” kijelölésére és nyilvántartására vonatkozó rendelkezések, valamint a nemzeti és az európai létfontosságú rendszerek kijelölésének, nyilvántartásának és ellenőrzésének részletesebb, egyéb kritériumokkal kiegészített szabályai.

A 2020. évi XXXI. törvény módosító rendelkezései alapján több változás is bekerült a Lrtv. szövegébe. Az alapvető szolgáltatásokat nyújtó szereplők azonosítása érdekében több pontban módosult az ágazatok és alágazatok tartalma.

1.2.1.4. Az Lrtv. végrehajtásához és az ágazatok szabályozásához kapcsolódó kormányrendeletek

A Lrtv. megszabta az ágazatokra vonatkozó, azok speciális szabályait és ágazatspecifikus kiegészítő rendelkezéseit meghatározó ágazati kormányrendeletek megalkotását. Az ágazatok különálló kormányrendeleteinek célja az ágazati kritériumok kidolgozása, a résztvevő hatóságok kijelölése és alapfeladataik meghatározása. Az Lrtv. által meghatározott 10 ágazat vonatkozásában végül kilenc ágazati kormányrendelet készült el.

⁷⁴ 2020. évi XXXI. törvény 123. §. Hatályos: 2020. VII. 1-től

⁷⁵ 2021. évi L. törvény 28. § (1). Hatályos: 2021. VII. 1-től

Az Lrtv. legfontosabb támogató eleme a végrehajtásáról szóló kormányrendelet (a továbbiakban: Lrtv.vr.) volt⁷⁶. A kormányrendeletet 2020.⁷⁷ és 2021.⁷⁸ években bővítették és módosították, melyek az Lrtv. módosításait, kiegészítéseit volt hivatott követni, illetve az azonosítási és kijelölési folyamat részletesebb leírásával és kiegészítéseivel a hatósági és az üzemeltetői oldal kommunikációját támogatta.

A végrehajtás érdekében az Lrtv.vr. újabb fogalmakat definiált a törvényben megfogalmazottakat kiegészítve. Bekerültek az „azonosítás”, az „azonosítási vizsgálat” és a „kockázatelemzés” fogalmi. Az Lrtv.vr. megadta az azonosítási jelentés elkészítésének szabályait és annak tartalmát, kiemelve az alapvető szolgáltatások vizsgálatát is, illetve a létfontosságú rendszerelemmé váló kijelölés és a visszavonás folyamatát. Hivatkozik a BM OKF honlapjára is, mely további segítséget és a folyamathoz szükséges okmányokat, okmánymintákat is tartalmazza.

Ki kell emelni, hogy az Lrtv.vr. már a potenciális létfontosságú rendszerelem azonosítási folyamatában is biztonsági összekötő személy meglétét igényli, akinek képzési követelményeit és foglalkoztatásának feltételeit ugyancsak részletesen taglalta.

Az alapvető szolgáltatást nyújtó szereplőként való azonosítás, illetve törlés automatikusan kapcsolódik a nemzeti létfontosságú rendszerelem kijelölési folyamatához, de külön elemzést és eljárást igényel, melynek eredményeképpen az üzemeltetőt felveszik az alapvető szolgáltatásokat nyújtó szereplők jegyzékébe is.

Az Lrtv.vr. a folyamat támogatása és követhetősége érdekében kötelezi az üzemeltetőt az Integrált Hatósági Rendszer (a továbbiakban: IHR) használatára, mely alkalmas a teljes azonosítási és kijelölési folyamathoz szükséges adat- és okmánykezelésre, különböző bejelentésekre, hivatalos kapcsolattartásra és a Lrtv. szerinti bírság fizetési kötelezettségének teljesítésére is. Jogi és technológiai problémák elhárítását követően az IHR végül 2022. január 01. után volt elérhető Integrált Hatósági Ügyviteli Rendszer néven. 2024 óta már nem elérhető, mivel az érvénybe lépő új jogszabályok alapján a hivatásos katasztrófavédelmi szervek egyes hatósági és szakhatósági hatáskörei a kormányhivatalokhoz kerültek.⁷⁹

⁷⁶ 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

⁷⁷ 375/2020. (VII. 30.) Korm. rendelet egyes kiberbiztonsági tárgyú és egyéb kormányrendeletek módosításáról

⁷⁸ 375/2021. (VI. 30.) Korm. rendelet az egyes hatósági eljárásokat érintő egyszerűsítések érdekében szükséges kormányrendeletek módosításáról

⁷⁹ <https://katasztrofavedelem.hu/36732/ihr-integralt-hatosagi-ugyviteli-rendszer-karbantartas> (letöltés: 2025.01.28.)

Az Lrtv.vr. tartalmazta a minden ágazatra vonatkozó horizontális kritériumok adatait, emberi veszteség, gazdasági, társadalmi, politikai, környezeti hatás és az ellátási láncot figyelembe vevő védelem kritériumának bontásában. 2020-ban történt módosítással az Lrtv.vr. tartalmába került be az alapvető szolgáltatások jegyzéke.

Az Lrtv.vr. a kijelölt létfontosságú rendszerelemek részére részletesen meghatározta az Üzemeltetői Biztonsági Terv (a továbbiakban: ÜBT) elkészítésének szabályait és pontos felépítését, az ellenőrzésre és együttműködésre vonatkozó szabályokat és a nyilvántartás és adtakezelés alapvetőbb előírásait. 2020-ban kiegészített Kormányrendeletben⁸⁰ új pontként jelet meg a kijelölt létfontosságú rendszerelem üzemeltetéséhez kapcsolódó, kötelezően végrehajtandó, éves komplex gyakorlat. A komplex gyakorlatot a hivatásos katasztrófavédelmi szerv központi szerve rendeli el, és az ágazati hatóságokkal együtt ellenőrzi és minősíti a végrehajtását.

Az Lrtv.vr. bár elég pontos keretet ad a védelem kialakításához, de a védelmi intézkedések konkrét tervezését az üzemeltető/tulajdonos kezébe adják, így ezek a tervek, illetve a megvalósítás erősen függ a kijelölt létfontosságú rendszerelem üzemeltetőjének és/vagy tulajdonosának anyagi lehetőségeitől, szakmai tudásától és hozzáállásától.

Az ágazatok vonatkozásában a létfontosságú rendszerelemek azonosításával, kijelölésével és védelmével kapcsolatos részletes szabályok kidolgozását az ágazati szakhatóságok hajtották végre és – a társadalombiztosítás ágazat kivételével – önálló ágazati kormányrendeletekben jelentették meg:

- energetika (2013);
- rendvédelmi szervek (2013);
- agrárgazdaság (2013);
- vízgazdálkodás (2013);
- egészségügy (2015);
- pénzügy (2015);
- honvédelem (2015);
- infokommunikáció (2017);
- közlekedés (2019).

Az energetikai ágazat szabályozása inkább technikai jellegű megközelítést adott, részletes, mérhető küszöbértékekhez kötötte a létfontosságú rendszerelemek azonosítását, különösen a

⁸⁰ 375/2020. (VII. 30.) Korm. rendelet

villamosenergia-, földgáz- és kőolajszektorban. Fontos megegyezni, hogy a kormányrendelet nem a tulajdonosokat, hanem az üzemeltetőket szólította meg, akik a tényleges működésért és a védelem megszervezéséért felelősek. A kormányrendelet külön kiemeli a villamosenergia-rendszer újraindítását biztosító képességek (Black Start) nyújtását, melyek önmagukban is kijelölési kritériummá válhatnak.

A rendvédelmi ágazat kormányrendelete szervezeti alapú és funkcionális megközelítést alkalmazott. A kijelölés folyamata nem számszerű küszöbértékekre, hanem az adott szervek alapfeladatainak kiesésére és azok pótolhatóságára összpontosít. A szabályozás nem tárgyalja az alapvető szolgáltatást nyújtó szereplők jegyzékének vizsgálatát.

Az agrárgazdasági ágazat szabályozása a termelési lánc figyelembe vételével készült. A rendelet részletesen felsorolja azokat a tevékenységeket és létesítményeket, amelyek létfontosságú rendszerelemmé válhatnak, a genetikai erőforrásoktól kezdve az élelmiszerfeldolgozáson át a logisztikai és ellátási rendszerekig. Egyedi sajátosság, hogy a biológiai pótolhatóság – például génbankok esetében – képezheti a kijelölés alapját. Az ágazatban a szakmai képesítés szerepe hangsúlyosabb, a biztonsági összekötő személynek az adott tevékenységhez kapcsolódó speciális végzettséggel is kellett rendelkeznie.

A vízgazdálkodási ágazat szabályozása rendszerszintű és infrastruktúra-központú volt. A kritériumok részletesen, funkcionális bontásban jelennek meg (ivóvízellátás, szennyvízkezelés, árvízvédelem) és egyértelmű küszöbértékekhez kötöttek. A kormányrendelet külön kiemeli az európai vízgazdálkodási létfontosságú rendszerelemek vizsgálatát, a határon átnyúló hatások esetében. Új fogalomként a kormányrendelet bevezeti a víz ágazatra vonatkozó rendkívüli esemény fogalmát.

Az egészségügyi ágazat szabályozása komplexebb, mivel nemcsak infrastruktúrákat, hanem szolgáltatási rendszereket és készleteket is vizsgál, melyekre külön biztonsági kategóriákat vezet be. Jelentős eltérés más ágazatok hatósági feladataihoz képest, hogy az azonosítási és kijelölési folyamathoz egy szakértői bizottságot hoznak létre.

A pénzügyi ágazat szabályozása viszonylag szűk és intézményközpontú. A kijelölés alapját elsősorban a piaci szerep, a részesedés és a rendszerstabilitásban betöltött szerep képezi. Sajátosság, hogy a rendelet nagymértékben a horizontális kritériumokra támaszkodik, és kevésbé tartalmaz ágazatspecifikus küszöbértékeket, ugyanakkor hangsúlyosan jelenik meg az informatikai rendszerek és az adatbiztonság védelme.

A honvédelmi ágazat szabályozása erősen eltért a többi ágazattól. Egyedülálló módon lehetőséget biztosított más ágazatok rendszerlemeinek honvédelmi célú kijelölésére, illetve bevezette a „kettős kijelölés” fogalmát. További sajátosság a gyorsított kijelölési eljárás, amely válsághelyzetekben rendkívül rövid határidőkkel működött. A szabályozás erősen centralizált, minden hatáskör a Honvédelmi Minisztérium szerveihez volt kötve.

Az infokommunikációs ágazat szabályozása a hálózati jellegre koncentrál. A kritériumok az országos lefedettségre, a lakossági elérésre és az állami működés támogatására épülnek. Emellett gazdasági küszöbértékek (pl. árbevétel) is megjelennek, ami más ágazatokban nem.

A közlekedési ágazat szabályozása elkülönítve kezeli alágazatait és hálózati szemléletű. A kijelölésnél első sorban a forgalmi jelentőséget, a nemzeti érdekeket és a közlekedési formák kapcsolódó csomópontjait vették figyelembe. Sajátosság, hogy nincs külön javaslattevő hatóság, ami nagyobb szerepet ad az üzemeltetőknek és a kijelölő hatóságoknak.

A mára hatálytalan ágazati kormányrendeletek bővebb ismertetőjét az 1. sz. melléklet tartalmazza.

1.2.2. Magyarország jelenleg hatályos szabályzói

1.2.2.1. 2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről

Ahogy az előző fejezetekben láthattuk, az (EU) 2022/2557 irányelv megjelenése mellett, hogy felülvizsgálta a kritikus infrastruktúrák korábban hatályos szabályzóit, modernebb, előremutató gondolkodásmódot hozott a területen. Ennek a gondolkodásmódnak az átültetése a magyar jogrendbe már a Kszetv. legelső bekezdésében fellelhető. A védelem és a szolgáltatások folyamatosságának biztosítása már nem elegendő megfogalmazás. A Kszetv. az állam, a társadalom és a gazdaság ellenálló képességének növeléséről, a nemzeti ellenálló képességi rendszer fejlesztéséről, az egyes függőségekből eredő ellátási láncok üzemfolytonos biztonságáról szól és kiemeli, hogy a kritikus szervezetek ellenálló képessége a nemzeti ellenálló képesség rendszerének meghatározó része. A kritikus szervezetek és a kritikus infrastruktúrák ellenálló képességével kapcsolatos feladatokért a katasztrófavédelmi törvény szerint a katasztrófák elleni védekezésért felelős miniszter a felelős.⁸¹

⁸¹ 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról, 8.§ (2) bekezdés, i) pont

A nagyobb léptékű szabályzói modernizálás, az új EU irányelvek megjelenése szükségessé tette a magyarországi kritikus infrastruktúrákkal kapcsolatos szabályzók felülvizsgálatát, módosítását. A jogalkotók úgy látták, hogy érdemesebb egy teljesen új, alapjaitól újraépített jogszabályi környezetet kialakítani a kritikus infrastruktúrák védelmére, illetve az EU irányelvekkel való összehangolás érdekében a kritikus szervezetek által üzemeltetett kritikus infrastruktúrák rezilienciájának növelésének szabályozására.

Az értelmező rendelkezések bővítésére, módosítására mindenképpen szükség volt, az EU irányelveivel és a magyarországi kibervédelmi szabályzókval való teljes összhang megteremtése érdekében. Bekerült a Kszetv. fogalmai közé több olyan új meghatározás, amelyek a hatósági eljárások, az EU és nemzeti felügyelet és feladatrendszer kialakítása érdekében szükségesek (pl.: kockázat alapú gondolkodás, függőség, ellátási lánc, kritikus munkakör). Új fogalomként került be a jogszabályba a „*kontrollált rendkívüli esemény*”, amely

„a kritikus infrastruktúra vagy az alapvető szolgáltatás olyan mértékű károsodását, sérülését, minőségének romlását vagy mennyiségének fennakadását eredményezi, amely nem jár a kritikus infrastruktúra vagy az alapvető szolgáltatás megszűnésével, kiesésével, nem éri el a rendkívüli esemény kezelésében érintett szervek irányába történő bejelentés küszöbértékét, és amelynek kezelését a kritikus szervezet és szerződött partnerei önállóan képesek végrehajtani”

Az kritikus szervezetek és infrastruktúrák kijelöléséhez szükséges, az ágazatoktól függetlenül vizsgálendő horizontális kritériumok a Lrtv.vr. megfogalmazásától teljesen eltérően, a Kszetv. modernebb gondolkodásmódjára tekintettel lettek kialakítva, előtérbe helyezve az interdependencia és a gazdasági szerep kérdéseit:

- szervezet alapvető szolgáltatása más entitástól függ vagy kölcsönös függőség létezik másik kritikus szervezettel vagy infrastruktúrával, akár szolgáltatás, illetve közúti vagy vasúti infrastruktúra tekintetében;
- szervezet nettó árbevétele a vizsgálatot megelőző 5 év során bármely évben meghaladta a 10 milliárd forintot;
- a szervezet Magyarországon egyedülként nyújtja az adott alapvető szolgáltatást;
- a szervezet alapvető szolgáltatásában bekövetkezett rendkívüli esemény jelentős hatással lehet a közrendre, a közbiztonságra, a közegészségügyre vagy katasztrófavédelmi, lakosságvédelmi, nemzetbiztonsági, terrorelhárítási szempontokra, függőségekre;

- alapvető szolgáltatásában bekövetkezett rendkívüli esemény jelentős rendszerszintű kockázatot idézhet elő, különösen azokban az ágazatokban, ahol a rendkívüli eseménynek határokon átnyúló hatása lehet, vagy az ellátási lánc sérül,
- a szervezet olyan üzemanyag töltőállomást üzemeltet, amely közlekedési vagy üzemanyag ellátási szempontból stratégiainak minősül, vagy
- a szervezet nemzetbiztonsági védelem alatt áll.

Az „*alapvető szolgáltatás*” fogalma módosított szövegezéssel, de alapjaiban azonos mondanivalójával megmaradt a Kszetv.-ben, de az „*alapvető szolgáltatást nyújtó szervezetek*” és a „*létfontosságú rendszerek helyét*” a kritikus szervezetek fogalma vette át:

„kritikus szervezet: olyan alapvető szolgáltatást nyújtó szervezet, amelyet a kijelölő hatóság a III. Fejezetben meghatározottak szerint kijelölt és elengedhetetlen Magyarország társadalmi, gazdasági stabilitásához és a biztonság, a környezet, a közegészségügy, a védelmi képességek és a nemzeti ellenálló képességi rendszer fenntartásához, ...”

a kritikus infrastruktúra fogalma pedig visszakerült a szabályzó rendszerbe:

„kritikus infrastruktúra: olyan eszköz, létesítmény, építmény, berendezés, hálózat, rendszer, vagy ezek része, amely az alapvető szolgáltatás nyújtásához szükséges, ...”

Így tehát, az alapvető szolgáltatást nyújtó szereplők és a korábban létfontosságú rendszerek egy eljárás alá kerültek, közös „*kritikus szervezet*” megnevezéssel. Megjegyzendő, hogy a magyarországi kibervédelmi törvény⁸² a kijelölt kritikus szervezeteket „*alapvető szervezet*” kategóriába is besorolja.

Annak érdekében, hogy a potenciális kritikus szervezetek a lehető legpontosabban megállapíthassák besorolásukat, a Kszetv. mellékletében elérhető táblázat foglalja össze az ágazatokat, alágazatokat és az alágazatokhoz tartozó alapvető szolgáltatások listáját.

Az „*Üzemeltetői biztonsági terv*” helyett, hasonló elvekkkel és tartalommal „*Ellenálló képességi terv*” került be a Kszetv. szövegébe.

Az (EU) 2022/2257 irányelv előírásainak megfelelően a Kszetv. elrendeli a kritikus szervezetek ellenállóképességének növelése tekintetében Magyarország nemzeti stratégiájának, illetve az

⁸² 2024. évi LXIX. törvény Magyarország kiberbiztonságáról

ehhez szükséges nemzeti kockázatértékelés elveinek kidolgozását, melyek 2025-ben külön kormányhatározatokban jelentek meg^{83,84}.

A Kszetv. részletesen taglalja a kritikus szervezetek és infrastruktúrák kijelölésének, hatósági felügyeletének, nyilvántartásának szabályait, az ellenállóképességért felelős vezető kötelmeit, melyeket az értekezésem 2. fejezetében vizsgálok.

Pozitív változás, hogy a kijelölt kritikus szervezetek támogatói rendszere, illetve annak lehetőségei már törvényi szinten megjelennek. A támogató funkciók legfelsőbb szerve az Ellenálló Képességért Felelős Vezetők Tanácsadó Bizottsága, mely közvetlen kapcsolatot biztosít a kritikus szervezetek és a hatóságok között. A támogatói rendszer lefontosabb előnye az együttműködés, mely lehetőséget teremt arra, hogy a magyarországi kritikus szervezetek és infrastruktúrák ne elkülönítve, hanem egy entitásként funkcionáljanak. Lehetőség van:

- módszerek, útmutatók, segédletek kidolgozására;
- az ellenálló képesség mérésére, tesztelésére szolgáló gyakorlatok megosztására;
- tanácsadó személy vagy csoport kijelölésére, kirendelésére;
- esettanulmányok közös elemzésére;
- az ellenállóképességért felelős vezetők központi továbbképzésére;
- pályázatok beadásának támogatására;
- tudományos kutatás, fejlesztés, publikáció közzétételére;
- ha szükséges és közérdekű célból indokolt, pénzügyi támogatás biztosítására.

A hatósági szinten is jelennek meg új szervezeti elemek. A kritikus szervezetek vonatkozásában az Egyedüli Kapcsolattartó Pont látja el a nemzetközi összekötő feladatokat, az Ellenálló Képesség Fejlesztési Munkacsoport pedig a nemzeti stratégia és feladatrendszer, illetve az ehhez kapcsolódó jogszabályi háttér kidolgozásáért felel.

1.2.2.2. Kormányrendelet a Kszetv. végrehajtásáról⁸⁵

⁸³ 1192/2025 (VI. 5.) Korm. határozat Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti stratégiáról

⁸⁴ 1191/2025 (VI.5.) Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti kockázatértékeléséről

⁸⁵ A 474/2024. (XII. 31.) Korm. rendelet a kritikus szervezetek ellenállóképességéről szóló törvény végrehajtásáról

Mivel a Kszetv. hatálytalanította a Lrtv.-t és a kapcsolódó kormányhatározatokat, a Kszetv.vr. kiadásának célja az azonosítási és kijelölési folyamat hatósági részleteinek újrafogalmazása, összefűzése.

A korábbi szabályozások szerinti ágazati kijelölő és javaslattévő hatóságok megszűntek. A Kszetv.vr. alapján az általános kijelölő hatóság a hivatásos katasztrófavédelmi szerv központi szerve⁸⁶, energetikai ágazat kijelölő hatósága pedig az állam villamosenergia-, földgáz- és távhőellátással, víziközmű-szolgáltatással, valamint állami hulladékgazdálkodási közfeladat díjszabályozásának előkészítésével kapcsolatos feladatait ellátó, önálló szabályozó szerve⁸⁷ lett.

A Kszetv.vr. tovább részletezi az európai és a nemzeti kritikus szervezetek kijelölési eljárásának szabályait, illetve első lépésként bevezeti a kritikus szervezetek és infrastruktúrák azonosítására vonatkozó szabályokat és előírja az ellenálló képességi terv (a továbbiakban: EKT) elkészítését. Mindezekről részletesebben az értekezés 2. fejezete szól.

A kritikus szervezetek kockázatértékelése tekintetében előírja az általános kijelölő hatóság által a honlapján közzétett ellenálló képességi mátrix (a továbbiakban EKM) és kockázatelemzési módszertani segédlet⁸⁸ alkalmazását, illetve általános megfogalmazással pontokba szedi a kockázatértékelés és kezelés feladatait.

Az „ágazati javaslattévő hatóság” megnevezés helyett az „ágazati szakhatóság” került be a Kszetv.vr. szövegezésébe, megváltozott feladatkörökkel. A Kszetv.vr. szerint a „*kijelölési eljárásokban előzetes szakhatósági állásfoglalásnak nincs helye*”, de a szakhatóságok sok helyen jelennek meg támogató, adatközlő funkcióval. Az azonosítási eljáráshoz, az ágazati kritériumok teljesülésének vizsgálatához, hatósági ellenőrzéshez megadja a szükséges adatokat a kijelölő hatóság részére. Részt vesz a kijelölő és ellenőrző hatóság felkérésére az ágazatspecifikus kritériumok vizsgálatában, a komplex ellenállóképességi gyakorlaton, ellenőrzéseken. Tagokat delegál az Ellenálló Képességért Felelős Vezetők Tanácsadó Bizottságába, az ideiglenes ágazati tanácsadó csoportokba. A Kszetv.vr. áttekintésekor jól látható, hogy a szakhatóságok feladatai nem csökkentek az ágazati kormányrendeletek megszűnésével, de hatáskörük, jogaik – a kritikus szervezetek vonatkozásában – átkerültek a kijelölő, ellenőrző és nyilvántartó hatóság kezébe.

⁸⁶ Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (2026.01.31.)

⁸⁷ Magyar Energetikai és Közmű-szabályozási Hivatal (2026.01.31.)

⁸⁸ XLSX alapú táblázatos formában letölthető a BM OKF weblapjáról (<https://www.katasztrofavedelem.hu/35635/letoltheto-dokumentumok-es-kitoltesi-segedletek>) (2026.02.07.)

A kritikus szervezetek ellenállóképességének mérésére – a korábbi szabályzóknak már szereplő – gyakorlatokat kell szervezni és végrehajtani. A gyakorlatok több szinten, akár eltérő szakmai elemek ellenállóképességének vizsgálatára is szervezhetők. A komplex ellenállóképességi gyakorlatot a kijelölő és ellenőrző hatóság rendeli el és ellenőrzi, az éves ellenállóképességi gyakorlatot a kritikus szervezet önállóan szervezi és hajtja végre. Ezen gyakorlatok szabályait a Kszetv.vr. részletesen megadja, de az ágazatspecifikus tervezési és szervezési feladatokat a szakhatóságok és a kritikus szervezetek kezébe adja.

A kritikus szervezetek támogatásáról a Kszetv. kiegészítéseként a Kszetv.vr. is hasonlóképpen rendelkezik.

A Kszetv.vr. nagyobb terjedelmű harmadik része a hatálytalanított ágazati kormányrendeletek helyében tárgyalja a különböző ágazatok ágazati kritériumait, részletesen, alágazati bontásban.

Fontos megjegyezni, hogy a kritikus szervezetek rezilienciájáról szóló (EU) 2022/2257 irányelvvel való jogharmonizáció miatt a honvédelmi és közigazgatási ágazat, illetve több alágazat szervezetei, infrastruktúrái nem jelölhetők ki kritikus szervezetté, infrastruktúrává.⁸⁹ Annak érdekében, hogy az ország védelme és a nemzetgazdaság szempontjából fontos alapvető szolgáltatásokat nyújtó ezen szervezetek, infrastruktúrák védelme folyamatos maradjon, a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvényben (a továbbiakban: VBÖ) tett módosítással ezen szervezetek és infrastruktúrák *jelentős szervezetekké, infrastruktúrákká* jelölhetők ki.

Az ágazati kormányrendeletekből átemelt részletes kritériumok is pontosításra kerültek, kibővültek, követve az (EU) 2022/2257 irányelvét:

Az ágazati kormányrendeletek alágazatai besorolásai nem változtak.

Az egészségügy ágazat alágazatai új csoportosításokba kerültek, figyelembe véve az alapvető szolgáltatások biztosítása szerinti felosztást. Így külön alágazatba került a gyógyszerellátás, az egészségügyi eszközellátás és a vérellátás, viszont összevont közegészségügyi alágazatba kerültek a laboratóriumi szolgáltatások, valamint külön betegellátás alágazatba az előzőekben nem sorolt egészségügyi szolgáltatások.

Az energia ágazatban megmaradtak a villamos energia, kőolaj, földgáz és távfűtés, távhűtés alágazatok és új alágazatként jelent meg a hidrogén, mely termelés, szállítás és tárolás szervezeteit, infrastruktúráit emeli ki.

⁸⁹ 2024. évi LXXXIV. törvény indoklás Kszetv-hez (Közlönyállapot: 2024.12.30.), 117-125., 127-128. §, 2. melléklet

Az infokommunikációs technológiák ágazatban szereplő alágazatok egy közös digitális infrastruktúra alágazat alá lettek besorolva, kiegészülve a DNS és doménnév szolgáltatásokkal, viszont kikerült a jogszabályból a postai szolgáltatás. Új alágazatként a világűr, űralapú szolgáltatások nyújtásának támogatása került be a kormányrendeletbe, ezen belül a műholdas rendszerek földi kiszolgáló létesítményeivel kapcsolatos szervezetek és infrastruktúrák jöhetnek szóba.

A társadalombiztosítás ágazat kikerült az ágazati felsorolásból, központi kormányzati közigazgatás ágazat került be, több pontban részletezett alapvető szolgáltatásokkal.

A közlekedés ágazatban megmaradtak a közúti, vasúti, vízi és légi közlekedés alágazatok, új alágazatként a tömegközlekedés került be a jogszabályba. A tömegközlekedés vonatkozásában szűkíti a kört, hogy a főváros és a megyeszékhelyek közösségi közlekedésére vonatkozó szervezetek és infrastruktúrák minősülhetnek kritikusnak. A Lrtv. a közlekedés alágazataként szerepeltette a logisztikai központokat, de a Kszetv.vr. már külön nem szerepelteti. A közlekedés alágazataiban szereplő kiszolgáló létesítmények ezeket a központokat lefedhetik.

A pénzügy ágazat alágazati közül a banki szolgáltatások és a pénzügyi piaci infrastruktúra kerül alágazati besorolásba, a korábbi készpénzellátás alágazat már nem szerepel külön besorolásban, mivel az alágazatok alapvető szolgáltatásai ezt lefedik.

A víz ágazatban az ivóvíz és a szennyvíz kezelésével kapcsolatos alágazatok szerepelnek, rövid, konkrét kritériumokkal, de nem került bele az új szabályozásba a felszíni és felszín alatti vizek minőségellenőrzése, a vízbázisok védelme és az árvízi védművek alágazati sem.

Nagy segítséget nyújthat és egységes értelmezést ad a kritikus szervezetek részére a Kszetv.vr. 1. sz. melléklete, mely meghatározza az ellenállóképességi szinteket és ellenállóképességi követelményeket sorol fel ezen szintek függvényében.

A Kszetv.vr. 1-3 ellenállóképességi szintet különböztet meg, három csoportban:

- a szervezet által nyújtott szolgáltatás és a rendkívüli esemény hatása alapján;
- a szervezet által nyújtott szolgáltatást igénybe vevők száma alapján;
- a szervezet által nyújtott szolgáltatás földrajzi lefedettsége alapján.

Az ellenállóképességi követelményeknek két csoportját különbözteti meg. Azon követelmények csoportja, melyekre az ellenállóképességi szinttől függetlenül intézkedni kell.

Ilyen követelmény a minőségirányítási rendszer, információbiztonsági rendszer működtetése, redundancia, beléptetés, fizikai védelem, stb.

Illetve azon követelmények csoportja, melyekre az ellenállóképességi szinttől függően kell intézkedni. Például egy 1-es (alacsony) ellenállóképességi szintű szervezet nem köteles a telephelyén kívül húzódó infrastruktúráit őriztetni, kamerával védeni. Egy 3-as szintű szervezetre szigorúbb védelmi követelmények vonatkoznak.

A Kszetv.vr. mellékleteiben részletes leírás található még az EKT tartalmi követelményeire, a jogszabálysértésekre és a közigazgatási bírság összegére.

1.2.2.3. Az ország védelme és biztonsága szempontjából jelentős szervezetek és infrastruktúrák védelmével foglalkozó jogszabályok

A kritikus szervezetek rezilienciájáról szóló (EU) 2022/2257 irányelvvel való jogharmonizáció miatt tehát a Kszetv. és a Kszetv.vr. nem vonatkozik a honvédelmi és közigazgatási ágazatokra, illetve több ágazat alágazataira, így ezek szervezetei, infrastruktúrái nem jelölhetők ki kritikus szervezetté, infrastruktúrává.⁹⁰

Ezen ágazatok, alágazatok szervezetei, infrastruktúrái viszont az ország védelme és a nemzetgazdaság szempontjából fontos alapvető szolgáltatásokat nyújtanak, ezért más irányú szabályozással el kellett érni, hogy ugyanazon jogok illessék és ugyanazon kötelezettségek terheljék ezeket a szervezeteket és infrastruktúrákat is, mint a kritikussá kijelölteket. A Kszetv.vr. módosító rendelkezései alapján, VBÖ kiegészítésével, módosításával ezek az említett szervezetek és infrastruktúrák az ország védelme és biztonsága szempontjából *jelentős szervezetekké és infrastruktúrává* jelölhetők ki, a következő ágazatokban és alágazatokban:

- Egészségügyi ágazat: mentési tevékenység, egészségügyi tartalékok képzése;
- Gyártás ágazat: elsődleges fémgyártás, gépgyártás, elektromos berendezések, készülékek és alkatrészek gyártása, közlekedési eszközök gyártása, vegyipar;
- Honvédelem ágazat: honvédelmi szempontból fontos rendszerek és létesítmények, védelmi ipar;
- Hulladékgazdálkodás ágazat: települési nem veszélyes hulladék gazdálkodás és veszélyes hulladék gazdálkodás;

⁹⁰ 2024. évi LXXXIV. törvény indoklás Kszetv-hez (Közlönyállapot: 2024.12.30.), 117-125., 127-128. §, 2. melléklet

- Infokommunikációs technológiák ágazat: postai szolgáltatások, IKT-szolgáltatások irányítása, futárszolgáltatás, digitális szolgáltatók;
- Közigazgatás ágazat: központi kormányzati közigazgatás, rendvédelmi szervek;
- Közlekedés ágazat: logisztika;
- Pénzügy ágazat: adó- és vámigazgatás;
- Víz ágazat: árvízi védművek, műtárgyak és tározók.

A VBÖ a stratégiai fontosságú szervezeteket és létesítményeket alapvetően a Kszetv. alapján kezeli, a Kszetv. rendelkezései az irányadóak, de fontos különbség, hogy mivel ezek az ország biztonsága szempontjából érzékeny területek, nem tartoznak az Európai Unió felügyelete alá. Ez azt jelenti, hogy róluk nem kell adatot szolgáltatni az Európai Bizottságnak, és nem minősülhetnek közös európai kritikus infrastruktúrának sem.

A VBÖ kiemelt módosítása, hogy a honvédelmi ágazat, speciális ágazati szabályok révén, szabad kezet kap a kijelölésben, sőt lehetősége van más ágazatokban honvédelmi szempontból jelentős fontosságúnak kijelölni azokat a szervezeteket, infrastruktúrákat, melyek nélkülözhetetlenek az ország védelméhez. Erre lehetősége van akár kettős kijelöléssel is. Az ország védelme és biztonsága szempontjából jelentős szervezetek és infrastruktúrák kijelölésével kapcsolatos ütközések elkerülése érdekében a VBÖ a következő fogalmakat határozta meg:

- *jelentős kettős kijelöléssel nem érintett szervezet, infrastruktúra*: olyan szervezet, infrastruktúra, amelyet csak a honvédelmi ágazati kijelölő hatósága jelölt ki nem honvédelmi ágazatban, az általános kijelölő hatóság sem kritikusnak, sem jelentősnek nem jelölte ki;
- *jelentős kettős kijelölésű szervezet, infrastruktúra*: olyan szervezet, infrastruktúra, melyet a honvédelmi ágazati kijelölő hatósága jelentőssé kijelölt és az általános kijelölő hatóság is kijelölte vagy kritikus, vagy jelentős szervezetté, infrastruktúrává;
- *jelentős honvédelmi ágazaton kívüli szervezet, infrastruktúra*: minden kettős kijelölésű jelentős szervezet, infrastruktúra és minden kettős kijelöléssel nem érintett jelentős szervezet, infrastruktúra;
- *jelentős honvédelmi ágazaton belüli szervezet, infrastruktúra*: az a jelentős szervezet, infrastruktúra, amelyet a honvédelmi ágazati kijelölő hatóság jelölt ki honvédelmi ágazatban;

- *jelentős honvédelmi kijelölésű szervezet, infrastruktúra*: minden honvédelmi ágazaton belüli jelentős szervezet, infrastruktúra és minden honvédelmi ágazaton kívüli jelentős szervezet, infrastruktúra összessége.

A VBÖ 2024. évi módosításához és kiegészítéséhez tartozó végrehajtási kormányrendelete az ország védelme és biztonsága szempontjából jelentős szervezetek ellenálló képességéről szóló 475/2024. (XII. 31.) Korm. rendelet (a továbbiakban: VBÖ.vr.), mely alapján az ország védelme és biztonsága szempontjából jelentős szervezetek és jelentős infrastruktúrák általános kijelölő hatóságaként, ellenőrző hatóságaként és nyilvántartó hatóságaként a hivatásos katasztrófavédelmi szerv központi szervét jelöli ki. Az ország védelme és biztonsága szempontjából jelentős honvédelmi szervezetek és jelentős honvédelmi infrastruktúrák honvédelmi ágazati kijelölő, ellenőrző és nyilvántartó hatóságaként pedig a honvédelemért felelős minisztert jelöli ki.

A VBÖ.vr. meghatározza a honvédelmi ágazatra vonatkozó különös szabályokat a kijelöléssel, nyilvántartással és ellenőrzéssel kapcsolatban és a Kszetv.vr. előírásaihoz hasonlóan ellenállóképességi terv készítését rendeli el a kijelölt jelentős szervezet részére.

A VBÖ.vr. tartalmazza a VBÖ által meghatározott ágazatok és alágazatok vonatkozásában a jelentős szervezetté, infrastruktúrává való kijelölés kritériumkövetelményeit ágazati, alágazati bontásban.

1.2.2.4. Kritikus szervezetekre vonatkozó információbiztonsági jogszabályok

A kritikus szervezetek és infrastruktúrák egyre inkább függenek az informatikai rendszerektől, sőt magától az internetes kapcsolattól is, ezért az információbiztonság kiemelten fontos ezen a területen. Az információbiztonsági jogszabályok hivatottak szabályozni a kritikus szervezetek működéséhez, a kritikus infrastruktúrák működtetéséhez szükséges információs rendszerek működtetését, védelmét, az adatvédelmet.

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: kiberbiztonsági törvény) megjelenése kiemelten fontos volt a NIS2 (EU) megjelenését követően, Magyarország kiberbiztonságának az Európai Unió kiberbiztonsági intézkedéseivel való összehangolása érdekében. A törvény a Kszetv.-el összhangban készült és kiemelten foglalkozik a kritikus szervezetek szabályozásával és működésük kibervédelmével.

A kiberbiztonsági törvény nagy részletességgel szabályozza az alapvető és fontos szervezetek kötelezettségeit, a kiberbiztonsági felügyelet hatósági és szervezeti feladatait, a sérülékenységvizsgálat végrehajtását, az incidenskezelés részleteit, a kiberbiztonsággal kapcsolatos felsőszintű szervezeti egységeket. A poszt-quantum titkosítással és védelemmel kapcsolatos szabályozás ebben a törvényben is megmaradt, igazítva a NIS2 által előírt hatósági és szervezeti követelményekhez.

A törvény a NIS2 alapján bevezeti az alapvető és a fontos szervezetek fogalmát, megadva a hazai viszonyokra vonatkozó kritikusság kritériumait és az azonosítás feltételeit. Érdekes kiemelni, hogy az adatok védelme érdekében keletkező kötelezettségeket nem konkrétan az üzemeltetőre vagy tulajdonosra terheli, hanem az elektronikus információs rendszer felett rendelkezési jogosultsággal rendelkező szervezetet, az adatkezelőt vagy az adatfeldolgozót nevezi meg.

A kibervédelmi törvény értelmében az elektronikus információs rendszerek védelmére kockázatmenedzsment rendszer kell létrehozni és felelős személy kell kijelölni, mely rendszerek lehetnek „*alacsony*”, „*jelentős*” vagy „*magas*” biztonsági osztályba soroltak.

A kiberbiztonsági törvény külön pontban foglalkozik az elektronikus információs rendszerek biztonságával kapcsolatos oktatással és képzésekkel, mind a kiberbiztonságért felelős személyek, mind a szervezetek munkatársainak vonatkozásában. Fontos, 2025-ben bevezetett módosítás, hogy 2028. január 1-től már csak elfogadott hazai vagy nemzetközi információbiztonsági képzettséggel rendelkező személy tölthet be információbiztonsági felelős szerepet és nem lesz lehetőség gyakorlati tapasztalattal kiváltani a végzettséget.

Kiemelendő, hogy a kibervédelmi törvény részletesen szabályozza a jogkövetkezményeket, így a figyelmeztetést, eljárást, bírságkiszabást, sőt, akár az elektronikus adatok ideiglenes hozzáférhetetlenné tételét és eltávolítását is. E rendelkezések célja a gyors állami beavatkozás lehetősége.

A Kormány a honvédelmi célú információs rendszerek különválasztása érdekében továbbra is két incidenskezelő központot működtet: a nemzeti kiberbiztonsági incidenskezelő központot és a honvédelmi incidenskezelő központot, melyek szoros együttműködésben, hasonló feladatkörrel, de elkülönített rendszerekkel működnek.

2025-ben megjelent érdekes módosítás, hogy a honvédelmi célú elektronikus információs rendszerek közé sorolhatók a nem honvédelmi szervezetnél lévő, de az ország védelme és biztonsága szempontjából jelentős információs rendszerek is, melyek nem kettős kijelölésűek.

A kiberbiztonsági törvény végrehajtásáról szóló kormányrendelet⁹¹ új fogalmakat is bevezet, főleg a kiberbiztonsági irányítás és felügyelet gyakorlati végrehajtását szolgáló technikai jellegű meghatározásokkal. Külön kiemeli a külföldi adatkezelésre és a nem privát felhőszolgáltatások igénybevételére vonatkozó szabályokat. A védelmi intézkedések meghatározása során a szervezeteknek figyelembe kell venniük az uniós szintű kockázatértékeléseket, valamint az ellátási láncok sérülékenységét. Amennyiben hiányosságokat tárnak fel, a szervezet köteles intézkedési tervet készíteni, amelyet a nemzeti kiberbiztonsági hatóság hagy jóvá. Külön alfejezet foglalkozik a kiberbiztonsági gyakorlatokkal, amelyek célja a szervezeti és technikai védelem működőképességének tesztelése. Az alapvető szervezetek számára a gyakorlatok rendszeres lefolytatása kötelező, a nemzeti kibervédelmi incidenskezelő központ pedig módszertani és értékelési szerepet lát el.

A rendelet a nemzeti kiberbiztonsági hatóságként a Nemzetbiztonsági Szakszolgálatot jelöli ki, míg a honvédelmi célú elektronikus információs rendszerek esetében a honvédelemért felelős miniszter látja el a hatósági feladatokat. A szabályozás rögzíti, hogy a honvédelmi kiberbiztonsági hatóságra – meghatározott kivételekkel – a nemzeti hatóságra irányadó rendelkezések alkalmazandók.

1.3. ÖSSZEFOGLALÓ TÁBLÁZAT ÉS RÉSZKÖVETKEZTETÉSEK

A nemzetközi közösség már az 1990-es évek végén felismerte a szükségességét és kifejezte azt a szándékát, hogy a kritikus infrastruktúrákat védeni kell. Hamar megszületett az EU kritikus infrastruktúrákkal kapcsolatos jogi háttere, mely megadta a témakör alapelveit, főbb irányait, a nemzetközi együttműködés lehetőségét, de a részletes szabályozást és a további feladatokat szinte 100 %-ban a nemzetek kezébe adta. A magyarországi jogi szabályozás a kezdetektől fogva leköveti az EU kritikus infrastruktúrákkal kapcsolatos tevékenységét, mely az alábbi összefoglaló táblázatból is jól kitűnik.

Megjelenés éve	Kiadás	Cím	Megjegyzés
2004	EU	COM(2004) 702 A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben	
2004	Nemzeti	2112/2004. (V. 7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól	
2005	EU	COM(2005) 576.; COM(2006) 786.	

⁹¹ 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról

		Zöld Könyv és a végleges Közlemény a létfontosságú infrastruktúrák védelmére vonatkozó európai programról	
2008	EU	COM(2008) 676 a létfontosságú infrastruktúrák figyelmeztető információs hálózatáról	CIWIN
2008	EU	2008/114/EK irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről	ECI
2008	Nemzeti	2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról	Zöld Könyv
2010	Nemzeti	1249/2010. (XI. 19.) Korm. határozat Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről	
2012	Nemzeti	2012. évi CLXVI. törvény A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről	Lrtv.
2013	Nemzeti	65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról	Lrtv.vr.
2013-2020	Nemzeti	Korm. rendeletek az ágazatok létfontosságú rendszerlemeinek azonosításáról, kijelöléséről és védelméről	
2013	Nemzeti	2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról	
2016	EU	(EU) 2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről	NIS
2021	Nemzeti	2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról	VBÖ
2022	EU	(EU) 2022/2555 irányelv az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről	NIS2
2022	EU	(EU) 2022/2557 irányelv a kritikus szervezetek rezilienciájáról	
2024	Nemzeti	2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről	Kszetv.
2024	Nemzeti	474/2024. (XII. 31.) Korm. rendelet rendelet a kritikus szervezetek ellenállóképességéről szóló törvény végrehajtásáról	Kszetv.vr.
2024	Nemzeti	475/2024. (XII. 31.) Korm. rendelet az ország védelme és biztonsága szempontjából jelentős szervezetek ellenálló képességéről	VBÖ.vr.
2024	Nemzeti	2024. évi LXIX. törvény Magyarország kiberbiztonságáról	
2024	Nemzeti	418/2024. (XII. 23.) Korm. rendelet	

		Magyarország kiberbiztonságáról szóló törvény végrehajtásáról	
--	--	--	--

1. sz. táblázat

Összefoglaltam és rendszereztem az elmúlt 20 évi releváns Európai Unió és a magyarországi jogszabályi háttérrel, a vizsgálatok alapján megállapítottam, hogy a magyarországi kritikus szervezetek és infrastruktúrák azonosításával, kijelölésével és védelmével kapcsolatos *nemzeti jogi szabályozás nemzetközi viszonylatban is magas színvonalú és naprakész*. A legfelső törvényi szinttől a kormányrendeletek útján részletes rendszert képez, összehangolva a kritikus és a jelentős szervezetek működését, mely rendszer az elmúlt évben is felülvizsgálatra és kiegészítésre került.

Megállapítottam, hogy a magyarországi elektronikus információs rendszerek védelmének jogi alapjait képező szabályozás hasonlóképpen többszintű, részletes és modern, *figyelembe veszi a kritikus és jelentős szervezetek működéséhez, a kritikus és jelentős infrastruktúrák üzemeltetéséhez szükséges elveket*.

Az elmúlt évek jogszabály felülvizsgálatai, módosításai jó irányban haladnak a függőségek és kölcsönös függőségek kérdésében, hiszen a jogszabályok szövegezésébe több helyre is beépült ezek vizsgálatának szükségessége. Viszont részletes módszertan nélkül, az azonosított szervezetek kezébe adott interdependencia vizsgálatok nem megfelelő mélységűek. Meglátásom szerint a jogszabályok csak *kevés esetben tartalmaznak iránymutatást az ágazatokon belüli és az ágazatok közötti mélyebb, összetettebb kölcsönhatások felmérésére*.

Az átfogó rendszerezéssel bizonyítottam, hogy jelenleg a magyarországi kritikus és jelentős szervezetekre vonatkozó jogszabályok között *nincs olyan módszertani dokumentum, mely részletesen tartalmazná az interdependencia mélyebb vizsgálatának gyakorlatát*.

A Kszetv.vr. „Az ellenállóképességi terv tartalmi követelményei” c. melléklete jelenleg is tartalmaz olyan pontokat, melyek az üzemeltetési folyamatra ható függőségek bemutatására, értékelésére vonatkoznak, illetve külön kiemeli az ellátási lánc bemutatását, de részletes, önálló interdependencia vizsgálatra nem ad módszertant, így ezeket a vizsgálatokat szervezetenként eltérően, szubjektív módszerekkel, vagy külső segítséggel hajtják végre.

Továbbá megállapítottam, hogy a jelenleg hatályos jogszabályok nem adnak elegendő gyakorlatban is alkalmazandó támogatást és módszertant a kritikus szervezetek részére, így a reziliencia kialakításának gyakorlati végrehajtása nem egységes.

A magyarországi kritikus szervezetek ellenálló képességéről szóló jogszabályok és előzményeik, valamint a kritikus szervezetek és kritikus infrastruktúrák azonosítási és kijelölési gyakorlatának áttekintése alapján, a hatályos jogszabályok lehetséges tartalmi fejlesztésével kapcsolatban a következő javaslatokat teszem:

1. Ágazati szakmai bizottságok létrehozása

A Kszetv. által meghatározott ágazatonként egy *Ágazati Szakmai Bizottság* jön létre, melynek tagjai:

- 531/2017. (XII.29.) Korm. rendelet⁹² által a kritikus szervezetekkel, infrastruktúrákkal kapcsolatos ügyekben, az adott ágazat szakmai csoportjára meghatározott szakhatóságokat képviselő szakértő, az Ellenálló Képességért Felelő Vezetők Tanácsadó Bizottságának tagja, az *Ágazati Szakmai Bizottság* elnöke;
- az adott ágazati szakhatóság által kijelölt, a Kszetv. 1. mellékletében meghatározott ágazati alapvető szolgáltatások tekintetében döntési jogkörrel rendelkező szakértő(k);
- Kritikus infrastruktúra védelmi biztonsági összekötő személy szakirányú továbbképzést, vagy ezzel egyenrangú, kritikus szervezetek ellenálló képességével kapcsolatos felsőfokú képzettséggel és az ágazati szakhatóság által előírt képzettséggel rendelkező szakértők;
- az adott ágazati szakhatóság által meghívott szakértők.

Feladatai:

- az ágazati szakhatóságok részére előírt feladatok támogatása;
- ágazati jelentések, vizsgálatok, gyakorlatok elemzése;
- fogadja a potenciális kritikus szervezetek önállóan megküldött azonosítási adatlapját;
- saját ágazata vonatkozásában, kritikus szervezetté, kritikus infrastruktúrává való kijelölési eljárás megindítására javaslatot tehet a kijelölő hatóság részére, az ágazati szakhatóság útján;
- ágazaton belüli interdependencia vizsgálatok végrehajtása;
- ágazatok közötti interdependencia vizsgálatok kezdeményezése más ágazatok *Ágazati Szakmai Bizottsága* felé.

2. Interdependencia mélyebb vizsgálata

⁹² 531/2017. (XII.29.) Korm. rendelet az egyes közérdeken alapuló kényszerítő indok alapján eljáró szakhatóságok kijelöléséről

A Kszetv.vr. módosításával előírja az EKT elkészítésének időszakára az interdependencia dimenzióit figyelembe vevő mélyebb vizsgálat végrehajtását, mely lehetővé teszi a nem kritikus, de kritikus szervezettel kapcsolatban lévő szervezetek, szolgáltatók alapvető interdependencia vizsgálatát is.

Az interdependencia mélyebb vizsgálata érdekében az EKT és az EKM módosítása, kiegészítése szükséges. Az értekezés 2.5. Az interdependencia vizsgálat c. alfejezete szerinti metodika felhasználásával az EKT. 5. pontja kiegészíthető, illetve az EKM új, 3. lapjára létrehozható az elemzési módszer.

Az interdependencia dimenzióit figyelembe vevő metodika az *Ágazati Szakmai Bizottságok* által az ágazati jellegzetességekkel kiegészíthető és az egységes végrehajtás érdekében a BM OKF weblapjáról elérhetővé tehető.

3. *Kritikus elem fogalma*

A Kszetv. fogalmai közé beemelt „*Kritikus elem*” fogalma és annak alkalmazása pontosabbá teszi a kockázatelemzések eredményeit, lehetővé teszi a célzott védelem kialakítását és a célirányos szervezeti vagy hatósági támogatás biztosítását.

4. *Kritikus szervezetek belső felkészítési rendszere*

A Kszetv. módosításával, a kritikus szervezetek ellenálló képességének fejlesztése érdekében, a kritikus szervezet ellenálló képességéért felelős vezető feladatköre (Kszetv. 20. § (4)) a kritikus szervezetek belső felkészítési rendszerének kialakításával bővül:

- kialakítja a kritikus szervezet belső, ellenállóképességgel kapcsolatos felkészítési rendszerét.

A Kszetv.vr. módosításával a kritikus szervezet ellenálló képességéért felelős vezető felkészítésekkel kapcsolatos feladatköre bővíthető (Kszetv.vr. 18. §):

- összeállítja a kritikus szervezet munkavállalói részére az ellenálló képességgel kapcsolatos képzésekre vonatkozó képzési programokat, külön tematika szerint a vezetők, a kritikus munkakörben foglalkoztatottak, a fizikai védelemben résztvevők, valamint az előző munkakörökbe nem tartozó adminisztratív és fizikai munkakörben dolgozó munkavállalók tekintetében;
- összeállítja a kritikus szervezet éves ellenálló képességgel kapcsolatos képzési tervét;

- megszervezi, és végrehajtja vagy felkéri a témában releváns szakembereket az ellenálló képességgel kapcsolatos képzések végrehajtására;
- az ellenálló képességgel kapcsolatos képzéseket követően a képzési programokban előírt visszaellenőrzések és értékelések eredményeit összesíti;
- évente egy alkalommal tapasztalatfeldolgozó megbeszéléseket tart a képzések résztvevőivel a beválási információk megosztása és az ellenálló képességgel kapcsolatos képzések további fejlesztése érdekében.

5. Adminisztratív támogatás kiegészítése

A Kszetv.vr. 2. melléklete az EKT tartalmi követelményeit tartalmazza, mely az 1.18.13. pontjában előírja az EKT-hoz kapcsolódó dokumentumok felsorolását. A kritikus szervezet napi életét, a hatósági és ágazati kapcsolattartást, ellenőrzést és mindennemű feladat tervezését elősegíti a jól kidolgozott dokumentációs hierarchia. Ennek érdekében az EKT kötelezően csatolt dokumentumai közé, az említett 1.18.13. pont módosításával a következő szövegezést javaslom:

- a kritikus szervezet teljes dokumentációs hierarchiáját, a dokumentumok egymáshoz való viszonyát és csoportjait bemutatva, kiemelve az Ellenálló Képességi Tervben hivatkozott dokumentumokat.

2. FEJEZET

A KRITIKUS SZERVEZETEK ÉS INFRASTRUKTÚRÁK AZONOSÍTÁSI ÉS KIJELÖLÉSI ELJÁRÁSÁNAK FOLYAMATA

2.1. A KRITIKUS ÉS JELENTŐS SZERVEZETEK ÉS INFRASTRUKTÚRÁK AZONOSÍTÁSÁNAK ÉS KIJELÖLÉSÉNEK RÉSZTVEVŐI

A kritikus és jelentős szervezetek, infrastruktúrák azonosítási, kijelölési folyamata és rezilienciájának kialakítása, fejlesztése sokszereplős folyamat. Az első fejezetben tárgyalt jogszabályok több pontban megadják a résztvevők hivatalos megnevezését, azok fő feladatait, illetve ki is jelölik ezen résztvevők kormányzati szereplőit.

Annak érdekében, hogy a folyamatban résztvevők jogait, kötelességeit, szerepüket tisztán lássuk, elemezni tudjuk, fontos kiemelni, hogy az azonosítás, kijelölés és a védelmi képességek kialakításának részfeladatai nem feltétlenül ugyanolyan prioritással bírnak minden résztvevő számára.

A kormányzati szervek felelősek a kialakított jogszabályi háttér betartásáért, betartatásáért, figyelembe véve a szervezetek képességeit. A kormányzati szervek prioritásként a jogszabályok maradéktalan betartását és a kijelölt kritikus és jelentős infrastruktúra legteljesebb védelmi és ellenálló képességeinek kialakítását látják.

A kritikus és jelentős szervezeteknek, illetve a kijelölt infrastruktúrák üzemeltetőinek természetesen kötelességük betartani a jogszabályokban előírt rendelkezéseket. Viszont üzemeltetői, tulajdonosi szempontból a prioritás mégis az üzemfolytonosság biztosítása és az erőforrások optimális – lehetőség szerint minimális – felhasználásával elérhető ellenálló képesség kialakítása lesz.

Ennek a két pólusnak a feloldása csak hatékony kommunikációval oldható meg.

A kritikus és jelentős szervezetek, infrastruktúrák azonosítási, kijelölési folyamatában, ellenálló képességük kialakításában a kormányzati és üzemeltetői oldaltól független, de szerencsés esetben velük szoros együttműködésben jelennek meg a különböző szakmai szervezetek, tanácsadók. Ezek lehetnek olyan szakértői, tanácsadói csoportok, informatikai szakértők, mérnökök, biztonsági szakemberek, jogi tanácsadók, akik az adott szakterület mélyebb

ismerőiként hathatós segítséget képesek adni a folyamat egyes részfeladataiban, a végeredmény hatékonyabb kialakításában.

Ugyancsak a kormányzati és üzemeltetői oldaltól függetlenül, de hatást gyakorolva jelenhetnek meg a folyamatban a magánszektor, a civil társadalom képviselői vagy más – adott ágazatban fontos – gazdasági, ipari szereplők.

2.1.1. Üzemeltető/Tulajdonos/Felelős

Sem a Kszetv. sem a VBÖ nem tesz különbséget üzemeltető, tulajdonos vagy felelős között, egységesen kritikus és jelentős szervezetként jelöli azokat az entitásokat, melyek alapvető szolgáltatás nyújtásában engedélyesek, rendelkezésre jogosultak vagy felelősök.

A jogszabályokban, az ágazati kritériumok kibontásánál viszont már nagyrészt „üzemeltető” szerepel, így az adott rendszerhez kapcsolódó szereplők feladata eldönteni, hogy az azonosítás, kijelölés és ellenálló képesség kialakításának feladataiban ki jogosult döntéseket hozni.

Szinte minden esetben elmondható, hogy a napi működésért felelős, a tulajdonos, a különböző rendelkezésekre jogosult vagy engedélyes nem egy személy vagy szervezet. Egy széles szolgáltatási portfólióval és nagy létszámú foglalkoztatottal rendelkező szervezet által üzemeltetett rendszer akár több tulajdonossal, a felelősségi viszonyokat szétválasztó – akár külső – szervekkel, szervezetekkel rendelkezhet.

Leggyakrabban vehető példa erre az esetre, mely alapján a létesítmény biztonságáért felelős szervezet és a biztonsági beruházások finanszírozásáért felelős szervezet nem csak különálló szervezetek, de nem is egy vezetői vonalon helyezkednek el. Az általam vizsgált pénzügyi kritikus szervezetek azonos létesítményben helyezkednek el, de a fizikai biztonságért egy harmadik, külső szolgáltató felelős, megbízási szerződés alapján. A két pénzügyi szervezet vezetése különálló, a beruházások finanszírozásáért közös fenntartó felel, a fizikai védelemért felelős szervezet független, különálló vezetéssel működik.

Előző példából látható, hogy a hatáskörök és felelősségi viszonyok egyértelmű meghatározása kulcsfontosságú. Ha nem teljesen világos, hogy ki vagy mely szervezet felelős a rendszerek egy-egy eleméért, vagy ha túl sok fél van megjelölve azonos felelősséggel és jogosultsággal, akkor az esetleges válsághelyzetek kezelése nehezebbé válik, a reziliencia sérül.

Fontos, hogy már az azonosítási eljárás kezdetén tisztázva legyenek ezek a hatáskörök és felelősségi viszonyok. Külön vizsgálatot igényel és *felelősségi megállapodásban, szerződésben* rögzítendő, hogy a Kszetv. által megfogalmazott kritikus szervezet vezetőségi és az infrastruktúra üzemeltetői körébe tartozó résztvevők milyen szinten és milyen hatáskörrel vesznek részt az azonosítási, kijelölési folyamatban és az előírt, megfelelő rezilienciával és védelemmel kapcsolatos intézkedések megvalósításában.

2.1.2. Kijelölő hatóságok

A Kszetv.vr. alapján az általános kijelölő hatóság a hivatásos katasztrófavédelmi szerv központi szerve⁹³, energetikai ágazatban az állam villamosenergia-, földgáz- és távhőellátással, víziközmű-szolgáltatással, valamint állami hulladékgyűjtési közfeladat díjszabályozásának előkészítésével kapcsolatos feladatait ellátó, önálló szabályozó szerve⁹⁴. A honvédelmi ágazatban, a VBÖ alapján a honvédelmi ágazati kijelölő hatóság⁹⁵ jogosult jelentős szervezetek és infrastruktúrák kijelölésére.

Legfőbb feladatuk az ágazati szakhatóságokkal és szakmai támogató szervezetekkel, illetve a folyamatban résztvevő felekkel együttműködve a kritikus szervezetek és infrastruktúrák azonosítása, kijelölése, a kijelölés fenntartása, megfelelő indokok alapján a kijelölés visszavonása.

A kijelölő hatóságok a kijelölési folyamat megindítása és lefolytatása céljából előzetes adatszolgáltatást kérnek a potenciális vagy már kijelölt kritikus szervezetektől. A horizontális kritériumok teljesülését az általános kijelölő hatóság, az ágazati kritériumok teljesülését az ágazati szakhatóság segítségével a megszólított szervezet végzi.

A kijelölési folyamat során a kijelölő hatóság vizsgálja az Európai Unió más tagállama számára nyújtott alapvető szolgáltatásokat és az Európai Bizottság által lefolytatott egyeztetési eljárás alapján európai kritikus szervezet vagy európai kritikus infrastruktúra határozatot hoz.

A kijelölő hatóságok alapvető, központi szerepet töltenek be a kijelölési folyamat után is kritikus szervezetek életében. Rajtuk keresztül történik az információáramlás a szakhatóságok, egyéb szervezetek és a kritikus szervezetek, illetve a kritikus infrastruktúrák üzemeltetői között,

⁹³ Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (2026.01.31.)

⁹⁴ Magyar Energetikai és Közmű-szabályozási Hivatal (2026.01.31.)

⁹⁵ Honvédelmi Miniszter (475/2024. (XII. 31.) Korm. rendelet 3.§ (2))

részt vesznek a kritikus szervezetek ellenőrzéseinek, gyakorlatainak szervezésében, lebonyolításában.

A honvédelmi ágazati kijelölő hatóság önállóan, de az általános kijelölő hatóság tájékoztatása mellett jogosult az ország védelme és biztonsága szempontjából jelentős honvédelmi kijelölésű szervezetek és infrastruktúrák kijelölésével összefüggő hatósági eljárások lefolytatására. Specialitás, hogy különleges jogrend időszakában a honvédelmi ágazati kijelölő hatóság gyorsított eljárás keretében, adatszolgáltatás beérkezése nélkül is dönthet, amennyiben az ország védelme és biztonsága szempontjából jelentős szervezet kijelöléséről van szó.

A honvédelmi szempontú különös szabályok⁹⁶ hatással vannak az általános kijelölő hatóság feladataira is, ezen specialitások a 2.2 alfejezetben, az azonosítás és kijelölés folyamatának bemutatásában szerepelnek.

2.1.3. Nyilvántartó hatóság

A kritikus és jelentős szervezetek és infrastruktúrák nyilvántartásának vezetése és a nyilvántartás adatainak kezelése központi szervnél történik, bizonyos kivételekkel. A Kszetv.vr. a kritikus, illetve a nem honvédelmi érdekből jelentős szervezetek és infrastruktúrák nyilvántartó hatóságként a hivatásos katasztrófavédelmi szerv központi szervét jelöli ki. Az ország védelme és biztonsága szempontjából jelentős, honvédelmi érdekből kijelölt szervezetek és infrastruktúrák tekintetében pedig a honvédelmi ágazati kijelölő hatóság (mint honvédelmi ágazati nyilvántartó hatóság) vezeti a nyilvántartást és kezeli az adatokat.

A VBÖ által meghatározott kettős kijelölés vagy a honvédelmi ágazaton kívüli honvédelmi kijelölés esetén a szervezetek és infrastruktúrák nyilvántartását és az adatok kezelését a honvédelmi ágazati és a központi nyilvántartó hatóság is végzi. Ebben az esetben a két nyilvántartó hatóság szoros együttműködésben kell, hogy dolgozzon, hiszen a különböző feladatokhoz szükséges adatlekérések eltérőek lehetnek, mind adattartalom, mind jogosultság tekintetében.

Adatlekérések történhetnek hatósági eljárások lefolytatása érdekében, rendkívüli esemény bekövetkezésekor az eseménykezelés támogatása érdekében, féléves, éves jelentések

⁹⁶ 2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról, 14/D.

elkészítéséhez, gyakorlatok előkészítéséhez, ágazati vagy központi ellenőrzések előkészítéséhez és végrehajtásához, illetve egyéb indokolt esetekben.

A központi nyilvántartó hatóság egyik kiemelt feladata a nyilvántartások alapján elkészített, kritikus szervezetekről és infrastruktúrákról készített jelentés megküldése évente a kormány részére. Viszont a Lrtv. által meghatározott nemzetközi kapcsolattartói jogosultsága megszűnt. Nemzetközi szervezet részére – beleértve az Európai Bizottságot is – csak a nemzetbiztonsági érdekek és az üzleti titokra vonatkozó érdekek figyelembevételével és az egyedüli kapcsolattartó ponton keresztül történhet adatszolgáltatás.

Jól látható, hogy a kritikus szervezetek és infrastruktúrák rezilienciájával kapcsolatos feladatok, védelmi képességek erősen függenek a naprakész, részletes nyilvántartástól és az azokhoz való gyors hozzáféréstől. Mivel a központi és a honvédelmi ágazati nyilvántartó hatóságok a nyilvántartásaikat, adatbázisaikat elkülönítve kezelik, valamint a központi nyilvántartó hatóság nem vesz részt az azonosítási és kijelölési folyamatban⁹⁷, így az adatok naprakészen tartása, a változások mielőbbi bejelentése nagyrészt a szervezetek, az infrastruktúra üzemeltetők és a szakhatóságok kezében van. Az adatok biztonságos kezelése és a szükség szerinti gyors rendelkezésre állás biztosítása pedig a két kijelölt nyilvántartó hatóság feladata.

Mindezekből jól érzékelhető, hogy a nyilvántartás és adatkezelés – a fejlett információs infrastruktúra ellenére – erősen függ az emberi beavatkozásoktól. Az IHR⁹⁸ megszűnésével az együttműködés lehetősége is szűkült, a kritikus szervezetekkel kapcsolatos ügyintézés a kormányhivatalok hivatalos bejelentő oldalán⁹⁹ lehetséges, melyen kiválasztva a „*Kritikus szervezetekkel kapcsolatos ügyintézés*” menüpontot, szöveges levél és csatolt dokumentum küldhető a BM OKF részére.

A központi nyilvántartó hatóság akár több millió forintos közigazgatási bírság kiszabására is jogosult, míg a honvédelmi ágazati kijelölő hatóságnak ilyen jellegű jogosultsága nincs.

2.1.4. Ágazati szakhatóságok

A kritikus és jelentős szervezetek, infrastruktúrák azonosítási és kijelölési folyamatában kiemelt szerepe van az ágazati szakhatóságoknak. Ezek a szervezetek vagy intézmények nem

⁹⁷ Kritikus Infrastruktúrák védelme I. – Dialóg Campus Kiadó – Budapest – 2019.

⁹⁸ Id.: 1.2.4. alfejezet; Integrált Hatósági Rendszer

⁹⁹ <https://katasztrofavedelem.hu/36732/ihr-integralt-hatosagi-ugyviteli-rendszer-karbantartas> (letöltés: 2025.01.28.)

rendelkeznek a kritikus szervezetté történő kijelöléshez szükséges hatáskörökkel, jogokkal, de rendelkeznek azokkal a szakmai kompetenciákkal, melyek az adott ágazatra vonatkoztatva képessé teszik őket átfogó, felső szintű szakmai ajánlások, iránymutatások kidolgozására.

Mivel ehhez a feladathoz elengedhetetlenek az átfogó szakmai kompetenciák, így ágazatonként és alapvető szolgáltatások szakmai csoportjaiként külön kijelölt szervezetek töltik be ezt a tisztséget. A korábbi ágazati kormányrendeletek megszűnésével az ágazati szakhatóságok kijelölése a következőképpen történik: a Kszetv. vr. 157. §-a módosította a 2017-ben megjelent, szakhatóságok kijelöléséről szóló kormány rendeletet¹⁰⁰, melynek 1. mellékletébe így bekerültek a kritikus és jelentős szervezetekkel, infrastruktúrákkal kapcsolatos ügyek. Az említett kormányrendelet¹⁰¹ a Kszetv. 1. mellékletében lévő táblázat alapvető szolgáltatásaira hivatkozik és szakmai csoportonként külön-külön rendelkezik a kritikus szervezetekkel és infrastruktúrákkal kapcsolatos szakhatóságok kijelöléséről.

A honvédelmi érdekeltségű alapvető szolgáltatások – mivel nem kritikus, hanem jelentős szervezetekről van szó – ugyanezen kormányrendelet¹⁰² egy másik táblázatban található. A táblázat hasonló felépítésű, a VBÖ által meghatározott alapvető szolgáltatások szakmai csoportjait figyelembe véve jelöli ki az ország védelme és biztonsága szempontjából jelentős szervezetek és infrastruktúrák ágazati szakhatóságait, melyek a továbbiakban már mindhárom kijelölő hatósággal kapcsolatban kell, hogy álljanak: általános kijelölő hatóság, energetikai kijelölő hatóság, honvédelmi kijelölő hatóság.

Mivel a Kszetv. és a VBÖ előírásai szerint minden szakmai állásfoglalást és javaslatot az ágazati szakhatóságoknak kell elkészíteniük, szorosan együtt kell működniük a kijelölő hatóságokkal és a szervezetekkel, illetve ezen felül még számos egyéb feladat is hárul rájuk:

- állásfoglalást ad ki a kritikus szervezet, kritikus infrastruktúra kijelölésére, a kijelölés fenntartására vagy a kijelölés visszavonására
- adatszolgáltatással, állásfoglalással támogatja a kijelölő hatóságokat az ágazati kritériumok teljesülésének vizsgálatában;
- adatszolgáltatással, állásfoglalással támogatja a kijelölő hatóságokat a kritikus és jelentős szervezetek EKT és ellenállóképességi mátrixának megfeleléségi vizsgálatában;

¹⁰⁰ 531/2017. (XII.29.) Korm. rendelet az egyes közérdeken alapuló kényszerítő indok alapján eljáró szakhatóságok kijelöléséről

¹⁰¹ 531/2017. (XII.29.) Korm. rendelet az egyes közérdeken alapuló kényszerítő indok alapján eljáró szakhatóságok kijelöléséről

¹⁰² 531/2017. (XII.29.) Korm. rendelet az egyes közérdeken alapuló kényszerítő indok alapján eljáró szakhatóságok kijelöléséről

- a Kszetv. által megadott feltételekkel önállóan végrehajthat ellenállóképességi ellenőrzéseket saját ágazata vonatkozásában;
- az általános kijelölő hatóságon keresztül igényelheti európai tanácsadó misszió létrehozását, illetve szakértőket delegálhat a csoportba;
- értékeli, elemzi az európai tanácsadó misszió megállapításait, bedolgozza állásfoglalását az Európai Bizottság részére készített tájékoztatóba;
- ágazati rendkívüli esemény bejelentésére szolgáló kapcsolati helyet jelöl ki vagy szükség szerint ügyleti szolgálatot üzemeltet, elemzi az ágazatához tartozó rendkívüli eseményeket és a tett intézkedéseket;
- az általános kijelölő hatóság és a kritikus szervezet képviselője mellett, részt vehet a komplex ellenálló képességi gyakorlatokon;
- segíti a kijelölő, nyilvántartó, ellenőrző hatóságokat a jogkövetkezmények kezelésében (mulasztások megszüntetésére intézkedik, határidőt szab, közigazgatási bírságot szab ki);
- tagot delegál az Ellenálló Képességért Felelős Vezetők Tanácsadó Bizottságába;
- támogatja, részt vesz a kijelölő hatóság és az Ellenálló Képességért Felelős Vezetők Tanácsadó Bizottsága által évente rendezett szakmai rendezvények szervezésében;
- szükség esetén tanácsadót delegál a kritikus és jelenős szervezetekhez, elemzi, értékeli a tanácsadó jelentését (honvédelmi ágazat kivételével, ahová tanácsadó nem rendelhető ki).

Fontos megjegyezni, hogy a honvédelmi ágazat a jelentős szervezetek és infrastruktúrák tekintetében az általános kijelölő hatóságon keresztül tarthat kapcsolatot az ágazati szakhatóságokkal, közvetlen kapcsolat csak egy esetben lehet:

„Az ország védelme és biztonsága szempontjából jelentős kettős kijelölésű szervezet kijelölése esetében a honvédelmi ágazati kijelölő hatóság a kijelölésről, a kijelölés fenntartásáról, a kijelölés visszavonásáról szakhatóság tájékoztatása mellett, de bevonása nélkül dönt.”¹⁰³

A már említett A 531/2017. (XII.29.) Korm. rendelet 21. pontjában lévő táblázatban szakhatóságként van feltüntetve a hivatásos katasztrófavédelmi szerv központi szerve is, a horizontális kritériumoknak való megfelelés vizsgálatára, a honvédelem ágazatban, illetve a villamos energia és a kőolaj alágazatokban.

¹⁰³ VBÖ.vr. 5. § (3)

2.1.5. Ellenőrzésbe bevont szervek

A kijelölt kritikus és jelentős szervezetek ellenőrzése egy ciklikus, több szereplő részvételével végrehajtott, több szakterületet képviselő, a szervezetek összehangolt munkájából felépülő folyamat kell, hogy legyen.

A Kszetv.vr. és a VBÖ.vr. a kritikus és jelentős szervezetek ellenőrző hatóságaként a hivatásos katasztrófavédelmi szerv központi szervét jelölte ki, egy kivétellel. A honvédelmi kijelölésű jelentős szervezetek ellenőrző hatóságaként a honvédelemért felelős miniszter lett kijelölve.

Az ellenőrzés több céllal és ennek megfelelően több szervezet irányából hajtható végre.

A kritikus szervezetek az egyedi ellenálló képességük vizsgálata érdekében *ellenálló képességi gyakorlatot* hajtanak végre, évente legalább egy alkalommal, kötelező jelleggel, melynek célja a szervezet ellenálló képességi tervében rögzített eszközök, módszerek alkalmazásának, a szervezeti felépítés alkalmasságának, valamint a rendkívüli események kezelésében részt vevő szervezetek, partnerek együttműködésének ellenőrzése. Az általános kijelölő hatóság által kiadott útmutató alapján, a kritikus szervezet ellenállóképességéért felelős vezető értékeli és dokumentálja a gyakorlatot, a jelentését az ellenőrző hatóság részére küldi meg.

A VBÖ nem ír elő ellenállóképességi gyakorlatot a kijelölt jelentős szervezetek részére, kivételként viszont a VBÖ.vr. az ország védelme és biztonsága szempontjából jelentős *honvédelmi ágazaton belüli* szervezetek esetén, éves rendszerességgel igen.

Az önálló ellenállóképességi ellenőrzéseket a szakhatóságok hajtják végre, célja kifejezetten az ágazatspecifikus elemzések, ellenállóképességi tesztek végrehajtása. Ezek az ellenőrzések az üzemfolytonosság biztonságát, ágazati szabályoknak megfelelő szabályosságát, az EKT alapján történő működés hatékonyságát, esetleges hiányosságait hivatottak feltárni. Ennek végrehajtásáról és eredményeiről készült jegyzőkönyvet a szakhatóságok kötelesek megküldeni az ellenőrző hatóságok felé.

A rendszeres vagy soron kívüli *komplex hatósági ellenőrzéseket* az ellenőrző hatóságok hajtják végre, mely során ellenőrzik:

- a kijelölt kritikus vagy jelentős szervezetek jogszabály szerű működését;
- az ellenállóképesség növelése érdekében hozott intézkedéseket;
- a nyilvántartó hatóságnál szereplő adatok aktualitását, helyességét;
- az EKT megfeleléseit;
- a kockázatértékelés, EKM szabályozottságát és megfeleléseit

- a szervezet vezetőségének tevékenységét az ellenállóképesség szempontjából;
- ellenálló képességéért felelős vezető tevékenységét és személyével kapcsolatos követelményeket;
- az előírt éves ellenállóképességi gyakorlat megfelelőségét;
- a kritikus szervezet és az érintett ellátási lánc tagjai, beszállítói együttműködésének megfelelőségét.

A magasabb szintű ellenőrzések egyik hatékony fajtája a *komplex ellenállóképességi gyakorlat*, melyet az általános kijelölő hatóság és a szakhatóságok részvételével és értékelésével hajtanak végre. Az előzőekben felsorolt ellenőrzési célok mellett, az ellenállóképességet teszik próbára és elemzik a működését speciális körülmények között is.

A nagy számú kijelölt kritikus és jelentős szervezet hatékony ellenőrzése szoros együttműködést kíván az ellenőrző hatóságoktól, az ágazati szakhatóságoktól és a szervezetektől egyaránt. Az egyeztetések alapján összeállított évi ellenőrzési terv tartalmazza az ágazati önálló ellenőrzéseket, a komplex hatósági ellenőrzéseket, a komplex ellenállóképességi gyakorlatokat is, melyeket együttesen hajtanak végre az érintett hatóságok.

Amennyiben az ellenőrzött szervezet többszöri javaslat, majd felszólítás ellenére sem pótolja a hiányosságokat, vagy javítja a hibákat, abban az esetben a jogszabályoknak megfelelően szankcionálható.

Az ország védelme és biztonsága szempontjából jelentős *honvédelmi ágazaton kívüli* kijelölésű szervezetek és infrastruktúrák ellenőrzését a két ellenőrző hatóság együtt hajtja végre. Az ország védelme és biztonsága szempontjából jelentős *honvédelmi ágazaton belüli* kijelölésű szervezetek és infrastruktúrák ellenőrzését viszont a honvédelmi ágazati kijelölő hatóság hajtja végre.

2.1.6. Ellenálló képességért felelős vezető

Előző alfejezetekből jól látható, hogy a kritikus és jelentős szervezetek, infrastruktúrák azonosítása, kijelölése, ellenálló képességének kialakítása, fejlesztése folyamatos és széleskörű szakmai kompetenciákat és kommunikációt igényel. A hatóságokkal való hatékony együttműködés, a védelmi és ellenálló képességek kialakítása és fejlesztése egyértelműen önálló szakterületet igényel bármely ágazathoz tartozó kritikus vagy jelentős szervezet esetén.

Ennek érdekében a Kszetv. a kritikus szervezeteket ellenálló képességért felelős vezető megbízására vagy foglalkoztatására kötelezi. A VBÖ ugyancsak kötelezi a jelentős szervezeteket ellenálló képességért felelős vezető megbízására vagy foglalkoztatására, a feladatrendszerét pedig a Kszetv. által meghatározott feladatrendszeréhez köti, a nemzetközi feladatok kivételével. A VBÖ.vr. kiemeli, hogy a nemzetközi feladatok kivételével, a Kszetv. és Kszetv.vr. *kritikus szervezet ellenállóképességért felelős vezetőre* vonatkozó előírásait a *jelentős szervezet ellenállóképességért felelős vezetőre* is érteni kell.

Az ellenállóképességért felelős vezetői beosztásokat betöltő személynek büntetlen előéletűnek kell lennie, illetve felsőoktatási intézményben megszerezhető, *kritikus infrastruktúra védelmi biztonsági összekötő személy szakirányú továbbképzési szakon* szerzett képesítéssel kell rendelkeznie. Jelenleg ez a képzés csak a Nemzeti Közszolgálati Egyetemen elérhető.¹⁰⁴ Az ezzel kapcsolatos részletekről és anomáliákról a 4.2.2. alfejezetben írok.

A kritikus és jelentős szervezetek ellenállóképességért felelős vezető főbb feladatai:

- kapcsolatot tart a kijelölő hatósággal, az ágazati szakhatósággal és egyéb hatóságokkal;
- felméri a szervezet és az infrastruktúra biztonságát befolyásoló általános, ágazati és szervezeti követelményeket, szabályozási környezetet;
- elkészíti és aktualizálja a kockázatértékelést és az EKM-ot;
- elkészíti és aktualizálja az EKT-t;
- értékeli a szervezet és az infrastruktúra ellenálló képességének helyzetét és javaslatot tesz az ellenálló képesség fejlesztésére;
- megszervezi a szervezet és az infrastruktúra ellenálló képességét befolyásoló szervezeti egységek közötti koordinációt, bevonja őket a részfeladatok kidolgozásába és rendszeresen beszámol a szervezet vezetője részére az ellenálló képesség helyzetéről;
- tervezi, szervezi és vezeti az éves ellenálló képességi gyakorlatokat.

Egy kritikus vagy jelentős szervezet akár több ellenállóképességért felelős vezetőt is alkalmazhat, annak érdekében, hogy minden általa nyújtott alapvető szolgáltatás és kritikus vagy jelentős infrastruktúra le legyen fedve.

Az ellenálló képességért felelős vezető adatait, végzettségét, elérhetőségét a nyilvántartó hatóság bekéri és nyilvántartja. Az Ellenálló Képességért Felelős Vezetők Tanácsadó Bizottságának tagsága viszont önkéntes.

¹⁰⁴ <https://kvi.uni-nke.hu/felvetelizoknek/kritikusinfrastruktura-vedelmi-biztonsagi-osszekoto-szemely-szakiranyu-tovabbkepzesi-szak> (letöltés: 2025.10.20.)

A Kszetv. alapján a kritikus és jelentős szervezeteket terhelik az ellenálló képességet, a védelmet és biztonságos üzemeltetést szolgáló mindennemű szervezeti és eszközrendszerrel kapcsolatban felmerült költségek. Ebből adódóan az ellenálló képességért felelős vezető felelőssége óriási. Meg kell találnia az optimális, priorizált középutat a hatósági megfelelés, a hatékony ellenálló képesség kialakítása és a szervezet– jogosan elvárt – minimális költségráfordítási igénye között.

2.1.7. Szakmai tanácsadó szervezetek

A szakértő és tanácsadó cégek, szakemberek, kutatók segíthetnek a kritikus és jelentős szervezetek, infrastruktúrák hatékonyabb védelmének, ellenálló képességének kialakításában, innovatív megoldások kidolgozásában, a fenyegetésekkel szembeni ellenálló képesség fejlesztésében.

A lehetséges belső üzemzavarok, fenyegetések elemzését és értékelését a kritikus és jelentős szervezetek, saját szakemberei képességeire építve képesek végrehajtani. A lehetséges külső fenyegetések elemzéséhez viszont gyakran szükséges külső szakértők igénybevétele, akik képesek olyan potenciális fenyegetéseket és kockázatokat feltárni, melyre szervezetek vezetőinek, szakembereinek nincs rálátása vagy szakmai háttere.

Ilyenek lehetnek az új fenyegetésekre választ adó biztonsági stratégiák, technológiák, mint például a terrorfenyegetettség, vagy a drónok egyre jobban terjedő alkalmazása. Ide tartozhatnak a fejlettebb informatikai védelmi eszközök, kibervédelmi megoldások, illetve az ezeket telepíteni képes cégek, szakértők.

Külső szakértő, tanácsadó személyekre lehet szükség olyan jogi, szabályozási kérdésekben, melyek túlmutatnak az adott kritikus vagy jelentős szervezet szakterületén, mint például a védelmi fejlesztésekkel kapcsolatos adminisztratív, humán erőforrást érintő kérdések.

A szervezetek napi életében résztvevő, technológiáját, infrastruktúráját üzemeltető személyzet felkészítése, speciális irányú kutatás, innováció is külső szakértő bevonását igényelheti, legfőképp abban az esetben, ha nemzetközi vagy több szereplős nemzeti együttműködésre is szüksége van a szervezetnek.

2.2. A KRITIKUS ÉS JELENTŐS SZERVEZETEK ÉS INFRASTRUKTÚRÁK AZONOSÍTÁSÁNAK ÉS KIJELÖLÉSÉNEK ELVI FOLYAMATA

A jogszabályi háttér és a kapcsolódó folyamatokban résztvevők eddigi áttekintésével jól látható, hogy a kritikus és jelentős szervezetek, infrastruktúrák azonosításának és kijelölésének folyamata erősen szabályozott, minden lépés a kijelölő hatóságok által meghatározott feladatokból és a szervezetek arra adott válaszából áll.

Mivel a kritikus és a jelentős szervezetek, infrastruktúrák kérdését különböző, de együtt alkalmazandó jogszabályok szabályozzák, illetve a kijelölő hatóságok önállóan és együtt is döntést hozhatnak, maga a kijelölés folyamata folyamatos kapcsolatot igényel a résztvevők között. A potenciális kritikus vagy jelentős szervezetek dolga egyszerűbb lett az új jogszabályok megjelenésével, a hatósági oldalnak viszont szorosabban kell fogni ezen szervezetek kezét, a törvényesség betartása érdekében.

2.2.1. Kritikus és jelentős szervezetek, infrastruktúrák azonosítása és kijelölése

Az Lrtv. alapján a potenciális létfontosságú rendszerek üzemeltetői kötelesek voltak önállóan azonosítási eljárást lefolytatni és azonosítási jelentést beküldeni az ágazati kijelölő hatóságuk részére, abban az esetben ha az általuk nyújtott szolgáltatás szerepelt az Lrtv. mellékletében.

A Kszetv. nem kötelezi önálló vizsgálatra a szervezeteket, az azonosításhoz és kijelölés megindításához szükséges előzetes adatszolgáltatást csak a kijelölő hatóságok kérhetnek be a szervezetektől. Egy szervezet hivatalosan akkor sem küldhet be önállóan kitöltött adatszolgáltatási lapot, ha a Kszetv. szerinti alapvető szolgáltatást nyújt.

A Kszetv. szerint a kijelölő hatóság *„rendszeresen monitorozza és értékeli az ágazatok, az alágazatok, az alapvető szolgáltatások, a lehetséges kritikus szervezetek és kritikus infrastruktúrák ellenálló képességi helyzetét.”* A VBÖ. és VBÖ.vr. ilyen jellegű monitorozást az általános kijelölő hatóság részére nem ír elő, viszont az ország védelme és biztonsága szempontjából jelentős szervezet, infrastruktúra nem honvédelmi kijelölésének jogát a kezébe adja. Ebből következhet, hogy előzetes monitorozási feladatai a jelentős szervezetek és infrastruktúrák tekintetében is vannak.

Az említett monitorozást és értékelést a következő beérkező információk segíthetik:

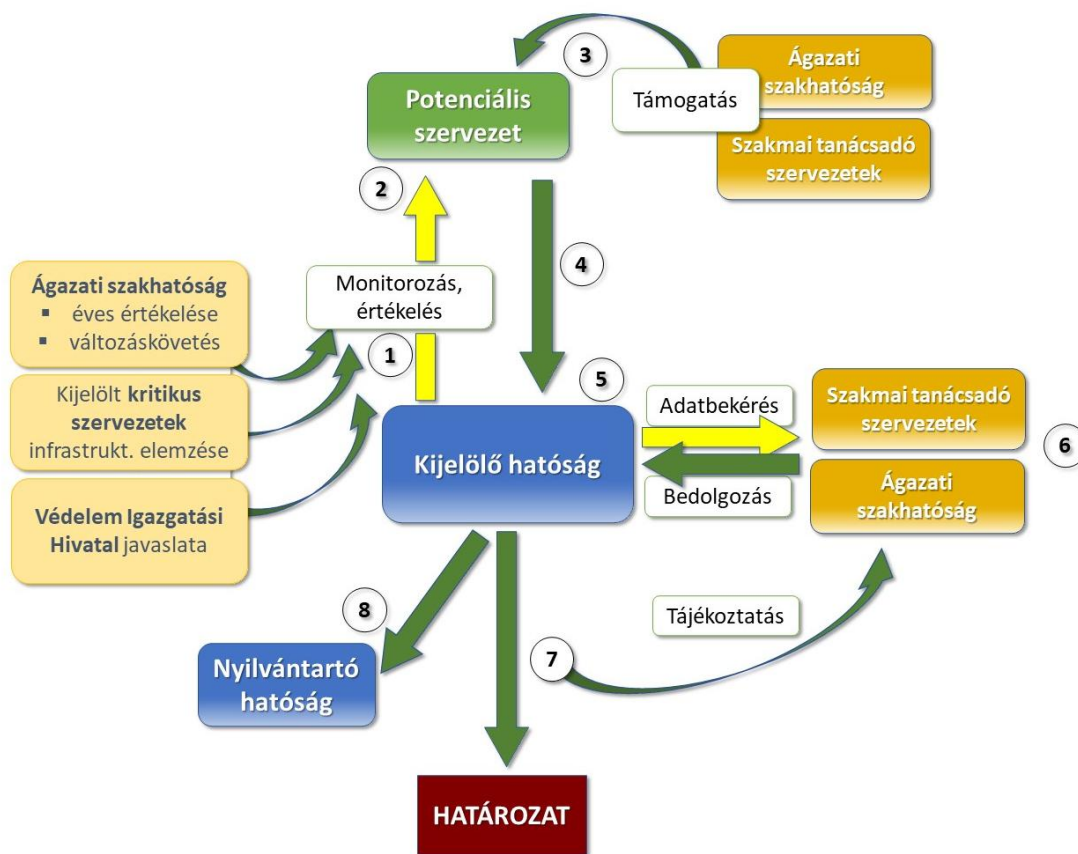
- az ágazati szakhatóságok a rendelkezésükre álló adatokat, engedélyeket, kimutatásokat tartalmazó előző évi értékeléséről szóló tájékoztatását a tárgyévet követő év január 31-ig megküldi az általános kijelölő hatóság részére (Kszetv.vr. 3. § (3));
- az ágazati szakhatóságok rendelkezésére álló adatok, engedélyek, kimutatások év közben változnak, a változások leírását 30 napon belül megküldi az általános kijelölő hatóság részére (Kszetv.vr. 3. § (3));
- a már kijelölt kritikus szervezetek folyamatosan értékelik a kijelölt és a ki nem jelölt infrastruktúráikat, melyekben ha változást tapasztal, 8 napon belül adatszolgáltatási lapot küld a kijelölő hatóság részére (Kszetv.vr. 4. § (4));
- a kijelölő hatóság további hatóságoktól, állami szervektől vagy gazdasági társaságoktól is kérhet adatszolgáltatást, a látókörébe került potenciális kritikus vagy jelentős szervezet kijelölésének folyamatában (Kszetv.vr. 7. § (5) c));
- a védelmi és biztonsági igazgatás központi szerve¹⁰⁵ javaslatot tehet a kijelölő hatóság részére kritikus szervezet kijelölésére irányuló hatósági eljárás megindítására (Kszetv.vr. 6. § (3)).

A kijelölő hatóság honlapjáról letölthető és a megszólított szervezet által kitöltött adatközlő lapnak tartalmaznia kell az alapvető szolgáltatásokra vonatkozó adatokat, a szervezetre vonatkozó személyi és szervezeti adatokat, a szervezet által használt kritikus és nem kritikus infrastruktúrák leírását, az ágazati és horizontális kritériumok teljesülésének vizsgálatát és az ehhez kapcsolódó adatokat, dokumentumokat, más érintett ágazatra, alágazatra vonatkozó adatokat, a Kszetv.vr. melléklete alapján javasolt ellenálló képességi szintre vonatkozó adatokat. Az adatközlő lap sablon egy MS Word alapú, kitöltendő táblázat. Kitöltése feltételezi a szervezet és kapcsolódó infrastruktúráinak előzetes felmérését és a kritikusság elemzését is, mivel olyan eldöntendő (igen/nem) kérdéseket tartalmaz, melyek előzetes vizsgálatot igényelnek. A megszólított szervezet az ágazati szakhatóság segítségével végzi el az adatszolgáltatást.

Amennyiben egy ágazat ágazati kritériumai módosulnak, vagy a kijelölt szervezetek tevékenységében, infrastruktúrák adataiban változás következik be, abban az esetben új adatközlő lapot kell beküldenie az érintett szervezetnek.

Összefoglalva tehát, egy adott szervezet kijelölése a következő elvi folyamat szerint zajlik (1. ábra).

¹⁰⁵ Védelem Igazgatási Hivatal, 337/2022 (IX. 7.) Korm. rendelet a Védelmi Igazgatási Hivatalról; 3.§



1. ábra: kritikus szervezetek kijelölésének folyamata¹⁰⁶

1. A kijelölő hatóság a Védelem Igazgatási Hivatal, a már kijelölt kritikus szervezetek, illetve az ágazati hatóságok adatai alapján monitorozást hajt végre.
2. A kijelölő hatóság a látókörébe került szervezettől előzetes adatszolgáltatást kér be.
3. A megszólított szervezet a kiadott formanyomtatvány kitöltéséhez előzetes szervezeti és működési vizsgálatot végez
4. A megszólított szervezet az adatlapját visszaküldi a kijelölő hatóság részére;
5. A kijelölő hatóság az adatlap értékelése alapján megindítja a kijelölési folyamatot.
6. Ágazati szakhatóság és szakmai szervezetektől bekért adatok alapján további információkat vizsgál:
 - jogszabályok alapján nemzeti kockázatok fennállnak;
 - horizontális kritériumok teljesülése;

¹⁰⁶ Saját szerkesztés a jogszabályok elemzése alapján

- ágazati kritériumok teljesülése, ha szükséges ágazati szakhatóságok állásfoglalása alapján;
 - további szakmai tanácsadó szervezetektől bekért releváns információk.
7. A vizsgálatok alapján a kijelölő hatóság határozatban dönt a kijelölésről vagy az eljárás kijelölés nélküli lezárásáról, melyről tájékoztatja a potenciális szervezetet és az ágazati szakhatóságot.
 8. A kijelölő hatóság a határozatot és a Kszetv. által előírt adatokat megküldi a nyilvántartó hatóság részére.

A megszólított szervezet akkor jelölhető ki kritikus szervezetté, ha Kszetv. szerinti alapvető szolgáltatást nyújt és legalább kettő horizontális, vagy egy ágazati kritériumot teljesít. A kijelölt kritikus szervezet infrastruktúrái nem minősülnek automatikusan kritikus infrastruktúrának. A kijelölt kritikus szervezet által használt infrastruktúrákat egyenként vizsgálni kell. Kritikussá akkor jelölhető ki egy adott infrastruktúra, ha Magyarországon helyezkedik el, a szervezet számára szükséges az alapvető szolgáltatás biztosításához és legalább egy horizontális vagy ágazati kritériumot teljesít. A kijelölő hatóság határozatában – a kijelölést indokló adatok mellett – meghatározza az ellenállóképességi sinthez tartozó követelményeket és 9 hónapos határidővel elrendeli az EKT elkészítését.

Honvédelmi ágazatban vagy más ágazatban, de honvédelmi érdekből jelentős szervezetté, infrastruktúrává történő kijelölés megindításához hasonló adatközlési lapot kér be a honvédelmi ágazati kijelölő hatóság, a VBÖ. által meghatározott alapvető szolgáltatásokat és a VBÖ.vr. ágazati kritériumait alapul véve az azonosításához. A honvédelmi ágazati kijelölő hatóság a horizontális kritériumok teljesülésének vizsgálatára a hivatásos katasztrófavédelmi szerv központi szervét kérheti fel, mint szakhatóságot. Amennyiben a vizsgált szervezetnél a honvédelmi ágazati kritériumok teljesülnek, úgy a honvédelmi kijelölő hatóság önállóan dönthet a kijelölésről, ebben az esetben az azonosítás folyamatába az általános kijelölő hatóságot nem vonja be, csak a kijelölési döntéséről tájékoztatja.

2.2.2. Kijelölt kritikus szervezetek feladatai

A kijelölő határozat véglegessé válását követően a kritikus szervezeteknek átfogó, folyamatos működési, szervezési és ellenőrzési kötelezettségei vannak, melyek célja az alapvető szolgáltatások zavartalan biztosítása és a szervezet ellenálló képességének fenntartása, fejlesztése. A Kszetv.vr. alapján a kritikus szervezet vezetése köteles gondoskodni az alapvető

szolgáltatás folytonosságáról, valamint a kockázatokkal arányos, minden releváns veszélyre kiterjedő védelem kialakításáról, figyelembe véve a függőségi viszonyokat és az esetleges dominóhatásokat.

A szervezet ellenálló képességével kapcsolatos feladatok tervezése, szervezése, végrehajtása igen szerteágazó, új kihívások jelennek meg a szervezet életében. Mindezek koordinálására ki kell jelölni egy ellenállóképességért felelős vezetőt, akinek feladatait, képesítési követelményeit a Kszetv. tartalmazza. Ő fogja össze a kritikus szervezet Kszetv. és Kszetv.vr. által előírt, az ellenállóképesség fenntartását és fejlesztését szolgáló feladatokat:

- EKT elkészítése, illetve az elkészítéséhez szükséges elemzések, vizsgálatok lefolytatása;
- az EKM elkészítése az EKT vizsgálati, kockázatelemzései alapján;
- az elemzések, vizsgálatok alapján, az EKT által meghatározott intézkedések bevezetése;
- fizikai védelem kialakítása, intézkedések bevezetése;
- a munkavállalók, beszállítók, szerződött partnerek részére az ellenálló képességgel összefüggő feladatrendszer kialakítása, együttműködés kialakítása;
- kritikus munkakörben foglalkoztatottak képzése, ellenállóképességgel kapcsolatos feladatrendszerük kialakítása;
- gyakorlatok, ellenőrzések tervezése szervezése;
- ellenálló képességgel kapcsolatos dokumentáció.

Ezekről a feladatokról, illetve részleteikről az értekezés további fejezetei szólnak.

2.3. ELLENÁLLÓ KÉPESSÉGI TERV (EKT)

Az EKT kritikus szerepet játszik a kritikus szervezetek ellenálló képességének kialakításában. A korábbi jogszabályokban Üzembiztonsági Tervnek nevezett okmány elkészítését már a 2080/2008. (VI.30.) a Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló kormányhatározat is szükségesnek ítélte, az Lrtv. pedig a legfelsőbb törvényi szintre emelte az Üzemeltetői Biztonsági Terv kötelező jellegű elkészítését. A Kszetv. által előírt EKT a kritikus szervezet teljes környezeti, biztonsági, védelmi leírását tartalmazza, így mind a kritikus szervezettel való kijelöléskor, majd a nyilvántartás, üzemeltetés és az ellenőrzések, gyakorlatok alkalmával is kiemelt figyelmet kap.

2020. előtt, bár az Lrtv. előírta az Üzemeltetői Biztonsági Terv elkészítését, de részletes tartalmi követelmények nem lettek megadva, így előfordult, hogy a már meglévő külső vagy belső védelmi terv lett kiegészítve vagy mindössze átnevezve. Az Üzemeltetői Biztonsági Terv tartalmi követelményeinek országos szintű egységesítése az Lrtv.vr. 2020-ban kiadott módosításával történt meg.

Az EKT tartalmi követelményeit a Kszetv.vr. tartalmazza, részletes mintát az EKT és a mellékletét képező EKM elkészítéséhez pedig a BM OKF honlapjáról lehet letölteni.¹⁰⁷ Az egységes formában elkészített EKT amellet, hogy igyekszik minden részletre kiterjedően megadni a kijelölt kritikus szervezet és kapcsolódó infrastruktúráinak adatait, környezetét, feltárt kockázatokat, védelmi intézkedéseit, fontos alapját képezi a pontos nyilvántartásnak és az ellenőrzések végrehajtásának is.

Az elkészített EKT-t a kijelölést követően 9 hónapon belül el kell küldeni a kijelölő hatóság részére minden mellékletével együtt, majd a kritikus szervezetnek minden év január 31-ig felül kell vizsgálnia.

2.3.1. Az EKT felépítése

A Kszetv.vr. az EKT tartalmi, a letölthető minta pedig a formai követelményeket határozza meg. Elkészítésekor fontos szem előtt tartani, hogy az EKT nem csupán biztonsági dokumentum, hanem egy átfogó működési térkép kell, hogy legyen, mely a szervezet teljes rendszerét átláthatóvá teszi.

Az EKT bevezető oldalai tartalmazzák az adminisztratív adatokat, a dokumentum verziókövetését és az adatgazdák megjelölését. Ez biztosítja, hogy a terv mindig aktuális maradjon és egyértelmű legyen a felelősség az áttekintéséért.

Az EKT 1. fejezete annak igazolására szolgál, hogy a szervezet megfelel a kritikus szervezetté vagy infrastruktúrává történő kijelölés feltételeinek. Ennek keretében be kell mutatni a horizontális és az ágazati kritériumok teljesülését, külön táblázatban a szervezetre és minden használt infrastruktúrára vonatkozóan. A kritériumok teljesülését (igen/nem) a kijelölő hatóság dönti el az ágazati szakhatóság bevonásával, az indoklás – kritériumonként külön – a szervezet feladata. Ebben a fejezetben kell kifejtetni a szervezet működésében, illetve a kapcsolódó

¹⁰⁷ <https://www.katasztrofavedelem.hu/35635/letoltheto-dokumentumok-es-kitoltesi-segedletek> (letöltés: 2026.02.07.)

infrastruktúrák üzemeltetésében érintett ágazatokat és alapvető szolgáltatásokat is, részletes leírással.

A 2. fejezet a szervezet és az általa üzemeltetett infrastruktúrák teljes körű ismertetését tartalmazza. A bemutatás a szervezet alapadatait, a kritikus infrastruktúra jellemzőit, tevékenységét és az általa nyújtott alapvető szolgáltatás részletes leírását tartalmazza. Külön hangsúlyt kap az üzemfolytonosság kérdése, beleértve a tervezett karbantartási vagy fejlesztési leállások kezelésének rendjét, illetve a környezeti tényezők bemutatása, mely szintén kiemelt fontosságú. Ide tartoznak a földrajzi, meteorológiai, hidrológiai és egyéb külső hatások, valamint a közelben található veszélyes létesítmények, amelyek befolyásolhatják a működést. Ez a rész a külső kockázatok azonosítása mellett az interdependencia kérdésével is foglalkozik. Külön pontban kell kifejtetni, hogy a kritikus szervezet és infrastruktúrái milyen hatással vannak a környezetében lévő veszélyes üzemekre.

A 3. fejezet tartalmazza – táblázatos formában – a szervezet teljes létszámának bemutatását, valamint a kritikus munkakörök és a minimálisan szükséges létszám meghatározását. A létszámadatokat szervezeti egységenként lebontva, a rendszeresített, kritikus és betöltött státusz szerint kell megadni. Ugyancsak ebben a fejezetben kell megadni a külső munkavállalók létszám adatait, tevékenységük és elérhetőségük szerint. Fontos a külső szolgáltatók által biztosított személyzet bemutatása is, mivel az alvállalkozók kiesése ugyanolyan működési kockázatot jelenthet, mint a belső erőforrások hiánya.

A 4. fejezet mutatja be a belső és külső kommunikációs rendszert, a válsághelyzeti kommunikációs stratégiát, valamint a tájékoztatási rendszereket és eszközöket. Kiemelt szerepet kap az ellenálló képességgel kapcsolatos felkészítés. A kommunikáció technikai kérdései mellett, ebben a fejezetben kapott helyet a kritikus munkakörben dolgozók, a vezetők és a rendkívüli események kezelésében résztvevők rendszeres képzésének leírása is.

Az 5. fejezet kifejezetten a dependencia, interdependencia kérdéskörével foglalkozik. A fejezet első táblázatában azt kell vizsgálni, hogy a kritikus szervezet, infrastruktúra hatással van-e alapvető szolgáltatásokra, vagy más alapvető szolgáltatások hatással vannak-e a szervezetre és infrastruktúráira. A táblázat tartalmazza az összes ágazat és alágazat minden alapvető szolgáltatását, melyre igen/nem válasz adható. Külön táblázat szolgál a feltárt dependencia és interdependencia okainak bemutatására, redundancia biztosítottságának kifejtésére. A letölthető mintában nincs erre külön alfejezet, de a Kszetv.vr. alapján, figyelembe véve az alapvető szolgáltatásokat, be kell mutatni a beszállítók rendszerét, illetve az ellátási láncot.

A 6. fejezet bemutatja az irányítási és a belső auditok rendszerét, a vezetői átvizsgálások és a változáskezelés mechanizmusait. Ki kell fejteni az értékelések, auditok rendszerességét, dokumentálását, eredmények kezelésének módszereit.

A 7. fejezet, a kritikus szervezet ellenálló képességének rendszere az EKT egyik központi eleme. Ez a fejezet mutatja be, hogy a szervezet milyen módon azonosítja a lehetséges kockázatokat, hogyan készül fel a speciális helyzetekre, milyen védelmi és biztonsági intézkedéseket alkalmaz, valamint hogyan biztosítja a szolgáltatás folyamatosságát speciális helyzetekben.

A fejezet bemutatja az ellenálló képességért felelős vezető szervezetben elfoglalt helyét, feladatait, hatáskörét és együttműködési kapcsolatait. Amennyiben több alapvető szolgáltatást is nyújt a kritikus szervezet, úgy több ellenálló képességért felelős vezetőt is alkalmazhat.

A Kszetv.vr. megadja az ellenállóképességi szintbe sorolás szabályait, a kijelölő hatóság pedig besorolja a kritikus szervezetet a megfelelő szintbe. A 7. fejezetben részletesen be kell mutatni, hogy a kritikus szervezetre megadott szint szerinti, Kszetv.vr. 1. melléklete által megadott követelmények pontosan hogyan teljesülnek. Ezek a követelmények nagyon részletesen, konkrét leírásokkal fogalmaznak, az egészségügyi, technológiai, kommunikációs biztosítottságról, a fizikai védelemről, létesítményekről, épületekről, a kritikus szervezet belső biztonsági szervezeti elemeiről, kapacitásokról kell részletes leírást adni.

A 8. fejezet célja a válságkezelési képességek bemutatása. Ide tartoznak – külön pontokban – a kontrollált rendkívüli események és a rendkívüli események megelőzésére és kezelésére szolgáló eljárások, nyilvántartások, belső jelentési folyamatuk bemutatása, a kezelésükben érintett személyek adatai, feladatainak leírása, illetve a rendkívüli események hatósági bejelentésének folyamatleírása.

A 9. fejezet a riasztási lánc leírása, melynek célja annak biztosítása, hogy rendkívüli esemény bekövetkezése esetén a szervezeten belül és azon kívül minden érintett szereplő a lehető legrövidebb időn belül értesüljön a helyzetről. A fejezet meghatározza az értesítés sorrendjét, a felelős személyeket, valamint az alkalmazandó kommunikációs csatornákat (telefon, elektronikus rendszer, ügyeleti szolgálat stb.). Fontos elem a döntési szintek elkülönítése, vagyis annak rögzítése, hogy mely események igényelnek vezetői, illetve felsővezetői beavatkozást. A riasztási rendszernek ki kell térnie a hatóságok, együttműködő szervezetek és szükség esetén a lakosság vagy az érintett ügyfelek tájékoztatására is. A rendszer hatékonyságát

rendszeres teszteléssel és gyakorlatokkal szükséges ellenőrizni, melynek leírása ugyancsak ebben a fejezetben történik.

A 10. fejezet mutatja be az évente végrehajtott gyakorlatok tematikáját és a résztvevők körét. Fontos pont az előző évi gyakorlat értékelése, a feltárt hiányosságok és a szükséges fejlesztési intézkedések leírása. A gyakorlatok témáit és eredményeit az EKM alapján kell megadni, mellékelve az igazoló dokumentumokat és a dátumot.

A 11. fejezetet abban az esetben kell kitölteni, amennyiben a kritikus szervezet honvédelmi érdekből is kijelölésre került (kettős kijelölés vagy jelentős honvédelmi ágazati kijelölés). Ismertetni kell az ebből fakadó kötelezettségeket és együttműködési formákat. A fejezet bemutatja a honvédelmi szervekkel való kapcsolattartás rendjét, a kijelölt kapcsolattartókat, valamint az információs szolgáltatás és együttműködés módját. Ide tartozik a honvédelmi ágazatra vonatkozó kritériumok és az abból fakadó kötelezettségek teljesítésének leírása is.

A 12. fejezet kifejezetten az ágazatspecifikus jellemzőket mutatja be. Részletes leírást kell adni az adott ágazatra jellemző technológiai, működési és biztonsági követelményekről, valamint azokról a speciális kockázatokról, amelyek a tevékenységből adódnak. A fejezet kidolgozása szoros kapcsolatot feltételez az ágazati szakhatósággal és szükség szerint egyéb szakmai szervezetekkel is.

A 13. fejezet a mellékletek felsorolását tartalmazza.

2.3.2. EKT kapcsolódó mellékletei, okmányai

Az EKT tartalmi áttekintésekor könnyen belátható, hogy az EKT több okmányból és adatcsoportokból álló dokumentum csomag, rendszerleírás.

Az adatok biztonságos kezelése és a változások folyamatos lekövetése érdekében érdemes olyan dokumentum csomagot létrehozni, melyben az EKT a fő dokumentum, és ehhez kapcsolódnak a kiegészítő tervek, adatok, részletező okmányok.

A BM OKF weblapjáról letölthető minta tartalmazza a kötelezően kitöltendő, a kijelölő hatóság által meghatározott formátumú mellékletek mintáját is. Ezek olyan adatokat is tartalmazhatnak, melyekre több esetben speciális adatkezelési szabályok vonatkoznak:

- a kritikus szervezet azonosító adatai, elérhetőségei;
- a kritikus infrastruktúrák azonosító adatai, elérhetőségei;

- a kritikus szervezet vezetésének, érintett szakterületek vezető tagjainak azonosító adatai, elérhetőségei;
- az ellátási lánc, illetve a kritikus infrastruktúra működése szempontjából kritikus műveletek, technológiák, szolgáltatások, termékek, alapanyagok, vevők, szolgáltatást igénybe vevők listája;
- az EKM, általános és ágazatspecifikus kockázatokkal (xlsx);
- a kritikus munkakörben foglalkoztatottak személyazonosító adatai, besorolásai (xlsx);
- az alapvető szolgáltatás nyújtásához szükséges gépjárművek nyilvántartása (xlsx).

A BM OKF weblapjáról letölthető minta előírja olyan mellékletek elkészítését is, melyre kötelező formát nem ad meg, de csatolandó az EKT-hoz:

- a szervezeti felépítést, struktúrát bemutató ábra, organogram;
- a kritikus szervezet járványügyi intézkedésekkel kapcsolatos terve;
- a kritikus infrastruktúra és környezetének felülnézeti (műholdas, drón) képe;
- hálózatos rendszereket üzemeltető kritikus szervezet esetén a teljes hálózati infrastruktúrájának bemutatása;
- az irányítási rendszer működtetésének igazolása, tanúsított rendszer esetén irányítási rendszer működését igazoló dokumentumok;
- Szervezeti és Működési Szabályzat;
- Üzemeltetési szabályzat;
- Karbantartási szabályzat;
- Rendkívüli esemény eljárásrend;
- Információbiztonsági szabályzat;
- Tűzvédelmi szabályzat;
- Munkavédelmi szabályzat.

Külön, minősített okmányokban érdemes összefoglalni azon adatokat, melyekre nincs külön rendelkezés, de tartalmuknál fogva szigorúbb kezelést igényelnek, vagy annak érdekében, hogy a bennük szereplő adatok változása ne tegye szükségessé az EKT komolyabb módosítását. Ilyenek lehetnek:

- ipari titkot tartalmazó eljárások, folyamatok;
- informatikai, védelmi rendszer felügyeleti beállításai, kódjai;
- honvédelmi szervekkel kapcsolatos speciális együttműködési adatok;
- pénzügyi adatok;
- egyéb, szigorú szabályok szerint kezelendő adatok.

Egy potenciális kritikus szervezet, mint munkáltató, alapesetben is kötelezett munkavégzés keretében keletkező egészségkárosodással és baleseti veszéllyel járó munkahelyi kockázatok vizsgálatára, elemzésére¹⁰⁸, illetve a veszélyes anyagokkal foglalkozó üzemek védelmi terveket kötelesek készíteni¹⁰⁹. A feltárt kockázatokhoz kapcsolódóan minden üzemnek, létesítménynek rendelkeznie kell különböző rendszerleírásokkal, védelmi, üzemzavar kezelési tervekkel, melyeket az EKT kidolgozása során össze kell hangolni, illetve a továbbiakban folyamatosan felül kell vizsgálni, módosítani, aktualizálni.

Ezekre az okmányokra az EKT megfelelő fejezetében hivatkozik, így egy adott rendszerleírás vagy terv módosításakor az EKT-t nem szükséges módosítani. Ilyenek lehetnek:

- részletes támogató technológiai leírások;
- Őr- és biztonsági szolgálatok szabályzata;
- fizikai védelmi terv;
- környezetvédelmi terv;
- kiürítési terv;
- egyéb, üzemspecifikus védelmi és technológiai tervek.

2.4. KRITÉRIUMOKRA ÉPÜLŐ KOCKÁZATELEMZÉS

Az előző alfejezetben elhangzott, hogy egy potenciális kritikus szervezet, mint munkáltató, alapesetben is kötelezett munkavégzés keretében keletkező egészségkárosodással és baleseti veszéllyel járó munkahelyi kockázatok vizsgálatára, elemzésére.¹¹⁰ A kockázatelemzések elvégzésénél alapfeltételezés, hogy a szervezet működésében minden jogszabályi és üzemi előírás megvalósul, maga a kockázatelemzés folyamata pedig nem más, mint becsléseket és feltevéseket tartalmazó veszélyelemzés.

Sorra kell venni mindazokat a lehetőségeket, melyek veszélyeztethetik az üzemfolytonosságot, mely veszélyhelyzetek valószínűségének és súlyosságának együttes hatásvizsgálata alapján – mint feltárt kockázat¹¹¹ – meghozható a szükséges védelmi, biztonsági intézkedés. Vagyis egy veszély abban az esetben minősül kockázatnak, ha bekövetkezésének valószínűsége nagyobb mint nulla.

¹⁰⁸ 1993. évi XCIII. törvény a munkavédelemről; 54. § (2) bekezdés

¹⁰⁹ 2019/2011. (X.20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről

¹¹⁰ 1993. évi XCIII. törvény a munkavédelemről; 54. § (2) bekezdés

¹¹¹ 1993. évi XCIII. törvény a munkavédelemről; 87. § (1/F) bekezdés

A továbbiakban a „rendkívüli esemény”, „kontrollált rendkívüli esemény”, „veszélyhelyzet” fogalmi között csak abban az esetben tesztek különbséget, ha a reziliencia és védelmi képességek tárgyalásánál ez releváns.

2.4.1. Az Ellenálló Képességi Mátrix (EKM)

Az EKM egy táblázatkezelő szoftverre optimalizált adatbázis, mely két különálló lapot tartalmaz. Az első lapon felsorolja a lehetséges *általános kockázatok* fajtáit, a második lapon pedig kockázati mátrix alapú elemzéshez ad meg *értékkészletet*, részletes magyarázattal. Az EKM áttekintéséhez szükséges szólnunk röviden a kockázati mátrix típusú elemzési módszerről, mely alapján érthetővé válik az EKM felépítése.

2.4.1.1. Kockázati mátrix

Ez a fajta elemzés alapesetben a már feltárt kockázatok két szempont szerinti kategorizálására épül. A két szempont, a kockázat valószínűsége és a kockázat következményeinek súlyossága adja a mátrix két dimenzióját. Mindkét szempont több fokozatra bontható. Minél több fokozat szerepel egy kockázati mátrixban, annál pontosabban meghatározható egy bizonyos kockázat potenciálja.¹¹²

Leggyakrabban a 3 (2. ábra) és az 5 fokozatú mátrixokat alkalmazzák a szervezetek kockázatelemzésének végrehajtására.

		Hatás		
		kicsi	közepes	jelentős
Valószínűség	ritka			
	gyakori			
	nagyon gyakori			

2. ábra: kockázati mátrix felépítése¹¹³

A kockázati mátrixban található színjelölések:

- zöld szín: alacsony kockázatú tényezők,
- sárga szín: közepes kockázatú tényezők,

¹¹² Fiath A. (2025): Vállalati kockázatkezelés komplex rendszere. Humán Innovációs Szemle. XVI. évf. 2025/2. 107-118.

¹¹³ Saját szerkesztés

- piros szín: magas kockázatot jelentő tényezők.

A kockázati mátrix celláinak színeként által kiadott mintázat változtatható. Látható, hogy minél több cellát foglal el a piros szín, annál szigorúbb a kockázatok kezelése, vagyis megállapítható, melyek azok a kockázatok, melyek prioritást élveznek a védelmi intézkedések kialakítása során.

2.4.1.1. Ellenálló Képességi Mátrix (EKM)¹¹⁴

Az xlsx kiterjesztésű EKM két fő részből áll. Az **első lapon** 92 lehetséges kockázat van megnevezve, – nem kockázati terület szerint, hanem ABC sorrendben – melyek felölelik a természeti és civilizációs katasztrófák, balesetek, szándékos infokommunikációs és fizikai károkozások, támadások lehetséges fajtáit. Minden egyes kockázathoz meg kell adni:

- a kockázat részletes leírását;
- a kockázat elemzés szerinti eredetileg fennálló, kiinduló állapotát. Lenyíló menüből lehet kiválasztani az értékkészletben megadott adatokat a valószínűség, a hatás és a kitettség tekintetében, illetve a kockázatkezelés módját és státuszát (aktív, nem aktív);
- a kockázat elemzés szerinti jelenlegi állapotát. Hasonlóképpen, lenyíló menüből lehet kiválasztani az értékkészletben megadott adatokat a valószínűség, a hatás és a kitettség tekintetében, melyből a táblázat automatikusan számolja a kockázat mértékét.
- az aktuális kockázatkezelés adatait. A kockázatkezelés módja – lenyíló menüből – *átruházás, elfogadás, elkerülés* és *kockázatcsökkentés* lehet. Ezen kívül meg kell adni az intézkedés leírását, a felelősök adatait, a határidőket és az igazoló dokumentumok megnevezését;
- tervezett kockázatcsökkentő intézkedéseket, az intézkedés célja, terve, határideje és felelőse adataival, leírásával.

A **második lap** az első lap kitöltéséhez szükséges értékkészlet magyarázatát és az értékek alapján automatikusan számolt kockázati mátrixot tartalmazza. A mátrix alapvetően három dimenzióval számol: valószínűség, hatás és kitettség (3. ábra), a következő módon:

$$\text{Kockázat értéke} = \text{Valószínűség} \times (\text{Hatás} + \text{Kitettség})$$

A *valószínűség* számszerűsítésére a bekövetkezés időintervallumát adja meg:

- nagyon ritka: 10 éven belül legalább egyszer bekövetkezik (1)

¹¹⁴ <https://www.katasztrofavedelem.hu/35635/letoltheto-dokumentumok-es-kitoltesi-segedletek> (Letöltés: 2026.02.22.)

- ritka: 5 éven belül legalább egyszer bekövetkezik (2)
- alkalmanként: 3 éven belül többször bekövetkezik (3)
- gyakori: 1 éven belül legalább egyszer bekövetkezik (4)
- nagyon gyakori: 1 éven belül többször bekövetkezik (5)

A *hatás* értéke már több összetevős. Az elhanyagolható (1), alacsony (2), közepes (3), magas (6) és katasztrofális (12) hatás értékeit külön-külön kell megadni működésre, személyekre, vagyokra, környezetre és hírnévre, melyekből a kockázati érték számításánál a legnagyobbat veszi alapul a képlet.

A *kitettség* úgy jelenik meg a mátrixban, hogy a hatás mértékét növeli. Számszerűsítve, ha nincs kitettség (0), ha egy fél irányából van kitettség (1), illetve ha több fél irányából van kitettség (2), mely hozzáadódik a hatás értékéhez.

		Hatás				
		elhanyagolható	alacsony	közepes	magas	katasztrofális
Valószínűség	nagyon gyakori	5	10	15	30	70
	gyakori	4	8	12	24	48
	alkalmanként	3	6	9	18	36
	ritka	2	4	6	12	24
	nagyon ritka	1	2	3	6	12

3. ábra: EKM felépítése¹¹⁵

Az EKM kockázati mátrix színek alapján látható, hogy az EKM öt szintet határoz meg a kockázatok kezelésére:

- azonnali beavatkozást igénylő, nem elfogadható kockázat;
- rövidtávon intézkedést igénylő kockázat;
- intézkedést igénylő kockázat;
- elemzés alapján elfogadható kockázat;
- elhanyagolható kockázat.

Az EKM bár részletes eredményekkel szolgál a kritikus szervezetre, infrastruktúrára veszély jelentő kockázatokat illetően, de helyes kitöltéséhez előzetes kockázatazonosításra, elemzésekre van szükség, melyhez ajánlást, módszert nem ad meg. Emellett nem ad megoldást a többszintű interdependencia vizsgálatára sem. Tehát egy potenciális kritikus szervezet az EKT és az EKM elkészítéséhez már olyan előzetes kockázatazonosítással kell, hogy rendelkezzen,

¹¹⁵ Saját szerkesztés a letölthető EKM minta alapján

mely végrehajtása esetenként meghaladhatja a szervezet munkavállalóinak képesítését, lehetőségeit.

Valós példa:

Az általam vizsgált pénzügyi kritikus szervezet esetében külön vizsgálatot igényelt, hogy egy humán eredetű járványhelyzet mennyiben befolyásolja a külső szolgáltatótól igénybe vett őrzésvédelmi szintet, illetve milyen jellegű előzetes és vészhelyzeti intézkedéseket kell bevezetni, mind a kritikus szervezet, mind a szerződött szolgáltató cég részéről.¹¹⁶ Ehhez a vizsgálathoz szükséges volt külső egészségügyi szakember bevonása.

2.4.2. Kockázatazonosítás és kockázatelemzés további lehetséges módszerei

Az előző alfejezetben már szóba került, hogy a kockázati mátrix alkalmazása a már feltárt kockázatok különböző szempontok szerinti kategorizálására épül. Vagyis az EKM részletes magyarázata mellett, a kockázatok azonosítása mindenképpen szükséges, az EKM celláit csak előzetes kockázatazonosítást és elemzést követően lehet helyesen kitölteni.

A kockázatelemzés hatékonyságának alapja a helyesen, széleskörűen meghatározott veszélyek és kockázati tényezők teljes körének azonosítása.¹¹⁷ Az azonosítás szakaszában nem kell (nem szabad) mérlegelni a felmerülő veszélyek, kockázatok hatását, súlyosságát, fontos, hogy lehetőség szerint az összes veszélyt és kockázatot azonosítsuk. A kockázatok azonosítására és a feltárt kockázatok elemzésére több módszer áll rendelkezésünkre, melyek az EKM helyes kitöltéséhez jól alkalmazhatók.

Brainstorming

Ötletelés. Napjainkban egyre elterjedtebb ez a fajta csoportos munkára, a csoporttagok különböző gondolkodásmódjára építő technika. Lényege, hogy egy konkrét vagy széleskörű problémafelvetésre a csoport tagjai saját gondolataikkal reagáljanak. A brainstorming eredménye nem maga a kész megoldás, hanem a felvetett probléma kiterjesztése, részekre tagolása, több oldalról való megközelítése, mely nagyban hozzájárul a későbbi hatékony

¹¹⁶ BakosT.: *Kijelölt létfontosságú rendszerelem védelme a pandémiás veszélyhelyzet idején*, Szemelvények a katonai műszaki tudományok eredményeiből III., szerk.: Földi László; Ludovika Egyetemi Kiadó, Budapest, 2022.

¹¹⁷ [42] Fiath A. (2025): Vállalati kockázatkezelés komplex rendszere. *Humán Innovációs Szemle*. XVI. évf. 2025/2. 107-118.

elemzésekhez. Fontos, hogy a résztvevők azonos szinten legyenek képesek részt venni a csoport munkájában, még akkor is, ha nincsenek azonos szakmai állásponton, vagy esetleg eleve más szakterületet képviselnek. A brainstorming technika helyes alkalmazásakor törekedni kell arra, hogy ne befolyásolja a csoport gondolkodását a szervezetben meglévő alá-fölé rendeltség.¹¹⁸

Interjú módszer

A kvalitatív, vagyis kisebb csoport részvételével végzett, de mélyebb betekintést adó módszerek közül az egyik legalapvetőbb az interjúk készítése. Személyenként végrehajtott interjú során, a felvetett problémához kötött irányított kérdésekkel mélyebb, részletesebb szakmai válaszok érhetők el. Lehet csoportos végrehajtása is, mely hasonlít ugyan a brainstormingra, de az interjút készítő szakember előre meghatározott kérdésekkel irányítja a beszélgetést.

Delphi módszer

A Delphi módszert az amerikai RAND Corporation fejlesztette ki az 1950-es években, hogy előre jelezze a technológia hadviselésre gyakorolt hatását. Azóta már több helyen és szakterületen elterjedt az alkalmazása. Lényege, hogy egy szakértőkből vagy érdekelt felekből álló csoport, akár online, akár írásban, de fontos, hogy anonim módon, kérdőív alapján fejt ki véleményét egy adott témában. Az összesített csoportválaszt a tagok ismét megkapják, melyet felülvizsgálva, megvitatta jutnak el a szakértői konszenzusig.¹¹⁹

Ellenőrző lista (Check List Analysis – CLA)

Korábbi tapasztalatokra és információkra épített sablon alapján végrehajtható elemzési módszer. Lényege, hogy egy adott probléma több összetevőjére van bontva, az összetevők részletes vizsgálatára pedig az ellenőrző lista tételeire adott válaszokból lehet következtetni. A tételekre olyan választ kell adni, melyek a sablonszerűen kialakított kritériumok szerint automatikusan ellenőrizhetők. A jól kidolgozott ellenőrző lista részletes információkat adhat a

¹¹⁸ A hatékony brainstorming titka. Kövecses Evelin – HR stratégia. (<https://www.profession.hu/hrfeed/a-hatekony-brainstorming-titka>) Letöltés: 2026.01.24.

¹¹⁹ RAND research organization. Delphi Method. (<https://www.rand.org/topics/delphi-method.html>) Letöltés: 2026.01.24.

felvetett problémáról, de a tételek csak nagyon szűk mozgásteret adnak az ok-okozati folyamatok megértésére. Ezért ezt a módszert mindig más módszerekkel együtt kell alkalmazni.

Technológiai folyamatok elemzése

Az iparbiztonsági elemzések végrehajtása során alkalmazhatóak a szabványos veszélyelemzési eljárások, melyek elsősorban a folyamatok, műveletek belső fenyegetettségének, veszélyeinek feltárására alkalmasak. Amennyiben maga a folyamat vagy művelet tartalmaz veszélyes elemet – például veszélyes anyag kezeléssel alapuló vagy tűzveszélyes technológia – több, nemzetközi szabványok által meghatározott eljárás létezik a műszaki rendszerek meghibásodási, megbízhatósági vizsgálatához, illetve a szükséges biztonsági szint megállapításához.

- IEC 61882 - HAZOP (működőképesség és veszélyelemzés)
- IEC 60812 - FMEA (hibamód és hatáselemzés)
- IEC 61025 - FTA (hibafa elemzés)
- IEC 62502 - ETA (eseményfa elemzés)
- LOPA (védelmi réteg elemzés)

Ezeket a szabványos elemzési módszereket a legtöbb esetben kombinálva alkalmazzák, ezzel kizárva az egyes elemzések gyenge és kihasználva az erős pontjaikat. Mivel ezek az elemzések részletesen tartalmazzák az alkalmazott technológiák pontjainak veszélyeztetettségét, illetve a veszélyhelyzetben adható válaszlépéseket, így nagyon jó alapot adhat a kritikus szervezetek és infrastruktúrák EKT és EKM, illetve a kapcsolódó terveinek kidolgozásához.¹²⁰

PESTEL-analízis

A külső környezeti tényezők részletesebb vizsgálatára alkalmazható a PESTEL/PESTLE analízis, mely elnevezés – hasonlóan az előzőhöz – a vizsgált tényezők angol megnevezésének kezdőbetűiből áll.¹²¹

- Political = Politikai környezet;
- Economic = Gazdasági környezet;
- Social = Társadalmi környezet;

¹²⁰ Kockázatmenedzsment – folyamat, elemzés és módszerek. OTRS Gr. (<https://otrs.com/hu/blog/biztonsag-megfeleles/kockazatmentedzsment-br-folyamat-elemzes-es-modszerek/>) Letöltés: 2026.01.24.

¹²¹ <https://nit-edu.org/wp-content/uploads/2022/04/PESTEL-Analysis-for-Small-Businesses.pdf>, 2023.12.18.

- Technological = Technológiai környezet.
- Environmental = Természeti környezet;
- Legal = Jogi környezet.

A PESTEL analízis általában stratégiai marketing és gazdasági tervezéshez, piackutatáshoz használható. A meghatározásából látható, hogy a vizsgálat tárgyát képező elem (vállalt, üzleti terv, folyamatterv, stb.) környezetének, tehát a rá ható külső körülményeknek a csoportokra bontásával határozza meg a kulcsfontosságú hatásokat. Előnye, hogy ezen hatások közé nem csak a veszélyeket, hanem a lehetőségeket is beemeli.

SWOT-analízis

(Strengths – Weakness – Opportunities – Threats) Erősségek – Gyengeségek – Lehetőségek – Veszélyek.

A SWOT-analízis nem ad részletes elemzést a kockázatokról, de segít azonosítani azokat a belső és külső tényezőket, melyek befolyásolhatják a biztonságos és folyamatos üzemeltetést.

	Pozitív	Negatív
Belső	<i>Erősségek (Strengths)</i>	<i>Gyengeségek (Weakness)</i>
Külső	<i>Lehetőségek (Opportunities)</i>	<i>Veszélyek (Threads)</i>

4. ábra: SWOT-analízis¹²²

A belső tényezőket képesek vagyunk befolyásolni, az erősségeket szinten tartani, vagy kihasználni, a gyengeségeket fejleszteni. Ide tartozhatnak a vezetőségi és munkavállalói képzettség, a vezetés hatékonysága, az anyagi háttér stabilitása, a technológiai fejlettség.

A külső tényezők azok a működésre, üzemeltetésre ható környezeti hatások, melyeket csak a legkritkább esetben tudunk befolyásolni. Lehetőséget jelenthet az új technológiák megjelenése, biztonsági trendek pozitív változása, melyekre építeni lehet. A veszélyek, fenyegetések pedig azok a külső tényezők, melyekre hatásunk nincs, de az ellenük való védelem kialakítása, a negatív helyzetekre való felkészülés segíthet az üzemfolytonosság megtartásában. Ilyen veszélyek lehetnek a környezeti, szociális veszélyek (éghajlatváltozás, társadalmi

¹²² Saját szerkesztés

feszültségek), fizikai fenyegetések, de ide sorolhatók a jogszabályi változások, a gazdasági recesszió is.

Hálózatelemzés (Network Analysis)

A hálózatelemzés egy hálózat különböző elemeit, mint csomópontokat és az ezek közötti kapcsolatok (Élek) szerkezetét és dinamikáját vizsgálja. A célja, hogy feltárja a rendszerben a kölcsönös függőségeket, meghatározza a legfontosabb szereplőket és elemezze a kapcsolatok erősségét. Az ehhez tartozó fokszám egy csomóponthoz kapcsolódó egyéb elemek száma, amely megmutatja, hogy egy adott elem mennyire van beágyazva a hálózatba. A csomópontok közötti kapcsolatok különböző típus szerint (információáramlási, kereskedelmi, diplomáciai stb.) elkülöníthetők, jellemezhetők lehetnek.

Főbb alkalmazási területei:

- Interdependencia vizsgálatok;
- Társadalmi hálózatok elemzése (pl. kapcsolati mintázatok feltárása, központi szereplők azonosítása stb.);
- Nemzetközi kapcsolatok és geopolitika (pl. országok kapcsolati hálójának feltárása súlyozás alapján is);
- Ellátási láncok és logisztika (pl. szerkezetek feltárása, kockázati pontok felismerése stb.);
- Pénzügyi rendszerek stabilitásának vizsgálata (pl. bankok sebezhetőségének, fertőzési kockázatának feltárása);
- Biológiai és egészségügyi kutatások (pl. rendszerek modellezésére, betegségek közötti kapcsolatok feltárása, járványok terjedésének modellezése stb.).¹²³

Input-output analízis (Leontief-modell)

Az input-output analízis, más néven Leontief-modell, egy közgazdasági matematikai módszer, amelyet Wassily Leontief dolgozott ki a gazdaság különböző ágazatai közötti fizikai függőség vizsgálatára.

¹²³ Bakos, T., Kovács, F. (2025): Az interdependencia dimenziói és a kritikus szervezetek vizsgálata. *Hadtudomány* 35(3), pp. 106–119.

A modell azt mutatja meg, hogyan függenek az egyes gazdasági szektorok egymástól: azaz melyik ágazat mennyi inputot, erőforrást, terméket vagy szolgáltatást használ fel más ágazatokból, illetve mennyi outputot, terméket vagy szolgáltatást állít elő, amelyet más ágazatok használnak fel. Két típust különböztet meg:

- Nyílt modell: feltételezi a külső keresletet a fogyasztót és azt számítja ki, mekkora összkibocsátás szükséges ennek kielégítéséhez.
- Zárt modell: a fogyasztást is a rendszer belső részének tekinti, minden szereplőt – beleértve a háztartásokat is – termelő szektornak tekint (pl.: a háztartások munkát adnak el és termékeket vesznek).¹²⁴

Rendszerelméleti megközelítés

A valóságot rendszerek összességeként értelmezi. Egy rendszerben különböző elemek és alrendszerek vannak, melyek kapcsolatban állnak egymással. Ezek a kapcsolatok az interakciók. Az egyes elemek viselkedése nem külön-külön, hanem az egész rendszer működésének részeként értelmezhető.

A rendszerelmélet alapvető fogalmai közé tartozik a visszacsatolás, amely lehet pozitív vagy negatív. A pozitív visszacsatolás olyan folyamatokra utal, amelyek során egy adott hatás felerősíti önmagát, míg a negatív visszacsatolás stabilizáló mechanizmusként működik a rendszerben. Például a globális hőmérséklet emelkedése fokozza a jégolvadást, amelynek következtében csökken a Föld felszínének fényvisszaverő képessége, ezáltal tovább nő a hőelnyelés és így a hőmérséklet is – ez egy klasszikus pozitív visszacsatolási kör. A rendszerek viselkedése ezen visszacsatolási mechanizmusok mentén alakul ki, amely meghatározhatja azok egyensúlyi állapotát, stabilitását vagy akár összeomlását is.

A rendszerelméleti megközelítés fontos elemei továbbá a hálózatok, az anyag- és energiaáramlások, valamint a rendszerek határainak meghatározása, melyek kulcsfontosságúak a komplex rendszerek működésének megértésében.

¹²⁴ Bakos, T., Kovács, F. (2025): Az interdependencia dimenziói és a kritikus szervezetek vizsgálata. *Hadtudomány* 35(3), pp. 106–119.

Az interdependencia vizsgálata szempontjából fontos megközelítés, mivel a kölcsönös kapcsolatok és a hálózati jelleg hangsúlyozására épül és segít megérteni, hogyan alakulnak ki összetett következmények sok egyszerű, egymással kapcsolatban lévő döntésből.¹²⁵

Klaszter- és korrelációelemzés

A klaszteranalízis és a korrelációelemzés az interdependencia vizsgálatok két különböző, de gyakran egymást kiegészítő módszere a statisztikában és adatbányászatban. Ezekkel nem egy függő változót vizsgálunk, hanem a változók vagy megfigyelések közötti kapcsolatokra, összefüggésekre vagy hasonlóságokra fókuszálunk.

Klaszteranalízis célja olyan homogén csoportokat (klasztereket) találni az adathalmazban, amelyek tagjai egymáshoz hasonlóak, de más csoportoktól eltérnek. Alkalmazása gyakori a piackutatásban (pl.: vásárlók szegmentálása viselkedés alapján), a biológiában (pl.: fajok vagy gének csoportosítása), vagy a társadalomtudományban (pl.: hasonló jellemzőkkel bíró csoportok azonosítása).

Korrelációelemzés két vagy több változó közötti kapcsolat erősségének és irányának vizsgálatára irányul. A korreláció nem jelent ok-okozati viszonyt, csak azt mutatja meg, hogy ha az egyik változó értéke módosul, azzal együtt jár-e a másik változó szisztematikus változása.

Rendszerbiztonsági és sebezhetőségi elemzések

Rendszerbiztonsági elemzések célja annak feltárása, hogy egy rendszer mely komponensei milyen mértékben befolyásolják egymás biztonságát és hogyan terjed egy biztonsági zavar a rendszeren belül.

Klaszterezés segítségével azonosíthatók a biztonsági szempontból egymáshoz közel álló modulok (pl.: hasonló konfigurációjú szerverek), majd korrelációval vizsgálható, hogy egy zavar gyakorisága és bizonyos rendszerelemek aktivitása között van-e kapcsolat. Klaszteranalízisnél csoportosíthatók azok az eszközök vagy felhasználók, amelyek hasonló kockázati profillal rendelkeznek (pl.: sok bejelentkezési hiba, elavult szoftver, nyitott portok, stb.). Korrelációelemzésnél vizsgálhatjuk, hogy van-e összefüggés a nyitott portok száma és a

¹²⁵ Bakos, T., Kovács, F. (2025): Az interdependencia dimenziói és a kritikus szervezetek vizsgálata. *Hadtudomány* 35(3), pp. 106–119.

behatolási kísérletek száma között. Ha szoros pozitív korreláció van, az azt jelenti, hogy az adott konfiguráció sebezhető.

A rendszerbiztonsági és sebezhetőségi elemzések során az interdependencia vizsgálatok segítenek összefüggéseket feltárni és prioritásokat meghatározni a védekezésben. Nemcsak az egyedi hibák, hanem azok hatása más rendszerekre is előtérbe kerül.¹²⁶

2.4.3. Kockázatelemzés eredményeinek ágazati és horizontális kritériumokra épülő kezelése

Minden kockázatelemzési módszer más és más oldalról közelít, más részekre fókuszál, ezért érdemes több módszer alkalmazásával létrehozni egy átfogó elemzést, mely alapján az EKT és EKM folyamatosan aktualizálható.

Az átfogó kockázatelemzés nem egy egyszeri alkalommal végrehajtott feladat, hanem egy permanens, ciklikus védelmi folyamat elengedhetetlen része. (5. ábra)



5. ábra: a kockázatelemzés ciklikussága¹²⁷

¹²⁶ Bakos, T., Kovács, F. (2025): Az interdependencia dimenziói és a kritikus szervezetek vizsgálata. *Hadtudomány* 35(3), pp. 106–119.

¹²⁷ Saját szerkesztés

A kiadott EKT és az EKM minta elemzésével megállapítható, hogy a felületesen elkészített dokumentumok nem fedik le teljes egészében a folyamatot, hiszen mindössze a 2. pontban lépnek be a ciklusba. Az 1. lépésben feltárt kockázatokat – újként vagy módosítással – be kell vezetni az EKM listájába, a hozott intézkedések alkalmazásának és a bevalás értékelésének eredményei alapján pedig folyamatosan pontosítani kell a dokumentumokat.

Az előző alfejezet pár példájából látható, hogy a kockázatazonosítás több módszerrel is végrehajtható. Fontos szem előtt tartani, – ahogyan azt korábban megállapítottam – hogy hatásától és valószínűségétől függetlenül minden lehetséges kockázatot azonosítsunk. A kockázatazonosítás eredményeit összesítve, azokat csoportokba rendezve nem csak a kockázatelemzés és az EKM elkészítése könnyíthető meg, de a végeredmény által kiadott mintázat a vizsgált szervezet, infrastruktúra veszélyeztetettségi típusát is kiadja, a veszélyeztetettség típusának meghatározása pedig a védelmi intézkedések és technológiák prioritizálását segíti elő.

Az azonosított kockázatok elemzése, kiértékelése a következő fontos lépés, melynek célja a kockázatok bekövetkezésekor létrejövő hatásmechanizmusok feltárása, a kockázati potenciál meghatározása.

Egy adott kockázat részletes hatásmechanizmusának feltárása több szempontból is lényeges. Segít megérteni a bekövetkezés pontos lefolyását, feltárja az egyéb kockázatokkal való kapcsolatát, pontosabban megállapíthatóvá válnak a hatásai, segít kialakítani a hatékony védelmi intézkedéseket. A kritikus szervezetek, infrastruktúrák tekintetében ez kiemelt feladat, hiszen a Kszetv. által meghatározott horizontális és a Kszetv.vr. által meghatározott ágazati kritériumok teljesülését ezen vizsgálatok alapján lehet igazolni vagy cáfolni. A kockázatelemzés az ágazati szakemberek részéről is tágabb értelmezést tesz szükségessé, hiszen a szakmai szempontokon kívül egyéb lehetséges hatások bekövetkezésének lehetőségét is vizsgálni kell, szükség lehet más ágazatok szakembereinek megkeresésére.

Példa, az általam vizsgált egészségügyi kritikus szervezet esetében: informatikus és gépész szakemberek megállapítják, hogy a vízellátó rendszer egy bizonyos elemének sérülése a teljes rendszer rövid idejű leállítását okozhatja, melynek hosszabb távon jelentkezhet negatív hatása a vízelosztó rendszerre és a végfelhasználóhoz eljuttatott víz minőségére is. A hatások tágabb értelmezésére – ezzel együtt külső szakértők bevonására – van szükség annak megállapításához, hogy milyen egészségügyi és ebből fakadóan milyen társadalmi és politikai hatások keletkezhetnek.

Fenti példa alapján látható, hogy a kritikus szervezetek esetében a kockázatelemzési módszerek tágabb értelmezése mellett, szükséges a nyitott, szakterületen túlmutató vizsgálat, illetve az ágazat egyéb területeivel, vagy más ágazatokkal való folyamatos kapcsolattartás, mely alapja lehet az ágazatokat és infrastruktúra hálózatokat átfogó interdependencia vizsgálatnak is.

2.5. AZ INTERDEPENDENCIA VIZSGÁLAT

Ahogy bevezetőmben említettem, napjainkra a társadalmakat működtető szolgáltatások igen magas fejlettségi szintet értek el és jelenleg is folyamatosan fejlődnek. Ennek az állandó rendelkezésre állásnak és fejlődésnek az alapja az, hogy a szolgáltatások és infrastruktúrák egymásra támaszkodnak, speciális hálózattal rendelkező rendszert alkotnak, mely óriási előnye, hogy képes a társadalmi elvárások apróbb változásainak lekövetésére is.

Ennek a rendszernek az előnye viszont egyben a hátránya is. Bármely változás a rendszerben, kihatással van a rendszer egyéb elemeire és előre nem, vagy csak nehezen meghatározható módon akár láncreakció szerű hatásokat is kiválthat.

A rendszerek elemei közötti kölcsönös függőséget, vagyis interdependenciát tehát feltétlenül figyelembe kell vennünk, ha egy adott rendszer stabilitását, rezilienciáját vizsgáljuk.

2.5.1. Az interdependencia dimenziói

A Kszetv. több pontjában érzékelteti, hogy a függőségek, kölcsönös függőségek kiemelt figyelmet érdemelnek és természetük nem feltétlenül lineáris. A Kszetv.vr. ezeket a vizsgálatokat a kritikus szervezetekre delegálja, de a végrehajtásához részletes leírást nem ad.

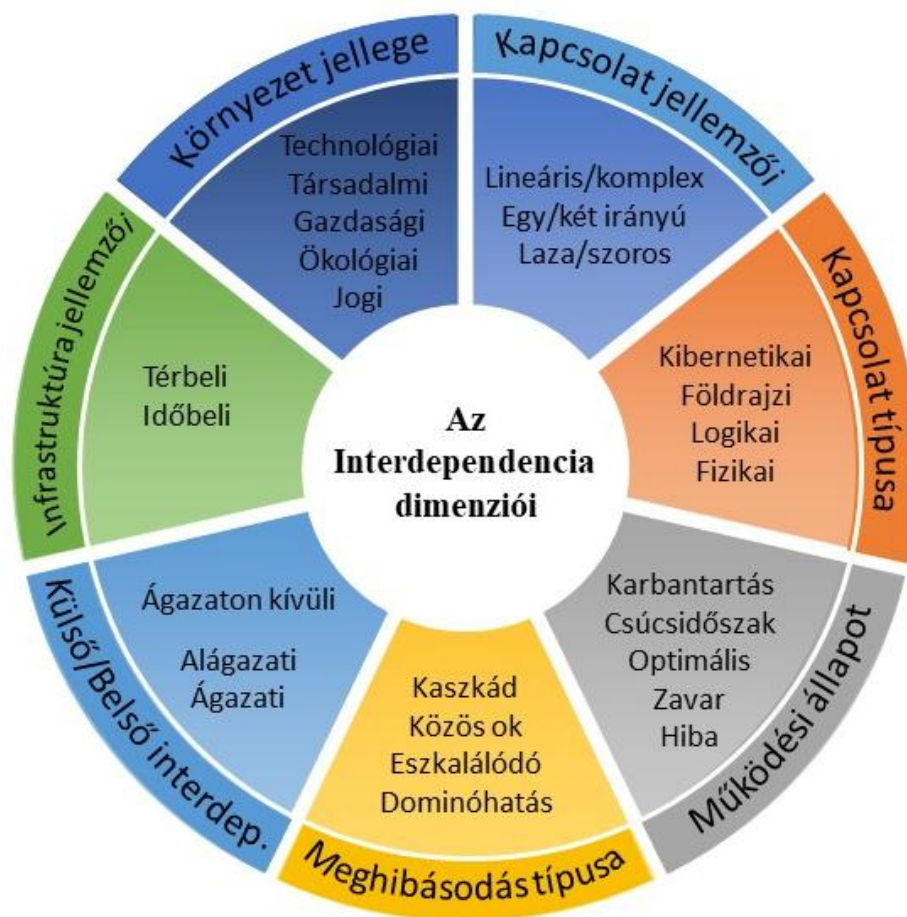
Az ilyen függőségek azonosítása, feltárása, vizsgálata komoly kihívást jelent. Bár az „*interdependencia*” kifejezés kölcsönös függőséget jelent, észrevehetünk olyan jelenséget, mely esetében két szervezet, szolgáltatás között egyirányú függőség, vagyis „*dependencia*” figyelhető meg.¹²⁸ Jelenleg a kiemelten fontos, kritikus szervezetek és infrastruktúrák olyan rendszert alkotnak, melyek topológiájában egyirányú és kölcsönös függőség is megfigyelhető. Mégis a rendszer egészét és bonyolult hálózatát tekintve biztosak lehetünk benne, hogy egy esemény több rendszeremet is érint és ha több lépésben is, de visszahat a kiinduló elemre. Éppen ezért joggal alkalmazhatjuk az interdependencia kifejezést. Ezt a következetességet

¹²⁸ Bakos 1978, 172, 376.

alkalmazva a továbbiakban egységesen az „interdependencia” kifejezést használom, csak abban az esetben használom a „dependencia” kifejezést, ha megkülönböztetésük releváns.

Az interdependencia feltárásánál és vizsgálatánál további figyelmet igényel, hogy magának a függőségnek a jellemzői több összetevőből, tényezőből állhatnak.

Ezen tényezők széles körét Steven M. Rinaldi, James P. Peerenboom és Terrence K. Kelly 2002-ben megjelent cikkükben hat dimenzióval írták le.¹²⁹ Az általuk behatárolt hat dimenzió nagyon jó alapot ad az interdependencia elemzéséhez, de szükséges napjainkra jellemző tényezőkkel kiegészíteni, illetve az elmúlt években végbement széleskörű változások (biztonsági, gazdasági, technológiai, környezeti stb.) miatt új dimenziókat, tényezőket megfogalmazni.



6. sz. ábra: az interdependencia dimenziói¹³⁰

¹²⁹ Kelly T. K., Peerenboom, J. P., Rinaldi, S. M. (2001): Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine,

¹³⁰ Saját szerkesztés

1. A környezet jellege

Ezek lehetnek a kritikus szervezet vagy infrastruktúra működését érintő technológiai, gazdasági, társadalmi, politikai, jogi, ökológiai és biztonsági tényezők. Ezen környezeti tényezők befolyásolhatják nem csak a normál működés rendjét, de a vészhelyzeti és helyreállítási műveleteket is.

Nem szabad figyelmen kívül hagyni azt sem, hogy maga a kritikus infrastruktúra vagy szervezet is befolyással bír a környezetére. Minél erősebb a környezeti tényezőkre gyakorolt hatása, annál szorosabb az a környezeti keret, melyen belül kell tartania működését. Ha egy magánkézben lévő kritikus szolgáltató társadalmi szerepet is betölt – például telekommunikációs cég – a gazdasági környezet és a kritikus szolgáltatókra vonatkozó állami jogi környezet egyaránt befolyásolja működését, mely komoly nehézségeket is okozhat, ha figyelembe vesszük a gazdasági és a jogi környezet közötti eltéréseket (állami korlátozások/jövedelmezőség).

2. A kapcsolat kiterjedése, mértéke és iránya

Az infrastruktúrák vagy szervezetek közötti kapcsolat lehet lineáris vagy komplex. Lineáris kapcsolat esetén közvetlenül követhető a kapcsolat vonala, könnyen megállapíthatók a függőség részletei, még abban az esetben is, ha kettőnél több szervezet vagy infrastruktúra alkotja. A komplex kapcsolat viszont olyan nehezen meghatározható kölcsönhatásokat tartalmaz, melyek alapján egy váratlan, nem tervezett eseménysorozat kimenetele nem látható, hiszen egy rendszeren belül több infrastruktúra, szervezet, szolgáltatás van egymással közvetett kapcsolatban, mely kapcsolatok kiterjedése, mértéke, iránya, típusa is eltérő lehet.

Ezen kapcsolatok mértéke lehet lazább vagy szorosabb, vagyis az a tulajdonság, hogy az infrastruktúrák vagy szervezetek milyen mértékben függenek egymástól. A laza kapcsolatok viszonylag rugalmasak, de minél szorosabb a kapcsolat, a rendszerben annál kevesebb rugalmasság marad a változó körülményekre vagy meghibásodásokra való reagálásra. A szoros, rugalmatlan kapcsolat súlyosbíthatja a problémákat, megkönnyítheti, gyorsíthatja az infrastruktúrák és így a kritikus szervezetek közötti láncreakció kialakulását.

A kritikus szervezetek, infrastruktúrák vizsgálatánál általában egyirányú függőségről beszélünk, vagyis a rendszerelem működésére hatással van egy adott szolgáltatás vagy infrastruktúra folyamatos jelenléte (energia, kommunikáció stb.), de a rendszerelem esetleges kiesése esetén az infrastruktúra vagy szolgáltatás üzemserű működése nem változik. A kétirányú, vagyis a kölcsönös függőség több kockázatot hordoz magában, de esetenként – akár technológiai vagy ellátási szükségszerűségből – számolni kell vele. Egy alapvető szolgáltatást

nyújtó ipari területet kiszolgáló informatikai rendszer magas energia igényét ellátó országos energetikai hálózat nem függ az adott informatikai rendszer működésétől, tehát a függőség egyirányú. Viszont ha a szóban forgó informatikai rendszer látja el az energetikai rendszer üzemeltetését is, kétirányú függőségről beszélhetünk. Ebben az esetben jól látható, hogy maga a rendszer sebezhetőbb, érzékenyebb a működési anomáliákra, hiszen – megfelelő védelmi intézkedések hiányában – az üzemfolytonosságban bekövetkező probléma a rendszeren belül újabb és újabb rendellenességeket generálhat.

3. A kapcsolat típusa

Az interdependencia alapját képező kapcsolat lehet fizikai, kibernetikai, logikai vagy földrajzi. A Kszetv. a függőség értelmezéseként mindössze ezt az egy dimenziót adja meg és nem tárgyalja ezeknek a kapcsolattípusoknak a mibenlétét: *„függőség: legalább két infrastruktúra, kritikus infrastruktúra, alapvető szolgáltatás, kritikus szervezet, alágazat, ágazat vagy állam (a továbbiakban együtt: entitás) közötti olyan logikai információs, fizikai vagy földrajzi kapcsolat, illetve összeköttetés, amely révén az egyik entitás állapota befolyásolja a másik entitását, vagy összefügg annak állapotával, ...”*¹³¹

Fizikai kapcsolat abban az esetben valósulhat meg, ha egy kritikus szervezet kimeneti terméke hatással van egy másik kritikus szervezet működésére. Például egy adott szervezet kimeneti terméke egy másik szervezet bemeneti alapanyagaként szolgál, vagyis egy fizikai termék az ellátási lánc része. Fizikai kapcsolat – melyben nem ellátási láncból adódik a függőség – úgy is kialakulhat, ha például egy ipari létesítmény károsanyagot bocsát ki, mely a megengedett határérték alatt van, de befolyásolja egy másik, kritikus szervezet (például egy biológiai kutató szervezet vagy biotermék gyár) tevékenységét, technológiáját a kibocsátott károsanyag természetes mozgásából adódóan.

Egy szervezet kiberfüggőséggel rendelkezik, ha állapota az információs infrastruktúrán keresztül továbbított információktól függ. Nem feltétlenül csak az informatikai szervezetekre vonatkozhat ez a kapcsolat, napjainkra a kiberfüggő szervezetek és infrastruktúrák száma már nagyon magas és egyre nő. Példaként a tömegközlekedés és az informatika függőségét említhetjük.¹³²

¹³¹ Kszetv. 6.§ 16. bekezdés

¹³² Dalicsek I., Répás S. (2015): Az információbiztonsági kockázatelemzés módszertani kérdései a kritikus infrastruktúra elemeket üzemeltető szervezetek esetében. Pro Publico Bono, 25.o

Ha egy helyi környezeti esemény több szervezet működésében, infrastruktúráiban is állapotváltozást idéz elő, ebben az esetben földrajzi függőségről beszélhetünk. Vagyis egy tűz vagy robbanási esemény mindegyikre hatással van, földrajzi közelségük miatt.¹³³

A logikai interdependencia inkább működési folyamatok egymásra hatásából keletkezhet, függetlenül a köztük lévő távolság vagy a fizikai, informatikai kapcsolattól. Logikai kapcsolat van például a jogalkotók és a termelő szervezetek között, hiszen egy jogszabály változása kihatással van a termelékenységre vagy annak költségeire. A termelők érdekvédelmi szervezetei – szerencsés esetben – visszajeleznek és hatással vannak a jogalkotókra.

4. A kritikus szervezet, infrastruktúra jellemzői

A kritikus szervezeteknek, infrastruktúráknak vannak olyan jellemzőik, melyek nem hagyhatók figyelmen kívül az interdependencia vizsgálatánál.

A térbeli lépték az a jellemző, mely megmutatja, hogy egy rendszerben milyen mélységig kell vizsgálni a működést az interdependencia elemzésénél. Ez lehet akár egy részegység (pl.: egy generátor), egy alrendszer (pl.: másodlagos elektromos ellátó rendszer), vagy egy rendszer, mely alrendszerek csoportja (pl.: telekommunikációs szolgáltató szervezet), vagy infrastruktúra mely több rendszerből áll (pl.: kommunikációs infrastruktúra), vagy akár infrastruktúrák és a környezet összekapcsolódó, teljes hálózata is.

Az időbeli lépték az a jellemző, mely az interdependencia vizsgálatokban releváns folyamatok időbeli tartományát mutatja. Ezek az időintervallumok a milliszekundumtól (pl.: informatikai hálózatok működése) akár több évet is felölelhetnek (pl.: fejlesztések, kapacitásbővítések). Az időbeli jellemző pontos meghatározása fontos az interdependencia modellekkel és szimulációval történő elemzésénél, hiszen ehhez kell kialakítani a válaszreakciókat és a műveletek sorrendjét. Fontos megjegyezni, hogy nem csak egy adott folyamat vagy esemény időbeli léptékét kell figyelembe venni, hanem azt is, hogy annak hatása milyen időintervallumra húzódik ki.¹³⁴

5. Működési állapot

A kritikus szervezetek és infrastruktúrák üzemi működése még normál időszakban is eltérést mutathat, például a csúcsideszakban és a csúcsideszakon kívüli működést összehasonlítva. Ha

¹³³ Kelly T. K., Peerenboom, J. P., Rinaldi, S. M. (2001): Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 15.o

¹³⁴ Kelly T. K., Peerenboom, J. P., Rinaldi, S. M. (2001): Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 21.o

figyelembe vesszük, hogy az éppen aktuális működési állapot milyen hatással van egy bekövetkező zavar vagy meghibásodás mértékére és időtartamára, akkor jól látható, hogy szélesebb spektrumban kell vizsgálni az adott szervezet vagy infrastruktúra lehetséges működési állapotait. Ide tartoznak az optimális tervezési működésen túl a csúcsidőszakok, esetleges túlterheléses időszakok, a javítás, karbantartás időszakai alatt fennálló működési állapotok. Kritikus infrastruktúrák és szervezetek esetében figyelembe kell vennünk olyan speciális eshetőséget is, mely esetben egy rendszeren belüli belső zavar mellett még biztosítható a normál, folyamatos üzem, vagyis kontrollált rendkívüli esemény következik be, de egy erre az időszakra érkező külső, interdependenciából adódó zavar már komoly károkat okozhat.¹³⁵

Az interdependencia vizsgálatánál fontos figyelembe vennünk a működés minden lehetséges állapotát, hiszen naivitás azzal számolni, hogy egy interdependenciából adódó zavar éppen az optimális üzemi működés közben éri a rendszert.

6. A meghibásodások típusa

A kritikus szervezetek, infrastruktúrák közötti interdependencia egyértelműen növeli a meghibásodások vagy zavarok kockázatát. Ennek vizsgálata érdekében külön kell választanunk egy adott szervezet vagy infrastruktúra belső működésében elkülöníthető zavarokat és az interdependenciából eredő, külső okok miatt bekövetkező meghibásodásokat, zavarokat.

Ezek az interdependenciából következő zavarok bekövetkezhetnek kaszkád vagy dominóhatás szerű, eszkalálódó vagy közös okokból kifolyólag.

Kaszkád szerű meghibásodás akkor következik be, ha egy infrastruktúrában bekövetkező zavar egy másik infrastruktúra egy komponensének meghibásodását okozza, mely ezt követően zavart okoz egy újabb infrastruktúrában. Ezek a zavarok – legrosszabb esetben – nem csak lineárisan, hanem szélesebb körben is végigfuthatnak az egymástól függő infrastruktúrák és szervezetek interdependens hálózatán, akár egymás hatását erősítve is.¹³⁶ A Kszetv.vr. mindössze erre az egy meghibásodás típusra tesz említést, melynek vizsgálatát ugyancsak az adott kritikus szervezet tisztségviselőinek hatáskörébe és felelősségébe adja.¹³⁷

¹³⁵ Kelly T. K., Peerenboom, J. P., Rinaldi, S. M. (2001): Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 22.o

¹³⁶ Joydeep B., Das A., Sen A. (2017): A Survey of Interdependency Models for Critical Infrastructure Networks. Arxiv.org. (<https://arxiv.org/abs/1702.05407>) Letölés: 2025.11.15., 2.o

¹³⁷ Kszetv.vr., 10.§ b) pont

Eszkalálódó zavarnak azt a jelenséget tekinthetjük, ha egy interdependenciából eredő zavar beérkezésekor éppen egy belső, előzőtől független zavar is fennáll, melyek együttesen már felerősítik egymás hatását az adott szervezetre vagy infrastruktúrára.

Közös okból eredő zavarokról akkor beszélhetünk, ha a különböző infrastruktúrák működésében egyidőben fellépő zavarok bár egymástól függetlenek, de azonos időben következnek be, egyazon okból. Ez lehet például természeti vagy ipari katasztrófa, terrorcselekmény, melyben egyszerre sérülnek telekommunikációs vezetékek, közlekedési vonalak stb. Ekkor több infrastruktúra zavara bár egymástól független, de például a földrajzi interdependencia miatt egyszerre lépnek fel, így erősségüket és a helyreállítás idejét növelhetik.¹³⁸

7. Belső/Külső interdependencia

A kritikus szervezetek és infrastruktúrák tekintetében, belső interdependenciáról beszélhetünk, ha a vizsgált rendszer elemek azonos ágazatba vagy alágazatba tartoznak. Az azonos ágazatba tartozó szervezetek, infrastruktúrák kölcsönös függőségének, vagyis az ágazati belső interdependencia vizsgálata nem csak az adott rendszer elemek kockázatelemzésének lehet része, hanem a teljes ágazat sérülékenységének feltárásában, az ágazat rendszereinek és egészének stabilitásához szükséges szabályok megalkotásában is fontos szerepe lehet, valamint kiemelt szerepe lehet az alágazatok ellenálló képességének elemzésénél.

Külső interdependencia vizsgálat esetén egy adott szervezettel, infrastruktúrával függőségi viszonyban lévő más szervezet, infrastruktúra ágazati hovatartozása nem releváns. Fontos információ a rendszer elemre ható hatás, illetve az a mechanizmus, mely alapján ez a hatás kialakul.

2.5.2. Az interdependencia vizsgálatának lépései

Egy adott kritikus szervezet vagy infrastruktúra minimális dependencia vizsgálata jelenleg is részét képezi a kijelölési folyamatban végrehajtandó, EKT és EKM elkészítéséhez szükséges kockázatelemzésnek, viszont érdemes a kockázatelemzés részeként mélyebb interdependencia vizsgálatot végrehajtani. Míg a kockázatelemzés az üzemfolytonosságot veszélyeztető közvetlen és a folyamathoz köthető veszélyeket vizsgálja, tehát belső körből indul, az

¹³⁸ Kelly T. K., Peerenboom, J. P., Rinaldi, S. M. (2001): Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 22.o

interdependencia vizsgálatához érdemes „kívülről” közelíteni. Vagyis figyelembe kell venni – lehetőség szerint – minden külső tényezőt, szolgáltatást, kapcsolatot és megvizsgálni, hogy milyen hatással vannak nemcsak a kritikus szervezet, hanem egymás működésére is. Külső körből indulni sokkal nehezebb, mint a meglévő belső információkra építeni, ezért érdemes külön az interdependencia vizsgálatára gyakorlati lépéseket felállítani.

Adott kritikus szervezet vagy infrastruktúra interdependencia vizsgálatának lehetséges gyakorlati lépéseire a következő javaslatot teszem:

1. Adatgyűjtés és feltérképezés
2. Kölcsönhatások azonosítása
3. Kockázatelemzés
4. Horizontális függőségelemzés
5. Rekurzív alkalmazás
6. Biztonsági intézkedések
7. Képzés, ellenőrzés

1. Adatgyűjtés és feltérképezés

Első lépésként szükséges meghatározni az összes szervezetet, infrastruktúrát, szolgáltatót, amelyekkel az adott szervezetnek, infrastruktúrának kapcsolata van. Teljes listát kell készíteni, függetlenül a kapcsolat típusától és tulajdonságaitól. Ez magában foglalja a látótérbe került szervezet, infrastruktúra vagy szolgáltató működési folyamatainak objektív feltérképezését is, mely azt jelenti, hogy a működési folyamat vizsgálata ne a szervezettel meglévő kapcsolata alapján kialakított előzetes feltételezéseken alapuljon, hanem ettől függetlenül, a teljes működési folyamatot adja meg. Ehhez szükség lehet a kritikus szervezettel vagy infrastruktúrával kapcsolatban lévő külső szervezet működési okmányainak vizsgálatán felül akár helyszíni bejárásokra és személyes interjúk végrehajtására is.

2. Kölcsönhatások azonosítása

A külső szervezet feltárt és vizsgált működési folyamatainak és az adott kritikus szervezet, infrastruktúra működési folyamatainak „egymás mellé helyezésével” azonosíthatók a kapcsolódási pontok, melyeken keresztül a folyamatok képesek hatni egymásra. Az előző részben tárgyalt dimenziók vizsgálata megadja ezen kölcsönhatásoknak a tulajdonságait és típusait, melyekkel feltérképezhető a kapcsolatok rendszere és a rendszer egészének jellemzői.

Külön figyelmet kell fordítani a kritikus beszállítók azonosítására, akár fizikai termék, akár valamely szolgáltatás tekintetében. Különböző helyzetek és események szimulálásával könnyebben felmérhetők a kritikus kapcsolódási pontok.

3. Kockázatelemzés

A kockázatértékelések több módszerrel végrehajthatók, de kifejezetten az előzőek alapján feltárt kapcsolatokra, kölcsönhatásokra kell fókuszálniuk. A módszerek különbözhetnek attól függően, hogy milyen mélységben és részletességgel szükséges végrehajtani a vizsgálatot illetve, hogy milyen jellegű folyamatot szükséges vizsgálnunk.

A kockázatelemzés módszereivel így meghatározható, hogy egy adott kapcsolatban fellépő zavar milyen valószínűséggel és milyen hatással jár. Vagyis meghatározható, hogy az adott kapcsolat jár-e függőséggel. Ha dependencia, interdependencia figyelhető meg, a 2. pontban meghatározott jellemzők felhasználásával, illetve a valószínűség és hatás vizsgálatával megállapítható a függőség kockázati értéke.

Az így feltárt függőségi kockázatokat érték szerint prioritizálva, illetve az egyes szolgáltatókat, kiszolgáló infrastruktúrákat hozzárendelve, kialakítható az adott kritikus szervezet vagy infrastruktúra közvetlen, első szintű függőségekre vonatkozó adatbázisa.

4. Horizontális függőségelemzés

Egy kritikus szervezet, infrastruktúra közvetlen függőségeinek adatbázisa még nem elegendő a rejtett rendszerkockázatok azonosításához. A kritikus szervezettel, infrastruktúrával közvetlen függőségi viszonyban lévő szervezetek, szolgáltatók egymáshoz viszonyított kapcsolatait is vizsgálni kell. A vizsgálat célja annak azonosítása, hogy a kritikus szervezetet kiszolgáló szolgáltatók és infrastruktúrák között fennállnak-e egymás közötti függőségek, amelyek a kritikus szervezet ellátásának biztonságát vagy a kritikus infrastruktúra üzemfolytonosságát befolyásolhatják.

Ennek keretében fel kell tárnunk, hogy a különböző szolgáltatók milyen közös infrastruktúrára, erőforrásokra vagy technológiai megoldásokra támaszkodnak. Különös figyelmet igényelnek azok az esetek, amikor több szolgáltató azonos külső szolgáltatót, energiaforrást vagy infokommunikációs rendszert használ. Az ilyen összefüggések rejtett sérülékenységet jelenthetnek, mivel egyetlen kiesés több, egymástól látszólag független szolgáltatás egyidejű zavarához vezethet. A vizsgálat során figyelemmel kell lenni arra is, hogy a szolgáltatók közötti kölcsönös kapacitásmegosztás vagy tartalékképzés rendkívüli helyzetben valóban növeli-e a rendszer ellenálló képességét vagy épp ellenkezőleg, túlterheléshez vezethet.

5. Rekurzív alkalmazás

Az 1-4. lépésekkel feltárható a kritikus szervezet, infrastruktúra közvetlen környezetének interdependencia rendszere. Az így meghatározott legfontosabb szolgáltatók és kiszolgáló infrastruktúrák esetében indokolt lehet azok hasonló elemzése, vagyis az 1-4. lépések mélyebb szintű rekurzív alkalmazása. Az újabb szintek interdependencia vizsgálatának célja a közvetett, többszintű függőségek feltárása, melyek láthatóvá teszik a kritikus szervezet, infrastruktúra működését befolyásoló másodlagos vagy harmadlagos függőségeket is.

Azonosíthatók azok a rejtett, közös függőségek, melyek több szolgáltatási szinten is kockázatot jelentenek. A módszer segít feltárni a rendszerszintű láncreakciók (L.: interdependencia 6. dimenzió) lehetséges útvonalait és terjedési mechanizmusait. A rekurzív alkalmazás addig ismételhető, amíg a feltárt kockázat a kritikus szervezet működésére már elfogadható vagy elhanyagolható.

A rekurzív megközelítés eredményeként egy többszintű, hierarchikus függőségi hálózat hozható létre, mely a *kritikus szervezet interdependencia kockázati térképe*. A meghatározott interdependencia kockázati térkép már beilleszthető az EKM kockázatelemzési struktúrájába, illetve alkalmazható annak kiterjesztésére, pontosítására, fejlesztésére.

6. Biztonsági intézkedések

Az interdependencia kockázati térkép alapján azonosított veszélyek megelőzésére, hatásainak csökkentésére, következményeinek kezelésére olyan forgatókönyvet szükséges összeállítani, mely megfelel az adott kritikus szervezet, infrastruktúra jellemzőinek és figyelembe veszi a közvetett függőségekből eredő egyéb hatásokat is.

A kidolgozott forgatókönyvek alapján már pontosabban becsülhetők az interdependenciából adódó veszélyhelyzetek kritikus szervezetre gyakorolt hatásai, így nagyobb látószögben tervezhetők az ellenálló képességgel, védelemmel kapcsolatos intézkedések, fejlesztések.

Az interdependencia kockázati térkép, valamint a kidolgozott forgatókönyvek alapján a kritikus szervezetek a releváns szolgáltatókkal együttműködve képesek hatékony védelmi intézkedések kidolgozására, a költségek optimalizálása mellett. A megfelelő intézkedések kidolgozása és az interdependenciával érintett szolgáltatókkal való együttműködés segít növelni a teljes rendszer rezilienciáját, minimalizálni a kockázatokat, illetve kialakítani a leghatékonyabb helyreállítási protokollokat.

A megfelelően létrehozott, interdependenciával kapcsolatos biztonsági intézkedések jól integrálódnak a meglévő rendszerekbe, kiegészítik azokat.

7. Képzés, ellenőrzés

A legjobban, legrészletesebben kidolgozott, rendszerhez illeszkedő biztonsági intézkedések is csak abban az esetben hatékonyak, ha az infrastruktúrát üzemeltető személyzet, a kritikus szervezet vezetői, munkatársai elsajátítják, megértik az abban leírt alapelveket, eljárásokat és gyakorlatokat, valamint az adott rendszer biztonsági politikájával képesek tudatosan azonosulni. Ezeket a képességeket és tudatosságot a 4. fejezetben tárgyalt képzésekkel, gyakorlatokkal lehet fejleszteni, továbbá ciklikusan végrehajtott, segítő szándékú, részletes ellenőrzésekkel támogatni. Fontos, hogy ez az alapelv – arányosság alapján – ugyanúgy vonatkozzon az interdependencia vizsgálattal feltárt szolgáltatók és kiszolgáló infrastruktúra üzemeltetői köreire is, mint a kritikus szervezet saját személyzetére.

2.6. RÉSZKÖVETKEZTETÉSEK

A kritikus szervezetek kijelölési eljárását elemezve, figyelemmel a Kszetv., VBÖ, és kormányrendeleteinek előírásaira, megállapítottam, hogy egy kritikus vagy jelentős szervezetnek – szinte minden esetben – több üzemeltetője, tulajdonosa, rendelkezésre jogosultja azonosítható, akár az állami vagy a magán szektorból is. A Kszetv. és a VBÖ a kritikus és jelentős szervezetekre és infrastruktúrákra vonatkozó előírásait, kötelezvényeit a „szervezet” részére címzi, vagyis a rendszer működésében résztvevő szereplőkre hárul az a feladat, hogy a különböző felelősöket, döntéshozókat, finanszírozót kijelöljék.

Megállapítottam, hogy a tulajdonos és a szakmai irányításért, vezetésért felelős személy vagy szervezet nem ugyanaz. Nagyobb, országos vagy nemzetközi lefedettséggel rendelkező kritikus szervezeteknél külön igazgatóságok jelennek meg az üzemeltetési, döntéshozói és a finanszírozási oldalra is. Több esetben a kritikus szervezet, infrastruktúra fejlesztéséért és finanszírozásáért felelős szervezetek nem részei a kritikus szervezetnek. Gyakori eset, hogy az elhelyezésére szolgáló létesítmény üzemeltetése, mely tartalmazza a napi működést és a biztonsági tevékenységet is, külső szolgáltatóhoz van kiszervezve.

A Kszetv.vr. 3.§ (1) bekezdés d) pontja előírja az adatszolgáltatást „*a kritikus szervezetre vonatkozó személyi és szervezeti adatokra*”, illetve a BM OKF weblapjáról letölthető, kötelező jelleggel kitöltendő adatszolgáltatási lap mellékletét képezik *a kritikus szervezet vezetésének, érintett szakterületek vezető tagjainak azonosító adatai, elérhetőségei*. Viszont az előző példákából kitűnik, hogy ezek a felelősségi körök túlmutathatnak a kritikus szervezet belső szervezeti struktúráján.

A vonatkozó törvények és kormányrendeletek egyike sem rendelkezik arról, hogy milyen módon szükséges a külső szolgáltatók felelőseinek megszólítása és felelősségi szintjüknek a meghatározása. Egy potenciális kritikus vagy jelentős szervezet kijelölése komolyabban is érintheti a szervezethez kötődő külső szolgáltatókat, szervezeteket, infrastruktúrákat – pl. szervezeti, finanszírozási kérdésekben – így mindenképpen szükséges ezen szolgáltatók, szervezetek vezetői, döntéshozói személyeinek azonosító adatait, elérhetőségét is feltüntetni, illetve szükség szerint a kijelölési folyamatban való részvételüket tisztázni.

Javaslom, hogy ezeket az adatokat ugyancsak a BM OKF weblapjáról letölthető, kötelező jelleggel kitöltendő adatszolgáltatási lap mellékletében fel kelljen tüntetni, illetve a felelősségi köröket a továbbiakban az EKT tartalmában is megjelenjenek. Ehhez az adatszolgáltatási lap és az EKT módosítása, kiegészítése szükséges.

A jogszabályok további elemzésével megállapítottam, hogy:

- a Kszetv. megjelenésével mindössze három kijelölő hatóság maradt, a két ágazati (honvédelmi jelentős, energetikai kritikus), illetve a többi ágazat vonatkozásában az általános kijelölő hatóság jelölhet ki jelentős és kritikus szervezetet és infrastruktúrát is;
- az alapvető szolgáltatást nyújtó szervezetek önállóan nem kezdeményezhetik az azonosítást, az azonosítás csak abban az esetben történik meg, ha a bizonyos szervezet a kijelölő hatóságok látóterébe kerül;¹³⁹
- a szakhatóságokat csak az adatközlő lap beérkezése után szólítja meg a kijelölő hatóság;¹⁴⁰
- a honvédelmi kijelölő hatóság a honvédelmi érdekből jelentős szervezetek kijelöléséről a szakhatóságok bevonása nélkül dönt.¹⁴¹

¹³⁹ Kszetv.vr. 3.§

¹⁴⁰ Kszetv.vr. 6.§

¹⁴¹ VBÖ.vr. 5.§ (3) bekezdés

Mindezek azt jelenthetik, hogy a kijelölő hatóságok leterheltsége és a beérkező adatok központi elemzése alapján egy csatornára szűkül a kritikus szervezetek, infrastruktúrák azonosítási és kijelölési eljárása, a jelentős szervezetek, infrastruktúrák azonosítása és kijelölése pedig két *különálló* csatornára.

Az azonosítás és kijelölés folyamatában a szűk, központosított csatornákon áramló, nagymennyiségű szakmai információ adattartalma csökken vagy torzul, mely problémát jelent. Így a döntés elnagyolt, vagy szubjektívvá válik.

Mindezen problémák megoldására a következő javaslatot teszem: a mára hatálytalan ágazati kormányrendeletek több esetben ideiglenes szakmai bizottságok létrehozását írták elő, melyek segítséget adtak a kijelölési folyamatban. Javaslom az *ágazati szakmai bizottságok intézményesített visszaemelését a hatályos jogszabályokba* az azonosítási és kijelölési folyamat támogatása céljából. (L.: 1.3. alfejezet)

A társadalmakat működtető szolgáltatások rendszerét és a rendszer egyes elemei közötti kapcsolatokat elemezve könnyen belátható, hogy az interdependencia kérdése rendkívül fontos a kritikus szervezetek és infrastruktúrák ellenálló képességének és védelmének vizsgálatában.

Az interdependencia vizsgálatára jelenleg nincs központilag kiadott, vagy a szervezetek által hozzáférhető minta. A Kszetv., a Kszetv.vr. előírásai, illetve a BM OKF weblapjáról letölthető EKT és EKM tartalmaz minimális szintű interdependenciára vonatkozó pontokat, de az interdependencia dimenzióira és vizsgálatára vonatkozó metodika nélkül a kritikus szervezetek által kidolgozott EKT, a legtöbb esetben mindössze egyirányú, közvetlen, technológiai dependencia vizsgálatot tartalmaz.

Az interakciók általános elveinek figyelembe vételével *meghatároztam az interdependencia dimenzióit és vizsgálatának lehetséges lépéseit*. Az interdependencia területekre bontott vizsgálatának lépéseit tárgyaló metodikát a kockázatelemzésbe szükséges beépíteni, melynek eredményei már könnyedén beilleszthetők az EKT megfelelő pontjaiba.

Javaslom az *egységesített módszerrel végrehatott interdependencia vizsgálatok jogszabály szintű bevezetését, majd az egységesített adatainak további elemzését*, a teljes, országos interdependencia térkép megvalósításának érdekében.

3. FEJEZET

A KRITIKUS SZERVEZETEK ÉS INFRASTRUKTÚRÁK FIZIKAI VÉDELME

3.1. LÉTESÍTMÉNYEK FIZIKAI VÉDELMÉNEK ELVEI

Az előző fejezetekből jól kitűnik, hogy a kritikus szervezetek és infrastruktúrák azonosítása és kijelölése olyan speciális jogi és szakmai ismereteket igénylő folyamat, mely a hatályos jogszabályok figyelembe vételével, helyes alkalmazásával, illetve az szervezetek, üzemeltetők, tulajdonosok, felelősök és a hatóságok közötti szoros együttműködéssel valósulhat meg. A kijelölést követően viszont el kell kezdeni a feltárt kockázatok alapján az ellenálló képességre vonatkozó protokollok kialakítását, a meglévő védelmi képességek fejlesztését, esetleg új intézkedések, védelmi létesítmények kiépítését. Ez a feladat már folyamatos, és sokkal nagyobb terhet jelent a kritikus szervezetekre és infrastruktúrák üzemeltetőire, tulajdonosaira és minden alkalmazottjára is, hiszen egy új, emelt szinten szükséges folytatniuk saját munkájukat és az egymással való együttműködést.

Egy kritikus szervezet minden vezetőjének és munkavállalójának – a saját feladatköréhez mérten – tisztában kell lennie az ellenálló képesség és védelem alapelveivel, a rendszer védelmi protokolljainak és létesítményeinek céljával és működésével.

3.1.1. A védelem fogalma

A szakterületek és jogszabályok különböző módokon értelmezik a védelem fogalmát. Szükséges meghatározni, hogy a kritikus szervezetek és infrastruktúrák védelme tekintetében milyen korlátokkal és értelmezéssel tekintünk ezen fogalmakra, annak érdekében, hogy pontosan vizsgálhassuk hatékonyságukat.

A „*védelem*” az egyik olyan alapkifejezésünk, amely mélyen beépült a szóhasználatunkba, az életünk minden területén, minden fellelhető szakterületen alkalmazzák. Éppen ezért nem is olyan egyszerű meghatározni az alapfogalmát, mivel a lexikonok, szótárak és szakkönyvek szinte önmaga szinonimáival magyarázzák a védelem egy-egy részterületének fogalmát. Érthető, hogy a 2000-es évek előtt keltezett művek a védelem fogalma alatt a fizikai és a jog védelmére asszociálnak, míg napjainkban egyre inkább bővül a kör, megjelennek az informatikai védelem, adatvédelem, hálózatvédelem elvei a fogalmakban.

„Vki testi épségének, életének, vmely dolog épségének, sértetlenségének tevékeny, cselekvő megőrzése, megoltalmazása, megvédése.”¹⁴²

„to keep someone or something safe from injury, damage, or loss”¹⁴³

A védelem kifejezés felhasználásával minden terület, szakterület kialakította a saját alapfogalmát, mely alapfogalmakat az adott szakterület sajátosságai jellemeznek. Külön példákat sem szükséges kiemelni, mégis érthető, hogy milyen különbségek lehetnek a rendvédelem, a környezetvédelem, az adatvédelem – és még hosszasan sorolhatnánk – fogalmak között.

Összességében viszont minden védelemmel kapcsolatos fogalom egy irányba mutat:

- fenntartani bizonyos személy, tárgy, folyamat, eljárás eredeti állapotát;
- biztosítani a védendő entitás további működését;
- megőrizni létezéséből és működéséből eredő értékét.

Ezt a meghatározást is igen tág értelemben kell vennünk, hiszen – például – a katonai terminológiában a védelem célja:

„az erőfölényben lévő ellenség előrevonásának akadályozása, támadóképességének megtörése, jelentős veszteségokozással támadásának megghiúsítása, visszaverése, a terep fontos körleteinek megtartásával, az erők és eszközök megőrzésével kedvező feltételek teremtése az eredeti helyzet visszaállításához, illetve a támadásba való átmenethez.”¹⁴⁴

Semmi a világon nem képes akkora károkat okozni, mint a háborús területen végrehajtott védelem.

A Kszetv. megfogalmazása már közelebb áll az előbbieken megállapított általános fogalomhoz, sőt, kiszélesíti a kritikus szervezetek és infrastruktúrák védelmének fogalmát:

„ellenálló képesség: valamely kritikus szervezet vagy infrastruktúra azon képessége, hogy egy rendkívüli eseményt, kontrollált rendkívüli eseményt megelőzzön, azzal szemben védekezzen, arra reagáljon, annak ellenálljon, azt

¹⁴² A magyar nyelv értelmező szótára – Akadémiai Kiadó, 1959-1962,

¹⁴³ <https://dictionary.cambridge.org/dictionary/english/protect> (letöltve: 2025.07.11.)

¹⁴⁴ A Magyar Honvédség Szárazföldi Haderőnemének harcszabályzata IV. rész – Magyar Honvédség kiadványa, 2013.

semlegesítse, azt enyhítse, ahhoz alkalmazkodjon és az esemény bekövetkezését követően működését helyreállítsa”¹⁴⁵

3.1.2. Létesítmények megközelíthetősége

A védelmi intézkedések alkalmazásának tekintetében az egyik legfontosabb tényező az idő. Az az idő, mely a rendkívüli esemény kialakulásától a védelmi intézkedés aktiválásáig eltelik, sok esetben csak percekben mérhető. A fizikai védelem területén ez az idő növelhető, vagy hatékonyan kihasználható a létesítmények megközelíthetőségének tervezésével. A terület zónákra bontásával, különböző fizikai akadályok létesítésével, hatékony észlelőrendszer kialakításával, helyszíni védelmi protokollok kidolgozásával, valamint ezek összehangolásával a fizikai védelmi hatékonyság növelhető.¹⁴⁶

Egy védett létesítmény (nagykövetség, veszélyes anyagokkal foglalkozó üzem, stb.) gépjárművel való megközelíthetőségének akadályozása vagy lassítása nagyban növeli a védelmi erők lehetőségeit a reakcióra.

3.1.2.1. Első biztonsági zóna – Külső környezet

A védendő létesítmény körüli beépítetlen terület az első védelmi zóna, mely kiterjedése és átláthatósága miatt megnehezíti az észrevétlen megközelítést vagy megfigyelést, illetve a nemkívánatos eszközök, szerkezetek vagy anyagok bejuttatását, legyen szó akár robbanóanyaggal megrakott teherautóról, vagy személyek illegális tevékenységéről. De kockázatcsökkentő hatása lehet a normál járműves és gyalogos tömegközlekedés távolabbra történő átvezetésének is. A biztonsági távolság méreteit a veszélyeztetettség mértéke, illetve a létesítmény környezetének lehetőségei határozzák meg.¹⁴⁷

Előfordulhat, hogy a védett létesítmény körül a beépítettség miatt már nem létesíthető a védelem szempontjából legmegfelelőbb távolság. Ebben az esetben a környezet átalakításával, kiegészítésével növelhető a védelmi képesség. Ilyen lehet a környező utak, forgalmi irányok

¹⁴⁵ Kszetv. 3.§ 8.

¹⁴⁶ Padányi J. (2006) A katonai műveletek terrorvédelme. *Nemzetvédelmi Egyetemi Közlemények*, (2006/3),

¹⁴⁷ Balogh, Zs. (2013) Katonai objektumok robbantásos cselekmények elleni védelmének lehetőségei. PhD értekezés. Budapest; NKE

áttervezése, parkolók létesítése, módosítása, illetve kiegészítő biztonságtechnikai eszközök telepítése.

Védelmi szempontból a tiszta, tágas, átlátható, jól megvilágított tereket kell preferálni. Kerülendőek a sikátorszerű kis utcák, a rosszul megvilágított térrészek. A megközelítési útvonalak kialakításánál figyelembe kell vennünk a mozgást akadályozó szerkezetek, eszközök és a létesítmény megközelíthetősége közötti egyensúlyt. A létesítmény gyors, ellenőrizetlen megközelítését nehezíti, ha nem alkalmazunk az épület homlokzatára merőleges utakat. A gyalogos és jármű forgalom elkülönítése növeli a terület ellenőrizhetőségének hatékonyságát, a szintbeli különbségek kialakítása – peremkő, emelt járdaszegély – növeli a védelmet. Ha lehetőség van rá, a széles járdaszakaszok kialakítása előnyös és védelmi képességük növelhető köztéri bútorok alkalmazásával, mint például a rögzített, nagy súlyú padok, virágtartó edények, melyek barikádként is funkcionálnak.

Az úttest, járda, épületek közötti területeken zöld felületek is kialakíthatóak. Fontos szabály, hogy a növényzet ne takarja a kontroll alá vont térrészeket. Lehetőleg a fák koronája ne nyúljon 180 cm alá és a cserjék – ha alkalmazzuk – ne emelkedjenek 90 cm fölé. Hosszú, folytonos, növényvel takart területek ne alakuljanak ki. A növények elburjánzása erősen csökkentheti a terület kontrollját, ezért folyamatos ápolást igényelnek.



7. sz. ábra: A budapesti Amerikai Nagykövetség külső zónája¹⁴⁸

¹⁴⁸ Forrás: Google Map utcakép, Amerikai Egyesült Államok Nagykövetsége, Budapest, Szabadság tér

A világítást célszerű úgy tervezni, hogy az alábbi szempontok érvényesüljenek:

- minden kontroll alá vont területet be kell világítani úgy, hogy minden térrész áttekinthető legyen;
- külső hatásokra ellenálló, az átlagosnál üzembiztosabb eszközöket kell alkalmazni;
- a világítóeszközök természetes színűek legyenek;
- a területet olyan irányból és magasságból világítsa be, hogy a fényforrás a területet használót ne zavarja a tisztán látásban, vagyis ne vakítson;
- a veszélyes vagy kiemelt zónákat a környezettől, színben és intenzitásban elütő módon kell megvilágítani;
- a folyamatos karbantartás mellett a működési zavarok gyorsan elháríthatók legyenek.

A létesítmény környezetében kialakított parkolók helyes megtervezésével és azok működési feltételeinek meghatározásával még tovább növelhető a külső zóna védelmi képessége.

Közvetlenül az épületek előtti parkolást lehetőség szerint tiltani kell, közlekedési táblákkal vagy más fizikai akadályokkal.¹⁴⁹

Célszerű a parkolókat a létesítmény egyes elemeitől megfelelő távolságra, jól megfigyelhetően kialakítani. Ha van rá lehetőség, az állandó jelleggel és az ideiglenesen a létesítmény környezetében parkoló járműveket el kell különíteni, akár beléptető rendszer és/vagy kerítés alkalmazásával.

¹⁴⁹ Bakos, T. (2018): Létfontosságú rendszerelemek megközelíthetősége, adott létfontosságú rendszerem megközelíthetőségi elemzése. *Műszaki Katonai Közlöny*, XXVIII/1.



8. sz. ábra: Fedett parkoló védőfallal¹⁵⁰

A parkoló kialakításánál – elsősorban a nagyobb károk okozására alkalmas emberi vagy természeti eredetű eseményekkel számolva – figyelembe lehet venni a parkolóhoz legközelebb álló épület funkcióját, szerkezeti kialakítását, anyagát is. Jó példa erre az Amerikai Védelmi Minisztérium ajánlása, mely alapján a nagy forgalmú középület esetén, őrzés nélküli parkoló távolsága téglapülettől 80 méter, vasbeton épülettől 20 méter kell, hogy legyen.

Amennyiben mindenképpen szükséges épület alatti garázs kialakítása, úgy gondoskodni kell a belépő járművek zsilip rendszerű mozgásakadályozásáról, a járművek azonosításáról, regisztrációjáról, átvizsgálásáról.

3.1.2.2. Második biztonsági zóna - a létesítmény területe

A második biztonsági zóna maga a jól elhatárolt létesítmény. Könnyen előfordulhat, hogy nincs lehetőség az előzőekben ismertetett, nagyobb távolságokat igénylő teljes méretű külső

¹⁵⁰ Forrás: <https://deluxebuilding.hu/fedett-parkolok/> Letöltés: 2026.04.08.

biztonsági zóna kialakítására. Ebben az esetben a megfelelő védelmi szint eléréséhez a különböző mechanikai és elektronikai védelmi eszközök nyújtanak megoldást.¹⁵¹

A veszélyeztetettség mértékétől, a rendelkezésre álló költségvetéstől, illetve a kialakítás objektív lehetőségeitől függően lehet megválasztani az alkalmazott technológiákat.¹⁵² A tervezéshez nagyon sok technikai eszköz, berendezés, elem áll rendelkezésre, így ebben az esetben is a védelem hatékonysága és a költségvetés – melybe beletartozik a beszerzésen kívül az üzemeltetés is – megfelelő egyensúlya a cél.¹⁵³

Biztonságtechnikai mechanikai eszközök:

- *vasbeton terelőelemek*: keresztmetszetük trapéz alakú, fejre állított „T” betűre hasonlít. Magasságuk típustól függően eltérő, a 80 cm-től akár a több méteres magasságig terjedhet. Az elemeket egymás mellé állítva a forgalom irányítására szolgál. Jól behatárolható vele a kötelező forgalmi sáv vagy a forgalomtól elzárt terület is. Alapozás és lerögzítés nélkül is alkalmazhatóak, így hamar átrakhatóak, ha a helyzet változása megköveteli. Alaphoz rögzíthető változatban is készül, mely megnöveli a védelmi képességét, viszont csökkenti mobilitását.¹⁵⁴
- *gyorskapu*: lehetővé teszi a gépjárművek részére a gyors ki- és beléptetést. Az alkalmazási területét meghatározza, hogy szükséges az alsó és felső vezetősín, esetleg az oldalsó megfogás számára elégséges hely biztosítása oldalirányban. A hagyományos kapuk nyitási sebessége átlagosan 0,2 m/sec, mely alkalmatlanná teszi őket a nagytömegű, gyors és ellenőrzött forgalom számára. A gyors kapu záródási sebessége 1 m/s. Létezik a gyorsan záródó kapuknak alsó sínen vezetett megoldása is, mely még félig zárt állapotában is megállítja a járművet. E típus előnye, hogy mindössze 30 cm mély alapozást igényel és záródási sebessége 2 m/s.

¹⁵¹ [67] Kovács, Z. (2013) Katonai objektumok IED elleni védelmének lehetséges technikai megoldásai. *Műszaki Katonai Közlöny*, XXIII/2.

¹⁵² Balogh Zs. (2013) Katonai objektumok robbantásos cselekmények elleni védelmének lehetőségei. PhD értekezés. Budapest; NKE

¹⁵³ Balogh Zs. (2013): Épületek robbantás elleni védelmének építészeti szempontjai. *TÁMOP-4.2.1.B-11/2/KMR „Robbantásos építményvédelem” kiemelt kutatási terület*. 6. fejezet

¹⁵⁴ Kovács T. (2013) A katonai táborok biztonsági rendszereinek kialakítása, különös tekintettel a robbantásos merényletek megelőzésére, azok hatásai csökkentésére. II. *Műszaki Katonai Közlöny*, (XXIII./1)

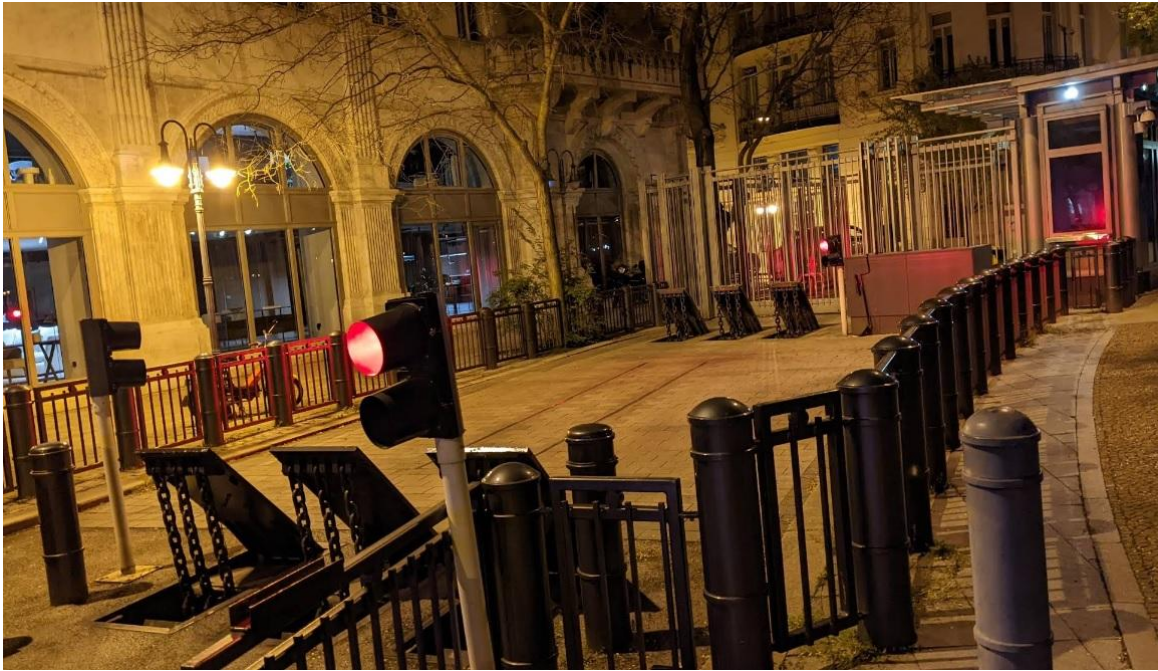


9. sz. ábra: biztonsági gyorskapu¹⁵⁵

- *forgalomkorlátozó oszlop*: a járművek elől elzárt terület biztosítására szolgál. 1 m magasságú, 10 – 30 cm átmérőjű, általában kör keresztmetszetű oszlop, melynek fej részébe kamera, irányjelző világítás, vagy egyéb elektronikai eszköz is beépíthető. A süllyeszthető típus alapozása a süllyesztés mélységét és a gépészetet is magában kell, hogy foglalja, viszont biztosítja a kontrollált áthaladást. A fix típusnál elegendő a 40 cm-es alapozási mélység. Lehetőség van 3-4 oszlop talpnál történő összekötése, majd telepítés után lehet kiönteni betonnal az oszlopokat és az alapot is. A fix típusokat telepítés után különféle utcabútorokkal lehet rejteni, például hirdetőablak, virágtartók, padok, stb.
- *fésűs vagy hidraulikus útzárak*: ezeket az úttorlaszokat arra tervezték, hogy a védett zónába idegen gépjármű nagy sebességgel és nagy súllyal se tudjon behatolni. Passzív állapotukban teljesen belesimulnak az útfelszínbe, manuális vagy automatikus aktiváláskor 1-2 másodpercen belül felemelkednek. Fordított üzemben alkalmazva kiemelt helyzetben van és csak a behajtásra jogosult jármű érkezésekor simul bele az

¹⁵⁵ Forrás: <https://hu.hongfahsd.com/turbine-hard-high-speed-door/> Letöltés: 2026.04.08.

úttestbe, biztosítva az akadálytalan áthajtást. 60-80 cm magasságig emelkednek fel, mely elegendő nagyobb jármű megállítására is.¹⁵⁶



10. sz. ábra: Süllyesztett hidraulikus útzár¹⁵⁷



11. sz. ábra: Balpro hidraulikus kapuelem védelmi üzemmódban¹⁵⁸

¹⁵⁶ Bakos T. (2023): Katonai műszaki-technikai újítások a MILENG COE 2022-es ipari napján I. rész. *Haditechnika*, 57(3),

¹⁵⁷ Forrás: Google Map, Amerikai Egyesült Államok Nagykövetsége, Budapest, Szabadság tér

¹⁵⁸ Forrás: https://www.kenno-shield.com/balpro/force-protection-balpro-products/balpro-hydraulic-road-barrier/kenno-tech_balpro_road-barrier_4/#main Letöltés: 2023.02.15.

- *sorompók*: a sorompók közismert típusa nem alkalmas a járművek megállítására, csak vizuális figyelemfelkeltésre használatosak. Jelzik a gépjármű vezetőjének, hogy adott helyen ellenőrzés vagy egyéb biztonsági okokból meg kell állni. Fokozott biztonsági igényű létesítmény esetén viszont érdemes a nagyobb terhelésre ellenálló sorompó telepítésével tervezni. Több típusa létezik – például az oldalról záródó, útfelszínből kiemelkedő, stb. – de közös tulajdonságuk, hogy zárt állapotban a nagy teherbírású sorompórúd mindkét vége rögzítve van, mély alapozású szerkezetekkel. A változtatható magassággal biztosítható a gyalogos és gépjármű forgalom különválasztása is.
- *kerítések*: a kerítések a körkörös védelemhez tartoznak. A vizuális figyelemfelkeltéstől akár a nehéz, gyorsan mozgó gépjárművek megállításáig terjedhet a védelmi képességük, technikai megvalósítás és a rendelkezésre álló költségektől függően. Az eredetileg gyalogosforgalomtól elzárt terület kijelölésére alkalmazott kerítés megerősíthető olyan alapozású oszlopokhoz rögzített galvanizált acélkábelekkel, mely szakítószilárdsága a 70 tonnát is eléri. Anyagukat tekintve lehetnek fém, beton, vasbeton, fa, műanyag, kő, élő sövény kerítések. Külalakjuknak a biztonsági előírásoknak való megfelelésen kívül csak a fantázia szab határt. Előnyük, hogy az alapfunkcióján kívül – mozgásakadályozás – felszerelhető egyéb eszközökkel is, melyek a védelmet tovább növelik. Ilyenek lehetnek a különböző biztonságtechnikai elektronikai eszközök, vizuális felderítést akadályozó kiegészítők, a környezetbe illeszkedő dizájn elemek.



12. sz. ábra: megerősített biztonsági fémkerítés¹⁵⁹

Biztonságtechnikai elektronikai eszközök:

- *elektronikus jelzőrendszerek*: az elektronikus behatolás jelző rendszerek a mechanikai és az élőerős védelmet egészítik ki. A kültéren és beltéren egyaránt alkalmazható rendszer a mechanikai védelem megközelítését is képes jelezni és riasztást ad a megadott határértékek átlépése esetén. Akkor igazán hatékonyak, ha minden védelmi zónában telepítve vannak, és a jelzéseik egy rendszeren belül kezelhetőek. A felületvédelem eszközei az épületek homlokzatát érő hatásokra érzékenyek, az esetleges behatolási kísérletet jelzik. Lehetnek falbontás érzékelők, vagy mágneses, illetve mechanikus nyílászáró érzékelők. Üvegfelületekre ragasztva az úgynevezett kontakt vagy akusztikus érzékelők is használhatóak.
- *megfigyelő rendszerek*: a zárláncú video megfigyelő rendszerek nem csak megfigyelésre, hanem a telepítés helyszínein történő tevékenység rögzítésére is alkalmasak. A kültéri vagy beltéri kamera fekete-fehér, színes, éjszakai vagy akár hőképet vagy más tartományú képet is adhat fixen, vagy mozgatható, nagyítható verzióban. Napjainkban a nagyfelbontású képek rögzítése mellett már elérhetőek a

¹⁵⁹ Forrás: <https://statedefenceco.com/our-portfolio-2/> Letöltés: 2026.04.08.

mesterséges intelligenciával támogatott azonnali analízisére képes szoftverek is (arcfelismerő, mozgásanalizáló, változásfigyelő, stb. szoftverek).



13. sz. ábra: MI analizáló szoftverrel támogatott biztonsági kerítés¹⁶⁰

¹⁶⁰ Forrás: <https://www.puretechsystems.com/> Letöltés: 2026.04.08.



14. sz. ábra: Raptor nagy hatótávolságú földi radar és EO/IR megfigyelő rendszer¹⁶¹

- *beléptető rendszerek*: elsősorban a személyek és járművek biztonsági regisztrációjára használhatóak, de a létesítmény, illetve a létesítményen belüli épületek, építmények több pontján alkalmazva pontos mozgás ellenőrzésre is alkalmasak. Mechanikai eszközökkel együtt alkalmazva az épületeken, építményeken belüli mozgások kontrollálására, akadályozására is használhatóak. Az elektronikus, programozható kártyás rendszerek mellett, főleg gépjárműves beléptetésekhez gyakran használják a nagyobb távolságban is pontos mikrohullámú azonosító rendszert. Napjainkban már egyre több helyen alkalmazzák a biometrikus azonosító rendszereket, melyek az ember fizikai tulajdonságai alapján végzik az azonosítást. Bár a biometrikus érzékelők fejlődésük révén ma már igen pontos adatokat szolgáltatnak, érdemes több jellemző tulajdonságot egyszerre mérni és egyszerre kezelni a megfelelő szintű védelem

¹⁶¹ Forrás: <https://www.army-technology.com/products/raptor-surveillance-system/#:~:text=IEC's%20Raptor%2C%20aptly%20named%20after%20birds%20of,large%20areas%20for%20int,ruders%20or%20enemy%20forces.> Letöltés: 2026.04.08.

kialakítása érdekében. Az elektronikus és biometrikus érzékelők egyidejű használata magas szintű azonosítást eredményez.

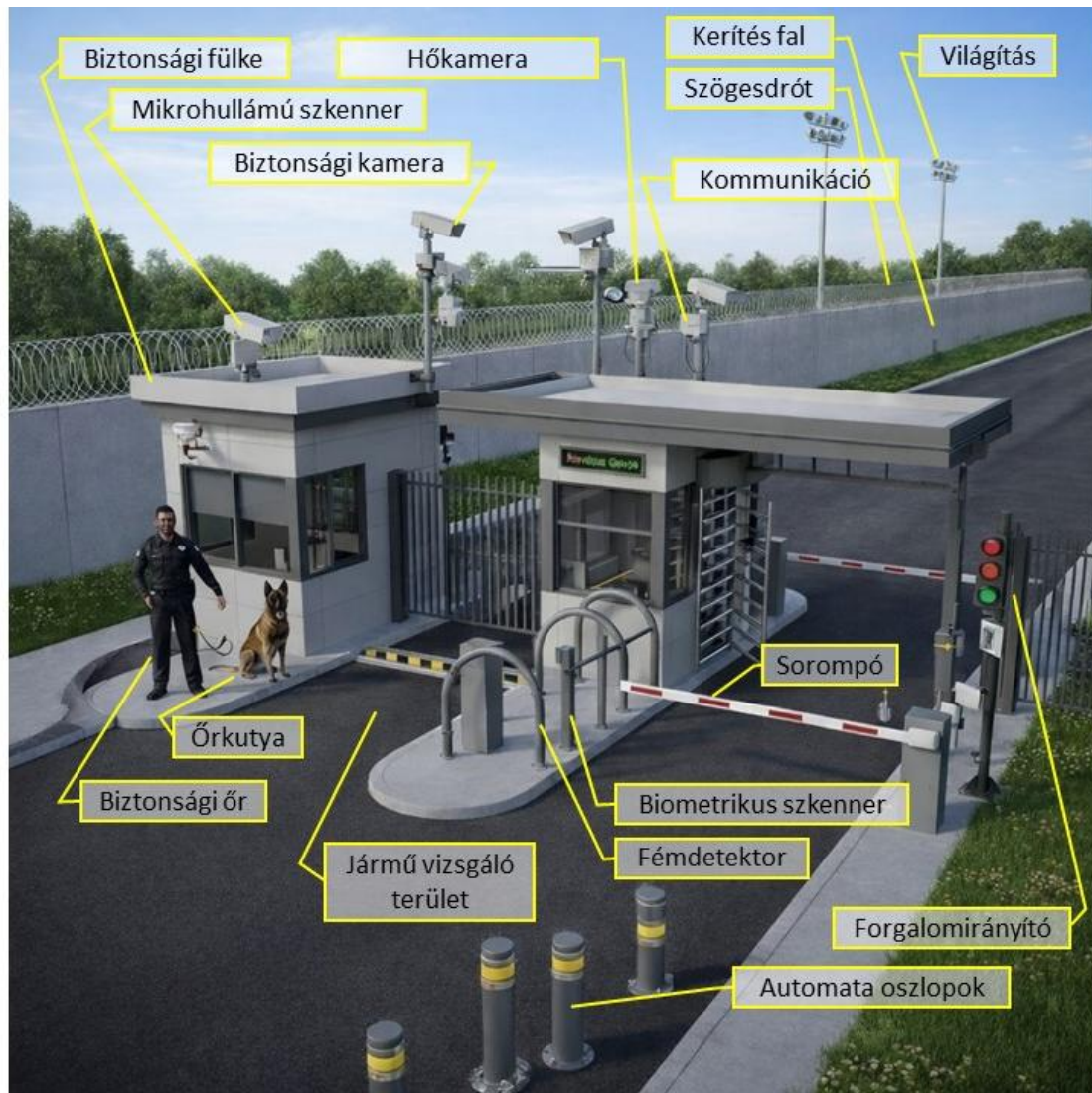


15. sz. ábra: biometrikus azonosítóval ellátott beléptető rendszer¹⁶²

- *detektáló rendszerek:* A detektorok kifejezetten bizonyos eszközök, anyagok felderítésére alkalmazhatóak. Legismertebb típusuk a fémdetektorok, melyek felépítésüktől függően a nagyobb fémtárgyakat vagy a vékony fémhuzalokat is képesek érzékelni. A röntgensugaras vizsgálók már képesek a szerves és szervetlen anyagokat is kimutatni, illetve alkalmasak nagyobb méretű tárgyak – tehergépjárművek – átvizsgálására is. A nagyfelbontású röntgensugaras vizsgálók képesek az átvilágított anyagok sűrűsége és az effektív atomszám alapján robbanóanyagok vagy egyéb anyagok felkutatására is. A milliméteres hullámhosszú átvizsgálók már a röntgen tartomány helyett az elektromágneses sugárzás milliméteres spektrumában működnek. Ezzel az eszközzel már a nem fémes eszközök, anyagok detektálása is lehetséges. Működése alapján ez az eszköz, egy többretegű háromdimenziós szkener, mely leképezi a detektorpanel elé állított személy kontúrját és láthatóvá teszi a testen elhelyezett tárgyakat, eszközöket, akár a ruházat alatt is.

¹⁶² Forrás: <https://wolveyesae.com/> Letöltés: 2026.04.08.

- *folyadékdetektorok*: Az elektromágneses rezonancia és az infravörös spektroszkópia elvét felhasználva a napjainkban használatos folyadékdetektorok pár másodperc alatt meg tudják állapítani az ellenőrizni kívánt folyadékról, hogy tartalmaznak-e bizonyos veszélyes anyagokat. Továbbfejlesztett változata a mágneses magrezonancia elvén alapuló folyadékvizsgáló készülék, mely érzékenységenek köszönhetően különbséget tud tenni akár az üdítő italok között is.



16. sz. ábra: modern, többrétegű ellenőrző-áteresztő rendszer¹⁶³

¹⁶³ Forrás: https://www.linkedin.com/posts/pradeeptamilan-%E0%AE%A4%E0%AE%AE%E0%AE%BF%E0%AE%B4%E0%AE%A9%E0%AF%8D-112800305_securityinfrastructure-civilengineering-activity-7427712479452975105-VIUU Letöltés: 2026.04.08. (Saját szerkesztésű magyar felirat)

3.1.2.3. A harmadik biztonsági zóna – belső kritikus elemek

A kritikus szervezet fogalmának¹⁶⁴ rekurzív alkalmazásával könnyen meghatározható egy kritikus szervezet vagy infrastruktúra *belső kritikus elemének* fogalma:

„A kritikus szervezet olyan belső szolgáltatást nyújtó eleme, mely elengedhetetlen a kritikus szervezet vagy infrastruktúra működési és üzemelési stabilitásához és a biztonság, a környezet, a munkavállalók egészsége, valamint a védelmi képességek és az ellenálló képességi rendszerek fenntartásához.”

A kritikus szervezetek, infrastruktúrák így definiált kritikus elemei biztosítják az üzemfolytonosságot és üzembiztonságot speciális időszakban is.

A kritikus elem lehet akár egy folyamatot irányító számítógép, vagy egy fő ellátást biztosító közmű, de akár egy kritikus munkakörben dolgozó munkavállaló munkahelye is.

A kritikus elemek elhelyezésére szolgáló létesítmények kiemelt védelmére *belső biztonsági zónákat* kell létrehozni, vagyis olyan speciális védelmi rendszereket, építményeket kell kialakítani, melyek bőven megfelelnek a szükséges védelmi szint követelményeinek és biztosítják a védett elem üzemelését, üzemfolytonosságát, speciális helyzetekben is.

3.1.3. Kritikus elemek létesítményeinek védelme

A védett létesítmények több szempont alapján osztályozhatók. Rendeltetésük szerint megkülönböztethetünk állami és diplomáciai, katonai és polgári védelmi létesítményeket, illetve a kritikus szervezetek, infrastruktúrák létesítményeit.

Funkciójuk szerint beszélhetünk a vezetési és biztonsági központok, kormányzati és katonai vezetési pontok, szervertermek, adatközpontok, kommunikációs rendszerek irányító helyiségei, informatikai és híradó központok, elektromos-, víz-, gázellátó rendszerek, illetve egyéb közművek főbb elemeinek elhelyezésére, védelmére szolgáló létesítményekről, illetve ide sorolhatók a személyi védelmet biztosító helységek, veszélyes- vagy speciális anyag és eszköz tárolók, valamint minden olyan létesítmény, mely a kockázatelemzés alapján a kritikus elem fogalom körébe tartozhat.¹⁶⁵

¹⁶⁴ Kszetv. 3.§ 30.

¹⁶⁵ Kovács F. (2025): Állami és katonai védett létesítmények létrehozása és fenntartása. NKE Katonai Műszaki Doktori Iskola, előadás, Budapest.

A védett létesítmények védelmi fokozatok szerinti osztályozására leggyakrabban a robbanásból származó többlet frontnyomásnak való ellenállás mértékét (I.–V. fokozatú létesítmények)¹⁶⁶ alkalmazzuk. A másik alapvető besorolási és minősítési kategória a radiológiai, biológiai vegyi és nukleáris (CBRN) védettség szintje szerinti besorolás. Ezt az alapvető képességet írja elő a NATO is a védett létesítményekre egy adott kategória felett.^{167,168} A CBRN védettség követelményeinek részletes ismertetésétől ezen értekezésben eltekintek.

Elhelyezkedésük alapján beszélhetünk felszíni, félig földbe ágyazott, föld alatti és alagúrendszerű védett létesítményekről.

3.1.3.1. Védett létesítmények illegális behatolás elleni védelme

A kritikus szervezetek és infrastruktúrák létesítményei megközelíthetőségének akadályozása, illetve a megközelítés ellenőrzése, irányítása mellett ugyanolyan fontos a belső védett létesítményeken belüli mozgások ellenőrzése, irányítása, szükség szerinti akadályozása.

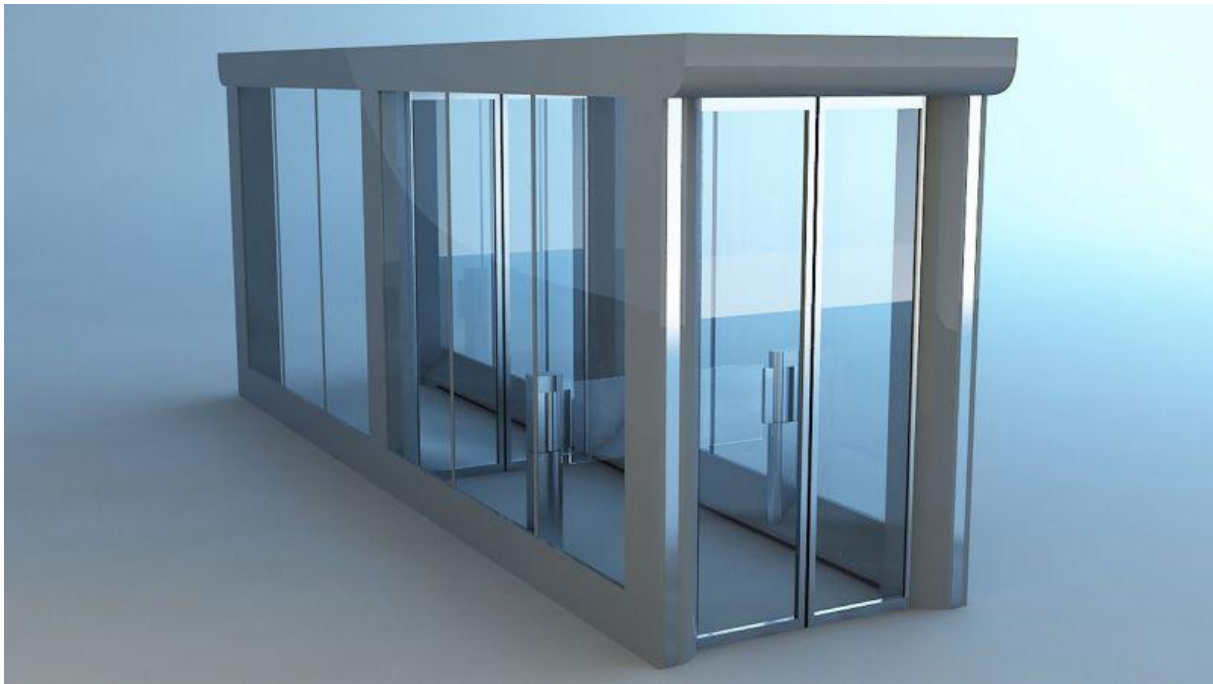
A 3.1.2. alfejezetben már szóba került az épületeken belüli mozgások koordinációja a védelem hatékonyságának növelése érdekében, de csak, mint kiegészítő eszköz. Az épületeken belüli élőerős őrzésvédelem, biztonságtechnikai eszköz használat és egyéb kapcsolódó védelmi eszköz, módszer hatékonyságát is lehet növelni az épületek, építmények belső tereinek védelmi szempontok szerinti kialakításával, mint például:

Zsilip rendszerű beléptető pontok alkalmazása, melyek segítenek megfigyelni, ellenőrizni a beléptetést, megállítani, elzárni a jogosulatlan belépést megkísérlő személyeket, és figyelemmel kísérni az egyes belépési pontokat.

¹⁶⁶ Kategóriákhoz tartozó nyomásérték: V. 0,03 Mpa, IV. 0,01 Mpa, III. 0,5 Mpa, II. 1,0 Mpa, I. 2,0 Mpa többletnyomás

¹⁶⁷ NATO: Allied Joint Doctrine for Force Protection. AJP-3.14. Brussels, 2007.

¹⁶⁸ NATO: Allied Joint Doctrine for the Conduct of Operations. AJP-3. Brussels, 2010.



17. sz. ábra: egyirányú személyi beléptető zsilip folyosó¹⁶⁹

Kerülni kell a biztonsági kontroll alól kieső terek kialakítását. A funkció nélküli kiszögeléseket, beugrókat lehetőleg be kell építeni, vagyis törekedni kell a geometriai folytonosság kialakítására, a jó átláthatóság érdekében.

A külső menekülő tűzlétrák, külső vezetésű villámhárítók nehezen ellenőrizhető, alternatív mozgási útvonalakat adnak, lehetőség szerint kerülni kell, vagy ha nem lehetséges, akkor komoly biztonságtechnikai védelemmel kell ellátni.

A talajszintről könnyedén elérhető nyílászárók nem csak jó behatolási pontok, hanem jó kapaszkodók is a felsőbb szintek eléréséhez. A használaton kívüli nyílászárókat érdemes megszüntetni, vagy védett oldalra helyezni, de amennyiben nem lehetséges, akkor biztonságtechnikai eszközökkel a védelmét meg kell erősíteni.¹⁷⁰

Bár az épületek alatt húzódó közművek, illetve épületen kívül húzódó szellőztető rendszerek, közműalagutak átalakítása a költségesebb védelmi intézkedések közé tartozik, de a rossz láthatóság, nehezen ellenőrizhető belső részei miatt a magas szintű védelem kialakítása kiemelt fontossággal bír.

¹⁶⁹ Forrás: <https://www.airport-suppliers.com/product/oneway-corridor/> Letöltés: 2026.04.08.

¹⁷⁰ Balogh Zs. (2013) Katonai objektumok robbantásos cselekmények elleni védelmének lehetőségei. PhD értekezés. Budapest; NKE

3.1.3.2. Védett létesítmények kialakításának követelményei

A fizikai védelem alapját a behatolás elleni védelem mellett a különböző hatásokkal szembeni ellenállás képezi. Kiemelt szerepet kap a környezeti hatások elleni védelem, amely magában foglalja a gáztömörség biztosítását, az elektromágneses impulzusok elleni védelmet, szükség esetén a hermetikus zárást radioaktív, vegyi és biológiai veszélyek ellen. Ide tartozik a robbanások lökéshullámai és repeszhatása elleni védelem, az épületszerkezetek dinamikai terhelésekkel szembeni ellenálló képessége, a tűzvédelmi rendszerek, speciális létesítmények esetén a biológiai biztonság is. Zárt létesítményekben való munkavégzés, illetve az esetleges hosszú idejű elzárkózás esetén figyelemmel kell lenni a pszichológiai feltételek biztosítására is.

Amennyiben szükséges és a lehetőségek is adottak, több technológia is rendelkezésre áll az épületek, építmények belső szerkezeti kialakításának megerősítésére, védelmi képességük fokozására. Már használatban lévő épület esetén a fő teherhordó szerkezet megerősítése komolyabb előkészületeket, több esetben a szerkezet megbontását igényli, új építmény esetén viszont előre tervezhető. Amennyiben erre nincs lehetőség, jó megoldás lehet a másodlagos teherhordó szerkezetek kialakítása. A nem teherhordó szerkezetek könnyebben cserélhetőek, a normál téglafalazat vagy egyszerű szerkezetű térelválasztó elemek helyett alkalmazhatók speciális felépítményű szerkezetek, elválasztó elemek, mint például mikrovasalatú beton lapok, kevlár vagy szénszálas cementált lapok, többrétegű panelek. Amennyiben nem szükséges a cseréje a nem teherhordó szerkezeteknek, védelmi képességük javítására ugyancsak több technológia is rendelkezésre áll. A különböző utólag felhordható anyagok, mint például a műgyanta bevonatok, vagy kevlár, illetve szénszálas ragasztott megerősítő bevonatok jelentősen növelhetik a falazat teherbírását, illetve az átütés elleni védelmüket.¹⁷¹ Speciális esetekben a belövés biztos üvegszerkezetek alkalmazására is van lehetőség.

Amennyiben szükséges a hermetikus védelem kialakítása, a bejáratoknál nyomásálló és gázzáró ajtók alkalmazhatók, valamint speciális szellőző- és légszűrő rendszerek építhetők ki, amelyek biztosítják a belső terek túlnyomását, a levegő tisztítását és keringtetését. Elzárkózás esetén szükséges a belső levegő visszakeringtetése, vagyis a belső levegő szűrés és kondicionálás utáni visszajuttatása a belső térbe, ezzel fenntartva az optimális környezetet.

Napjainkban a védett létesítmények kialakítására az adatközpontok adnak jó példát. Az adatközpontok működése szempontjából alapvető követelmény a magas rendelkezésre állás,

¹⁷¹ Antal Ö. (2014): Az épületek védelmének korszerű lehetőségei házi készítésű robbanóeszközök ellen. Műszaki Katonai Közlöny, (XXIV./1)

ezért ennek érdekében redundáns energiaellátási rendszereket alkalmaznak, beleértve a szünetmentes tápegységeket, akkumulátor parkokat és a dízel aggregátorokat, amelyek akár hosszabb ideig is képesek biztosítani az energiaellátást. A jövőben az ipari energiatárolók is előtérbe kerülhetnek. A klimatizálás szintén kritikus tényező, mivel a berendezések működéséhez alacsony páratartalom és szűk hőmérsékleti tartomány szükséges. Kiemelt követelmény a folyamatos monitoring és felügyeleti rendszerek kialakítása, melyek lehetővé teszik az esetleges hibák gyors felismerését és kezelését.

Óriási költséggel jár, de az üzletmenet-folytonosság (BCP) maximális biztonságát jelenti egy kritikus szervezet teljes redundanciája. Ebben az esetben a szervezet működéséhez szükséges minden infrastruktúra, adat és szoftver többszörözött, földrajzi szempontból is elkülönített, és a kulcsbeosztásokban lévő munkavállalók is képesek egymás munkaköreinek szükség szerinti átvételére.

A jövőbeli fejlesztések iránya a hibrid fenyegetésekhez való alkalmazkodás. Ide tartozik a digitális infrastruktúrák fokozott védelme, a föld alatti és megerősített létesítmények korszerűsítése és fejlesztése, valamint az energiahálózatok és speciális ipari objektumok biztonságának növelése. Egyre nagyobb szerepet kapnak a jövőben az olyan új típusú fejlesztett védett létesítmények, mint a moduláris atomreaktorok, a hadiipari, kísérleti, biológiai létesítmények, génbankok, nemzeti értéktárgyak tárolói, vagy az űrtechnológia és annak kiszolgáló földi állomásai.¹⁷²

3.1.3.3. Védett létesítmények drónok elleni védelme

Az elmúlt évek egyik legújabb biztonsági kihívása tagadhatatlanul a pilóta nélküli járművek (drónok) megjelenése és gyors fejlődése. A vízalatti, vízi, szárazföldi, légi drónok napjainkban egyre komolyabb fenyegetést jelentenek a kritikus infrastruktúrákra, mivel ezek az eszközök viszonylag olcsón hozzáférhetők, könnyen módosíthatók és sokféle módon alkalmazhatók akár támadási, akár felderítési célokra.

A védekezés egyik kulcseleme a drónok időben történő észlelése, melyre több detektálási módszer is alkalmazható. Ide tartozik a vizuális felismerés vagy hőképtétel érzékelése kamerarendszerekkel, a hangalapú észlelés mikrofonok segítségével, a rádiófrekvenciás kommunikáció felderítése, vagy a rádiólokációs (radar) alapú megfigyelés. Mindegyik

¹⁷² Kovács Ferenc c. egyetemi tanár Védett létesítmények c. KMDI előadása (2026) alapján

módszerek megvan az előnye, de vannak korlátaik is, hiszen minden felderítési, detektálási módszer ellen lehet védekezni. A hőkamerás érzékelés hatékonyságát csökkentheti a hőelvezetés technikai megoldása, míg az akusztikus észlelés nehézségeit a környezeti zajok növelik. A vizuális rendszerek időjárásfüggők, a rádiófrekvenciás módszerek pedig nem működnek autonóm módon közeledő drónok esetén. Mindezekből következik, hogy egyetlen detektálási módszer önmagában nem elegendő, a hatékony észlelő rendszer több különböző elven működő érzékelők kombinációjára épül. Logikus, hogy minél több, egymástól független és különböző elven működő érzékelő kerül alkalmazásra, annál nagyobb az esély arra, hogy a drónt időben észlelik.

A detektálás után a következő lépés a drón semlegesítése. Ide tartozik a lövedékkel, rakétával vagy lézeres eszközzel való megsemmisítés, a hálóval történő elfogás, az elektromágneses impulzussal való károsítás, a kommunikációs jelek zavarása, valamint a GPS-jel manipulálása. Ezek a technológiák különböző körülmények között eltérő hatékonysággal működnek. Például a ballisztikai és lézeres rendszerek időjárásfüggők, míg a rádiózavarás hatástalan lehet autonóm drónokkal szemben. A detektáláshoz hasonlóan logikus, hogy minél több, egymástól független és különböző elven működő elfogó rendszer kerül alkalmazásra, annál nagyobb az esély arra, hogy a drónt időben semlegesítik.



18. sz. ábra: Iron Beam nagyteljesítményű lézeres légvédelmi rendszer¹⁷³

A detektálási és semlegesítési rendszerek hatékonyságát valós körülmények között érdemes mérni, mivel számos tényező befolyásolja az eredményeket. Ilyen tényezők lehetnek a környezeti viszonyok, az időjárás, a napszak, a drón típusa, a mozgási mód.

A technikai rendszerek mellett nagyban növeli a drónok elleni védelmet ha megelőző intézkedéseket is alkalmazunk. Ilyen lehet például a tiltott drónzónák kijelölése, a munkavállalók és a biztonsági személyzet differenciált képzése, a létesítmények álcázása vagy a korábban már tárgyalt, zónákra bontott fizikai védelmi kialakítása.¹⁷⁴

3.1.4. Élőerős őrzés-védelem

¹⁷³ Forrás: <https://www.jfed.net/goodnewsisrael/israels-iron-beam-fully-operational-to-hit-missiles-along-with-drones> Letöltés: 2026.04.08.

¹⁷⁴ Łukasiewicz J., Kobaszyńska – Twardowska A. (2022): Proposed method for building an anti-drone system for the protection of facilities important for state security. Security and Defence Quarterly, 3/2022 vol. 39.

Az élőerős őrzés-védelem a személy- és vagyónvédelem egyik alapvető formája, amelynek jogi kereteit Magyarországon a 2005. évi CXXXIII. törvény¹⁷⁵ határozza meg. A jogszabály szerint személy- és vagyónvédelmi tevékenységnek minősül a természetes személyek életének és testi épségének védelme, az ingatlanok és ingóságok őrzése, a szállítmányok kísérése, a pénz- és értékszállítás, valamint a rendezvények biztosítása és az ezekhez kapcsolódó szervezési, irányítási feladatok ellátása.

Az élőerős védelem ennek a tevékenységi körnek az a formája, amely során a feladatokat megfelelő szakképesítéssel és hatósági igazolvánnyal rendelkező személy – jellemzően vagyónőr vagy biztonsági őr – személyes jelenléttel, folyamatos fizikai felügyelet mellett végzi.

Az élőerős őrzés lényegét az emberi jelenlét és a biztonsági képzettség adja, amely magában foglalja a területfelügyeletet, a beléptetés és kiléptetés ellenőrzését, a jogosulatlan behatolás megakadályozását, a rendkívüli események felismerését, dokumentálását, valamint szükség esetén az azonnali intézkedést és a hatóságok értesítését. A fizikai jelenlét igen komoly megelőző hatással rendelkezik, mivel látható módon csökkenti a nem kívánt cselekmények számát és lehetővé teszi a gyors reagálást olyan helyzetekben is, melyek technikai rendszerekkel önmagukban nem kezelhetők.

Az élőerős védelem jelentősége különösen hangsúlyos a kritikus szervezetek és infrastruktúrák esetében. E létesítmények esetében a biztonsági kockázatok nemcsak vagyon elleni cselekményekből, hanem szándékos károkozásból, terrorcselekményekből, belső visszaélésekből vagy működési zavarokból is fakadhatnak.

A kritikus infrastruktúrák védelmében az élőerős őrzés pótolhatatlan szerepet tölt be, mivel az emberi döntéshozatal és helyzetértékelés képessége lehetővé teszi a komplexebb, gyorsan változó rendkívüli események kezelését. A vagyónőr képes a technikai jelzések értelmezésére, a gyanús magatartások felismerésére, a belső szabályok betartatására, valamint a szükséges operatív intézkedések megtételére, amely a kritikus szervezetek és infrastruktúrák biztonságának és üzemfolytonosságának alapvető feltétele.¹⁷⁶

Az élőerős védelmet minden esetben a biztonsági rendszer részeként kell működtetni, amelyben a humán erőforrás a mechanikai és elektronikai védelmi megoldásokat egészíti ki és felügyeli. Mindebben a robotizáció alapvető változásokat hozhat a jövőben.

¹⁷⁵ 2005. évi CXXXIII. törvény a személy- és vagyónvédelmi, valamint a magánnyomozói tevékenység szabályairól

¹⁷⁶ [37] Boruzs H. (2024): Physical protection characteristics of critical infrastructures hungary – the armed security guard. Biztonságtudományi Szemle, IV/1.

A jogszabály szigorú személyi és működési feltételeket állapít meg a tevékenység végzéséhez, amely a feladat jelentőségét tükrözi. A személy- és vagyonvédelmi tevékenység végzéséhez rendőrség által kiadott igazolvány, megfelelő szakképesítés, büntetlen előélet, valamint – külső szolgáltató esetén – működési engedély és felelősségbiztosítás szükséges. Ezen felül, a rendőrség nyilvántartási és ellenőrzési jogkörrel rendelkezik a jogszerű működés biztosítása érdekében.

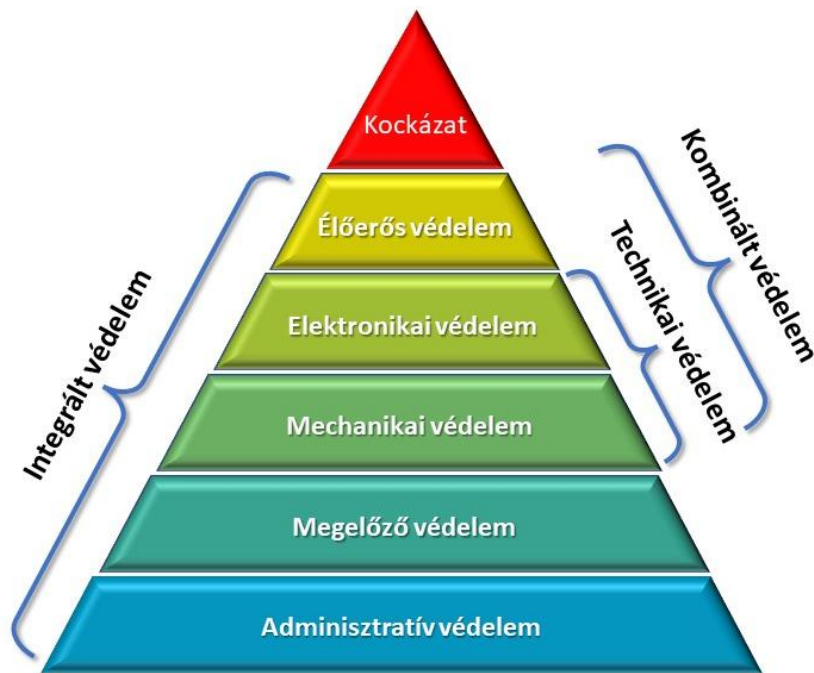
Összességében az előerős őrzés-védelem a kritikus szervezetek és infrastruktúrák ellenálló képességének és fizikai védelmének egyik kulcseleme.

3.1.5. Átfogó védelem

Az arányos és átfogó védelem kialakítása a kritikus szervezetek és infrastruktúrák sebezhetőségének és fenyegetettségének csökkentését, az ellenálló képesség növelését jelenti, ezen belül legfontosabb feladata az üzemfolytonosság biztosítása különleges viszonyok között is. A kockázatelemzés alapján, az EKT részletes kidolgozásával már megkezdődik az átfogó védelmi képesség kialakítása, mely sok esetben újabb – akár üzemfolytonossági, technológiai, akár külső – kockázatok feltárásával és minden esetben plusz költségfordítással jár.

A védelem fogalmának vizsgálata azt is mutatja, hogy a védelem felépítése erősen függ attól, hogy mely szakterülettel áll kapcsolatban (jogi védelem, informatikai védelem, fizikai védelem, munkavédelem, tűzvédelem, stb.). Viszont bármely szakterületet vesszük alapul, a védelem minden esetben több elemből, illetve több rétegből kell, hogy felépüljön (6. ábra):¹⁷⁷

¹⁷⁷ Szabó S., Tóth R. (2013): Repülőterek kialakítása, létesítményeinek kritikus elemei, védelmük lehetséges műszaki megoldásai. *Repüléstudományi Közlemények*, XXV. évfolyam, 2. szám. 89-113.



19. sz. ábra: Átfogó védelem elemeinek egymásra épülése¹⁷⁸

- *Adminisztratív védelem:* azon jogszabályok, szabványok, előírások, melyek megteremtik az adott létesítmény, építmény védelmi igényeinek alapját, meghatározzák a védelem főbb irányait és módszereit.
- *Megelőző védelem:* ide tartozik a kockázatelemzés és a kockázatelemzés eredményeinek vizsgálata, a védelmi prioritások kialakítása, illetve az ezen adatok alapján elkészített védelmi tervek és intézkedések, melyek betartása, betartatása már önmagukban is egy bizonyos védelmi szintet képesek biztosítani.
- *Mechanikai védelem:* a biztonságtechnikai mechanikai védelmi eszközökkel, a megközelíthetőséggel és a megfelelő szerkezeti kialakítások alkalmazásával elérhető védelem.
- *Elektronikai védelem:* a biztonságtechnikai elektronikai védelmi eszközökkel, illetve az informatikai védelmi és elemző rendszerek hatékony alkalmazásával elérhető védelem.
- *Élőerős védelem:* ide tartoznak azon szervezetek, melyek tagjai jogszabályban meghatározott joguknál fogva őrzésvédelmi feladatokat láthatnak el. Rendelkezhetnek szolgálati fegyverrel, egyéb kényszerítő eszközökkel, joguk van a szintjüknek megfelelő intézkedések meghozatalára.

¹⁷⁸ Szabó S., Tóth R. (2013): Repülőterek kialakítása, létesítményeinek kritikus elemei, védelmük lehetséges műszaki megoldásai. *Repüléstudományi Közlemények*, XXV. évfolyam, 2. szám. 106.o

Kombinált védelem

Kombinált védelemről abban az esetben beszélhetünk, ha az előzőekben tárgyalt védelmi elemeket egymással párhuzamosan, egymás mellett alkalmazzuk. Leggyakoribb példa a kombinált védelemre az élőerős védelem és a mechanikai védelem együttes alkalmazása elektronikai védelmi eszközökkel kiegészítve.

Integrált védelem

Integrált védelem esetén az előzőekben tárgyalt védelem elemeit nem csak egymás mellett, kombinálva alkalmazzuk, hanem a különböző szintek és módszerek kialakításánál ezen védelmi elemek sajátos tulajdonságait is egymáshoz igazítjuk. Valamennyi védelmi szint, intézkedés, módszer és megoldás úgy van kialakítva, hogy egyes részüik részét képezi a másoknak, az átfedések logikusan kötődnek a védelem egészéhez, ezzel növelve a rendszer stabilitását és hatékonyságát.

Átfogó védelem

Az átfogó védelem abban az esetben valósul meg, ha a 2.4. alfejezetben tárgyalt folyamatos és ciklikusan végrehajtott kockázatelemzés eredményeit felhasználva a védelmi rendszert is folyamatosan és ciklikusan felülvizsgáljuk, a biztonsági környezethez igazítjuk. Ha az előzőekben tárgyalt védelmi elemeket kiegészítve megjelentetjük a rendszerben azon területeket is, melyek nem rendelkeznek védelemmel, vagyis fennmaradó kockázatként jelennek meg, akkor vizsgálhatjuk bekövetkezésük hatását a teljes rendszerre.

Átfogó védelem akkor valósul meg, ha ezen fennmaradó kockázatok bekövetkezésének hatása a védelmi rendszer stabilitására és az üzemfolytonosságra elhanyagolható.

Összefoglalva tehát látható, hogy egy kritikus szervezet vagy infrastruktúra bármely védelmi területének átfogó jellege csak úgy valósulhat meg, ha a védelem minden elemében megjelenik a kockázatértékelés eredménye és a ciklikusság elvének megfelelően felülvizsgálva frissül.

A hatékony fizikai védelem kialakításában természetesen prioritásként jelenik meg a biztonságtechnikai eszközök és az élőerős védelem alkalmazása, de igazán hatékony csak akkor lesz a fizikai védelmi rendszer, ha átfogó jelleggel épül fel:

- a jogszabályokban megadott módon lehetőség van a mozgások ellenőrzésére, korlátozására. Szabványok és előírások tartalmazzák a lehetséges módszereket, eljárásokat;
- a kockázatelemzések alapján megelőző intézkedések kialakítására van lehetőség, ciklikusság biztosítja a védelmi intézkedések hatékonyságának szinten tartását, fizikai védelmi tervek tartalmazzák a részleteket és kapcsolódó pontokat;
- a mechanikai védelmi eszközök arányosak a feltárt kockázatokkal és veszélyekkel, nem terheli túl a védett létesítmény üzemelését, de hatékonyan eléri célját;
- az elektronikai védelem teljes körűen kiegészíti a fizikai védelem szintjeit, hatékonyan támogatja a prioritásban kiemelt elemeket;
- az élőerős védelem az előző pontokban felsorolt elemekkel együtt hatékonyan képes ellátni feladatait, felkészítések és gyakorlatok révén hatékonyan képes kezelni a speciális helyzeteket és rendkívüli eseményeket;
- minimális az olyan fennmaradó kockázat, melynek bekövetkezése esetén a fizikai védelmi rendszer hatékonysága csökkenhet.

3.1.6. Relatív védelem¹⁷⁹

Az átfogó védelem mellett fontos beszélnünk a relatív védelem fogalmáról, amely szerint a biztonsági megoldásokat nem abszolút, hanem az adott körülményekhez igazított módon kell kialakítani. Ez azt jelenti, hogy a létesítmény védelmi szintjét az elérhető anyagi erőforrások, a környezeti adottságok, valamint a fizikai és technológiai lehetőségek figyelembevételével határozzák meg. A cél minden esetben az, hogy a kialakított védelem legalább a minimálisan elvárt biztonsági követelményeket teljesítse, miközben optimálisan használja fel a rendelkezésre álló erőforrásokat.

A gyakorlatban ez gyakran kompromisszumos megoldásokat jelent. Ideális esetben például egy szerverterem föld alatti, megerősített létesítményben kerülne elhelyezésre, amely természetes és mesterséges védelmet egyaránt biztosít a külső hatásokkal szemben. Azonban sok esetben a helyhiány, a magas beruházási költségek vagy a meglévő infrastruktúra korlátai ezt nem teszik lehetővé. Ilyen helyzetekben a tervezés során alternatív megoldásokat kell keresni, például

¹⁷⁹ Kovács F. (2025): Állami és katonai védett létesítmények létrehozása és fenntartása. NKE Katonai Műszaki Doktori Iskola, előadás, Budapest.

belső, védettebb épületrészek kijelölésével, megerősített szerkezeti elemek alkalmazásával, illetve korszerű biztonságtechnikai rendszerek beépítésével.

A relatív védelem tehát egy optimalizációs folyamat eredménye, amelyben a kockázatelemzés kulcsszerepet játszik. Ennek során azonosítják a potenciális fenyegetéseket, értékelik azok valószínűségét és hatását, majd ennek alapján határozzák meg a szükséges védelmi intézkedéseket.

A relatív védelemre való törekvés előnye, hogy rugalmasan alkalmazkodik a változó körülményekhez, és lehetővé teszi a költséghatékony, ugyanakkor megfelelő szintű biztonság megvalósítását.

3.2. LÉTESÍTMÉNY FIZIKAI VÉDELME NEK TERVE

A Kszetv.vr. alapján részletezett EKT-hez hasonlóan, a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 219/2011. (X. 20.) Korm. rendelet tartalmazza a meghatározott küszöbértéket meghaladó veszélyes anyagokkal foglalkozó üzemek kötelezően elkészítendő belső és külső védelmi terveinek tartalmi és formai követelményeit.

Egy küszöbértéket meghaladó veszélyes anyagokkal foglalkozó üzem jó eséllyel kritikus vagy jelentős szervezetként is kijelölhető, ebben az esetben mind a katasztrófavédelmi, mind a kritikus és jelentős szervezetek védelmére vonatkozó jogszabályokat kötelesek betartani. A jogalkotók munkáját dicséri, hogy az azonosítástól a védelmi tervezésig és védelmi infrastruktúra kialakításáig tartó folyamat pontos végrehatása, mindkét oldal szabályzóit kielégíti. A Kszetv. alapján bekérhető adatközlő lap, illetve az EKT, hozzáértő szakember kezében a 219/2011. (X. 20.) Korm. rendelet által előírt biztonsági jelentés alapján könnyen elkészíthető. A részletes biztonsági és kockázatelemzés mindkét oldal szabályzóinak érdekeit szolgálja. A 219/2011. (X. 20.) Korm. rendeletben előírt külső és belső védelmi terv, valamint az EKT egységesen elkészíthető úgy, hogy tartalmukban egymásra hivatkozva tökéletesen kiegészítsék egymást és a védelem maximális hatékonyságát szolgálják.

A 219/2011. (X. 20.) Korm. rendelet nem hivatkozik az EKT-re és a Kszetv. sem hivatkozik a külső és belső védelmi tervekre, de mindkét jogszabály előírja az egyéb védelmi terveknek való megfelelést is. Ebből kifolyólag nincs alá-fölé rendeltségi viszony az említett tervek között, de lehetőség van alárendelt, részletező tervek készítésére és ezekre való közös hivatkozásra. Ebből

kifolyólag, a továbbiakban a külső és belső védelmi tervek részletes tartalmával az értekezésben nem foglalkozom.

A 2.3. alfejezetben az EKT-re mint egy több okmányból és adatcsoportokból álló dokumentum csomagra hivatkoztam, mely arra is lehetőséget ad, hogy az említett külső és belső védelmi terveket, illetve az ezekhez kapcsolódó egyéb terveket is integrálhassák a teljes dokumentációba.

Ebbe a teljes védelmi dokumentációba tartozik a fizikai védelmi terv is.

3.2.1. Fizikai Védelmi Terv kialakítása, felépítése

Az EKT-hez kapcsolódó részletező védelmi terveknek sem a típusára, sem formai és tartalmi követelményeire nem ad meghatározást a Kszetv., illetve a Kszetv.vr. Az EKT és EKM alapján jól elkészített kockázatelemzés és a kockázatokra adott megfelelő válaszok és intézkedések megfelelő fizikai védelmet kell, hogy adjanak a létesítmény számára, viszont a tervezhetőség, átláthatóság, illetve a később szükséges módosítás és hatékony fejlesztés érdekében érdemes a fizikai védelemmel kapcsolatos elemeket külön *Fizikai Védelmi Tervbe* kiemelni.

Az atomenergia alkalmazása körében, a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló 190/2011. (IX. 19.) Korm. rendelet ad rövid leírást a *Fizikai védelmi terv* tartalmi követelményeire, de ez a kormányrendelet kifejezetten a nukleáris létesítmények, nukleáris hulladéktárolók, nukleáris anyag és radioaktív sugárforrás tárolására kialakított helyszínek fizikai védelmével foglalkozik. A kritikus és jelentős szervezetekre, infrastruktúrákra vonatkozó jogszabályok szerinti átdolgozással és a katonai objektumok fizikai védelmére vonatkozó szakmai kiegészítésekkel, alkalmas lehet egyéb területek fizikai védelmi tervének kidolgozására is.

Fentiek alapján a kritikus vagy jelentős szervezetekké, infrastruktúrává kijelölt létesítmények Fizikai védelmi tervének (a továbbiakban: FVT) formai és tartalmi követelményeire az alábbi javaslatot adom.¹⁸⁰

3.2.1.1. FVT első fejezet: Általános bemutatás

¹⁸⁰ Az FVT kritikus szervezetekre és infrastruktúrákra vonatkozó hivatkozásait a jelentős szervezetek és infrastruktúrák FVT kidolgozásánál is alkalmazni lehet.

A FVT-hez kapcsolódó általános adatokat tartalmazza. Elsődleges a FVT céljának deklarációja, illetve az EKT-re való hivatkozás, hiszen az abban lévő alapadatokra kell, hogy épüljön a fizikai védelem rendszere, tehát a FVT is. Szükséges meghatározni a kritikus szervezet, infrastruktúra ellenállóképességi szintjének megfelelő, fizikai védelmére vonatkozó alapkövetelményeket, hiszen ezek szervezetenként, infrastruktúránként eltérhetnek.

Figyelemmel kell lenni arra, hogy a kidolgozandó FVT önállóan alkalmazható legyen-e, vagy kizárólag az EKT-ben meghatározottakkal együtt. Önálló FVT kidolgozására abban az esetben lehet szükség, ha a fizikai védelemi tevékenység ki van szervezve egy olyan külső szolgáltató felé, akinek nincs jogosultsága az EKT teljes tartalmának megismeréséhez. Amennyiben a FVT az EKT-vel együtt alkalmazandó, – ezt ki kell emelni a FVT első fejezetében – abban az esetben nem szükséges újra megadni minden általános adatot, csak azokat, melyek a fizikai védelemmel kapcsolatban felmerülhetnek.

Itt szükséges megjeleníteni a különböző adminisztratív információkat: fizikai védelemért felelős szervezeti egység vagy szerződött szolgáltató neve, székhelye, címe, elérhetőségei, nyilvántartási adatai; felelős személy, kapcsolattartó személyek neve, beosztása, elérhetősége.

Fontos tisztázni a felelős cég és személyek egymáshoz, a rendszerelem üzemeltetőjéhez, illetve a biztonsági összekötő személyhez való rendeltségi viszonyukat, ezzel együtt a fizikai védelemért felelős szervezetek, személyek függőségi viszonyait.

Amennyiben szükséges, ebben a fejezetben lehet bemutatni annak a szervezetnek a működését, mely a fizikai védelmet igényli. Ez megegyezhet az EKT-ben megjelölt szervezettel is, ebben az esetben elegendő a hivatkozás. Ha az EKT nem teljes egészében hozzáférhető a fizikai védelemért felelős szerződött szolgáltató számára, akkor a szükséges mértékig lehet részletezni a védendő létesítményhez kapcsolódó szervezet tevékenységét, szervezeti struktúráját, irányítási rendszerét, illetve a létesítményben zajló tevékenységek és folyamatok általános leírását.

Fizikai védelem tervezésénél fontos információ a védendő létesítmény teljes személyzetének leírása, létszámokkal, illetve a munkaköri státuszokkal, ezen belül a kritikus munkakörökben dolgozók száma és fizikai elhelyezkedésük részletei.

3.2.1.2. FVT második fejezet: Létesítmény zónái, helyszínrajza, építmények elhelyezkedése

Az EKT 2. fejezete tartalmazza a kritikus szervezet és infrastruktúra környezetének bemutatását. A FVT 2. fejezete ennél részletesebben kell, hogy bemutassa a védendő létesítmény közvetlen környezetét és belső struktúráját.

A 3.1.2. alfejezetben részletezett három zóna szükség szerint, a mélységben tagolt védelem elvét követve tovább bontható. A külső (első) védelmi zóna tovább bontható felügyelt és ellenőrzött zónákra, vagyis olyan területekre, ahol bárki mozoghat korlátozás nélkül, de elektronikai eszközökkel (pl.: kamerák) folyamatos felügyelet alatt áll a forgalom, míg az ellenőrzött zónákban a mozgást már korlátozhatják (pl. közlekedési táblákkal vagy más fizikai akadályokkal). A második biztonsági zóna, a létesítmény területe is tovább bontható őrzött, fokozottan őrzött és szigorúan őrzött zónákra, melyek egymás határain belül helyezkednek el így biztosítják a harmadik, belső zóna erős védelmét. Ezeket a zónákat helyszínrajzon kell jelölni, jól kiemelve a zónák pontos határát, számát, megnevezését.

Részletes, méretarányos térképekkel, leírásokkal szükséges bemutatni a létesítmény megközelítésére alkalmas utakat, útvonalakat, területeket. Fel kell tüntetni a közvetlen környezetben található építményeket, vasutakat, vízfelületeket, illetve azok adatait.

Ugyancsak részletes, méretarányos térképekkel, leírásokkal kell bemutatni a létesítmény belső felépítését is, jelölve az épületeket, mozgási pályákat, utakat, illetve minden olyan tényezőt, amely befolyásolhatja a fizikai védelmet és a mozgást. Ezeket a külső és létesítményen belüli elemeket koordinátákkal is meg kell adni.

A kiemelt, fontosabb építményeket külön is részletezni kell. Meg kell adni az építmény funkcióját, a funkcióhoz köthető tevékenységeket, melyek leírását részletes helyszínrajzzal kiegészítve kell bemutatni.

3.2.1.3. FVT harmadik fejezet: Fizikai védelem szervezeti felépítése, dokumentációs rendszere

A fizikai védelemért felelős szervezeti egység vagy szerződött szolgáltató neve, székhelye, címe, elérhetőségei, nyilvántartási adatai, illetve a felelős személy, kapcsolattartó személyek neve, beosztása, elérhetősége megjelenik a FVT első fejezetében is, így ha szükséges elegendő hivatkozni erre a részre.

Az FVT ezen fejezete már részletesen tartalmazza a fizikai védelemért felelős szervezet/szervezetek részletes felépítését, működési rendjüket, személyzetük leírását. Ilyenek

lehetnek a fizikai biztonsági összekötők (ha több szükséges), biztonsági vezetők, alcsoport vezetők, illetve a biztonsági őrség, fegyveres biztonsági őrség, belső elhárító erők alcsoportjai, azok vezetői.

Ebben a fejezetben kell részletezni a kritikus szervezet fizikai védelméért felelős személyek, alcsoportok jogosultságait, köteleit, tevékenységi körüket, velük szemben támasztott követelményeket, megkülönböztetve normál, speciális és vészhelyzeti időszakokat. Pontosan meg kell határozni az alá- és fölérendeltségi viszonyokat, a helyettesítés szabályait, a belső kommunikáció formáját és hálózatát.

A működéshez szükséges okmányok, formanyomtatványok (pl.: szabályzatok, jelentések, igazolványok, nyilvántartások, naplók) rendszere is ebben a fejezetben kaphat helyet. A minták a mellékletekben is helyet kaphatnak, de a vezetésük rendje, kezelésük leírása ebben a fejezetben történik. Az alcsoportok szabályzatait (őrutasítás, fegyveres biztonsági őrség szabályzata, belső elhárító erők utasítása, stb.) minden esetben a jogszabályoknak megfelelően kell elkészíteni, az FVT ezen fejezetében viszont meg lehet adni ezen szabályzatok elkészítésének helyi viszonyokra vonatkozó különös szabályait.

3.2.1.4. FVT negyedik fejezet: Az alkalmazott fizikai védelmi rendszer

Ebben a fejezetben történik az alkalmazott elektronikai és mechanikai védelmi rendszer részletes leírása. Mivel a teljes védelmi rendszernek és részelemeinek külön műszaki leírása, terve kell hogy legyen, ezért ezekre ebben a fejezetben mindenképpen hivatkozni kell.

A műszaki leírások, tervek tartalmazzák a rendszerek és alrendszerek működtetésének, alkalmazásának feltételeit, az üzemeltetés és karbantartás szabályait, az FVT ezen fejezetének a feladata pedig ezen rendszerek, alrendszerek működésének összehangolása, az egységes üzemeltetés feltételeinek, feladatainak leírása. Ehhez szükséges az üzemeltetők kijelölése, az alrendszerekkel kapcsolatos jogosultságaik, feladataik leírása.

Ahhoz, hogy ezek a rendszerek, alrendszerek összehangolása hatékony lehessen, át kell emelni és részletesebben ki kell bontani az EKT által tárgyalt kockázatok és veszélyhelyzetek közül releváns elemeket. Ha szükséges, részletesen elemezni lehet a behatolási útvonalakat, külső és belső elkövetők lehetséges taktikáit, illetve kiemelten a tárgyalt biztonsági rendszerek, rendszerelemek egymástól való függőségét, vagyis a rendszer belső interdependenciáját.

Itt is meg kell különböztetnünk normál, speciális és vészhelyzeti időszakokat, illetve ezeken kívül szabályozni kell a karbantartás időszakának speciális feladatait is, ehhez kapcsolódva meg kell határozni az említett időszakok minimálisan teljesítendő védelmi követelményeit.

3.2.1.5. FVT ötödik fejezet: Be- és kiléptetés rendje

A személyek és járművek be- és kiléptetésének rendje egy komplex, a kialakított fizikai védelmi rendszer egyéb elemeivel szoros összhangban lévő szabályozott eljárásrendszer. Célja, hogy a személyazonosság és a jogosultság figyelembevételével a kritikus szervezeten belüli és környezetében történő mozgásokat folyamatosan ellenőrzés alatt lehessen tartani, elkülönítve a zónákat, helyiségeket, járműveket, személyeket, alkalmazottakat, vendégeket.

A be- és kiléptetés eljárásrendszere összességében egy olyan adminisztratív eleme a fizikai védelemnek, mely alkalmas a kritikus szervezet és infrastruktúra létesítményeiben tartózkodók azonosítására, mozgásának lekövetésére és ezen adatok folyamatos, visszakereshető naplózására is. Mindezekből következik, hogy a be- és kiléptetés rendszerét úgy kell kialakítani, hogy megfeleljen a személyes adatok kezeléséről szóló jogszabályoknak.

Az FVT 4. fejezetében a be- és kiléptetés elektronikai és mechanikai biztonságtechnikai eszközeinek leírása külön alfejezetbe kerülhet, így megkönnyítve az FVT 4. és 5. fejezetek összehangolását, illetve az ezen a területen dolgozó alkalmazottak képzését, szinten tartását.

A be- és kiléptetés rendjének szabályozása szorosan kapcsolódik az élőerős őrzés-védelem szabályaihoz, de kiegészítő tervekkel is lehet pontosítani. Ilyen kapcsolódó terv lehet – szükség szerint például – a kíséresi terv, ideiglenes biztosítási terv, együttműködési terv, riadóterv, stb.

Az élőerős őrzés-védelem központja a fizikai védelem rendszerének vezérlésére, ellenőrzésére szolgál, ennek megfelelően a be- és kiléptetés vezérlőjét is itt kell elhelyezni, belső, fokozottan őrzött zónában és a megfelelő védelmi intézkedések mellett kell üzemeltetni. Ennek részletei az FVT minden fejezetében megjelennek, de az őrutasításban összefoglalhatók.

3.2.1.6. FVT hatodik fejezet: Együttműködés rendje

A fizikai védelem hatékony működésének, illetve rendkívüli események esetén a gyors és összehangolt fellépés biztosításának egyik legfontosabb pillére, a kritikus szervezet különböző elemeinek együttműködési képessége egymással, illetve a külső szervekkel.

A Kszetv. és Kszetv.vr. alapján meg kell különböztetni a kontrollált rendkívüli esemény és a rendkívüli esemény küszöbértékéhez igazodó bejelentések és a szervezeti belső jelentések küldésének és fogadásának rendjét, valamint a különböző szintű elemek gyors tájékoztatásának rendjét. A kritikus szervezet minden szervezeti egységének meg kell határozni, hogy mely esetekben, kinek, milyen tartalommal köteles jelentést adni, illetve a fogadó félnek ezeket a jelentéseket hogyan kell kezelni. Ezen belül az FVT 6. fejezete kifejezetten a fizikai védelemmel kapcsolatos bejelentésekre, jelentésekre, tájékoztatásokra fókuszál. Ide tartoznak a kommunikációs csatornák, a kapcsolattartó személyek, a riasztási és értesítési lánc, az adatvédelem leírásai, meghatározásai.

Az együttműködés rendjének kialakításánál ezen jelentésekre, bejelentésekre való tevékenységeket kell meghatározni és összehangolni mind a belső szervezeti elemek, mind a Kszetv. előírásainak megfelelő hatóságok, illetve a külső együttműködők, erők vonatkozásában.

A belső szervezeti elemek, belső elhárító erők, valamint az élőerős őrzés-védelem közös feladataira eljárási rendeket kell kidolgozni, illetve meg kell határozni az ebben résztvevők képzésének és gyakoroltatásának rendjét is.

A külső együttműködők és külső elhárító erők (rendőrség, katasztrófavédelem, egyéb hatóságok) értesítésének rendjét, illetve a végrehajtandó feladatokat is ebben a fejezetben lehet részletesen meghatározni, figyelembe véve a Kszetv. előírásait.

3.2.1.7. FVT hetedik fejezet: Képzés és gyakorlatok rendje

A képzések, gyakorlatok fontosságára, rendszeres végrehajtásának hatékonyságnövelő hatására a korábbi fejezetekben is felhívtam a figyelmet. A fizikai védelemi rendszer hatékony működtetése sem képzelhető el a részleteket ismerő és alkalmazni tudó személyzet nélkül.

Az EKT nem tartalmaz részletes leírást a kritikus szervezetek ellenállóképességének fenntartása és fokozása érdekében végrehajtandó belső képzésekről, ezért a különböző területek képzéseinek leírását, követelményeit a belső képzésekre vonatkozó tervekbe szükséges kifejteni. (L.: 4. fejezet) A fizikai védelmi rendszerrel kapcsolatos képzéseket – az egyéb területekéhez hasonlóan – több szintre és eltérő tartalomra kell bontani, attól függően, hogy mely munkakörökben dolgozó alkalmazottak részére készül.

A képzések és gyakorlatok rendjét egymásra épülő, ciklikus rendszerben kell kialakítani. Bizonyos szintű, fizikai védelemre vonatkozó képzést a kritikus szervezet és infrastruktúra létesítményeinek területére állandó belépési engedéllyel rendelkező minden személy kell, hogy kapjon, beosztástól, feladatkörétől függetlenül.

A fizikai védelmi rendszerben foglalkoztatottak részére többszintű, ciklikus elméleti és gyakorlati képzéseket kell kialakítani, melyek egymásra épülnek és részei a Kszetv.vr. által előírt ellenálló képességi és komplex gyakorlatokat is magában foglaló képzési rendszernek.

A képzések és gyakorlatok rendjét úgy kell kialakítani, hogy a Kszetv.vr. által előírt ellenálló képességi és komplex gyakorlat végrehajtásának időszakára a kritikus szervezet minden tagja képes legyen a kontrollált rendkívüli esemény és a rendkívüli esemény bekövetkezésekor előírt feladatai végrehajtására.

3.2.1.8. FVT nyolcadik fejezet: Felülvizsgálat és ellenőrzés rendje

A Kszetv. és a Kszetv.vr. rendelkezik a kritikus szervezetek ellenálló képességének tervszerű, komplex, hatósági auditálásáról, melynek célja a jogszabályoknak és előírásoknak való megfelelés, az ellenálló képesség fenntartásával és fejlesztésével kapcsolatos intézkedések teljesülésének ellenőrzése, illetve az ellátási lánc és a beszállítói együttműködés megfelelőségének vizsgálata.

A fizikai védelmi rendszer belső felülvizsgálatának és ellenőrzésének rendjét úgy kell kialakítani, hogy kiterjedjen a technológiai, a humán és az alkalmazott eljárások, módszerek területére is.

Ezen felülvizsgálatok és ellenőrzések lehetnek:

- időben ciklikusak (éves, negyedéves vagy technológiai időszakhoz kötött) vagy egyediek;
- eltérő szintűek (a rendszer elemeire, részeire vonatkozó, vagy teljes);
- területre vonatkozó (technológiai, humán, módszertani) vagy komplex vizsgálatok.

Fontos és az FVT ezen fejezetében meghatározható az ellenőrzésekből eredő tapasztalatok feldolgozásának és a technológiai, humán, módszertani területekre való visszaforgatásának módja, melynek módszertana ugyancsak meghatározható az FVT-ben.

A felülvizsgálatok és ellenőrzések végrehajtása minden esetben segítő szándékú, a tapasztalatok minél nagyobb számú kinyerésének eszköze kell, hogy legyen.

3.2.2. Kapcsolódó védelmi tervek

A kritikus szervezetek és infrastruktúrák ellenálló képességének fenntartása – a normál időszakon kívül a speciális időszakokban és rendkívüli esemény esetén is – csak rendszerszintű, összehangolt működtetéssel valósítható meg, szoros együttműködésben az interdependenciában érintett egyéb szervezetekkel, infrastruktúrákkal.

Ehhez az összetett, integrált rendszerhez többszintű, egymással összefüggő tervek és dokumentáció szükséges, melyek kezelését, felülvizsgálatát, fejlesztését a jól kialakított dokumentáció hierarchia biztosíthatja. (L.: 4. fejezet)

3.2.2.1. Taktikai szintű védelmi tervek

A kritikus szervezetek védelmének alapvető védelmi terve az EKT. Egy szervezet fő védelmi tervének szükségességét, illetve annak tartalmi és formai követelményeit az adott szervezet tevékenységéhez kapcsolódó jogszabályok határozzák meg. A teljesség igénye nélkül, akár a légiközlekedés védelme, az élővizek védelme, az árterületek védelme, a veszélyes anyagokkal foglalkozó üzemek védelme (stb.) érdekében létrehozott hatályos jogszabályok mindegyike előírja a veszélyeztetettség elemzés és védelmi terv elkészítését.

Pár sorban érdemes külön említeni a veszélyes anyagokkal foglalkozó üzemek védelmi terveit, mivel a felső küszöbértékű veszélyes anyagokkal foglalkozó üzemek kritikus szervezetté is kijelölhetők. A veszélyes anyagokkal foglalkozó üzemek védelmi terveiről a katasztrófavédelemről szóló 2011. évi CXXXVIII. törvény határoz, tartalmukról pedig a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 219/2011. (X. 20.) Korm. rendelet. A szabályzók alapján a veszélyes anyagokkal foglalkozó üzemek üzemeltetői belső és külső védelmi tervet kötelesek készíteni, melyet biztonsági elemzés és jelentés előz meg.

A *belső védelmi terv* a súlyos balesetek megelőzésével és az ellenük való védekezéssel kapcsolatos feladatok végrehajtására készül, részletezve a személyi és technikai feltételeket, a használandó erőket, módszereket. E feltételeket, erőket, illetve a kapcsolódó infrastruktúrát az üzemeltető felelőssége megteremteni, kialakítani, finanszírozni. A 219/2011. (X. 20.) Korm. rendelet részletesen megadja a belső védelmi terv tartalmi követelményeit, melyek több átfedést

is tartalmazhatnak egyéb jogszabályokban előírt védelmi tervekkel, így a kritikus szervezetek részére előírt EKT-vel is.

A *külső védelmi terv* a veszélyes anyagokkal foglalkozó üzemek környezetének védelmére készül. Ennek érdekében, a külső védelmi terv alapját képező biztonsági jelentést – a védendő adatok kivételével – minden, a veszélyeztetettségi környezetben lévő település polgármesteri hivatalának meg kell küldeni, melyet közzététellel, közmeghallgatással együtt véleményeznek. Az üzemeltető által elkészített külső védelmi terv elkészítésében a mentőszolgálat, a rendőrség, az illetékes környezetvédelmi, természetvédelmi, valamint népegészségügyi hatáskörében eljáró fővárosi és vármegyei kormányhivatalok, valamint vízügyi hatóság is részt vesz. A biztonsági elemzés és a külső védelmi terv elfogadása után már az érintett települések településrendezési elveit is komolyan érinti. A veszélyességi övezet határainak megközelíthetősége, környezetének beépíthetősége, fejleszthetősége a továbbiakban szigorúbb engedélyhez kötött.

Ahogy az előző fejezetekből is jól látható, minden kritikus szervezet működését és védelmét több jogszabály szerint kell összehangolni. A felső szintű védelmi tervek pontos összehangolásával és a kiegészítő tervek pontos, részletekre kiterjedő elkészítésével nem csak a jogszabályokban előírt kötelezettségeknek lehet megfelelni, de az ellenálló képesség és a védelem is hatékonyan fokozható.

3.2.2.2. Kiegészítő védelmi tervek

A hatékony védelemhez szükséges kockázatelemzés, valamint a felső szintű tervek a legfontosabb meghatározó elemei a kritikus szervezetek és infrastruktúrák működése, üzemfolytonossága és hatékony védelme kialakításának. A 2. fejezetben tárgyalt EKT és kapcsolódó mellékletei közé besorolt FVT, illetve az FVT mellé- és alárendeltségébe besorolt tervek a már említett dokumentum hierarchia szerint alkotnak egy rendszert. Ebben az alfejezetben kifejezetten az FVT-vel kapcsolatban álló egyéb tervekre adok pár példát.

A kiegészítő védelmi tervek már erősen szervezet specifikusak kell, hogy legyenek, az azokban leírt módszerek, tevékenységek, eljárások kifejezetten az adott szervezetre, illetve annak részegységeire szabva. Jellegüket tekintve lehetnek operatív vagy technikai tervek.

Az operatív tervek módszereket, protokollokat leíró tervek, melyek szorosan kapcsolódnak a szervezet működési rendjéhez, kifejezetten a helyi sajátosságokra épülnek, mint például:

- katasztrófa utáni helyreállítási terv (Disaster Recovery Plan (DRP));
- veszélyhelyzeti reagálási terv;
- őrutasítás;
- kommunikációs terv;
- evakuációs terv;
- belső felkészítési terv;
- képzési programok;
- ellenőrzési terv;
- stb.

A technikai tervek főleg végrehajtói és műszaki jellegű dokumentumok, melyek egy adott feladat végrehajtására, részegység, eszköz, szoftver működésére, védelmére vonatkoznak. Ilyen lehet például:

- biztonsági eszközök alkalmazási terve;
- energiaellátási terv;
- statikai ellenőrzési terv;
- képzés levezetési terv;
- stb.

3.3. RÉSZKÖVETKEZTETÉSEK

A fejezetben felhívom a figyelmet arra a tényre, hogy egy kritikus szervezet létesítményei, kritikus infrastruktúra a kijelölése pillanatában már kialakított belső terekkel, nagyrészt fix, tőle független környezettel rendelkezik. Egy normál napi működésű szervezet, infrastruktúra akár sűrűn beépített területen, lakóövezetben, nagy forgalmú környezetben is lehet (pl. közlekedési, logisztikai infrastruktúra), így kritikussá történő kijelölése esetén a megközelíthetőség, illetve a fizikai védelem szigorítása komolyabb nehézségekbe ütközik, a zónák kialakítása komoly költségeket jelenthet, de belső fizikai védelmi adottságaik javíthatók.

Ezen nehézségek, költségek minimalizálása és a hatékony védelem fenntartása érdekében a fizikai védelem minden aspektusára ki kell térni. A kritikus szervezetek és infrastruktúrák tekintetében a jogszabályok nem írnak elő nagy részletességgel védelmi módokat, az üzemeltető felelőssége, hogy a képességeikhez mérten leghatékonyabb fizikai védelmet kialakítsa. A 3. fejezetben *részletesen megadom a területek zónákra való osztásának lehetőségeit*, illetve a zónákon belüli védelmi lehetőségeket, eszközöket, módszereket.

A kritikus infrastruktúra fogalmának rekurzív alkalmazásával megalkottam a *kritikus szervezetek kritikus elemeinek* fogalmát. Mivel egy adott szervezet, infrastruktúra kritikusságának előzetes elemzését és veszélyeztetettségének vizsgálatát a jogszabályok az üzemeltetők kezébe adja, elengedhetetlen az üzemeltetők rekurzív gondolkodásának kialakítása. Tehát nem elegendő megállapítani egy adott szervezet vagy infrastruktúra kritikusságát és azt az ágazati és horizontális kritériumokra bizonyítani, hanem szükséges vizsgálni a részegységeit, azok tagjait és a tagok elemeinek hatását is a teljes rendszer működőképességére és az üzemfolytonosságra. A *kritikus elemek* vizsgálatával pontosítható a helyük, szerepük a rendszerben, könnyebben meghatározható a szükséges védelem szintje és módja. A *kritikus elem* fogalmának alkalmazhatósága érdekében a jogszabályok módosítása szükséges (L.: 1.3. alfejezet).

A megközelíthetőség és a fizikai védelem aspektusait alapul véve, elemezve a különböző jogi szabályzókat, *javaslatot tettem a kritikus szervezetek fizikai védelmi tervének felépítésére és kidolgoztam az elemeit*, mely korábban szakirodalomban még nem jelent meg.

Megvizsgáltam több, konkrét kijelölt kritikus szervezet és infrastruktúra biztonsági és védelmi rendszerét¹⁸¹, összevettem a jelenleg hatályos releváns jogszabályokkal, melyek alapján meghatároztam az FVT fejezeteinek jegyzékét úgy, hogy a fizikai védelem minden aspektusát érintse és könnyen integrálható legyen az egyéb üzemeltetéshez, védelemhez kapcsolódó tervekhez.

Az FVT tartalmi elemeinek részletes magyarázata olyan segítséget adhat az üzemeltetők kezébe, mely hatékony fizikai védelem kiépítését teszi lehetővé a szükséges erőforrások minimalizálásával.

¹⁸¹ Hozzáférést kaptam honvédelmi jelentős szervezet, nemzeti és európai pénzügyi kritikus szervezet, nemzeti biztonsági kritikus szervezet kijelölési és üzemeltetési dokumentumaihoz. A pontos megnevezésük, elhelyezkedésük nem nyilvános.

4. FEJEZET

KRITIKUS SZERVEZETEK ÉS INFRASTRUKTÚRÁK REZILIENCIÁJÁNAK FEJLESZTÉSI LEHETŐSÉGEI

A létesítményeik fizikai védelme kiemelt fontosságú a kritikus szervezetek és infrastruktúrák ellenálló képessége és az üzemfolytonosság szempontjából. Az előző fejezetekből láthattuk, hogy a fizikai védelem az átfogó védelem fontos része, több területből áll, melyek szoros kapcsolatban állnak nem csak egymással, de az átfogó védelem és üzemeltetés egyéb területeivel is.

A fizikai védelem módszerei, eszközei, technikai berendezései folyamatos fejlesztést igényelnek, figyelemmel a biztonsági környezet változásaira, a modern technológiák folyamatos, gyors fejlődésére. A módszerek és eszközök egyre hatékonyabbak, a műszaki megoldások egyre megbízhatóbbak, mégis még napjainkban is az *emberi tényező a rendszer leggyengébb láncszeme*. A biztonsági erők, az üzemeltetők, a létesítmény vagy infrastruktúra napi használói döntéseikkel és viselkedésükkel alapvetően befolyásolják a védelmi intézkedések eredményességét. A figyelmetlenség, a rutinból fakadó hibák, a szándékos vagy véletlen károkozás súlyos biztonsági incidenseket okozhat.

A védelem eszközeinek fejlesztésével, az alkalmazott technológiák modernizálásával minimalizálható az emberi tényező a rendszeren belül, de teljesen nem zárható ki. Fontos megjegyeznünk azt is, hogy egy rendszer minél modernebb, minél kevésbé függ az emberi tényezőtől, annál bonyolultabb és emellett magasabb beüzemelési, üzemben tartási és karbantartási költségekkel jár, illetve speciális képzettséget és személyi állományt igényel.

Tehát meg kell találni az adott kritikus szervezet vagy infrastruktúra fizikai védelméhez leginkább megfelelő eszközöket, technológiákat és ki kell alakítani az üzemeltetésükhöz alkalmas, célirányosan képzett humán erőforrást.

Ebben a fejezetben arra keresek választ, hogy hogyan lehet a fizikai védelem hatékonyságát növelni – adott eszközrendszer és technológia mellett – a rendszerszintű gondolkodás, tudatosság és belső képzések kialakításával.

A kritikus szervezetekre és infrastruktúrákra vonatkozó megállapításaim az ország védelme és biztonsága szempontjából jelentős szervezetek és infrastruktúrák esetében is relevánsak.

4.1. KRITIKUS SZERVEZETEK DOKUMENTÁCIÓ HIERARCHIÁJA

A különböző szintű tervek, dokumentumok logikus rendben egymáshoz kapcsolt rendszere elősegíti a hatékony és szabályszerű működést, a fejlesztések rendszerhez való pontos igazítását, az ellenőrzések hatékonyságát, a fejlesztési, bekerülési és üzemeltetési költségek tervezését, lehetőség szerinti minimalizálását. Ennek eléréséhez egy adott kritikus szervezetnek saját dokumentáció hierarchiával kell rendelkezni, a tevékenységére és saját tulajdonságaira szabott felső szintű tervekkel és azokra épülő saját szabályzókkal, utasításokkal.

4.1.1. Kritikus szervezetek dokumentáció hierarchiájának kialakítása

Egy szervezet működésének és üzemeltetésének alapfeltétele a célokkal, valamint a tevékenységi körhöz kapcsolódó jogszabályi és szakmai követelményekkel összhangban álló dokumentációs rendszer megléte,¹⁸² melyben a kritikus szervezetté történő kijelölést követően a reziliencia, vagyis az üzemfolytonosság fenntartása és a védelmi szint megfelelő biztosítása kerül a középpontba.

Ennek érdekében a meglévő szabályozási és működési alapokat felül kell vizsgálni abból a szempontból, hogy azok milyen mértékben képesek támogatni a szervezet működését normál és rendkívüli, illetve megváltozott körülmények között is. A jól kialakított dokumentáció hierarchia biztosítja, hogy a szervezet dokumentumai ne csupán a külső elvárásoknak feleljenek meg, hanem aktívan támogassák a szervezet ellenálló képességét és védelmét, ezáltal a kritikus szervezet és infrastruktúra megbízható és fenntartható működését.

A kritikus szervezetté való kijelölés folyamata, az üzemeltetés folyamata, az ellenállóképesség fenntartása és a hatékony védelem kialakítása komoly adminisztratív tevékenységgel jár. Az így keletkezett dokumentumokat áttekintve ki kell alakítani a hierarchia rendszert, ki kell jelölni a dokumentum hierarchia szintjeit, illetve elhelyezni a meglévő dokumentumokat a rendszerben.

¹⁸² Minőségügy alapjai – IV. ISO 9001. *Miskolci Egyetem Vezetéstudományi Intézet.* (2011) (<http://www.szervez.uni-miskolc.hu/blaci/minmen/index.html>) Letöltés: 2026.02.05.



20. sz. ábra: Dokumentum hierarchia szintjei¹⁸³

Egy szervezet stratégiai szintű dokumentumai határozzák meg a szervezet felépítését, működését, céljait. Tartalmuk adja meg azt a keretet, melyen belül minden tevékenység, eszköz, módszer, jövőbeli fejlesztés és terv a szervezet létrehozásának célját szolgálja. Ilyen dokumentumok lehetnek például a szervezeti alapszabályok, alapító okiratok.

Taktikai szintre kerülnek azok a dokumentumok, melyek alapján a már elkülönített tevékenységeket meg lehet szervezni, a stratégiai elveket részletes szabályzatokká, ágazati vagy biztonsági kézikönyvekké lehet alakítani. Ahogy korábban láthattuk, ide sorolható az EKT, mely a kritikus szervezet ellenálló képességét és a hatékony védelem kialakítását hivatott összefogni. De ide sorolhatók a Szervezeti és Működési Szabályzatok, a veszélyes anyagokkal foglalkozó szervezetek külső és belső védelmi tervei is. A taktikai szintre, a meglévő dokumentumokba épülhetnek be a szervezeti belső felkészítések céljai.

Az operatív szintű dokumentumok már konkrétabb, a mindennapi működés során alkalmazandó eljárásokat, protokollokat tartalmaznak, adott témakörökre bontva, melyre példákat az EKT-t és az FVT-t tartalmazó alfejezetek hoznak. Erre a szintre sorolhatók a szervezeti célokkal összhangban elkészített belső felkészítési terv, illetve a tervben szereplő képzésekre vonatkozó képzési programok.

¹⁸³ Saját szerkesztés

A technikai szintű dokumentumok konkrét részelemek, egységek kezelésére, ideiglenesen bevezetendő szabályokra vonatkozó utasítások, eszköz specifikus műszaki leírások, konfigurációs beállítások lehetnek, illetve a felkészítések vonatkozásában ide tartozhatnak a konkrét képzések, gyakorlatok levezetési tervei, anyagi-technikai biztosítási tervei, végrehajtási utasításai.

A kialakított dokumentum hierarchia szintjei és tartalma szervezetenként eltérő lehet, a szervezet tevékenységi körétől függően, de minden esetben a hatályos jogszabályokkal, szabályzókkal összhangban kell lennie.

Az elkészített dokumentumokat a kialakított hierarchia szerint össze kell kapcsolni, ki kell alakítani a hivatkozási rendszert. Minden dokumentumnak egyértelműen utalni kell a felette álló dokumentumokra és a kapcsolódó egyéb dokumentumokra is.

Szükséges meghatározni a hozzáférés körét, a jogosultságokat. Ez nem csak annak eldöntését jelenti, hogy ki férhet hozzá a dokumentumhoz. Pontosán meg kell határozni, hogy egy adott dokumentumot, illetve annak részeit a kritikus szervezeten belüli munkavállalók és vezetők, vagy a kritikus szervezettel kapcsolatban lévő külső személyek milyen mértékig ismerhetik meg. Ezen jogosultságok meghatározásának fontos szerepe van a továbbiakban a dokumentumok felülvizsgálati, fejlesztési folyamataiban és a hatékony működés és védelem kialakításához szükséges felkészítések megszervezésében.

4.1.2. Dokumentációk felülvizsgálata, fejlesztése

A biztonsági, gazdasági, technológiai környezet, a szabályzók változása egyértelműen szükségessé teszi a kritikus szervezetek és infrastruktúrák dokumentációinak folyamatos felülvizsgálatát, fejlesztését, melyet az előző alfejezetben bemutatott dokumentáció hierarchia kialakítása nagyban elősegít.

A dokumentumok felülvizsgálata és fejlesztése lehet ciklikus, ütemezett vagy egyedi.¹⁸⁴

Ciklikus felülvizsgálatnál meg kell adni az időközöket (például egy vagy két éves ciklus), melyek alapján a felülvizsgálat tervezhető. Ütemezett felülvizsgálatról akkor beszélhetünk, ha valamely technológiai folyamat, adott protokoll, vagy egyéb tevékenységet követően írjuk elő a dokumentációk felülvizsgálatát. A dokumentációs hierarchia minden szintjén lévő összes

¹⁸⁴ Pénzügyi kritikus szervezet EKT alapján.

dokumentumra elő kell írni ciklikus vagy ütemezett felülvizsgálatot, de ezektől függetlenül előfordulhatnak olyan események – jogszabály változás, technológiai fejlesztés, protokoll változás, incidens – melyek megkövetelik a dokumentumok egyedi, haladéktalan felülvizsgálatát és ha szükséges fejlesztését is.

A felülvizsgálat hatékonyságát növeli, ha nem csupán a vezetés és a szűkebb alkalmazói kör, hanem – lehetőség szerint – a különböző szakmai területek is bevonásra kerülnek. A tapasztalatfeldolgozás ebben a feladatban kiemelt jelentőségű, hiszen a beosztott munkatársak gyakorlati tapasztalataik révén olyan hiányosságokra is rávilágíthatnak, amelyek a vezetői szinten esetleg rejtve maradnak.

Kritikus szervezet bizonyos dokumentumai esetén a felülvizsgálat lépései akár a szervezet keretein is túlmutathatnak (például az EKT), hatósági, ágazati szervekkel vagy egyéb szervezetekkel való együttműködést igényelnek, vagy témájukból aódoan többkörös (biztonsági, gazdasági, jogi, stb.) kidolgozói és véleményezési folyamaton kell, hogy átsessenek. Annak érdekében, hogy a fejlesztések, módosítások minél hamarabb a rendszer részei legyenek, ki kell jelölni a felelősöket, meg kell határozni a dokumentum felülvizsgálatán belüli mérföldköveket, határidőket, melyek már prioritizálva tartalmazzák a folyamat lépéseit.

Minden komolyabb módosítás, fejlesztés több dokumentumot is érint bizonyos mértékben. Ha a dokumentumok egy jól kidolgozott hierarchikus rendszerben helyezkednek el, a pontosan vezetett hierarchia térkép és naplózott verziókövetés alapján a teljes dokumentációs rendszer naprakész marad a módosításokat követően, mely pozitív hatással van a szervezet ellenálló és védelmi képességeire is.

Dokumentáció hierarchia hatása a védelmi képességekre

A komplex rendszerek kezelhetőségének alapja a strukturált és átlátható vezetési rendszer, a vezetési rendszerek egyik legfontosabb pillére pedig az előző alfejezetekben tárgyalt hierarchikus, folyamatosan fejlesztett dokumentációs rendszer.

Egy gazdálkodó vagy infrastruktúrát üzemeltető szervezet működése akár alapjaiban is megváltozhat a kritikus szervezetté történő kijelölésekor. A védelmi képességei, ellenálló képességet biztosító módszerei, eszközei, technológiája magasabb szintre való fejlesztést igényelnek. Változnak a szervezet biztonságpolitikai alapelvei, kockázatvállalási szintjei, hosszútávú céljai és fejlesztési tervei. A jól kialakított, vizuális elemekkel megerősített

dokumentációs hierarchia átláthatóságot teremt a fejlesztendő komponensek rendszerében, könnyen észrevehetőek azok a területek, melyek alul- vagy túlszabályozottak. Ezeket az anomáliákat, hiányosságokat kiemelve, illetve a teljes rendszer elemeit áttekintve kifejezetten az üzemfolytonosságra és a védelemre koncentrálnak lehet végrehajtani a kritikus szervezetté való átállást, mellyel költségeket és időt is megtakaríthat a szervezet.

A dokumentáció hierarchia alkalmazásával minden belső szabályzó, terv és utasítás egymással összefüggésben, de saját szintjén áll rendelkezésre, így könnyen hozzáférhető módon gyorsabban megadhatók a feladatok, felelősségek, jogosultságok. Ez a tulajdonság speciális helyzetekben csökkenti a védelmi rendszer reakcióidejét, ezzel növeli hatékonyságát.

A kritikus szervezeteknek kijelölésük után a Ksze.tv. és a Kszetv.vr. előírásai szerint is kötelességük a védelmi képesség éves felülvizsgálata, illetve az erre épülő ellenállóképességi és komplex gyakorlat végrehajtása. A felülvizsgálatból és a gyakorlati tapasztalatokból eredő információk napi működésbe és a dokumentációkba való beépítése elengedhetetlen, hiszen az elavult dokumentáció a védelmi képességek gyengülését eredményezheti, mivel a gyakorlatban alkalmazott eljárások eltávolodhatnak az aktuális kockázati viszonyoktól. Tehát a frissített és fejlesztett dokumentáció növeli a rezilienciát, mivel az újként megjelenő fenyegetésekhez igazodó eljárásokat tartalmaz, mely növeli a védelem hatékonyságát, elősegíti a gyorsabb helyreállítást válsághelyzetekben.

Fontos kiemelni, hogy a hierarchikus rendszerben lévő, naprakész szabályzatok, tervek, utasítások tervezett felülvizsgálatait és fejlesztéseit nyomán az incidensekből levont tapasztalatok intézményesített formában épülnek be a működésbe, így ez a tudás nem marad az egyéni tapasztalatok szintjén.¹⁸⁵

4.2. KRITIKUS SZERVEZETEK SZEMÉLYI ÁLLOMÁNYÁNAK FELKÉSZÍTÉSE

Ahogy a fejezet bevezetőjében elhangzott, a kritikus szervezetek védelmi rendszere bármennyire fejlett is legyen, annak leggyengébb láncszeme a megkerülhetetlen emberi tényező.

Annak érdekében, hogy a figyelmetlenségből, a rutinból fakadó hibák, a szándékos vagy véltlen károkozásból eredő biztonsági incidensek elkerülhetők legyenek vagy számuk és hatásuk

¹⁸⁵ Drót L. (2022): *A Magyar Honvédség békeműveleti tapasztalat-feldolgozási rendszere és továbbfejlesztési lehetőségei*. Doktori értekezés. Budapest: NKE

minimális legyen, az egyik leghatékonyabb módszer a folyamatos, minden szintre kiterjedő felkészítés. A fegyveres szervek belső felkészítési rendszerének fő célja a veszélyhelyzetekre való felkészítést tartja középpontban, felépítése pedig több szintű és prioritizált, ezért – meglátásom szerint – a kritikus szervezetek munkavállalóinak felkészítési rendszeréhez jól alkalmazható. Természetesen a megfelelő szakmai módosításokkal. A következő alfejezetek kidolgozásánál figyelembe vettem a fegyveres szervezetek felkészítési elveit, de fő célom a kritikus szervezetek belső felkészítési rendszerére való átültetés volt.

Egy folyamatosan, megfelelően működő szervezet minden tagja – vezetők és beosztottak egyaránt – részt vesz bizonyos szintű és tartalmú szakmai felkészítésen, hiszen a szervezetbe való belépéstől kezdve szükségük van a beosztásuk ellátásához szükséges tudásra, a szervezet sajátosságaiból eredő specialitásokra, a napi feladatok ellátásához szükséges ismeretekre. Ezek az ismeretek lehetnek külső forrásból (oktatási intézményből) hozott, vagy belső képzésekből, tapasztalatokból eredő ismeretek, de lényeges, hogy a szervezeten belüli ismeretátadás olyan rendszert alkosson, mely a szervezet minden tagját eléri, rugalmasan képes reagálni a szükséges változtatásokra és képes a hatékony ismeretátadására.¹⁸⁶

Egy szervezet tagjainak, munkavállalóinak szakmai ismeretei, tapasztalatai, illetve ezen ismeretek szintje nagyban befolyásolja a szervezet működésének hatékonyságát. Kritikus szervezetté való kijelölést követően ezek a meglévő szakmai ismeretek ki kell, hogy egészüljenek a veszélyhelyzetekre és rendkívüli eseményekre vonatkozó ismeretekkel, a speciális időszakokra jellemző kommunikációs, védelmi és szakmai képességekkel.

4.2.1. Felkészítés célja, rendszere, alapelvei

Kritikus szervezetté való kijelölést követően egy meglévő, már működő felkészítési rendszerbe könnyen integrálhatók a magasabb üzemfolytonossági elvárásokra és a védelmi képességekre vonatkozó felkészítés követelményei, mely nem csupán a tudás átadását jelenti, hanem egy komplex fejlesztési folyamat kell, hogy legyen.

4.2.1.1. A felkészítések célja

¹⁸⁶ Ált/24 Magyar Honvédség Kiképzési Doktrína. (2013) Magyar Honvédség kiadványa, Budapest

Összefoglalva tehát, a korábbi fejezetekben vizsgált témaköröket figyelembe véve, a felkészítések célja:¹⁸⁷

a) szabályozóknak való megfelelés biztosítása.

A kritikus szervezet és infrastruktúra üzemeltetői, vezetői, munkavállalói ismerjék és alkalmazni is tudják a szabályzóknak leírtakat, ezzel biztosítva, hogy a szervezet megfeleljen az előírt követelményeknek és auditoknak. A jogszerű működés erősíti a külső és belső bizalom fenntartását is.

b) az emberi tényezőtől eredő kockázatok minimalizálása.

A felkészítések fejlesztik a döntéshozatali képességet, növelik a felelősségtudatot, felkészítik a szervezet tagjait a fenyegetések felismerésére és megelőzésére, akár szándékos, akár gondatlan cselekményekről, incidensekről van szó.

c) az alkalmazott ágazati és védelmi technológiák hatékony használatának fokozása.

Az alkalmazott speciális védelmi technológiák, módszerek ismerete még nem elegendő. A felkészítések révén az üzemeltetőknek készség, jártasság szinten szükséges a védelmi eszközöket, módszereket hatékonyan alkalmazni, szem előtt tartva a biztonsági szempontokat, ezzel csökkentve az incidensekre adott reakcióidőt és növelve az eredményességet.

d) a biztonságtudatosság és a szervezeti kultúra fejlesztése.

A felkészítéseknek szemléletformáló szerepe is van. A cél, hogy az üzemeltetők a napi munkavégzésük során is tudatosan kezeljék a biztonsági kérdéseket és felismerjék saját szerepüket a szervezet ellenálló képességének fenntartásában. A tudatosság fejlesztése hozzájárul egy olyan szervezeti kultúra kialakításához, melyben a védelem közös felelősség.

4.2.1.2. A felkészítések rendszere

A bevezetőben említett komplex felkészítési rendszer akkor hatékony, ha több alkotórészből épül fel, mely alkotórészek egymással összhangban, egymást támogatva képesek az ellenálló képesség fenntartásához és fejlesztéséhez szükséges tudás átadására, képességek és jártasságok kialakítására.¹⁸⁸ A megfelelő keretrendszer alkalmazva a kritikus szervezetek már saját jellegzetességeiket figyelembe véve képesek kialakítani hatékony felkészítési metodikájukat.

¹⁸⁷ Ált/24 Magyar Honvédség Kiképzési Doktrína. (2013) Magyar Honvédség kiadványa, Budapest, 2.1.3. fejezet

¹⁸⁸ Ált/24 Magyar Honvédség Kiképzési Doktrína. (2013) Magyar Honvédség kiadványa, Budapest, 2.1.2. fejezet

A felkészítési rendszer alapját a kritikus szervezet működése szempontjából releváns jogszabályok, ágazati szabályzók mellett, az a technológiai és biztonsági környezet adja, melyben az adott szervezetnek működni kell. A szabályzók adják a keretet, hiszen a szabályos működést minden helyzetben biztosítani kell, a technológiai és biztonsági környezet pedig megadja a felkészítés irányát és prioritásait, melyeknek követniük kell a változásokat.



21. sz. ábra: a felkészítés rendszere¹⁸⁹

Egy kritikus szervezet működése meghatározza, hogy milyen szakmai tudású munkavállalókra van szükség, illetve az egyes beosztásokhoz milyen mélységű és jellegű kompetenciák tartoznak, de a felkészítési rendszer hatékonysága nagymértékben függ a vezetők és a képzésért felelős szakemberek hozzáállásától is.

Minden munkakörhöz szükséges egy alap szakképesítés, amely formális oktatásban, szakképzésben szerezhető meg, majd ezt kiegészíthetik további szakmai képzések, amelyek fejlesztik a munkavállalók kompetenciáit, javítják a hatékonyságot, elősegítik a beosztások közötti átjárhatóságot és ezzel a szervezeti bizalmat és együttműködést, tehát összességében növelik a szervezet rezilienciáját. Ezek a képzések azonban idő- és költségigényesek mind a

¹⁸⁹ Saját szerkesztés

munkavállaló, mind a szervezet számára, ezért a vezetők feladata a szakképzések tudatos tervezése és prioritizálása.

A kritikus szervezeten belül, önerőből szervezett belső képzések bár nem adnak hivatalosan elismerhető szakképesítést, de a szervezet számára számos előnnyel bírnak. A kialakított belső képzés programja teljes egészében a szervezet céljaihoz, aktuális működési sajátosságaihoz szabható. A szervezeten belül bármely szakmai csoport részére testre szabható, figyelembe véve az adott körnek szükséges szakmai tudást, a munkakörnyezetet és az adott munkakörök időgazdálkodását is. Mindezek mellett költséghatékony és rugalmasan alakítható.

Az önképzés, önfejlesztés több szempontból is fontos eleme a felkészítési rendszernek. A belső képzések bármennyire is a szakmai csoportok igényeire szabottak, az egyéni célok csak önképzéssel érhetők el. Önképzéssel naprakészen tartható és elmélyíthető a személyes szakmai tudás, az egyéni karriercélok irányába fordíthatók a megszerzett ismeretek, mellyel a szakember egy adott terület specialistájává is válhat. Ezzel növelve egyéni versenyképességét és a szervezet működési stabilitását is.

Fontos kiemelni, hogy az önképzés, önfejlesztés minden esetben az egyén saját döntése, így a legfontosabb alapja a motiváció. A negatív motiváció („*Ha nem képezem magam, akkor kirúghatnak.*”) hosszútávon hátrányokkal jár a szervezet számára, ezért kizárólag pozitív motivációs eszközöket érdemes használni. A pozitív motiváció erősíthető szervezeti támogatással is. Ha a szakképesítések megszerzését – illetve általában a szakmai tudást – a közép és felsővezetők nyíltan, pozitív értéként tekintik és lehetőségekhez mérten támogatják, az pozitív hatással lesz a munkavállalók önképzési igényére is. Ez az önképzésre való igény támogatható elismerésekkel, jutalmakkal, az oktatásban vagy képzésekben résztvevők rugalmas munkaidejének kialakításával, erőforrások biztosításával. A kitűzött egyéni cél, ha szervezeti támogatással is párosul, folyamatos motivációt biztosíthat a munkavállalónak és növeli az önképzésre való igényt.

Napjainkban egy adott szakterületen megszerzett tudás olyan előnyt jelent, mely a versenytársak által nem másolható, oktatással, képzéssel, önképzéssel szinten tartható, sőt a gyűjtött tapasztalatokkal kiegészülve egyre értékesebbé válik. Ez „*a tudás ma a nyersanyagokhoz, emberi erőforrásokhoz, pénzforrásokhoz hasonlóan fontos erőforrássá vált.*”¹⁹⁰

¹⁹⁰ Bakacsi Gyula: *A szervezeti magatartás alapjai*, Alaptankönyv Bachelor hallgató számára, Budapest, Semmelweis Kiadó, 2015., 315.

Viszont ez az egyéni tudás akkor válhat igazán szervezeti tudás részévé, ha mindenki számára elérhetővé válik és elterjed, vagyis felhasználhatóvá válik a szervezet más tagjai számára is.¹⁹¹ Ennek legmegfelelőbb formája a tapasztalatok átadása, mely szervezeti szinten megfelelően koordinálva tapasztalatfeldolgozásként is működhet. Akkor mondhatjuk, hogy egy tapasztalatot feldolgoztunk, ha a felismert új tapasztalat, új tudásként lett értelmezve, tudatosan beépül a szervezeti rendszerbe és elterjedésével változást is generál¹⁹². A felismert tapasztalat szintjétől függően lehet egyéni szakmai, közbülső szintű szervezeti, vagy rendszer szintű, a teljes szervezetet érintő új tapasztalat, így ettől függően a feldolgozása is különböző szinteken kell, hogy megtörténjen. A tapasztalatfeldolgozás legfontosabb alapelve, hogy nem értékel, nem mond ítéletet, hanem segítő szándékkal feltárja a hibákat, segítve a javítás és fejlődés folyamatát.

Előzőkből jól látható, hogy a felkészítési keretrendszer elemei akkor működnek hatékonyan, ha egymással szoros kapcsolatban állnak és együtt elégítik ki a szervezet tudás igényét és adják meg képességeit, így képezik alapját a további fejlődésnek. A kritikus szervezetek esetében – hasonlóan az emelt szintű biztonsági követelményekkel rendelkező szervezetekhez – nem elegendő a kialakított szervezeti tudás szinten tartása. Mivel a biztonsági környezet folyamatosan változik, a veszélyeztető tényezők állandó fejlődést mutatnak, így a szervezet munkavállalóinak képességeit is folyamatosan fejleszteni kell, amellet, hogy a korábban megszerzett ismereteket, képességeket se veszítsék el.

Mindezekből következik, hogy a felkészítések rendszere nem lineáris, hanem olyan ciklikus mintázatokat mutató fejlődési spirál, mely tartalmazza a megszerzett tudás visszatérő ismétlését, megerősítését, az erre épülő új tudás beépítését, valamint az újonnan érkező munkavállalók gyors felzárkóztatását is.

4.2.2. Kritikus szervezetek személyi állománya felkészítésének jelenlegi helyzete

A Kszetv. valamint a kapcsolódó szabályzók előírják, hogy egy kritikus szervezet köteles ellenállóképességért felelős vezetői beosztást létesíteni, felelős vezetőt kijelölni vagy megbízni.

¹⁹¹ Drót L. (2022): *A Magyar Honvédség békeművelési tapasztalat-feldolgozási rendszere és továbbfejlesztési lehetőségei*. Doktori értekezés. Budapest: NKE

¹⁹² CSDP Missions and Operations: Lessons Learned Processes. EU Parliament Directorate-general for External Policies. EXPO-SEDE_ET (2012) 457062_EN.pdf ([https://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/457062/EXPO-SEDE_ET\(2012\)457062_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/457062/EXPO-SEDE_ET(2012)457062_EN.pdf)) Letöltés: 2025.10.18.

A törvény megadja a kritikus szervezet ellenállóképességéért felelős vezető kijelölésének vagy megbízásának szabályait, illetve összefoglalja feladatait. Jelenleg a kritikus szervezetek tekintetében a Kszetv. és a Kszetv.vr. mindössze az ellenállóképességért felelős vezető végzettségére ad meg konkrét előírásokat, a további felkészítések felelősségét a szervezet vezetőjére, illetve tanácsadóként az az ellenállóképességért felelős vezetőre bízza.

4.2.2.1. Kritikus infrastruktúra védelmi biztonsági összekötő személy szakirányú továbbképzés

A Kszetv.vr. 17. §-a írja elő, hogy a kritikus szervezetek ellenállóképességéért felelős vezetőknek kritikus infrastruktúra védelmi biztonsági összekötő személy szakirányú továbbképzési szakon szerzett képesítéssel kell rendelkeznie, mely képzés jelenleg¹⁹³ a Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Katasztrófavédelmi Intézet portfóliójában érhető el.

A képzés időtartama két félév, a bemeneti követelmény egy BSc alapképzés megléte, mely nincs szakmai területhez kötve. A képzési program szerint, a képzés célja *„olyan korszerű jogi és szakmai ismeretekkel rendelkező szakemberek képzése, akik komplex módon képesek a létfontosságú rendszerek és létesítmények védelmével kapcsolatos üzemeltetőt érintő biztonsági összekötői szakmai feladatok ellátására.”* A kompetencialeírás szerint a végzetek ismerik az iparbiztonság és a kritikus infrastruktúra védelem jogi és közigazgatási szabályozásrendszerét, tisztában vannak az alapfogalmakkal, ágazati sajátosságokkal, eljárásokkal, módszerekkel. Képesek alkalmazni a jogszabályokban leírtakat, képesek a kritikus infrastruktúrák védelméből adódó üzemeltetői szakmai feladatok tervezésére, végrehajtására, illetve az ezzel kapcsolatos kapcsolattartói tevékenység koordinálására.

A kritikus infrastruktúra védelmi biztonsági összekötő személy szakirányú továbbképzési szak a tanterv alapján mindkét félévben 100 kontakt órát tartalmaz, hét különböző tantárgy közötti elosztásban, levelező munkarendben. A tantárgyak – szakmai prioritás szerint – 8 és 26 közötti óraszámmal rendelkeznek, az elmélet/gyakorlat aránya az első félévben 78%/22%, a második félévben 66%/34%. A 13 tantárgy közül 8 kollokviummal, 4 gyakorlati jeggyel, egy félévközi értékeléssel zárul, illetve a szakdolgozat készítés is tárgyként szerepel a tanrendben. A

¹⁹³ *Kritikus infrastruktúra védelmi biztonsági összekötő személy szakirányú továbbképzési szak.* NKE Rendészettudományi Kar.

(<https://rtk.uni-nke.hu/oktatas/szakiranyu-tovabbkepzesi-szak/a-kritikus-infrastruktura-vedelmi-biztonsagi-osszekoto-szemely-szakiranyu-tovabbkepzesi-szak>) (letöltve: 2025.10.08.)

szakdolgozat leadását követően a hallgatók záróvizsgát tesznek, melynek eredményes értékelése és a tantárgyak teljesítése a feltétele az oklevél megszerzésének.

A Lrtv.vr. hatályon kívül helyezésével megszűnt az a lehetőség, hogy az ágazatnak megfelelő BSc alapképzés megléte mellett védelmi igazgatási, katasztrófavédelmi, rendészeti igazgatási, tűzvédelmi, iparbiztonsági, polgári védelmi képzettséggel, vagy 5 év iparbiztonsági, rendvédelmi gyakorlattal is be lehetett tölteni biztonsági összekötői pozíciót. Az Iparbiztonsági BSc szakirányon végzett szakemberek – a szakirány képzési programja szerint – bőven teljesítik a kritikus infrastruktúra védelmi biztonsági összekötő személy szakirányú továbbképzési szak programjában megfogalmazott kompetenciákat, a jelenleg hatályos Kszetv.vr. alapján viszont mégsem tölthetnek be ellenállóképességért felelős vezető beosztást a szakirányú továbbképzést igazoló okmány nélkül.¹⁹⁴ A Kszetv.vr. soraiból ugyancsak kimaradt az 5 év iparbiztonsági, rendvédelmi gyakorlattal rendelkezők előnye.

A szabályozó környezet változásával, szélsőséges esetben olyan ágazati BSc alapképzéssel rendelkező személy is betölthet ellenállóképességért felelős vezetői beosztást, aki mindössze az 1 éves kritikus infrastruktúra védelmi biztonsági összekötő személy szakirányú továbbképzési szakon szerzett képesítéssel rendelkezik és korábban nem szerzett iparbiztonsági vagy közigazgatási ismereteket. A kritikus infrastruktúra védelmi biztonsági összekötő személy szakirányú továbbképzési szak tantervét áttekintve feltételezhető, hogy a tapasztalattal nem rendelkező személyek tudása nem elegendő az ellenállóképességért felelős vezetői beosztás betöltésére.

4.2.2.2. Ellenálló képességért felelős vezetők továbbképzése

A kritikus szervezetek ellenálló képességéért felelős vezetők szakmai felkészültségének naprakészen tartása érdekében került kiadásra az 59/2024. (XII. 23.) BM rendelet¹⁹⁵, mely a kritikus szervezetek ellenálló képességéért felelős vezetők továbbképzésére vonatkozó szabályokat tartalmazza. A BM rendelet értelmében a továbbképzést a Katasztrófavédelmi Oktatási Központ szervezi, képzési díj ellenében, melyen az ellenállóképességért felelős vezetők évente egy alkalommal kötelesek részt venni. A BM rendelet nem rendelkezik a

¹⁹⁴ Bleszity J., Kátai-Urbán L., Vass Gy. (2024): A kritikus infrastruktúra védelmi felsőoktatási tapasztalatok a kritikus szervezetek ellenállóképességéről szóló szabályozás tükrében. Polgári Védelmi Szemle, 2024. évi Különszám

¹⁹⁵ 59/2024. (XII. 23.) BM rendelet a kritikus szervezet ellenálló képességéért felelős vezető rendszeres továbbképzésére vonatkozó szabályokról

továbbképzés konkrét óraszámáról, tartalmáról és időpontjáról. Ezekről a részletekről, illetve a képzés formájáról (jelenléti vagy e-learning) a Katasztrófavédelmi Oktatási Központ dönthet.

A Katasztrófavédelmi Oktatási Központ honlapján elérhető információk szerint¹⁹⁶ 2025-ben két tanfolyam lett meghirdetve, a balatonföldvári Jogar Konferencia és Továbbképző Központba. A továbbképzések két napos időtartamban, minden nap 10.00 órai kezdéssel lettek meghirdetve a következő programmal:

1. rész: Szabályozási keretrendszer
2. rész: Hatósági feladatrendszer
3. rész: Ellenálló képességért felelős vezető feladatrendszere
4. rész: Ellenálló képességi terv követelményrendszere

Véleményem szerint egy kevés tapasztalattal rendelkező ellenállóképességért felelős vezető tudásának felzárkóztatására ez a továbbképzés nem alkalmas, viszont a részvétellel komoly kapcsolati tőkére tehet szert.

4.2.2.3. Kritikus szervezetek részére előírt felkészítések

A kritikus szervezetek munkavállalóinak képzésére, oktatására vonatkozó feladatokat a Kszetv. és a Kszetv.vr. az ellenállóképességért felelős vezető hatáskörébe adja, rövid, általános megfogalmazással.

A Kszetv. az értelmező rendelkezések között tér ki arra, hogy az EKT a kritikus munkakörben foglalkoztatottak oktatásának és a gyakorlatok végrehajtásának különböző szervezeti intézkedéseit is tartalmazza.¹⁹⁷

A Kszetv.vr. már több pontjában is említi az ellenálló képességért felelős vezető kritikus szervezeten belüli képzésekkel kapcsolatos feladatait. Meg kell jegyezni, hogy a Kszetv.vr. a belső képzésekre oktatásként és felkészítésként is hivatkozik:

a kritikus szervezet ellenálló képességéért felelő vezető

- a) biztosítja a kritikus munkakörben foglalkoztatottak, valamint a rendkívüli esemény kezelésben érintett munkavállalók oktatásához szükséges tematikát;

¹⁹⁶ Ellenálló képességért felelős vezetők továbbképzése. KOK Tanfolyami meghirdető (<https://kok.katasztrofavedelem.hu/37926/tanfolyami-meghirdeto>) Letöltés: 2025.10.08.

¹⁹⁷ Kszetv. 3.§ (11) bekezdés

- b) biztosítja az új belépők oktatásához szükséges tematikát;
- c) félévente összesíti az események tapasztalatait és szükség esetén módosítja az oktatási tematikát;
- d) évente egy alkalommal biztosítja a kritikus szervezet vezetőjének, a kritikus munkakörben foglalkoztatottak, valamint a rendkívüli esemény kezelésben érintettek oktatását, felkészítését a rendkívüli eseményekkel összefüggésben.

A belső képzésekhez (oktatáshoz) szükséges személyi és tárgyi feltételeket a kritikus szervezet vezetője biztosítja.

Az EKT is említi a belső képzéseket, de mindössze a minőségirányítási rendszer részét képező belső audit rendszer személyei és a kritikus munkakörökben dolgozó munkavállalók tekintetében. A képzés programjára, tartalmára mintát nem ad.

4.2.3. A kritikus szervezetek ellenálló képességével kapcsolatos belső képzés

Véleményem szerint a kritikus szervezetek rezilienciája növelhető a rendszerszintű gondolkodás és tudatosság kialakításával, melynek legfontosabb eszközei a belső felkészítések. Nem elegendő a szervezeti vezetők, auditorok és a kritikus munkakörben dolgozók képzése. A rendszerszintű gondolkodás csak rendszerszintű belső felkészítéssel érhető el, a tudatosság kialakítására minden kritikus szervezetnél dolgozó munkavállalónak szüksége van. Ahhoz, hogy minden munkavállaló a részére szükséges információkhoz jusson, folyamatos, ciklikus és következetes belső felkészítési rendszert kell felépíteni (9. ábra).



22. sz. ábra: a belső felkészítés végrehajtásának folyamata¹⁹⁸

Annak érdekében, hogy a kritikus szervezet ellenálló képessége speciális, illetve veszélyhelyzetben is biztonságosan fennmaradjon, külön hangsúlyt kell fektetni a szakmai, ágazati és védelmi területekre vonatkozó ismeretekre is. A képzések szervezőinek nagy segítséget nyújt napjaink leggyorsabban fejlődő területe a mesterséges intelligencia. A mesterséges intelligencia segíthet abban, hogy a képzésszervezők a kreatív és elemző feladatokra koncentráljanak, míg a monoton munkát automatizálja. Ma már összetett

¹⁹⁸ Saját szerkesztés

problémák megoldására és összefüggések felismerésére is képes, de hatékony használatához megfelelő eszközválasztás, szakmai tudás és alkalmazási készség is szükséges. A mesterséges intelligencia nem helyettesíti az oktatókat, hanem növeli munkájuk hatékonyságát.¹⁹⁹

A belső képzések tervezésének, szervezésének elméleti alapjai bármely szakterületen alkalmazhatók, viszont értekezésem céljából adódóan, ezekben az alfejezetekben a védelmi belső képzésekre, illetve az ellenállóképességért felelős vezető felelősségébe tartozó képzésekre fókuszálok.

4.2.3.1. A belső képzések alapelvei

A szervezet védelmével, biztonságos működésével kapcsolatos belső képzések programját az ellenállóképességért felelős vezetőnek kell kidolgoznia, a szervezet vezetőinek jóváhagyásával. Az alapelvek ismerete és alkalmazása nem csak a képzési program kidolgozásában nyújt segítséget, de a képzések eredményessége, a képzési célok elérése is könnyebben megítélhető.²⁰⁰

1. A kritikus szervezet **vezetőinek felelőssége**, hogy minden munkavállaló rendelkezzen a munkakörének megfelelő végzettséggel. Ez elérhető az adott munkakörre jelentkezők szakmai szelektálásával, illetve – amennyiben a szabályzók megengedik – a munkakör betöltésével egyidejű szakmai oktatásra való beiskolázással. A vezetők felelőssége azonban ennél több. A vezetők kötelesek a szakmai felkészítés menedzselésére, beleértve a munkavállalók továbbképzését, a belső képzések kialakítását, a tapasztalatok feldolgozását, az önképzés támogatását, illetve a feltételek biztosítását.

2. A belső képzéseknek pontosan követniük kell a felső szintű, az ágazati és a szervezeti szabályzók által **előírt szabályokat, szabványokat**. A szervezeti reziliencia egyik legfontosabb tulajdonsága a szervezeten belüli együttműködési képesség, mely akkor a leghatékonyabb, ha a felkészítések – ezen belül a belső képzések – egységesen értelmezett alapokra épülnek. A szabályoktól eltérő, szokásokra épülő tevékenység a hétköznapi működésben a hatékonyság látszatát kelti, de kritikus, veszélyes helyzetekben megakaszthatja a működés folyamatát, mely a továbbiakban zavart vagy rendkívüli eseményt okozhat.

¹⁹⁹ Petruska F. (2025): Mesterséges intelligencia: Tanulmánykötet a mesterséges intelligencia gyakorlati alkalmazásáról. *NKE Közigazgatási Továbbképzési Intézet*. Budapest

²⁰⁰ Ált/24 Magyar Honvédség Kiképzési Doktrína. (2013) Magyar Honvédség kiadványa, Budapest, 2.2. fejezet

A szabványos belső képzés azt is takarja, hogy azonos szintű munkavállalók azonos szintű tudással rendelkezzenek a kritikus szervezetek működéséhez és védelméhez szükséges ismeretekből, így együttműködésük akkor is biztosított, ha eltérő szakterületen dolgoznak.

3. A képzések tervezésénél, végrehajtásánál külön **figyelmet kell fordítani a biztonságra**, vagyis arra, hogy a legkevésbé se veszélyeztesse az üzembiztonságot és főleg ne a felkészülők, munkavállalók testi épségét. A legártalmatlanabbnak tűnő bemutató, vagy egyszerű gyakorlat is tartalmazhat kockázatot, nem beszélve a nagyobb volumenű gyakorlatokról, képzési szándékú tesztekéről, melyek a kritikus helyzetek realisztikus bemutatását is magukban foglalhatják.

4. A belső képzések tervezésében, szervezésében a **fokozatosság elvét** is figyelembe kell venni. Az elérendő cél érdekében a fokozatosság elvére épülő képzések tervezése, megszervezése viszont már oktatásmódszertani alapokat is igényel. A megszerzendő ismereteket szelektálni kell, szintekre bontani, majd úgy felépíteni, hogy a ciklikus képzés révén először az előkészítő ismeretek, majd az alkalmazó és ezt követően a megerősítő ismeretek kerüljenek átadásra. A képzések előrehaladtával az új információk aránya, mennyisége csökken, helyét a minőségi ismeretek veszik át.

5. A képzések erőforrásigényesek. Már a legegyszerűbb, alapismereteket tartalmazó elméleti képzés is emberi, anyagi erőforrást és időt von el a szervezet működéséből, a komolyabb gyakorlatok erőforrásigénye pedig már az egész szervezet működésében érezhető hatásokat generál. Nem szükséges mindenkinek minden információhoz azonnal hozzájutni, hiszen ez óriási erőforrást vonna el a működéstől. A fokozatosság elvét figyelembe véve, kihasználva a ciklikus képzés tulajdonságait, **munkavállalókra differenciált és ismeretanyagra priorizált képzést** kell kialakítani, mellyel komoly erőforrás takarítható meg. Könnyű belátni, hogy más ismeretanyagot és eltérő módszert igényel az új belépők képzése, mint a tapasztaltabb munkavállalóké, illetve a szervezet tagjainak szakterületük és vezetési szintjük szerint is eltérő igényeik lehetnek. A ciklikusság így is biztosítja, hogy a szervezet minden tagja összességében mindig megkapja a teljes, szükséges ismeretanyagot és tudásuk állandóan friss maradjon.

Hasonló megfontolásból a képzés ismeretanyaga is priorizálható. A vezetők kijelölhetik, hogy az adott képzési ciklusban (negyedéves, féléves, éves) mi legyen a fő irány: szakmai ismeretek megerősítése, védelmi vagy technológiai ismeretek kerüljenek előtérbe, vagy a szervezetet érintő globális, ágazati változások megismerése, rögzítése, stb.

6. A Kszetv.vr. előírja, hogy a kritikus szervezet vezetője biztosítja „*az oktatásokhoz a kritikus szervezet ellenálló képességéért felelős vezető szempontjai figyelembevételével meghatározott személyi és tárgyi feltételeket*”. A képzések végrehajtásához **szükséges erőforrások biztosítása** egy gazdálkodó szervezetnél – a képzések szempontjából – központi kérdés. Fontos összehangolni a rendelkezésre álló erőforrásokat és a képzésekhez szükséges erőforrások biztosítását, hiszen nem lehetséges (nem célszerű) megkövetelni egy képzési cél elérését a hozzá szükséges erőforrások nélkül, vagy csökkenteni az erőforrásokat a képzési cél változatlan követelésével. Amennyiben a szükséges erőforrások rendelkezésre állnak, az ellenállóképességért felelős vezető felelőssége, hogy a képzési célok teljesüljenek, vagy nem teljesülés esetén a hiba okának kivizsgálása.

7. A képzésekkel kapcsolatos felelősségi körök, tervezési, szervezési elvek, erőforrások mellett hasonlóképpen fontos a **fejlődést támogató** ismeretanyag létrehozása. A belső képzések ismeretanyagát úgy kell összeállítani, hogy a szervezet tagjai számára alkalmazható legyen, ne csak az információátadás legyen a cél. Ennek legfontosabb lépése az 5. pontban már említett ismeretanyag priorizálása, de a továbbiakban magának az ismeretanyagoknak is fejlődniük kell. Folyamatosan felül kell vizsgálni az ismeretanyagot, frissíteni, fejleszteni a globális, ágazati, védelmi eseményeket figyelembe véve. Egy képzést záró megbeszélés, a tapasztalatok feldolgozása és felhasználása a szervezet belső képzési rendszerének fejlődését szolgálja, valamint fontos előnye, hogy elősegíti a szervezet tagjainak rendszerszintű gondolkodását és a szervezethez való lojalitásukat is.

8. A belső képzések kialakításának legelső lépése a képzési célok meghatározása, a képzés végén pedig e **célok elérését kell igazolni**. Törekedni kell arra az ideális folyamatra, melyben csak akkor kezdhető meg egy új képzési szint, ha az előző szint **hitelesítve** lett, vagyis a képzési szint céljait elértük. Létezhet több olyan belső képzés is, melyeket az aktuális információk, változások gyors átadására hoztak létre, ezekben a képzés célja elérhető egyszerű részvétellel. Viszont a magasabb szintű belső képzések (pl. biztonságot, üzemfolytonosságot érintő képzések) erősebb hitelesítést igényelnek. Ilyenek lehetnek a szerzett tudás visszaellenőrzése, gyakorlati alkalmazásának ellenőrzés melletti végrehajtása, tervezett felsőbb szintű vezetői ellenőrzés végrehajtása, stb.

4.2.3.2. A belső képzések programjai

Egy kritikus szervezet képzési tervének tartalmaznia kell az összes belső képzés programját, melyek a szervezet tagjainak szükségesek ahhoz, hogy beosztásukat a legjobb tudásuk szerint,

hatékonyan elláthassák. Sok esetben viszont az új belépők a hozott képzettségükkel és tudásukkal kerülnek egy adott beosztásba és a kollégákkal való együttműködés révén, illetve a beosztásban eltöltött bizonyos idő alatt szerzik meg azt a tudást amely kifejezetten a szervezeti célokhoz illeszkedik.

Bár a tapasztalatszerzés az egyik legfontosabb és legerősebb eszköze a szükséges tudás megszerzésének (és része a felkészítési rendszernek), de nem szabad teljes egészében erre alapozni a szakmai fejlődést, mivel nem irányított. Az irányított, szervezeti célokhoz kapcsolódó szakmai fejlődés alapjai a szervezeti belső képzések, melyek egymáshoz kapcsolódnak, egy rendszert alkotnak, kiegészülnek a külső képzésekkel és a szerzett tapasztalatokkal.

A szervezet munkavállalói számára a betöltött munkakörükhöz kapcsolódó szakmai felkészítés szükséges. Az alapelveknél említett, munkavállalókra differenciált és ismeretanyagra priorizált képzés úgy érhető el, ha szakterületenként külön képzési programot alkalmazunk, melyek az adott szakterület alapismereteitől a speciálisabb ismeretek felé fokozatosan haladnak. Ezt a rendszert használva minden beosztáshoz meghatározható, hogy melyik képzési programból, milyen szintig szükséges eljutni a képzési célok eléréséhez. Az értekezés céljához igazodva, példaként a kritikus szervezetek fizikai védelmével kapcsolatos belső képzés programjának tervezetét és annak alkalmazását vizsgálom.

Képzési program felépítésére a felnőttképzésről szóló 2013. évi LXXVII. törvény 12. §-a ad rövid vázlatot, mely használható, de jelen összefüggésben nem kötelező érvényű, mivel egy kritikus szervezet nem szervezetszerű képző intézmény.

A kritikus szervezetek képzési programjának tartalma eltér az akkreditált képző intézmények részére előírt tartalmi elemektől, alapjaiban a tartalmi elemek három csoportba sorolhatók. A képzés alapadatait, a képzés tárgyköreit és tematikáját, valamint a képzési célok elérésének mérési és értékelési rendjét tartalmazó csoportokra.

A kritikus szervezetek képzési programjának felépítésére a következő elvi javaslatot adom. A javaslathoz kapcsolódó *mintát* a 2. melléklet tartalmazza.

1. A képzés alapadatai tartalmazzák:
 - a képzés megnevezését, mely legyen egyértelmű, megkülönböztethető a többi – esetleg hasonló témájú – képzéstől. A könnyebb adminisztráció és hivatkozás érdekében, több képzés esetén alkalmazhatunk képzési kódokat;

- a képzésért felelős nevét elérhetőségét, beosztását. Több név is megadható, ha például más felel a szervezésért, végrehajtásért, ellenőrzésért, de pontosan meg kell adni a felelősségi köröket;
- a célcsoport rövid meghatározását, a részvétel feltételeit. A célcsoport lehet szakmai (pl. biztonsági őrök), vagy általános (pl. új belépők), szűkebb (pl. felsővezetők), vagy akár a szervezet teljes állománya. A részvétel feltételeként megadhatunk beosztást, szakterületet vagy akár előfeltételként bizonyos képzettség, képzés meglétét;
- a képzés tervezett időszükségletét, összóraszámát. Az óraszám lehet javasolt vagy kötelező, illetve itt szükséges megadni, hogy az összórák száma hogyan oszlik meg elméleti és gyakorlati órákra. Ha a képzés önképzést is igényel, ebben a pontban meg lehet adni a javasolt önképzési összóraszámot is;
- a képzés leírását, mely röviden összefoglalja a képzés szakmai tartalmát, illetve ebben a pontban megadható, hogy ezeket az ismereteket egyszeri alkalommal, vagy meghatározott időközönként ciklikusan szükséges átadni;
- a képzés célját és a megszerezhető kompetenciákat. A képzés céljának meghatározása a képzés szervezőjének ad támpontot, hiszen kijelöli a végrehajtás irányát és súlyát. Egy képzés célja lehet új ismeret közlés, szinten tartás, beosztásra vagy feladatra való felkészítés. Eltérő célok esetén eltérő lehet a tananyagegységek súlyozása, az értékelés rendje, az elmélet és gyakorlat aránya, stb. Hasonló okkal szükséges megadni az elérendő kompetenciákat, melyeket külön kell választani az elsajátítás mélysége szerint. Megadhatjuk, hogy a képzésen résztvevők milyen információkat ismerjenek meg, milyen tevékenységekre legyenek képesek, illetve megadhatjuk a kialakítandó attitűdjeiket²⁰¹.

2. A képzés tárgykörei és tematikája:

A képzés szakmai tartalmát olyan részegységekre kell bontani, melyek önmagukban is kezelhetők, akár szakmai, akár szervezési szempontból. Ezek az önállóan is kezelhető képzési egységek a tárgykörök. A tárgykörök céljai a képzés fő céljának irányába mutatnak, felépítése tükrözi az elérendő kompetenciákat, azok megszerzésére épül. A tárgykörök különbözhetnek

²⁰¹ „Adott eseménnyel szemben tanúsított magatartás”; „viselkedés, modor” – Bakos, Fábíán: Idegen szavak és kifejezések szótára; Budapest (1978.)

egymástól óraszámokban, képzési módszerükben, személyi és tárgyi feltételeikben és természetesen szakmai tartalmában;

- a tárgykörök tematikája tartalmazza a szakmai tartalom részletes leírását. A tematika leírásának módjával a képzés szervezője eldöntheti, hogy mennyire ad szabad kezet az oktatóknak:
 - a.) ha a tematika megadja az egyes foglalkozások részletes tartalmát és óraszámát, attól az oktató csak nagyon szűk keretek között térhet el. Ennek előnye, hogy oktatótól és hallgatótól függetlenül az átadott tudás egységes, pontosan tervezhető, a visszaellenőrzés következetesen végrehajtható, mérhető.
 - b.) ha a tematika megadja az egyes foglalkozások részletes tartalmát, de az óraszámokat nem köti meg, akkor az oktató a tananyagrészeket súlyozottan dolgozhatja fel, a hallgató felkészültségétől és igényeitől függően.
 - c.) ha a tematika a tárgykörre vonatkoztatva részletes, de összesített szakmai célokat fogalmaz meg, akkor az oktatóknak szabad keze van abban, hogy ezeket a célokat hogyan éri el. Ezzel a felelősséget is az oktató kezébe adja, tapasztalatait, szakmai tudását felhasználva neki kell döntenie a tananyagrészek súlyozásáról, a visszaellenőrzés módjáról a mérés értékeléséről. Előnye, hogy a tananyagba könnyen beilleszthetők az új információk, rugalmasabban alakítható, frissíthető a tárgykör.
- a tárgykörök elsajátítása, az önképzés támogatása érdekében meg kell adni a releváns és az ajánlott szakirodalmat. Kötelező releváns szakirodalmak esetében a képzést szervezőnek biztosítani kell a hozzáférést az anyagokhoz, akár online, akár valós formában.

3. A képzési célok elérésének mérési és értékelési rendje tartalmazza:

- a kimeneti követelményeket, melyek vonatkozhatnak a foglalkozásokon való részvételre (kötelező/nem kötelező), a hiányzás mértékére (%), az ismeretlenőrzés végrehajtására.
- az ismeretek ellenőrzésének rendjét. Figyelembe véve a képzés célját és a tananyag típusát, a visszaellenőrzés rendjének és módszerének kiválasztása több tényezőtől függ. Fontos tényező, hogy milyen mélységig igényli a képzést szervező a tanult ismeretek visszaellenőrzését, illetve, hogy mennyi időt szán annak végrehajtására. Vizsgálni kell, hogy a megszerzett tudás mely módszerrel ellenőrizhető vissza a leghatékonyabban. Az

online tesztek, szóbeli vizsgák, vagy a közös projektfeladatok, gyakorlatok mind eltérő tudás, képesség mérésére alkalmasak. Befolyásoló tényezők – többek között – az erőforrások és szakemberek rendelkezésre állása is.

4.2.3.3. A belső képzések programjainak alkalmazása

Egy kritikus szervezet képzési terve, mely széleskörűen tartalmazza a belső képzések programját, jól alkalmazható akár egyedi, konkrét alkalomra szabott képzés összeállítására, vagy szakterületekre szabott, eltérő szintű és tartalmú képzések összeállítására is.

A széleskörű alkalmazás alapja, hogy a képzési programok tárgyköreit modulszerűen kell kialakítani – ahogyan az előző alfejezetben szerepel – a tárgykörök önmagukban is kezelhetők legyenek, akár szakmai, akár szervezési szempontból. Így a tárgykörök összefűzésével egyedi, az aktuális képzési célnak legmegfelelőbb képzés állítható össze. A modulszerűen összefűzött tárgykörökhöz adhatunk meg irányóraszámokat, mellyel beállítható az adott képzés ideje és erőssége is.²⁰²

A modulszerűen kialakított képzések további előnyei:

- fix képzési programmal rendelkező képzések is kiegészíthetők más képzési programból átvett tárgykörökkel;
- az óraszámok a rendelkezésre álló időhöz, illetve a képzési célokhoz igazodva megadhatók, tárgykörönként külön-külön is, így megadható az adott képzés fő prioritása;
- lehetőség van az egyes szakterületek alapismereteinek átoktatására, mely erősíti a munkavállalók egymás közötti és a szervezethez való kapcsolatát, elősegíti a rendszerben való gondolkodást;
- könnyen frissíthető, aktualizálható a tananyagtartalom, a tananyagfejlesztés hatékonyan végrehajtható;
- a modulszerű tárgykörök a célzottabb értékelést is megkönnyítik, pontosabban meghatározhatók a képzés és a résztvevők erősségei és fejlesztési irányai.

Összességében a jól kialakított, önmagukban is kezelhető, modulszerű rendszerbe helyezett tárgykörökből álló képzési programok, jó alapjai lehetnek korábban említett fejlődési spirál kialakításának.

²⁰² Kiképzési Program a Magyar Honvédség műszaki katonái részére. (2014) – LEKTORÁLT, nincs kiadva

4.3. KIJELÖLT KRITIKUS SZERVEZET BELSŐ FELKÉSZÍTÉSÉNEK ELLENŐRZÉSE

A szervezeti belső felkészítések ellenőrzése olyan komplex, többlépcsős folyamat, amelynek célja a felkészítés minőségének biztosítása és hatékonyságának mérése. A vezetői szintű ellenőrzés szorosan kapcsolódik a szervezet stratégiai céljaihoz és az emberi erőforrás menedzsment minőségbiztosítási elveihez, ezért végrehajtásába minden szakterületi vezetőt és szakértőt be kell vonni, az ellenőrzés eredményeit pedig meg kell osztani a jogosultak körével.

A vezetői szintű ellenőrzésnek át kell fognia a szervezet felkészítési struktúrájának teljes egészét, a teljes felkészítési folyamat (9.sz. ábra) áttekintését.²⁰³

A felkészítési folyamat egyes elemei különböző felelősségi körökhöz tartoznak, eltérő szakmai ismereteket igényelnek, eltérő időben és helyen jelennek meg a folyamatban. Ezért az egyes elemek ellenőrzését is úgy kell tervezni, szervezni és végrehajtani, hogy az információk összekapcsolhatók maradjanak, ne vesszenek el az elemzés során.

Egy teljes rendszerre kiterjedő, alapos, mélységben végrehajtott ellenőrzés nem csak a felkészítések hatékonyságát képes javítani, de szükséges a Kszetv. által előírt ellenőrzések végrehajtásához is. Vagyis a hatékonyság növelhető, a ráfordított erőforrások csökkenthetők általa.

Jelenleg a belső felkészítések ellenőrzésére a Kszetv. központi, reziliencia vizsgálatára kiterjedő komplex hatósági ellenőrzés keretében valósul meg, de a felkészítések eredményességének ellenőrzése a szervezet vezetőjének, illetve tanácsadóként az az ellenállóképességért felelős vezetőnek a feladata. A jogszabályok ezzel a feladattal kapcsolatban nem rendelkeznek.

Jelenleg a kritikus szervezetek belső felkészítési rendszerének auditálása nem valósul meg. Több esetben az ellenőrzés a végrehajtott belső képzést követően, a résztvevők visszaellenőrzésben merül ki, mely elnagyolt, szubjektív. Reprezentatív adatok hiányában nem valósítható meg a képzések hatásvizsgálata a munkateljesítményre, az egyéni fejlődésre, a szervezet hatékonyságának és védelmi képességeinek fejlődésére.

²⁰³ Ált/24 Magyar Honvédség Kiképzési Doktrína. (2013) Magyar Honvédség kiadványa, Budapest, 4.5. fejezet

4.3.1. Szervezeti belső felkészítés vezetői szintű ellenőrzésének metodikája

Az előző alfejezetekből kiemelendő, hogy a felkészítési rendszer egyes elemeinek ellenőrzését úgy kell tervezni, szervezni és végrehajtani, hogy az információk összekapcsolhatók maradjanak, ne vesszenek el az elemzés során, így alkalmazhatók legyenek a szervezet működési és védelmi hatékonyságához szükséges felkészítések elemzéséhez és fejlesztéséhez. Ez a szervezeti belső felkészítés ellenőrzésének egyik fő célja. Ez a cél a belső felkészítések ellenőrzésére kidolgozott metodika következetes alkalmazásával elérhető.²⁰⁴

Az ellenőrzés vezetői szintje – ebben az esetben – azt jelenti, hogy az ellenőrzés eredményei a szervezet vezetésének stratégiai terveit, döntéseit megerősítik, vagy pozitív változtatás irányába terelhetik.

4.3.1.1. Szervezeti belső felkészítés vezetői szintű ellenőrzésének követelményei

Annak érdekében, hogy a belső felkészítés ellenőrzése megfelelő metodika szerint alkalmazható legyen és elérje célját, meg kell felelnie a következő követelményeknek:

*Közvetlen vizsgálatokkal alátámasztott, rendszer-alapú megközelítéssel működik.*²⁰⁵

Közvetlen vizsgálati módszerekkel a felkészítési rendszer azon elemei vizsgálандók, melyek további alrendszerre való bontása már nem hoz releváns információt, illetve a közvetlen vizsgálatból befolyó eredmények szükségesek a rendszer-alapú vizsgálatok végrehajtásához. Ilyen lehet például a képzési okmányok formai követelményeinek áttekintése, a képzések helyszíneinek ellenőrzése, egyes képzések végrehajtásának idő és létszám adatainak összehasonlítása, stb.

A rendszer-alapú vizsgálatnál a rendszer elemeinek egymáshoz való viszonya, a rendszer és alrendszereinek működőképessége, hatékonysága és megbízható értékelhetősége vizsgálható. Ilyen vizsgálat lehet például az egyes képzési folyamatok szakmai szabályzóknak való megfelelése, a képzésen átadott információk megjelenése és hatása a munkafolyamatokra, stb.

A közvetlen vizsgálatokat és a rendszer-alapú vizsgálatokat megfelelő metodika mellett együttesen kell alkalmazni.

²⁰⁴ Kresalek P. (2014): A vállalati ellenőrzés alapjai. Oktatási segédanyag.

²⁰⁵ Honvédelmi Minisztérium fejezet egységes belső ellenőrzési kézikönyve. *Honvédelmi Minisztérium* (2023)

Illeszkedik a szervezet stratégiai céljaihoz.

A szervezeti belső felkészítés minden esetben a szervezet stratégiai céljaihoz kapcsolódik, így az ellenőrzésének is követelménye, hogy képes legyen ennek megvalósulását vizsgálni.

Segítő szándékú, eredményei a fejlődést szolgálják²⁰⁶

Az ellenőrzés nem lehet számonkérő jellegű vagy öncélú. Az ellenőrzés végrehajtása során feltárt képzési hiányosságokat, hibákat az érintett szakterület munkatársaival, vezetőivel együtt kell elemezni, priorizálni és ha lehetséges akkor javítására protokollt javasolni.

Objektív

A belső képzések ellenőrzése csak abban az esetben tekinthető hitelesnek, ha objektív. Vagyis az elemzés előre meghatározott és mérhető kritériumokra épül és eredményét nem igazítják a szervezet vagy a vezetők aktuális elvárásaihoz. A felkészítések hatékonyságát és fejleszthetőségét súlyosan korlátozza, ha a felkészítések eredményeit a vezetők elégedettsége érdekében torzítják.

Rendszeres, folyamatos

A szervezeti belső felkészítés hatékonysága a képzések folyamatos és ciklikus végrehajtási és fejlesztési struktúrájára épül. Ez a fejlődés nem valósulhat meg, ha a felkészítési rendszer nem tartalmaz visszacsatolást, vagyis a rendszeres ellenőrzés a képzések ciklikusságát követve része kell, hogy legyen a teljes felkészítési folyamatnak.

Átlátható, jól dokumentált

A tervszerű és jól dokumentált ellenőrzések és elemzések lehetővé teszik a képzések nyomon követhetőségét, a fejlődési spirál hosszú távú értékelését, a felkészítésekkel kapcsolatos döntéshozatal támogatását. A vezetők és a munkavállalók számára is elérhető, átlátható ellenőrzési dokumentáció növeli a felkészítési rendszer iránti bizalmat és ezzel a rendszerszintű gondolkodást és tudatosságot.

Releváns információkat ad

Az ellenőrzési folyamat során akkor kaphatunk releváns információkat, ha a begyűjtött adatok eleve alkalmasak megjelenítésre és feldolgozásra ²⁰⁷. Vagyis az ellenőrzés során keletkezett adat – jellemzői alapján – elhelyezhető a rendszerben (mikor, milyen

²⁰⁶ Ált/24 Magyar Honvédség Kiképzési Doktrína. (2013) Magyar Honvédség kiadványa, Budapest, 4.6.4. fejezet

²⁰⁷ 2024. évi LXIX. kiberbiztonsági tv. 4.§ - <https://njt.hu/jogszabaly/2024-69-00-00#SZ116>

körülmények között, milyen céllal jött létre), elegendő részletességű, pontosságú és olyan formátummal rendelkezik, mely érthető a feldolgozó személyek részére.

Megfelel a törvényességi követelményeknek

Az ellenőrzési folyamat szükségszerűen érinti az etikai, adatvédelmi és törvényességi szempontokat, hiszen a résztvevők, munkavállalók személyes adatai, kompetenciái, a szervezet belső működési és biztonsági adatai is tartalmazhatnak releváns információkat.

Az értékelés nem lehet diszkriminatív, nem sértheti az emberi méltóságot, és nem irányulhat a munkavállalók indokolatlan ellenőrzésére vagy megbélyegzésére. Ha az ellenőrzés eredményei negatív következményekkel járnak (pl.: hátrányos megkülönböztetés, pénzbeli elmaradás) azzal a szervezet belső felkészítési rendszerébe vetett bizalom is súlyosan sérül.

4.3.1.2. Szervezeti belső képzések vezetői szintű ellenőrzésének végrehajtása²⁰⁸

A minden részletre kiterjedő ellenőrzési metodika nem más, mint a felkészítési rendszer egyes elemei vizsgálatának összessége, mely térbeli és időbeli rendszerbe foglalja:

1. az ellenőrzés előkészítését,
2. a részellenőrzések végrehajtását,
3. a megállapítások összefűzését,
4. az ellenőrzés hatékonyságának vizsgálatát (ellenőrzés minőségbiztosítása),
5. a megállapítások hasznosításának feladatait.

1. Az ellenőrzés előkészítése

A szervezet vezetői által meghatározott ellenőrzési követelmények alapján meg lehet határozni az ellenőrzés területeit, melyek alapján kiválasztható az adott terület ellenőrzésére legalkalmasabb módszer. A kiválasztott módszer alapján meghatározható az ellenőrök száma, szakterülete, illetve behatárolható az ellenőrzés időtartama.

Kritikus szervezeteknél az ellenőrzés folyamán szükség lehet nem nyílt dokumentumokba való betekintésre is. Az ellenőrzésbe bevont személyek esetében külön figyelmet kell fordítani arra,

²⁰⁸ 167-41/2014. MH Kiképzési és Doktrinális Központ Ellenőrzési Program. (2014)

hogy – amennyiben szükséges – a megfelelő szintű engedéllyel rendelkezzenek a betekintéshez, akár ideiglenes jelleggel is.

2. Az ellenőrzés végrehajtása

Egy kritikus szervezet felkészítési rendszerének ellenőrzése nem csupán a belső képzések vizsgálatából áll, hiszen – ahogyan a megelőző alfejezetekben kifejtettem – vizsgálni kell a képzések célját, végrehajtását, illetve mérhető eredményeit a szervezet működésében. Egy jól előkészített ellenőrzés széleskörű és hatékony, de nem akadályozhatja a szervezet aktuális munkafolyamatait, működését.

Az ellenőrzés követelményeinél említett közvetlen vizsgálatokat és a rendszer-alapú vizsgálatokat együttesen kell alkalmazni. Hatékony ellenőrzés végrehajtásakor nem is nélkülözheti egyik típus a másikat.²⁰⁹ Hiszen egy szervezet felkészítési rendszerének rendszer-alapú ellenőrzése csak akkor teljes, ha az eredményeit közvetlen vizsgálatokkal is alá tudjuk támasztani. Illetve a képzések közvetlen vizsgálatának eredményei csak abban az esetben hasznosak, ha alá tudjuk támasztani a rendszerben való relevanciájukat.

A rendszerek alapfogalmából kiindulva²¹⁰ a rendszer-alapú vizsgálat a rendszerelemek közötti kölcsönhatások vizsgálatából áll, melynek célja a rendszer belső szabályai helyes működésének ellenőrzése. Ez egy nagyon általános meghatározás, de a kritikus szervezetek felkészítési rendszerének rendszer-alapú ellenőrzése levezethető belőle, ha az egyes képzéseket tekintjük a rendszer elemeinek és a képzések alapelvei adják a szabályokat.

A közvetlen vizsgálatok lehetnek:

- elemző eljárások (adatok összehasonlítása, statisztika, egyéb elemző módszer);
- közvetlen részletes vizsgálat (megfigyelés, szemrevételezés, kísérlet, próba, stb.).

A közvetlen vizsgálatok konkrét adatokat szolgáltatnak, ezért van szükség a rendszer-alapú vizsgálatokra is, hogy ezekből az adatokból és köztük lévő összefüggésekből következtetéseket vonhassunk le.

²⁰⁹ Kresalek P. (2014): A vállalati ellenőrzés alapjai. Oktatási segédanyag. 46.o

²¹⁰ Von Bertalanffy, L.: General System Theory: Foundations, Developments, Applications. 1968. New York, Braziller.

A különböző vizsgálati módszerekkel begyűjtött releváns információk felhasználásával és az ellenőrzés céljának figyelembevételével megállapított következtetések már megmutatják az ellenőrzött terület működését.

3. Az ellenőrzés ellenőrzése (minőségbiztosítás)

Egy vezetői szintű ellenőrzés idő és erőforrásigényes, ezért fontos, hogy hatékony legyen, vagyis eredményei relevánsak legyenek a szervezet életében. Ez elérhető az ellenőrzések megfelelő minőségbiztosításával.

Egy kritikus szervezet belső felkészítési rendszerének vezetői szintű ellenőrzési metodikája és az ellenőrzés minőségbiztosítása nem feltétlenül igényel komolyabb erőforrásokat, költségeket. Az ellenőrzések minőségbiztosításának alapvető tényezői könnyen beépíthetők a felkészítési rendszerbe, illetve könnyen illeszthetők a meglévő erőforrásokra.

4.3.1.3. Szervezeti belső képzések vezetői szintű ellenőrzési eredményeinek hasznosítása

Ha az ellenőrzésekre úgy tekintünk, mint egy lehetséges fejlesztési eszközre, akkor olyan információkhoz juthat a szervezet, melyek a napi üzemeltetéstől a stratégiai döntési szintekig növelik a hatékonyságot, illetve rövid és hosszú távon is segítik a szervezet üzembiztonságát. Ennek eléréséhez mind a szakmai, mind a vezetői szinteken meg kell jelennie a tudatosságnak, a fejlődésre, fejlesztésre való igénynek, hiszen ahogyan a felkészítések ellenőrzési eredményeit fel lehet használni más területek fejlesztésében, úgy az egyéb szakterületek ellenőrzési eredményeinek is meg kell jelennie a szervezeti felkészítésekben. Az így létrejövő rendszer csak abban az esetben fejlődik és növeli az üzembiztonság hatékonyságát, ha az ellenőrzés eredményeit hasznosítjuk, vagyis a megállapítások, következtetések és javaslatok alapján intézkedések is születnek²¹¹.

Az képzési ellenőrzések eredményei fontos szerepet játszhatnak abban, hogy meghatározzák és felismerjék a szervezet erősségeit és fejlesztendő területeit. Előtérbe kerülhetnek olyan szervezeti kompetenciák, melyekre akár önálló szervezeti belső képzések is kialakíthatók, vagy láthatóvá válik, mely esetben lehet szükség külső felkészítés igénybevételére.

²¹¹ Kresalek P. (2014): A vállalati ellenőrzés alapjai. Oktatási segédanyag. 90.o

Nem utolsó szempont, hogy a részletes elemzésekkel ellátott ellenőrzés igazolhatja a felkészítési rendszer szükségességét, a befektetett erőforrások indokoltságát, a képzések szervezeti szintű hatékonyságát, és főképp az ellenálló képesség növelését a felkészítési rendszer által.

A Kszetv. a kritikus szervezetek részére ellenálló képességi és komplex gyakorlatot ír elő, mely eredményeinek elemzése az éves ütemezésű komplex hatósági ellenőrzés része. Az ellenálló képességi gyakorlatra való belső felkészítés és ellenőrzés az előzőekben említett előnyök mellett, elősegíti a hatósági feladatok gyorsabb és hatékonyabb végrehajtását és gördülékenyebb kommunikációt eredményez a hatóságokkal.

4.4. RÉSZKÖVETKEZTETÉSEK

A 4. fejezetben azt vizsgáltam, hogy a kritikus szervezetek rezilienciája hogyan növelhető a szervezet belső felkészítési rendszerének fejlesztésével és alkalmazásával. Rámutattam, hogy a védelmi technológiák folyamatos fejlődése mellett, napjainkban a leggyengébb láncszem az emberi tényező, ezért kerestem olyan fejlesztési lehetőségeket, melyek az emberi tényező hatékonyabb működését eredményezhetik.

Az emberi tényező a kritikus szervezetek védelmi rendszerébe adminisztratív eszközökkel kapcsolódik, minden vezető és munkavállaló a szabályzók, utasítások, szerződések alapján látja el feladatait. Ennek okán fontos, hogy a kritikus szervezetek átfogó dokumentációs hierarchiával rendelkezzenek. A 4.1. alfejezetben bemutattam egy kritikus szervezet részére megfelelő dokumentációs hierarchia felépítését és rámutattam, hogy a helyesen kialakított és folyamatosan fejlesztett dokumentáció hierarchia jól alkalmazható a védelmi képességek fejlesztése során, mellyel költségeket és időt is megtakaríthat.

A szervezetek zökkenőmentes működése a munkavállalók szakmai tudásán, illetve a megszerzett kompetenciáikon múlik.

A jogszabályok elemzésével *igazoltam, hogy nincs olyan szervezeti vezető vagy munkavállaló, akinek ne lenne plusz feladata egy szervezet kritikus vagy jelentős szervezetté való kijelölését követően.* A jogszabályok és a jelenleg elérhető releváns képzések elemzésével *igazoltam, hogy nem elegendő a Kszetv. és a kapcsolódó jogszabályok által említett vezetői és összekötői felkészítés a speciális helyzetekre, rendkívüli eseményekre való felkészüléshez.* Sőt, létezhetnek olyan kritikus vagy jelentős szervezetek és infrastruktúrák, melyek esetében az

interdependenciából adódó külső szolgáltatók, szervezetek részére is ki kell terjeszteni bizonyos szintű kapcsolati és biztonsági felkészítést.

Annak érdekében, hogy a kritikus szervezetek speciális helyzetekre történő felkészítése könnyen integrálható legyen a kijelölés előtti felkészítési rendszerbe, külön kell választanunk az elemeit és meg kell határoznunk azokat az alapelveket, melyek keretet adnak a megvalósításához. A 4. fejezetben *javaslatot adtam a kritikus szervezetek felkészítési keretrendszer felépítésére* és azokra az alapelvekre, melyek betartásával kialakítható az előbbiekben említett és szükséges felkészítés.

Elemeztem a kritikus szervezetek személyi állománya felkészítésének jelenlegi helyzetét, mely alapján *igazoltam, hogy nem elégíti ki egy kritikus szervezet magasabb szintű védelmére és ellenálló képességére vonatkozó követelményeket*. Ezzel bizonyítottam, hogy egy szervezet kritikus szervezetté való kijelölését követően, mindenképpen igényli a belső vezetői, védelmi és speciális üzembiztonsági képzések végrehajtását.

Kidolgoztam a kritikus szervezetek belső képzésének tervezéséhez szükséges képzési program tartalmi elemeit, mely a képzés alapelveinek figyelembe vételével és a 2. mellékletben található minta felhasználásával alkalmas a kritikus vagy jelentős szervezetek vezetőinek és munkavállalóinak kiegészítő biztonsági, védelmi képzésére.

Mivel a kritikus szervezetek munkavállalóinak felkészítésére vonatkozó feladatokat a Kszetv. és a Kszetv.vr. az ellenállóképességért felelős vezető hatáskörébe adja, így a belső felkészítések hatékonyságának mérését, ellenőrzését is a kritikus szervezetnek önállóan, saját hatáskörben és erőforrásai felhasználásával kell végrehajtaniuk. Ennek előnye, hogy könnyen összeegyeztethető az aktuális folyamatokkal, a legkevésbé terheli meg a szervezet működését, hátránya viszont, hogy könnyen ad szubjektív végeredményt, objektivitás csak a végrehajtók és vezetők következetességével érhető el.

A kritikus szervezetek belső felkészítésére fókuszálva kialakítottam egy ellenőrzési metodikát, mely a felkészítés ellenőrzésének követelményeit és a végrehajtás lehetséges lépéseit, módszereit tartalmazza. Fontos szempont kritikus szervezetek esetében, hogy a belső felkészítések és azok ellenőrzésének végrehajtása a lehető legkisebb mértékben befolyásolják a folyamatos üzemeltetést és biztonságot, amellet, hogy lehetőség szerint minél nagyobb mértékben járuljanak hozzá a kritikus szervezet védelmének és üzembiztonságának hatékonyságához. Az ellenőrzési metodika kialakításánál igyekeztem ezt az elvet követni.

5. ÖSSZEGZÉS

Az értekezés 1. fejezetben a kritikus infrastruktúrák védelmének európai és hazai szabályozási környezetét és annak előzményeit tártam fel. A áttekintés szükséges annak érdekében, hogy a hazai rendszert mind szabályozás, mind végrehajtás tekintetében értékelni lehessen.

Az elemzés rámutatott arra, hogy az EU már a 2000-es évek elejétől stratégiai kérdésként kezeli a kritikus infrastruktúrák védelmét. A COM(2004) 702 közlemény először határozta meg a létfontosságú infrastruktúra fogalmát, kiemelve, hogy ezek kiesése súlyos hatással lehet a társadalom biztonságára, gazdaságára és működésére. A dokumentum már akkor külön hangsúlyozta az interdependenciát, vagyis azt, hogy az egyes ágazatok egymás működésétől függenek, ami rendszerszintű sérülékenységet eredményez. Az ezt követő dokumentumok – az európai Zöld Könyv és az EPCIP – megerősítették, hogy a kritikus infrastruktúrák védelme csak több szereplő együttműködésével valósítható meg. A szubszidiaritás elve szerint az EU csak a határokon átnyúló infrastruktúrák esetében avatkozik be, míg a nemzeti infrastruktúrák azonosítása és rezilienciájának kialakítása a tagállamok feladata. A 2008/114/EK irányelv már konkrét kötelezettségeket fogalmaz meg az európai kritikus infrastruktúrák azonosítására és védelmére, ugyanakkor csak általános kereteket ad, az ágazati kritériumok meghatározását a tagállamokra bízta. Az (EU) 2022/2557 irányelv megjelenése jelzi a területen végrehatott modernizálást, fejlesztéseket. Szoros kapcsolatot teremt a kibervédelmi területtel és kiterjeszti az irányelv hatályát a társadalom számára fontossá vált ágazatokra is. A nemzetek infrastruktúráinak azonosítását és rezilienciájának kialakítása továbbra is teljes egészében a tagállamok kezébe adja. Ez a megközelítés magában hordozza, hogy a különböző nemzetek szabályozásai között jelentős különbségek alakulhatnak ki és a végrehajtás minősége nagymértékben az adott ország intézményi és módszertani fejlettségétől függ.

A fejezetben kitértem a kiberbiztonsági szabályozás fejlődésére is (NIS és NIS2 irányelvek), amelyek a digitalizáció növekedésével egyre szigorúbb követelményeket írnak elő a kritikus és alapvető szervezetek számára. A NIS2 külön hangsúlyozza a kockázatelemzést, az üzletmenet-folytonosságot, az ellátási lánc biztonságát és a rendszeres képzéseket. Ez kapcsolódik *a kutatás egyik céljához, amely a szervezeten belüli felkészítési rendszer szükségességét vizsgálja, és megerősíti annak relevanciáját.*

Az 1. fejezetben az európai szabályozás áttekintését követően részletesen elemeztem a magyarországi jogszabályi rendszert is, amely a kezdetektől az uniós irányelvekre épül, de a saját nemzeti viszonyokat veszi figyelembe. A 2080/2008. (VI. 30.) kormányhatározat, mely fontos mérföldkőként tartalmazta a Kritikus Infrastruktúra Nemzeti Programjáról szóló Zöld

Könyvet, példa értékűen teszi meg az EU irányelve alapján meghatározott lépéseket. Ezt követően, több éves szakmai munka eredményeképpen megalkották az Lrtv. és Lrtv.vr. szabályzókat, melyek pontosították az alapfogalmakat, és meghatározták az ágazatokat, a nemzeti, illetve az európai létfontosságú rendszerelemekkel kapcsolatos kijelölés vagy visszavonás folyamatát, a hatóságok feladatát, valamint a folyamathoz kapcsolódó résztvevőket és feltételeket. Az előírás szerinti ágazati kormányhatározatok kidolgozásával széleskörű szakmai elemzés és munka indult meg a létfontosságú rendszerek azonosítása és védelme területén.

A 2024-ben megjelent kibervédelmi törvény, Kszetv. és Kszetv.vr., módosított VBÖ, VBÖ.vr. elemzésével látható, hogy a magyar szabályozási rendszer több egymásra épülő jogszabályból áll, melyek meghatározzák a kritikus és jelentős szervezetekhez kapcsolódó fogalomkört, az ágazati besorolásokat, a kijelölési kritériumokat, valamint a hatósági felügyelet rendjét. A rendszer központi eleme a kritikus szervezetek ellenálló képességének fejlesztéséről szóló jogi keret, amely egységes fogalomrendszerbe vonta a korábbi létfontosságú rendszerelemeket és az alapvető szolgáltatást nyújtó szereplőket. Ez a megközelítés a reziliencia szemlélet erősödését jelzi és összhangban áll az európai szabályozással.

Az európai és hazai jogszabályok elemzésével *megállapítottam, hogy elsősorban a szereplők körét és feladatait határozzák meg, de kevés iránymutatást adnak az egyes speciális helyzetek kezelésére, az elemzések mélységére vagy az alkalmazandó módszerekre.* A kritikus szervezetekkel kapcsolatos hazai jogszabályi környezet gyorsan és jól követi az EU fejlesztési irányait, de *meglátásom szerint a 2024. évben végrehajtott jelentős változás beszűkítette a hatóságok és a szakterületek közötti kommunikációt.*

Ez közvetlenül igazolja a kutatás első hipotézisét, miszerint a *jogi szabályozás fejlett, de még nem tekinthető teljesen kiforrottnak és a gyakorlati végrehajtás során nem minden esetben nyújt elegendő támogatást.* Ideiglenes szakmai bizottságok létrehozásával, a vizsgálatok interdependenciára való kiterjesztésével, a kritikus szervezetek munkavállalóinak képzésével, adminisztratív támogatással a rendszer tovább fejleszhető.

A hazai rendszer értékelése során az is megállapítást nyert, hogy a szabályozás egyre nagyobb hangsúlyt fektet az interdependenciák figyelembevételére és a nemzeti szintű kockázatértékelés kialakítására, ugyanakkor *a gyakorlati megvalósítás még további módszertani fejlesztést igényel.*

A 2. fejezet fő kutatási célja annak bemutatása volt, hogy a magyarországi jogi és intézményi rendszer miként szabályozza a kritikus szervezetek azonosítását és kijelölését, a jelenleg hatályos jogszabályok hiányosságai mely területeken jelentkezhetnek, illetve ezen hiányosságok milyen módon lennének orvosolhatók. A nemzeti kritikus infrastruktúrák azonosítási és kijelölési folyamatát elemezve, a hiányosságok pótlására és a folyamat fejlesztésére a következő javaslatokat teszem.

A hatósági és ágazati kommunikációs csatornák kiszélesítésének igényét jelzi, hogy – kutatásaim szerint – a kritikus szervezetek és infrastruktúrák azonosítása és kijelölése, de főképp a kijelölést követő védelem és ellenálló képesség kialakítása olyan felelősségi köröket érint, melyek túlmutatnak a kritikus szervezet belső struktúráján. Egy kritikus szervezet finanszírozásáért vagy fizikai védelméért felelős szerv/szervezet/tanács több esetben nem is része a kritikus szervezet belső döntési mechanizmusának. Ilyen esetekben az ellenálló képesség kialakításának hatékonysága és költségeinek csökkentése komoly szakmai vitákat generálhat, melyekre a hatósági oldalon nincs ráhatása. *Javaslom ágazati szakmai bizottságok létrehozását, jogszabályi háttérének kialakításával, a közvetlenebb, szakmai szempontból szélesebb kapcsolat a hatóságok munkáját és a szervezetek döntéshozatali rendszerét egyaránt támogatná.* (L.: 1.3. alfejezet)

A 2. fejezet részét képezte az EKT, az azzal kapcsolatos EKM és egyéb kockázatelemzési módszerek áttekintése. A szabályzók előírásait és a BM OKF weblapjáról letölthető EKT mintát elemezve megállapítottam, hogy a szükséges mértékben és jól kidolgozott EKT nem lehet egy önálló dokumentum. A jól kidolgozott EKT rendszerbe kell, hogy foglalja az adott kritikus szervezet összes működésre, üzemeltetésre, védelemre, veszély- és vészhelyzet elhárításra vonatkozó terveit, okmányait.

Az EKT egyik kiemelt melléklete az EKM, mely nagyon jó mintát ad a kritikus szervezetek részére a már azonosított kockázatok valószínűség/hatás szerinti elemzéséhez. Viszont a szabályzók és a minták ennél mélyebbre nem nyúlnak. Bár az EKM majdnem 90 példát ad a kockázatok lehetőségeire, a lista pedig bővíthető, de a kritikus szervezetek önálló kockázatazonosításához nem ad módszertant. A 2. fejezetben *javaslatot adtam a kockázatazonosításhoz alkalmazható különböző módszerekre.*

Az 1. fejezetben a jogszabályokat, a 2. fejezetben az azonosítási és kijelölési folyamatot elemezve igazoltam, hogy a függőségek elemzésére már sokkal nagyobb hangsúlyt helyeznek, de az interdependencia mélyebb elemzésére módszertan nem található. *Meghatároztam az interdependencia különböző dimenzióit és területeit,* mellyel összevetve a szabályzókat és

mintákat megállapítottam, hogy *a hazai szabályzók és minták vagy túl általánosan, vagy mindössze az egyirányú, közvetlen, technológiai dependencia vizsgálatokra fókuszálnak. Ezzel alátámasztottam az interdependenciára vonatkozó kutatói hipotézisemet.*

A 3. fejezetben a kritikus szervezetek és infrastruktúrák fizikai védelmének részleteit tekintetem át. A kritikus szervezetek létesítményeinek és infrastruktúráinak környezetében, a fizikai tér zónákra osztásával vizsgáltam a megközelíthetőség és a mozgások kontrollálására és korlátozására alkalmazható elveket, technikai eszközöket és módszereket, figyelembe véve a napjainkban kiemelt figyelmet érdemlő drónok elleni védelmet.

Több kijelölt kritikus szervezet és infrastruktúra, valamint védett létesítmény vizsgálatával *megállapítottam, hogy a fizikai védelmi követelményeknek való megfelelés jelentősen függ a kritikus szervezet, infrastruktúra adott fizikai környezetétől, a szervezet tagjainak tudásától és – több esetben – a kijelölt kritikus szervezet anyagi erőforrásaitól.* A kritikus szervezetté történő kijelölést követően a megközelíthetőség, a biztonsági technológiák, a megemelt védelmi szint kialakítása komoly tervezési nehézségeket okozhat a szervezet részére, ha a közvetlen környezet már sűrűn beépített vagy az anyagi források a nagyberuházások tekintetében korlátozottak.

Megállapítottam, hogy amennyiben *figyelembe vesszük az átfogó védelem összetevőit és a fizikai védelem kiépítésének szükséges elemeit, mindemellett megvizsgáljuk a kritikus szervezetek ágazati és fizikai tulajdonságait, jól látható, hogy jelentős eltérések mutatkoznak a védendő létesítmények és infrastruktúrák jellemzői között,* ezért csak komoly tervezéssel, beruházással és folyamatos fejlesztéssel valósítható meg a hatékony, a kritikus szervezet képességeivel arányos, az ellenálló képesség megfelelő szintjét támogató fizikai védelem.

A 3. fejezet alapján *igazoltam, hogy szükség van részletesebb módszertani útmutatásra a védelmi tervek elkészítéséhez és fejlesztéséhez,* mivel a kritikus szervezetek biztonsága nem csupán technikai vagy adminisztratív kérdés, hanem komplex, rendszerszintű feladat, amely a szervezet teljes működését érinti.

A kritikus szervezetek és infrastruktúrák fizikai védelmének megfelelő szintű kialakítása érdekében, a megközelíthetőség és a létesítményvédelmi elvek figyelembe vételével *kidolgoztam a kritikus szervezetek létesítményeinek Fizikai Védelmi Tervét,* részletezve az egyes alfejezeteinek tartalmi felépítését.

A 4. fejezet központi célja annak vizsgálata volt, hogy hogyan lehet a kritikus szervezetek ellenálló képességének és fizikai védelmi rendszerének hatékonyságát növelni az emberi és adminisztratív tényezők fejlesztésével.

A biztonsági környezet változik, a védelmi módszerek és eszközök fejlődnek, ebből következik, hogy a jogszabályokban előírt kötelezettségek teljesítése önmagukban nem garantálják az ellenálló képesség növekedését, sőt, amennyiben a szervezeten belüli szereplők nem rendelkeznek a megfelelő ismeretekkel az emelt szintű üzemeltetéshez, úgy a szinten tartáshoz sem elegendők. A kritikus szervezetek vezetői szintjétől az operatív szinten dolgozó munkavállalókig rendelkezniük kell a munkakörükhöz megfelelő mélységű ellenálló képességi ismeretekkel (követelmények, védelmi tervek, eljárásrendek, stb.) annak érdekében, hogy az adott szervezet kritikus szervezatként képes legyen funkcionálni.

A hatályos jogszabályok és a jelenleg elérhető, kritikus szervezetekre vonatkozó képzések elemzésével megállapítottam, hogy *a kritikus szervezetek ellenálló képességének szinten tartásához és fejlesztéséhez nem elegendő az előírt képzések teljesítése, a rendszerben való gondolkodás és védelmi tudatosság csak a szervezetek belső felkészítési rendszerének kialakításával érhető el.*

Egy felkészítési rendszer kialakításához több szakirodalom is rendelkezésre áll, melyek mélyen tárgyalják a képzési struktúra felépítését, kialakítását, működtetését, de a kritikus szervezetek sajátosságait figyelembe vevő, az ellenálló képességre vonatkozó módszertani ajánlások jelenleg nem érhetőek el. Egy teljes, komplex felkészítési rendszer kialakítása és működtetése komolyabb erőforrásokat igényel, ezért fontos, hogy olyan módszereket és felkészítési eszközöket, támogató elemeket adjunk a kritikus szervezetek kezébe, melyek az ellenállóképességi szintjükkel arányos és hatékony.

A kritikus szervezetekre szabott felkészítési rendszer bemutatása mellett, a 4. fejezetben kiemeltem két olyan támogatási lehetőséget, mely a védelmi tevékenységekbe való integrálást is elősegítik:

Javaslom, hogy jogszabály írja elő a kritikus szervezetek részére hierarchikus dokumentációs rendszer fenntartását, melybe a felkészítési rendszer dokumentációs elemei is bekerülnek.

A belső felkészítési rendszer eredményeinek mérése és a felkészítésből, eredmények hasznosításából befolyó tapasztalatok feldolgozása is fontos része a felkészítési rendszernek, hiszen a belső felkészítésekre igénybe vett anyagi erőforrások, illetve a felkészítések alkalmazhatósága ezzel válnak hitelesítetté, jogossá.

Javaslom, hogy a belső felkészítési rendszer ellenőrzési metódusa is részét képezze a központi ellenőrzési folyamatnak.

A megfelelően felépített és folyamatosan fejlesztett belső felkészítési rendszer, dokumentációs hierarchia, értékelési és tapasztalat feldolgozási rendszer jelentős időt és ezzel költséget is megtakaríthat a kritikus szervezet részére, az ellenálló képesség fejlesztése során.

ÚJ TUDOMÁNYOS EREDMÉNYEK

1. Azonosítottam a kritikus szervezetek és kritikus infrastruktúrák kijelölési folyamatában és támogatásában lehetséges fejlesztési irányokat, melyek alapján javaslatot tettem a hatályos jogi szabályzók tartalmi módosítására.
2. Meghatároztam a kritikus szervezetek és infrastruktúrák interdependenciájának dimenzióit, figyelemmel a kritikus szervezetek és infrastruktúrák jellemzőire.
3. Kidolgoztam a kritikus szervezetek és infrastruktúrák interdependencia vizsgálatának gyakorlatban alkalmazható módszerét.
4. Kidolgoztam a kritikus szervezetek és kritikus infrastruktúrák jellemzőit figyelembe vevő fizikai védelmi terv elkészítéséhez szükséges metodikát és a Fizikai Védelmi Terv tartalmi elemeit.
5. Kidolgoztam a kritikus szervezetek személyi állományának belső felkészítésére vonatkozó képzési alapelveket, metodikát és a hozzá kapcsolódó képzési program mintát.
6. Meghatároztam a kritikus szervezetek belső felkészítését támogató dokumentációs hierarchia és ellenőrzési rendszer kialakításának alapelveit.

AJÁNLÁSOK, KUTATÁSI EREDMÉNYEK ALKALMAZÁSI LEHETŐSÉGEI

A kutatás eredményei a kritikus szervezetek biztonságával foglalkozó több szereplő számára is kínálnak alkalmazási lehetőségeket, módszertani és szervezeti fejlesztési irányok megfogalmazásával. Meglátásom szerint a jogszabályi megfelelés és a tényleges ellenálló képesség között különbség figyelhető meg, mely a szereplők közötti kommunikáció kiszélesítésével javítható.

A kutatás a kritikus szervezetek üzemeltetői számára támogatást adhat az Ellenálló Képességi Terv fejlesztése és a védelmi dokumentációk (ezen belül a fizikai védelem) rendszerszintű

felülvizsgálatához, a szervezeti dokumentációs struktúra egységesítéséhez, az azonosítható kockázatok és a kritikus szervezetek közötti interdependencia mélyebb feltárásához, valamint a reziliencia növelését célzó fejlesztési programok kialakításához. Az eredmények különösen hasznosak lehetnek azok számára, akik a kijelölést követően szembesülnek a megnövekedett követelmények gyakorlati megvalósításával és felmerülő költségeivel.

A kutatás kiemelt jelentőséggel bír az ellenálló képességért felelős vezetők és a szervezet biztonsági szakemberei számára is. A bemutatott módszertani megközelítés alapot ad belső képzési programok kidolgozásához vagy továbbfejlesztéséhez, a vezetői és operatív szintű felkészítési rendszerek kialakításához, rendszeres gyakorlatok és visszacsatolási mechanizmusok bevezetéséhez, valamint a szervezeti biztonságtudatosság erősítéséhez. Fontos kiemelni, hogy a védelem módszerei és technológiai fejlesztése mellett az emberi tényező a szervezeti ellenálló képesség egyik meghatározó eleme, mely fejlesztése elkerülhetetlen.

A kutatási eredmények a hatóságok és szabályozó szervek számára is hasznosíthatók. Az elemzés hozzájárulhat további módszertani útmutatók és szakmai ajánlások kidolgozásához, a hatósági ellenőrzések szakmai tartalmának fejlesztéséhez, a konzultációs és támogató rendszerek bővítéséhez.

A képző intézmények és szakmai továbbképzési szervezetek számára a kutatás alapot nyújthat a képzések tananyagának fejlesztéséhez, szakmai tréningek kialakításához, ágazatspecifikus oktatási programok kidolgozásához. Ez különösen indokolt a kritikus szervezetekkel szemben támasztott, folyamatosan bővülő reziliencia- és biztonsági követelmények miatt.

Az eredmények alkalmazhatók továbbá ágazati és szakmai szervezetek együttműködésében is. Az interdependencia elemzések támogatják az ágazati reziliencia fejlesztését, a közös válságkezelési együttműködést.

6. ALKALMAZOTT RÖVIDÍTÉSEK

1	BM	Belügyminisztérium
2	BM OKF	Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság
3	CEPS	Centre for European Policy Studies
4	CIP	Critical Infrastructure Protection
5	CIWIN	Critical Infrastructure Warning Information Network
6	CLA	Check List Analysis
7	COVID19	coronavirus disease 2019
8	CSIRT	Computer Security Incident Response Team
9	DNS	Domain Name System
10	DRP	Disaster Recovery Plan
11	ECI	European Critical Infrastructure
12	EKM	ellenálló képességi mátrix
13	EKT	Ellenálló Képességi Terv
14	ENISA	European Network and Information Security Agency
15	EPCIP	European Programme for Critical Infrastructure Protection
16	ETA	Event Tree Analysis
17	EU	Európai Unió
18	FMEA	Failure Mode and Effects Analysis
19	FTA	Fault Tree Analysis
20	FVT	Fizikai Védelmi Terv
21	HAZOP	Hazards and Operability
22	HM	Honvédelmi Minisztérium
23	IHR	Integrált Hatósági Rendszer
24	IKT	Információs és Kommunikációs Technológia
25	KIV	Kritikus Infrastruktúra Védelem
26	Kszetv.	2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről
27	Kszetv.vr.	474/2024. (XII: 31.) Korm. rendelet a kritikus szervezetek ellenállóképességéről szóló törvény végrehajtásáról
28	LOPA	Layer of Protection Analysis
29	Lrtv.	A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről” szóló 2012. évi CLXVI. törvény
30	Lrtv.vr.	A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről” szóló 2012. évi CLXVI. Törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. Rendeletet
31	NATO	North Atlantic Treaty Organisation
32	NIPP	National Infrastructure Protection Plan
33	NIS	Network and Information Systems Directive
34	NKIV	Nemzeti Kritikus Infrastruktúra Védelem
35	PESTEL	Political, Economic, Social, Technological, Environmental, Legal - analysis
36	SWOT	Strengths – Weakness – Opportunities – Threats

37	TÁMOP	Társadalmi Megújulás Operatív Program
38	ÜBT	Üzemeltetői Biztonsági Terv
39	VBÖ	A védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény
40	VBÖ.vr.	Az ország védelme és biztonsága szempontjából jelentős szervezetek ellenálló képességéről szóló 475/2024. (XII. 31.) Korm. rendelet

7. ÁBRJEGYZÉK

1. sz. ábra	Kritikus szervezetek kijelölési folyamata
2. sz. ábra	Kockázati mátrix felépítése
3. sz. ábra	EKM felépítése
4. sz. ábra	SWOT analízis
5. sz. ábra	A kockázatelemzés ciklikussága
6. sz. ábra	Az interdependencia dimenziói
7. sz. ábra	A budapesti Amerikai Nagykövetség külső zónája
8. sz. ábra	Védett parkoló védőfallal
9. sz. ábra	Biztonsági gyorskapu
10. sz. ábra	Süllyesztett hidraulikus útzár
11. sz. ábra	Balpro hidraulikus kapuelem védelmi üzemmódban
12. sz. ábra	Megerősített biztonsági kerítés
13. sz. ábra	MI analizáló szoftverrel támogatott biztonsági kerítés
14. sz. ábra	Raptor nagy hatótávolságú földi radar és EO/IR megfigyelő
15. sz. ábra	Biometrikus azonosítóval ellátott beléptető rendszer
16. sz. ábra	Modern, többretegű ellenőrző-áteresztő rendszer
17. sz. ábra	Egyirányú személyi beléptető zsilip folyosó
18. sz. ábra	Iron Beam nagyteljesítményű lézeres légvédelmi rendszer
19. sz. ábra	Átfogó védelem elemeinek egymásra épülése
20. sz. ábra	Dokumentum hierarchia szintjei
21. sz. ábra	A felkészítés rendszere
22. sz. ábra	A belső felkészítés végrehajtásának folyamata

8. FELHASZNÁLT IRODALOM

- [1] 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.
- [2] 161/2019. (VII. 4.) Korm. rendelet a közlekedési létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.
- [3] 1993. évi XCIII. törvény a munkavédelemről
- [4] 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról.
- [5] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
- [6] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- [7] 2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről
- [8] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról
- [9] 2112/2004. (V. 7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól
- [10] 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- [11] 249/2017. (IX. 5.) Korm. rendelet az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- [12] 330/2015. (XI. 10.) Korm. rendelet a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- [13] 359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről
- [14] 360/2013. (X. 11.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- [15] 374/2020. (VII. 30.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

- [16] 375/2020. (VII. 30.) Korm. rendelet egyes kiberbiztonsági tárgyú és egyéb kormányrendeletek módosításáról
- [17] 375/2021. (VI. 30.) Korm. rendelet az egyes hatósági eljárásokat érintő egyszerűsítések érdekében szükséges kormányrendeletek módosításáról
- [18] 474/2024. (XII. 31.) Korm. rendelet a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról
- [19] 512/2013. (XII. 29.) Korm. rendelet az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről
- [20] 540/2013. (XII. 30.) Korm. rendelet a létfontosságú agrárgazdasági rendszerlemek és létesítmények azonosításáról, kijelöléséről és védelméről. (p. 4)
- [21] 541/2013. (XII. 30.) Korm. rendelet a létfontosságú vízgazdálkodási rendszerlemek és vízi létesítmények azonosításáról, kijelöléséről és védelméről. (p. 4)
- [22] 65/2013. (III. 8.) Korm. Rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról. (p. 1)
- [23] Alexander, C., Johansson, J. és Rydén Sonesson, T. (2021) Governance and interdependencies of critical infrastructures. *Sweden Safety Science*, 142.
- [24] Ált/24 Magyar Honvédség Kiképzési Doktrína. (2013) Magyar Honvédség kiadványa, Budapest
- [25] Antal Ö. (2014): Az épületek védelmének korszerű lehetőségei házi készítésű robbanóeszközök ellen. *Műszaki Katonai Közlöny*, (XXIV./1), 107-119.
- [26] Argonne National Laboratory (2015): ANL/GSS-15-4 *Analysis of Critical Infrastructure Dependencies and Interdependencies*
- [27] Az Európai Közösségek Bizottsága (2005) COM(2005) 576 végleges, *Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról*. Brüsszel.
- [28] Az Európai Közösségek Bizottsága (2006) COM(2005) 786 végleges, *A Bizottság közleménye a létfontosságú infrastruktúrák védelmére vonatkozó európai programról*. Brüsszel.
- [29] Az Európai Közösségek Bizottsága COM(2004) 702 végleges, *Critical Infrastructure Protection in the fight against terrorism*. (2004) Brüsszel

- [30] Az Európai Unió Tanácsa (2008) *2008/114/EK irányelv, Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről...* Brüsszel.
- [31] Bakos, F. (1978) *Idegen szavak és kifejezések szótára*. Budapest: Akadémiai Kiadó.
- [32] Balogh, Zs. (2013) *Katonai objektumok robbantásos cselekmények elleni védelmének lehetőségei*. PhD értekezés. Budapest; NKE
- [33] Báthy, S. (2015) A létfontosságú rendszerelemek védelmének jelentősége a honvédelem rendszerében. *Katonai Logisztika*, 23(1), 5-11.
- [34] Bleszity J., Kátai-Urbán L., Vass Gy. (2024): A kritikus infrastruktúra védelmi felsőoktatási tapasztalatok a kritikus szervezetek ellenállóképességéről szóló szabályozás tükrében. *Polgári Védelmi Szemle*, 2024. évi Különszám 220-236.
- [35] Bognár, B. et al. (2015) *Létfontosságú rendszerek és létesítmények védelme, Kézikönyv...* Budapest: NKE.
- [36] Bognár, B., Kátai-Urbán, L. és Vass, Gy. (2014) A létfontosságú rendszerek és létesítmények védelméről szóló szabályozás végrehajtása Magyarországon. *Bolyai Szemle*, 23(2), 105–112. o.
- [37] Bonnyai, T. (2014) *A kritikus infrastruktúra védelem elemzése a lakosságfejlesztés tükrében*. Doktori értekezés. Budapest: NKE.
- [38] Boruzs H. (2024): Physical protection characteristics of critical infrastructures Hungary – the armed security guard. *Biztonságtudományi Szemle*, IV/1., 41-52.
- [39] *Critical Foundations, Protecting America's Infrastructures: The Report...* (1997) USA
- [40] Dalicsek I., Répás S. (2015): Az információbiztonsági kockázatelemzés módszertani kérdései a kritikus infrastruktúra elemeket üzemeltető szervezetek esetében. *Pro Publico Bono*, (4), 22-33.
- [41] Daruka, N. (2013) *A bűnös célú/terror jellegű robbantások és az ellenük való védekezés lehetőségei*. Doktori értekezés. Budapest: NKE.
- [42] Drót L. (2022): *A Magyar Honvédség békeműveleti tapasztalat-feldolgozási rendszere és továbbfejlesztési lehetőségei*. Doktori értekezés. Budapest: NKE.
- [43] Engler, Á. (2015) A közúti áruszállítás szerepe a kritikus infrastruktúrában. *Hadmérnök*, 10(2), 148-159.
- [44] *European Security Strategy* (2009) Brüsszel.

- [45] Fiath A. (2025): Vállalati kockázatkezelés komplex rendszere. *Humán Innovációs Szemle*. XVI. évf. 2025/2. 107-118.
- [46] Generisk Kft. *HAZOP, Hibafa, Eseményfa, Hibamód és hatáselemzés*. (<https://www.generisk.hu/hibafa-HAZOP-esemenyfa.html>) Letöltés: 2025.07.01.
- [47] Giannopoulos, G., Filippini, R. és Schimmer, M. (2013) *Risk assessment methodologies for Critical Infrastructure Protection*. JRC Scientific and Policy Reports
- [48] Gyarmati, J. (2013) Kritikus infrastruktúra kockázatának modellezési lehetőségei. *Bolyai Szemle*, 22(1), 51–62. o. (p. 5)
- [49] Haig, Zs., Hajnal, B. et al. (2009) *A kritikus információs infrastruktúrák meghatározásának módszertana*. ENO Advisory Kft. (p. 5)
- [50] Haig, Zs. és Kovács, L. (2012) *Kritikus Infrastruktúrák és kritikus információs infrastruktúrák*. Budapest: NKE. (p. 5)
- [51] Hammerli, B. (2010) *Protecting critical infrastructure in the EU*. Brussels, CEPS Task Force Report
- [52] Hart S., Ramsay, J. D. (2011): Guide for Homeland Security Instructors Preparing Physical Critical Infrastructure Protection Courses. *Homeland Security Affairs* (<https://www.hsaj.org/articles/59>) Letöltés: 2024.02.03.
- [53] Horváth, A. (2009) A vasúti közlekedés terrorfenyegetettségének jellemzői a városokban. *Hadmérnök*, 4(3), 180-189.
- [54] Horváth, A. (szerk.) (2013) *Fejezetek a kritikus infrastruktúra védelemből. Kiemelten a közlekedési alrendszer*. Budapest, MHTT
- [55] Joydeep B., Das A., Sen A. (2017): A Survey of Interdependency Models for Critical Infrastructure Networks. *Arxiv.org*. (<https://arxiv.org/abs/1702.05407>) Letölés: 2025.11.15.
- [56] Károlyi, L. (2007) *A kritikus infrastruktúrák védelme és az operatív erők tevékenységirányítása...* Doktori értekezés. Budapest: ZMNE.
- [57] Kelly T. K., Peerenboom, J. P., Rinaldi, S. M. (2001): Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, 11–25.
- [58] Kovács F. (2005): Az infrastruktúra kritikus elemeinek felmérése, védelmének és helyreállításának megszervezésére vonatkozó intézkedési javaslatok. *Gazdasági és Közlekedési Minisztérium (GKM)*, Budapest.

- [59] Kovács F. (2006): Defence of the critical infrastructure. New Challenges in the Field of Military Sciences 2006 : 4th International Scientific Conference, Budapest, Magyarország, ZMNE *Bolyai János Katonai Műszaki Főiskolai Kar.* (<http://hadmernok.hu/kulonszamok/newchallenges/kovacs.html>)
- [60] Kovács F. (2011): Repülőterek és légiirányítás a kritikus infrastruktúra részeként. *Repüléstudományi közlemények.* Ludovika Egyetemi Kiadó, XXIII:2. online konferencia kiadvány
- [61] Kovács F. (2024): A kritikus infrastruktúra stratégiai szerepe az orosz-ukrán háborúban. *Hadtudomány*, 34:3, pp 29-39.
- [62] Kovács F.; Román Zs. (2016): Épületek robbantás elleni védelmének szabályozási kérdései. *Műszaki Katonai Közlöny*, XXVI : 3. pp. 93-104., 11 p.
- [63] Kovács F. (2008): A kritikus infrastruktúrák elméleti alapjai. *IVB Innovációs klubnap*, oktatási anyag.
- [64] Kovács F. (2008): A kritikus infrastruktúra biztonsági kérdései. *Gazdasági és Közlekedési Minisztérium (GKM)*, Budapest.
- [65] Kovács F. (2008): Európai szempontból létfontosságú hazai közlekedési infrastruktúrák elemzése: tanulmány. *Gazdasági és Közlekedési Minisztérium (GKM)*, Budapest.
- [66] Kovács T. (2012) A katonai táborok biztonsági rendszereinek kialakítása, különös tekintettel a robbantásos merényletek megelőzésére, azok hatásai csökkentésére. *Műszaki Katonai Közlöny*, (XXII./3), 70-83.
- [67] Kovács T. (2013) A katonai táborok biztonsági rendszereinek kialakítása, különös tekintettel a robbantásos merényletek megelőzésére, azok hatásai csökkentésére. II. *Műszaki Katonai Közlöny*, (XXIII./1), 36-50.
- [68] Kovács T. (2013) A katonai táborok biztonsági rendszereinek kialakítása, különös tekintettel a robbantásos merényletek megelőzésére, azok hatásai csökkentésére. III. *Műszaki Katonai Közlöny*, (XXIII./2), 122-133.
- [69] Kovács, Z. (2012) Fontos létesítmények IED elleni védelme. *Műszaki Katonai Közlöny*, (k), 35-44. o. (p. 8)
- [70] Kovács, Z. (2013) Katonai objektumok IED elleni védelmének lehetséges technikai megoldásai. *Műszaki Katonai Közlöny*, (2), 114-125. o. (p. 8)
- [71] Kovács, Z. (2016) Physical perimeter security of military facilities. *Bolyai Szemle*, 79-89. o. (p. 13)

- [72] Kovács, Z. (2016) Barriers for physical protection of military facilities... *Vojenská Reflexie*, 86-99. o. (p. 13)
- [73] Kresalek P. (2014): A vállalati ellenőrzés alapjai. Oktatási segédanyag. (https://www.kodolanyi.hu/konyvtar/images/tartalom/File/kiadvanyok/a_vallalati_ellenorzes_alapjai.pdf) Letöltés: 23025.10.10.
- [74] Łukasiewicz J., Kobaszyńska – Twardowska A. (2022): Proposed method for building an anti-drone system for the protection of facilities important for state security. *Security and Defence Quarterly*, 3/2022 vol. 39.
- [75] Mógor J., Földi, L. és Solymosi, J. (2008) Lépések a kritikus infrastruktúra védelmének magyarországi szabályozása felé. *Hadmérnök*, 3(4), 15-28.
- [76] Mórocz Á. és Pellérdi, R. (2013) A metró, mint kritikus infrastruktúra. *Hadmérnök*, 8(3), 101–110.
- [77] Munk S. (2008) A kritikus infrastruktúrák védelme információs támadások ellen. *Hadtudomány*, 18(1-2), 95-106.
- [78] Nagy R. (2006) A kritikus infrastruktúra védelme és katasztrófavédelmi aspektusai a terrorizmus tükrében. *Kard és toll*, 7(3), 56-64.
- [79] Nagy R. (2011) *A kritikus infrastruktúra védelme elméleti és gyakorlati kérdéseinek kutatása*. Doktori értekezés. Budapest: ZMNE.
- [80] Nagy R.; Halász L. (2008): Monitorink és lakossági riasztó rendszer és a kritikus infrastruktúra-védelem összefüggései. *Hadmérnök*, 3(2)
- [81] *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets* (2003) USA
- [82] *NIPP 2013 - Partnering for Critical Infrastructure Security and Resilience*. (2013) USA.
- [83] Padányi J. (2006) A katonai műveletek terrorvédelme. *Nemzetvédelmi Egyetemi Közlemények*, (3), 200-205. o.
- [84] Padányi J. (2023): A katonai műveletek hatása a környezetre. *Hadtudomány*. 33. E-szám. 1-19.
- [85] Petit F., Lewis L. P. (2019): Critical infrastructure interdependency analysis – Operationalising resilience strategies. UNDRR, Letöltés: 2026.02.26. https://www.preventionweb.net/files/66506_f415finallewisandpetitcriticalinfra.pdf

- [86] Petruska F. (2025): Mesterséges intelligencia: Tanulmánykötet a mesterséges intelligencia gyakorlati alkalmazásáról. *NKE Közigazgatási Továbbképzési Intézet*. Budapest
- [87] Petruska F. (2018): A terrorfenyegetettség EU trendjei az EUROPOL vonatkozó jelentése alapján. *Katonai Jogi és Hadijogi Szemle*, 6/1. 121-139.
- [88] Potóczy Gy. (2010): Áttekintés a kritikus infrastruktúra védelem jelen helyzetéről, a továbblépést nehezítő tényezők elemzése útján. *Hadmérnök*, 5(2), 203-218.
- [89] Potóczy Gy. (2015) *A postai szolgáltatások biztonsága és a kritikus infrastruktúra védelem korszerű követelményei a postai liberalizáció tükrében*. Doktori értekezés. Budapest: NKE.
- [90] Précsényi Z.; Solymosi J. (2007): Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé. *Hadmérnök*, 2(1), 65-76.
- [91] Précsényi, Z. és Solymosi, J. (2008) Kritikus infrastruktúrák azonosítása: körkép az EU-ban és az USA-ban tapasztalható nehézségekről. *Hadmérnök*, 3(1), 59-69.
- [92] ProMan Consulting (2020). *Kockázatelemzés módszertana, a kockázatmenedzsment fogalma*. (<https://promanconsulting.hu/kockazatkezeles-kockazatmenedzsment/>)
Letöltés: 2025.09.18.
- [93] Rácz L. (2012): Kritikus infrastruktúra védelem hazai és nemzetközi szabályozási rendszere. *Hadmérnök*, 7(2), 166-172.
- [94] RAND research organization. *Delphi Method*. (<https://www.rand.org/topics/delphi-method.html>)
- [95] Renda A. (2010) *Protecting critical infrastructure in the EU*. Centre for European Policy Studies.
- [96] Ronyecz L. (2016): Létfontosságú rendszerek és létesítmények védelmével kapcsolatos nemzetközi tapasztalatok vizsgálata, azok integrálásának lehetőségei hazai rendszerben. *Műszaki katonai Közlöny*, 26(2), 197-209.
- [97] Szabó S., Kovács T., Kovács Z. (2007): Korszerű műszaki technikai eszközök I. *Bolyai Szemle*, 16(1).
- [98] Szabó S., Kovács, Z. (2014): Improvizált robbanóeszközök hatásai ellen történő védelem „Defencell” készlettel. *Műszaki Katonai Közlöny*, 41-53.

- [99] Szabó S., Tóth R. (2013): Repülőterek kialakítása, létesítményeinek kritikus elemei, védelmük lehetséges műszaki megoldásai. *Repüléstudományi Közlemények*, XXV. évfolyam, 2. szám. 89-113.
- [100] Szamosi B. (2014): Kockázatértékelési elméletek alkalmazhatósága a kritikus infrastruktúrákra. *Bolyai Szemle*. XXIII. 2014/2. 66-74.
- [101] **Székely Cs.** (2014). A környezeti kockázatok kezelése. *Gazdaság & Társadalom* 2014/1., 15-28.
- [102] Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara (2023). *Kockázatértékelési módszerek és lehetőségeik a fizikai védelem területén.* (<https://szakmaikamara.hu/kockazattertekelesi-modszerek-es-lehetosegeik-a-fizikai-vedelem-teruleten/>) Letöltés: 2025.09.20.
- [103] Varga P. (2012): *Kritikus információs infrastruktúrák vezeték nélküli hálózatának védelme*. Doktori értekezés. Budapest: NKE.
- [104] Vass A., Maros D., Berek, L. (2015): Az interdependencia kérdése az energetikai rendszer és a híradástechnika esetén a kritikus infrastruktúrák biztonsága védelmében. *Bolyai Szemle*, 24(3), 9-32.

9. SZERZŐ PUBLIKÁCIÓS JEGYZÉKE

- [1] Bakos, T. (2017) ‘A honvédelmi létfontosságú rendszerelemek azonosításáról és kijelöléséről I.’, *Hadmérnök*, 12(1. különszám), pp. 234–240.
- [2] Bakos, T. (2018a) ‘A hadi mozgás- és manőverakadályozás kialakulása, fejlődése’, *Műszaki Katonai Közlöny*, 28(1), pp. 319–334.
- [3] Bakos, T. (2018b) ‘A mozgásakadályozó tevékenység hatása az illegális migráció útvonalainak változásaira’, *Műszaki Katonai Közlöny*, 28(3), pp. 213–232.
- [4] Bakos, T. (2018c) ‘Létfontosságú rendszerelemek megközelíthetősége, adott létfontosságú rendszerelem megközelíthetőségi elemzése’, *Műszaki Katonai Közlöny*, 28(1), pp. 335–352.
- [5] Bakos, T. (2021) ‘Physical Protection of Military Camps’, *Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata*, 31(E-szám), pp. 186–193.
- [6] Bakos, T. (2022) ‘Kijelölt létfontosságú rendszerelem védelme a pandémiás veszélyhelyzet idején’, in Földi, L. (szerk.) *Szemelvények a katonai műszaki tudományok eredményeiből III*. Budapest: Ludovika Egyetemi Kiadó, pp. 13–26.

- [7] Bakos, T. (2023a) ‘Katonai műszaki-technikai újdonságok a MILENG COE 2022-es ipari napján I. rész’, *Haditechnika*, 57(3), pp. 37–43.
- [8] Bakos, T. (2023b) ‘Katonai-műszaki-technikai újdonságok a MILENG COE 2022-es ipari napján II. rész’, *Haditechnika*, 57(4), pp. 28–32.
- [9] Bakos, T. (2023c) ‘NATO-követelmények a rögtönzött robbanóeszközök elleni tevékenység (C-IED) kiképzésében’, *Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata*, 33(2), pp. 17–29.
- [10] Bakos, T. (2024) ‘A létfontosságú rendszerek azonosításáról, kijelöléséről és védelméről szóló hatályos magyar jogi dokumentumok’, *Műszaki Katonai Közlöny*, 34(Különszám), pp. 217–231.
- [11] Bakos, T. és Kapusza, B. G. (2023) ‘A Magyar Honvédség új hídvető képessége – Leopard 2 Leguan’, *Műszaki Katonai Közlöny*, 33(1), pp. 41–51.
- [12] Bakos, T. és Kovács, F. (2025) ‘Az interdependencia dimenziói és a kritikus szervezetek vizsgálata’, *Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata*, 35(3), pp. 106–119.
- [13] Ember, I., Bakos, T. és Kugyela, L. (2021) ‘Moduláris betonfal alkalmazási lehetőségei a robbanás elleni védelemben’, *Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata*, 31(3), pp. 77–90.
- [14] Kovács, Z., Dénes, K., Ember, I. és Bakos, T. (2022) ‘Európai Bölény: a WiSENT 2 többrendeltetésű műszaki gép’, *Műszaki Katonai Közlöny*, 32(2), pp. 25–41.
- [15] Mező, A. és Bakos, T. (2015) ‘Új szótár segíti a magyar nemzeti katonai terminológia egységes használatát’, *Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata*, 143(4), pp. 119–124.

MELLÉKLETEK

1. SZÁMÚ MELLÉKLET

A magyarországi kritikus infrastruktúrákkal kapcsolatos korábbi, hatálytalan jogszabályok részletes összefoglalója

Az 1. fejezetben tárgyalt, mára hatálytalan szabályzók kibővített összefoglalója alapja lehet további kutatásoknak, rávilágíthat olyan részletekre, melyek az új szabályozásból már kimaradtak.

Magyarország Kormányának 2080/2008. (VI. 30.) Korm. határozata a Kritikus Infrastruktúra Védelem Nemzeti Programjáról – Zöld könyv

2008-ban került kiadásra a 2080/2008. (VI. 30.) kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról, mely fontos mérföldkőként tartalmazta a Kritikus Infrastruktúra Nemzeti Programjáról szóló Zöld Könyvet. A kormányhatározat példa értékűen teszi meg az Európai Unió Tanácsának 2008/114/EK irányelve alapján meghatározott lépéseket. Legfelső szinteken határozza meg a felelősöket, többszereplős konzultációkat rendel el az ágazatok részére, elrendeli a hazai infrastruktúra létfontosságú elemeinek védelméről szóló részletes szabályozási koncepció összeállítását, figyelembe véve a hazai, az európai és a NATO szabályzókat, az üzemeltetők és tulajdonosok alkotmányos kötelezettségeit és kiemelten a honvédelem szempontjából fontos, kritikus infrastruktúra védelmére vonatkozó követelményeket.

A kormányhatározat 1. melléklete – maga a Zöld Könyv – alapként szolgált a további konzultációk és feladatok végrehajtásához. Fő célkitűzése, hogy biztosítsa a nemzeti kritikus infrastruktúrák védelméről szóló nemzeti program megvalósítását, a jogszabályi környezet megalkotását, összegezze a kormányzati szereplők nemzeti kritikus infrastruktúrák védelmére vonatkozó álláspontját. Fontos eleme, hogy először definiálja a kritikus infrastruktúrák fogalmát és határozza meg a lehetséges ágazatok körét.

A Kritikus Infrastruktúra fogalma a Zöld Könyv szerint:

„Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.

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.”

A nemzeti kritikus infrastruktúrák védelmében három főbb szintet céloztak meg:

4. **Megelőzés és védelem**, a legnagyobb kockázatú elemek beazonosításával, a kockázatok csökkenthetőségének elemzésével és védelmi intézkedések alkalmazásával;
5. **Felkészülés és jelzés**, az infrastruktúra tulajdonosok és üzemeltetők, valamint az állami szervek megfelelő felkészítésével;
6. **Üzemfolytonosság és ellenálló képesség biztosítása**, a működés visszaállíthatóságára, helyettesíthetőségre vonatkozó képességek, intézkedések tervezésével, fejlesztésével, bevezetésével.

A „következmény alapú kritikusság” megközelítés alapját a következmények elfogadható mértékének meghatározása képezi (*kis hatású, komoly zavar, válsághelyzet*), amely a következő kategóriák szerint elemezhető:

- **kiterjedés szerint**: a veszteség földrajzi terület szerint értelmezhető;
- **súlyosság**: nincs hatás, minimális, mérsékelt vagy jelentős hatással járó zavar. A súlyosság meghatározásánál az is fontos tényező, hogy mely területet érinti a zavar.

Ezek alapján a Zöld Könyv megkülönböztet:

- Társadalmi hatást: érintett lakosság száma;
 - Gazdasági hatást: a gazdasági veszteség jelentősége;
 - Környezeti hatás: a környezetre gyakorolt zavar, kár mértéke;
 - Politikai hatást: állam és intézményei iránti bizalom csökkenése;
 - Közegészségügyi hatást: áldozatok, betegségek, súlyos sérülések száma;
 - Pszichológiai hatást: pl. vásárlói magatartás, általános viselkedés megváltozása;
 - Kölcsönös függőségi hatást: az interdependenciák erőssége, száma;
 - Alternatívák vizsgálatát: adott infrastruktúra elem nem, vagy csak nehezen helyettesíthető.
- **időbeli hatás**: arra vonatkozik, hogy egy adott infrastrukturális elemmel kapcsolatos veszteség mennyi idő elteltével fejthet ki jelentős hatást, illetve a zavar mennyi ideig kezelhető komoly hatás nélkül.

A Zöld Könyv a kritikus infrastruktúrákat veszélyeztető tényezők körét három főbb csoportba osztotta:

- szándékos cselekmények,

- természeti eredetű veszélyek,
- civilizációs, technológiai veszélyek,

valamint kiemeli, hogy támogatja az EPCIP megközelítést, vagyis alapelveként kezeli a minden fajta veszéllyel szembeni védelemre való felkészítést terrorizmus prioritással. Emellett a nemzeti Kritikus Infrastruktúra Védelem (a továbbiakban: KIV) Programjának kidolgozása és végrehajtása során a következő alapelveket határozta meg:

- **szubszidiaritás:** a tulajdonosok és az üzemeltetők felelőssége, hogy saját létesítményeik védelmét megtervezzék és arra vonatkozóan döntéseket hozzanak. a Kormányzatnak elemző, szabályozó, ellenőrző és támogató szerepe van;
- **kiegészítő jelleg:** a KIV kiegészíti a fennálló ágazati biztonsági intézkedéseket, szabályozási struktúrákat, nem azonos a fennálló veszélyhelyzet kezelés és beavatkozás rendszerével;
- **rugalmasság:** folyamatos felülvizsgálatot igénylő program, a mindenkori változásokra és kihívásokra gyorsan reagálni képes;
- **arányosság:** a védekezési stratégiák és intézkedések arányosak a mindenkori veszéllyel, melyet megfelelő kockázatkezelési módszerekkel lehet elérni. Így – ideális esetben – a védelem nem ró aránytalanul nagy terheket a szereplőkre;
- **finanszírozás:** a védelemmel kapcsolatos intézkedések finanszírozása a közreműködő szereplők felelőségi és érdekeltségi szintjéhez igazodik, figyelemmel a megállapított kockázati prioritásokra, ugyanakkor arányban áll a szereplők pénzügyi lehetőségeivel;
- **titkosság:** a kritikus infrastruktúrák védelmére vonatkozó információk cseréjének alapja a bizalom és a titkosság, mivel bizonyos információk felhasználhatók a létesítmények működésének megzavarására;
- **horizontális és ágazati megközelítés:** minden miniszter a hatáskörébe tartozó ágazat tekintetében önállóan felel az Nemzeti KIV-ben foglalt feladatai ellátásért, az ágazati feladatok végrehajtásának koordinációjáért;
- **szereplők közötti együttműködés:** valamennyi jogszabályban megszólított szereplő részt vesz a kritikus infrastruktúrák védelmében. Meghatározott feladataival és felelősségével összhangban valamennyi szereplőnek együtt kell működnie, és hozzá kell járulnia a Nemzeti KIV kidolgozásához és végrehajtásához.

A Zöld Könyv egycsatornás koordinációs és döntéshozatali mechanizmust javasolt, melyhez meghatározta a különböző szereplők főbb feladatait. Így a Kormány, a későbbiekben kijelölésre kerülő központi NKIV koordináló szerv, az államigazgatási szervek, valamint a tulajdonosok

és üzemeltetők legfőbb feladatait, a teljes kritikus infrastruktúra azonosítási, kijelölési folyamat végrehajtása érdekében, valamint a kijelölt kritikus infrastruktúra elemek védelmének fejlesztésében, illetve a folyamatos kapcsolattartás érdekében. Ezek a feladatok a végrehajtás sorrendjében:

7. fogalmak tisztázása, a keretrendszer alapjainak lefektetése, mely nem eredményezhet párhuzamos szabályozást, ütközést a hatályos jogszabályokkal;
8. szektorelemzés, ágazati fogalmak, kritériumok meghatározása;
9. interdependencia elemzés;
10. kockázatelemzés, veszélyanalízis;
11. védelmi intézkedések tervezése, bevezetése;
12. a végrehajtás ellenőrzése, értékelése.

Mindezekon felül a határozat elrendeli a CIWIN-hez történő csatlakozás lehetőségeinek vizsgálatát is. A Zöld Könyv felveti a lehetőségét egy CIWIN hálózathoz kapcsolható, de önálló nemzeti, bizalmas információkezelésre alkalmas, fokozott védelmet élvező informatikai és hírközlési rendszer működtetését.

1249/2010. (XI. 19.) számú, „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” szóló határozat

Az előző pontban tárgyalt kormányhatározat és a Zöld Könyv alapján a nemzeti kritikus infrastruktúrák védelmével kapcsolatos szakértői munka megkezdődött. Az Európai Unió Tanácsának 2008/114/EK tanácsi irányelve alapján az európai kritikus infrastruktúrák védelmével kapcsolatos ügyekben kapcsolattartó pont kijelölése volt szükséges. A 1249/2010. (XI. 19.) számú kormányhatározat a belügyminisztert jelölte ki az európai kritikus infrastruktúra védelem nemzeti kapcsolattartójaként és annak koordinációjára, valamint az Európai Bizottság részére évente küldendő jelentés elkészítésére.

Ennek érdekében felhatalmazta, hogy a 2008/114/EK tanácsi irányelv alá tartozó ágazatok felelős minisztereivel együtt megbeszéléseket, egyeztetéseket folytasson más tagállamok kapcsolattartóival és az Európai Bizottsággal.

Emellett elrendelte egy szakmai munkacsoport létrehozását, az európai és a nemzeti kritikus infrastruktúrák azonosításához szükséges kritériumrendszert kidolgozása, valamint a

potenciális európai kritikus infrastruktúrák azonosításának és kijelölésének felülvizsgálata érdekében. A szakmai munkacsoport tagjainak jelölte ki:

- a belügyminisztert;
- a nemzeti fejlesztési minisztert;
- a nemzetgazdasági minisztert;
- a közigazgatási és igazságügyi minisztert;
- a honvédelmi minisztert;
- az Alkotmányvédelmi Hivatal képviselőjét;
- a Magyar Energia Hivatal képviselőjét;
- a Magyar Kereskedelmi és Engedélyezési Hivatal képviselőjét;
- a Nemzeti Biztonsági Felügyelet képviselőjét;
- a Nemzeti Közlekedési Hatóság képviselőjét;
- a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF) képviselőjét;
- az Országos Rendőr-főkapitányság képviselőjét;
- a Terrorelhárítási Központ képviselőjét.

A kormányhatározat külön pontban rendelte el a honvédelmi érdekből kritikus infrastruktúrák védelmére vonatkozó intézmény- és követelményrendszer kidolgozását, melyért a honvédelmi minisztert tette felelőssé.

A nemzeti fejlesztési miniszter részére külön feladatokként intézkedik az azonosított európai kritikus infrastruktúrák kijelölésére, az azonosításhoz és kijelöléshez szükséges jogszabályok felülvizsgálatára és – amennyiben szükséges – módosítására, illetve ehhez kapcsolódó kritikus infrastruktúra védelmi konzultációs fórum felállítására, melyen a kormányzati szereplőkön kívül a kijelölt kritikus infrastruktúrák üzemeltetői és tulajdonosai is részt kell, hogy vegyenek.

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

Az előző pontban tárgyalt kormányhatározat alapján létrehozott munkacsoport a nemzeti „Zöld Könyv”, az európai és nemzeti irányelvek, valamint konzultációk és több éves szakmai munka eredményeképpen megalkotta a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényt, mely a kihirdetést követő negyedik hónapban, 2013. március elsején lépett hatályba.

A törvény pontosítja az alapfogalmakat, és meghatározza az ágazatokat, a nemzeti, illetve az európai létfontosságú rendszerelemekkel kapcsolatos kijelölés vagy visszavonás folyamatát, az általános javaslattevő hatóság feladatát, valamint a folyamathoz kapcsolódó feltételeket.

A törvény alkalmazásában – többek között – a következő fogalmak kerültek meghatározásra:

- **ágazati kritérium:** azok a szempontok, az azokhoz tartozó küszöbértékek, műszaki vagy funkcionális tulajdonságok, amelyek egy eszköz, létesítmény rendszerelemének megzavarása vagy megsemmisítése (a továbbiakban együtt: kiesés) által kiváltott hatásra vonatkoznak, és amelyek teljesülése esetén az eszköz, létesítmény, rendszer vagy azok része létfontosságú rendszerelemmé jelölhető ki azzal szoros összefüggésben, hogy mely ágazatba tartozik;
- **horizontális kritérium:** 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;
- **létfontosságú rendszerelem védelme:** a létfontosságú rendszerelem funkciójának, folyamatos működésének és sértetlenségének biztosítását célzó, a fenyegetettség, a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányuló valamennyi tevékenység;
- **létfontosságú rendszerelem:** az 1. mellékletben meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához - így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, - és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna;
- **nemzeti létfontosságú rendszerelem:** e törvény alapján kijelölt létfontosságú rendszerelem, amelynek kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt elsősorban Magyarországon lenne jelentős hatással;

- **üzemeltető:** az a természetes, jogi személy vagy jogi személyiség nélküli szervezet, aki vagy amely az eszköz, létesítmény, rendszer rendszerelemének tulajdonosa, engedélyese, rendelkezésre jogosultja vagy napi működéséért felelős.

A későbbiekben, az (EU) 2016/1148 (NIS) irányelv megjelentését követően, többször is módosításra, pontosításra kerültek az alapfogalmak, illetve új fogalmak kerültek a törvény értelmező rendelkezései közé²¹²:

- **alapvető szolgáltatás:** a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához szükséges, elektronikus információs rendszertől függő, az alapvető szolgáltatások jegyzékében feltüntetett szolgáltatás;
- **alapvető szolgáltatások jegyzéke:** az alapvető szolgáltatások listája, amely az érintett központi államigazgatási szervek bevonásával kerül összeállításra és kormányrendeletben meghatározásra;
- **alapvető szolgáltatást nyújtó szereplő:** az a szervezet vagy gazdasági szereplő, amely
 - o alapvető szolgáltatást nyújt,
 - o az általa nyújtott alapvető szolgáltatás elektronikus információs rendszerektől függ,
 - o az általa nyújtott alapvető szolgáltatást érintő biztonsági esemény - kormányrendeletben meghatározott - jelentős zavart okozna szolgáltatás nyújtásában és
 - o az erre irányuló eljárásban alapvető szolgáltatást nyújtó szereplőként került azonosításra;
- **helyszíni ellenőrzést lefolytató szerv:** az ágazati kijelölő hatóság, a szakhatóság, a kijelölési eljárásban részt vevő, véleménynyilvánító szerv, és jogszabály alapján helyszíni ellenőrzés lefolytatására jogosult szerv;
- **rendkívüli esemény:** olyan külső vagy belső behatás, amely a kijelölt nemzeti vagy európai rendszerelem rendeltetésszerű működését, üzemfolytonosságát jelentős mértékben veszélyezteti, akadályozza, és amely megfelel jogszabályban foglalt kritériumoknak.

Az európai létfontosságú rendszerelem fogalmát még 2021-ben pontosították²¹³, mely alapján – a korábbi megfogalmazástól eltérően – a kijelölés a nemzeti létfontosságú rendszerelemek köréről veszi alapul:

²¹² 2020. évi XXXI. törvény 123. §.

²¹³ 2021. évi L. törvény 28. § (1).

- **európai létfontosságú rendszerelem:** nemzeti létfontosságú rendszerelemmé kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős hatással lenne - az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve - legalább két tagállamra.

A törvény részletesen tárgyalja a nemzeti létfontosságú rendszerelemek azonosításának és kijelölésének, valamint az azonosítás vagy kijelölés visszavonásának teljes folyamatát, megadva a lépéseket és a különböző lépések és feladatok egymáshoz viszonyított határidejét.

2020-tól kezdődően új paragrafusokként kerültek be a törvénybe – illetve több alkalommal módosultak is – a nemzeti létfontosságú rendszerelemek körén belül kiemelt védelmet igénylő „*alapvető szolgáltatásokat nyújtó szereplők*” kijelölésére és nyilvántartására vonatkozó rendelkezések, valamint a nemzeti és az európai létfontosságú rendszerek kijelölésének, nyilvántartásának és ellenőrzésének részletesebb, egyéb kritériumokkal kiegészített szabályai. Ezen részleteket az értekezés 2. fejezetében fejtem ki bővebben.

A 2020. évi XXXI. törvény módosító rendelkezései alapján több változás is bekerült a Lrtv. szövegébe.

A Lrtv. ágazatokat és alágazatokat tartalmazó 1. melléklete is kiegészült illetve módosult:

- az energia ágazat alágazatai közé bekerült a távhő szolgáltatás;
- az egészségügy ágazatnál az aktív fekvőbetegek ellátása alágazat kiegészült a működtetésükhöz szükséges szolgáltatásokkal;
- Infokommunikációs technológiáknál korábban megtalálható vezetékes és vezeték nélküli elektronikus hírközlési szolgáltatások, vezetékes és vezeték nélküli hírközlő hálózatok, rádiós távközlés, űrtávközlés alágazatok helyére – összefoglaló megnevezéssel – az elektronikus hírközlési szolgáltatások, elektronikus hírközlő hálózatok alágazat került.

Az Lrtv. végrehajtásához és az ágazatok szabályozásához kapcsolódó kormányrendeletek

A Lrtv. megszabta az ágazatokra vonatkozó, azok speciális szabályait és ágazatspecifikus kiegészítő rendelkezéseit meghatározó ágazati kormányrendeletek megalkotását. Lefontosabb céljuk az ágazati kritériumok kidolgozása, a résztvevő hatóságok konkrét megnevezése és alapfeladataik meghatározása. Az Lrtv. által meghatározott 10 ágazat vonatkozásában végül kilenc ágazati kormányrendelet készült el.

Meg kell jegyezni, hogy a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról szóló 474/2024. (XII. 31.) Korm. rendelet hatálytalanította az ágazatok létfontosságú rendszerelemeinek azonosításáról és kijelöléséről szóló kormányrendeleteket, de szakmaiságuk okán érdemes részletesen áttekinteni ezeket a jogszabályokat, mivel helyettesítésük jelenleg²¹⁴ még nem történt meg.

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

Az Lrtv.vr. a 2012. évi CLXVI. törvény végrehajtásának legfontosabb támogató eleme. A kormányrendeletet 2020.²¹⁵ és 2021.²¹⁶ években bővítették és módosították, mely az előző pontban tárgyalt 2012. évi CLXVI. törvény módosításait, kiegészítéseit volt hivatott követni, illetve az azonosítási és kijelölési folyamat részletesebb leírásával és kiegészítéseivel a hatósági és az üzemeltetői oldal kommunikációját támogatta.

A végrehajtás érdekében a Kormányrendelet újabb fogalmakat definiált a törvényben megfogalmazottakat kiegészítve:

- **azonosítás:** az a folyamat, amely során a lehetséges létfontosságú rendszerelemeket kockázatelemzés, valamint az ágazati és horizontális kritériumok alapján meghatározzák;
- **azonosítási vizsgálat:** az a folyamat, amelynek eredményeképpen az üzemeltető magára vonatkoztatva, az ágazati és horizontális kritériumok teljesülésének lehetőségét elemezve és értékelve azonosítási jelentésében nemzeti vagy európai létfontosságú rendszerelemmé történő kijelölésre, a kijelölés visszavonására vagy a kijelölés fenntartására vonatkozó javaslatot tesz;
- **kockázatelemzés:** fenyegetettségi és kockázati tényezők vizsgálata a rendszerelemek sebezhetőségének, valamint a megzavarásuk vagy megsemmisítésük által okozott következmények értékelése céljából.

Ahhoz, hogy egy rendszer vagy rendszerelem kijelölt létfontosságúként legyen nyilvántartva, az első lépés az azonosítási folyamat végrehajtása. A Kormányrendelet megadja az azonosítási

²¹⁴ 2025.01.30. nappal bezárólag

²¹⁵ 375/2020. (VII. 30.) Korm. rendelet

²¹⁶ 375/2021. (VI. 30.) Korm. rendelet

jelentés elkészítésének szabályait és annak tartalmát, kiemelve az alapvető szolgáltatások vizsgálatát is. Hivatkozik a BM OKF honlapjára is, mely további segítséget és a folyamathoz szükséges okmányokat, okmánymintákat is tartalmazza. Az azonosítási eljárást követi az a döntési folyamat, mely az adott rendszerlem létfontosságúvá történő kijelölésével, a folyamat kijelölés nélküli lezárásával vagy a kijelölés visszavonásával járhat.

Ki kell emelni, hogy a Kormányrendelet már a potenciális létfontosságú rendszerlem azonosítási folyamatában is biztonsági összekötő személy meglétét igényli, akinek képzési követelményeit és foglalkoztatásának feltételeit ugyancsak részletesen taglalta.

Az alapvető szolgáltatást nyújtó szereplőként való azonosítás, illetve törlés automatikusan kapcsolódik a nemzeti létfontosságú rendszerlem kijelölési folyamatához, de külön elemzést és eljárást igényel, melynek eredményeképpen az üzemeltetőt felveszik az alapvető szolgáltatásokat nyújtó szereplők jegyzékébe is.

A Kormányrendelet kötelezi a potenciális vagy kijelölt létfontosságú rendszerlem üzemeltetőjét, tulajdonosát, illetve a biztonsági összekötő személyt az Integrált Hatósági Rendszer (a továbbiakban: IHR) használatára. Az IHR alkalmas a teljes azonosítási és kijelölési folyamathoz szükséges adat- és okmánykezelésre, különböző bejelentésekre, hivatalos kapcsolattartásra és a Lrtv. szerinti bírság fizetési kötelezettségének teljesítésére is. Jogi és technológiai problémák elhárítását követően az IHR végül 2022. január 01. után volt elérhető Integrált Hatósági Ügyviteli Rendszer néven. 2024-ben az érvénybe lépő új jogszabályok alapján a portál már nem elérhető, mivel a hivatásos katasztrófavédelmi szervek egyes hatósági és szakhatósági hatáskörei a kormányhivatalokhoz kerültek.²¹⁷

A Kormányrendelet a kijelölt létfontosságú rendszerlemek védelmével kapcsolatban részletesen meghatározza az Üzemeltetői Biztonsági Terv elkészítésének szabályait és pontos felépítését, az ellenőrzésre és együttműködésre vonatkozó szabályokat és a nyilvántartás és adtakezelés alapvetőbb előírásait. Ezek a pontok bár elég pontos keretet adnak a védelem kialakításához, de a védelmi intézkedések konkrét tervezését az üzemeltető/tulajdonos kezébe adják, így ezek a tervek, illetve a megvalósítás erősen függ a kijelölt létfontosságú rendszerlem üzemeltetőjének/tulajdonosának anyagi lehetőségeitől, szakmai tudásától és hozzáállásától.

²¹⁷ <https://katasztrofavedelem.hu/36732/ihr-integralt-hatosagi-ugyviteli-rendszer-karbantartas> (letöltés: 2025.01.28.)

2020-ban kiegészített Kormányrendeletben²¹⁸ új pontként jelet meg a kijelölt létfontosságú rendszerelem üzemeltetéséhez kapcsolódó, kötelezően végrehajtandó, éves komplex gyakorlat. A komplex gyakorlatot a hivatásos katasztrófavédelmi szerv központi szerve rendeli el, és az ágazati hatóságokkal együtt ellenőrzi és minősíti a végrehajtását.

A Kormányrendelet mellékleteiben találhatóak meg az azonosítás és kijelölés folyamatához szükséges horizontális kritériumok adatai, melyek a következők:

1. **Veszteségek kritériumai:** pontosan számszerűsíti az adott idő alatt bekövetkezett halálesetek vagy súlyos sebesülések számát.
2. **Gazdasági hatás kritériumai:** pontosan számszerűsíti a gazdasági veszteség mértékét, a népesség és az egy főre eső bruttó nemzeti jövedelem százalékos arányában kifejezve.
3. **Társadalmi hatás kritériuma:** sűrűn lakott területen (több mint 300 fő/km²) a lakosságot káros pszichológiai és közegészségügyi hatás éri.
4. **Politikai hatás kritériumai:** a rendelet szerint ha *„az állam és intézményei iránti közbizalom megszűnése, valamely állami szerv működésképtelenné válása miatt a lakosság biztonságérzete kritikus szint alá csökken”*.
5. **Környezeti hatás kritériumai:** pontosan számszerűsíti a kimenekítés, kitelepítés minimális létszámát (10 000 fő), illetve a tartósan szennyezett terület nagyságát (100 km²), kiegészítve a természetes vizek, tájegységek, kiemelkedő területek *„negatív változásaival”*.
6. Jelentős változás a 375/2020. (VII. 30.) Korm. rendelet által bevezetett **védelem kritériuma**, mely figyelembe veszi a létfontosságú rendszerelem ellátási láncban betöltött szerepét, illetve sérülés, zavar esetén a mentés, kárfelszámolás, katasztrófák elleni védelem végrehajtására való komolyabb hatásait.

További mellékletek tartalmazzák az alapvető szolgáltatások jegyzékét, az Üzemeltetői Biztonsági Terv részletes felépítésének adatait és a hatósági eljárásokhoz kapcsolódó bírságok aktuális összegeit.

374/2020. (VII. 30.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

²¹⁸ 375/2020. (VII. 30.) Korm. rendelet

Az energetikai ágazat már 2013-ban kidolgozta a törvényben előírt kormányrendeletet.²¹⁹ A nemzetközi és hazai energetikai szabályozásban történt módosítások, a Lrtv. és a Lrtv.vr. tartalmában történt módosítások okán 2020-ban új energetikai vonatkozású kormányrendelet került kiadásra.

Az energetikai ágazathoz kapcsolódó létfontosságú rendszerek, rendszerelemek azonosítási, kijelölési folyamatában és védelmük kialakításában a Kormányrendelet a tulajdonosokat nem szólítja meg. Minden ehhez kapcsolódó jogosultság és feladat a villamosenergia-rendszer engedélyesét (engedéllyel rendelkező kezelőjét/üzemeltetőjét), a kőolaj és cseppfolyós szénhidrogén termékekhez kapcsolódó létesítmény üzemeltetőjét, a földgáz és gáz termékekhez kapcsolódó létesítmény rendszerüzemeltetőjét, illetve az ezekhez kapcsolódó technológiai hírközlési és informatikai rendszerek üzemeltetőit terheli.

Az energetikai ágazatban az ágazati kijelölő hatóság a következők szerint lett kijelölve:

- a villamosenergia, a földgáz és a távhő rendszerek tekintetében a Magyar Energetikai és Közmű-szabályozási Hivatal;
- a kőolajipar (kivéve a kőolajtermék-tárolást és kőolajfeldolgozást), illetve a földgáztermelés tekintetében a bányafelügyeleti hatáskörben eljáró Kormányhivatalok Bányászati Osztályai és Bányafelügyeleti Főosztálya²²⁰;
- a kőolajtermék-tárolás és kőolajfeldolgozás tekintetében a mérésügyi és műszaki biztonsági feladatkörében eljáró fővárosi és megyei kormányhivatalok, melyek irányítását a Magyar Kereskedelmi és Engedélyezési Hivatal gyakorolja.

A kormányrendelet az Lrtv.-ben meghatározott feltételeket kiegészítve, konkrétabb meghatározásokkal fogalmazza meg az *európai létfontosságú rendszerelemek ágazati kritériumait*, illetve külön pontban a *nemzeti létfontosságú rendszerelemek ágazati kritériumait*.

A villamosenergia-termelés, átviteli és elosztó hálózatok jellemző adataira építő ágazati kritériumok mellett kiemeli, hogy nemzeti létfontosságú rendszerelemként kell azonosítani minden olyan szervezetet vagy gazdasági szereplőt, mely érvényes akkreditációval rendelkezik Black Start szolgáltatás nyújtására, vagyis jelentős kiesés esetén fontos szerepe van az erőművek és villamosenergia rendszerek feszültségmentes állapotból történő visszaállításában. A villamosenergia-rendszerek biztonságával kapcsolatban nagyon fontos kapcsolódó

²¹⁹ 360/2013. (X. 11.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

²²⁰ <https://mbfsz.gov.hu/szakmai-kapcsolatok>

jogszabály a villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről szóló 280/2016. (IX. 21.) Korm. rendelet. Ez a kormányrendelet a villamosenergia-rendszerben fellépő krízisek és válsághelyzetek kezelésére ad utasításokat, megszólítva az energetikai politikai vezetést, az elektromosenergia gazdasági szereplői és az alapvető ipari felhasználókat is.

A kőolajipar és földgázszolgáltatás tekintetében az európai és nemzeti létfontosságú rendszerelemek ágazati kritériumai a szolgáltatás és kapacitás kiesésének időbeli és mennyiségi mutatóiból kerültek levezetésre.

A kormányrendelet röviden, de konkrétan meghatározott adattal rendelkezik a távhőrendszerről is. Nemzeti létfontosságú rendszerelemként kell azonosítani azt a rendszerelemet, mely kiesése legalább 20 000 felhasználó vagy díjfizető fűtési és melegvíz-célú felhasználását érinti.

Ahhoz, hogy egy energetikai szolgáltatót szükséges-e felvenni az alapvető szolgáltatást nyújtó szereplők jegyzékébe, a rendelet részletesen, konkrét értékekkel kiegészítve határozza meg a jelentős zavar mértékét, az energia ágazathoz tartozó küszöbértékeket, valamint a rendkívüli eseményekre vonatkozó részletes ágazati szabályokat.

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.) Korm. rendelet módosításáról

A rendelet a belügyminiszter közvetlen irányítása alá tartozó országos hatáskörű önálló szerveket külön nevesítve jeleníti meg és meghatározza a kijelölő és javaslattévő hatóságot.

Kijelölő hatóságként jelöli meg a hivatásos katasztrófavédelmi szervnek az üzemeltető telephelye szerinti területi szervét:

- az Alkotmányvédelmi Hivatal,
- a Nemzetbiztonsági Szakszolgálat,
- a Nemzeti Információs Központ,
- a Büntetés-végrehajtás Országos Parancsnoksága és szervei,
- a Nemzeti Védelmi Szolgálat,
- az Országos Rendőr-főkapitányság és szervei,
- az Országos Idegenrendészeti Főigazgatóság, valamint

- a Terrorelhárítási Központ vonatkozásában.

BM OKF és szervei vonatkozásában az általános rendőrségi feladatok ellátására létrehozott szervnek üzemeltető telephelye szerinti területi szervét jelöli meg, mint kijelölő hatóság.

Ágazati javaslattevő hatóságként BM OKF-t, a Büntetés-végrehajtás Országos Parancsnokságát, az Országos Rendőr-főkapitányságot jelöli meg, azon rendszer, létesítmény vonatkozásában, melynek üzemeltetőjét irányítja vagy felügyeli.

A Lrtv.vr. 3.§-a hivatásos katasztrófavédelmi szerv központi szervét jelöli meg általános javaslattevő hatóságként a közrend, közbiztonság, lakosságvédelem, alkotmányvédelem, nemzetbiztonság, terrorelhárítás szempontjaira tekintettel, de a rendvédelmi kormányrendelet ezt a jogkört elveszi:

- a BM OKF,
- az Alkotmányvédelmi Hivatal,
- a Nemzetbiztonsági Szakszolgálat,
- a Nemzeti Információs Központ,
- a Büntetés-végrehajtás Országos Parancsnoksága és szervei,
- a Nemzeti Védelmi Szolgálat,
- az Országos Rendőr-főkapitányság és szervei,
- az Országos Idegenrendészeti Főigazgatóság, valamint
- a Terrorelhárítási Központ vonatkozásában.

Ezen szervek tekintetében a kijelölő hatóság csak az üzemeltető kérésére, az üzemeltetési azonosítási jelentés tartalma, valamint a rendészeti kormányrendeletben megfogalmazott ágazati kritériumok alapján dönthet a kijelölésről. Ezek az ágazati kritériumok konkrét adatokat, mutatókat csak szűken tartalmaznak, egy adott szerv alapfeladatának kiesését, illetve a pótolhatóság idő intervallumát határozzák meg.

A közbiztonság-védelem ágazat létfontosságú rendszerei vonatkozásában az ellenőrzést koordináló és a helyszíni ellenőrzést lefolytató felelősként a katasztrófák elleni védekezésért felelős minisztert jelöli meg.

2016 után több módosítás is bekerült a kormányrendeletbe, melyek a belügyminiszter irányítása alá tartozó szervek szervezeti és alapfeladataikban történt változásokat követték le.

Jelentősebb kiegészítés a 375/2020. (VII. 30.) kormányrendelet alapján került be, mely meghatározza a Közbiztonság-védelem ágazatban rendkívüli esemény fogalmát és tartalmát.

A rendvédelmi kormányrendelet nem tartalmaz utasítást vagy feladatot az alapvető szolgáltatást nyújtó szereplők, vagy az Lrtv.vr. 3. mellékletét képező alapvető szolgáltatások jegyzékének vizsgálatára.

540/2013. (XII. 30.) Korm. rendelet a létfontosságú agrárgazdasági rendszerlemek és létesítmények azonosításáról, kijelöléséről és védelméről

Az agrár ágazat, az energetikai ágazathoz hasonlóan az Lrtv. kiadását követően azonnal megkezdte az ágazati kormányrendelet előkészítését és 2013-ban – 2014. január 01-i hatállyal – meg is jelent.

A rendelet értelmében az agrár ágazathoz tartozó létfontosságú rendszerlem kijelölését, illetve visszavonását – az üzemeltetőkön kívül – a vármegyei kormányhivatalok is kezdeményezhetik javaslattevő hatóságként, a Nemzeti Élelmiszerlánc-biztonsági Hivatal élelmiszerlánc-biztonsági és állategészségügyi hatósági hatáskörében, illetve a növény- és talajvédelmi hatósági hatáskörében eljárva. Az agrár ágazatot illetően kijelölő hatóságként a Nemzeti Élelmiszerlánc-biztonsági Hivatalt jelöli meg.

A nemzeti létfontosságú rendszerlemmé való kijelölésre az agráripár szereplőit külön pontokban említi meg, pontosan meghatározva a rájuk vonatkozó minimális kritérium tételeket:

- növényi és állati genetikai erőforrásokat megőrző génbank;
- vetőmag-előállító létesítmény;
- állati oltóanyag előállító és az oltóanyag-előállítás nélkülözhetetlen komponensének beszállítója;
- emlősállatok vágását és vágóhídi darabolását végző létesítmény;
- baromfihús feldolgozását, tartósítását végző létesítmény;
- hús-, baromfihús-készítmény gyártást végző létesítmény;
- egyéb gyümölcs-, zöldségfeldolgozást, tartósítást végző létesítmény;
- tejfeldolgozást végző létesítmény;
- malomipari termékek gyártását végző létesítmény;
- kenyér, friss pékáru gyártását végző létesítmény;
- termelést, illetve elosztást végző létesítmények;
- élelmiszer-kereskedelmi tevékenységet végző létesítmény;
- magas kapacitással rendelkező főzőkonyhát, valamint a nemzeti vagy európai létfontosságú rendszerlemként kijelölt kórház ellátását biztosító főzőkonyhát;

- és 2. kategóriájú állati eredetű melléktermék-feldolgozást végző létesítmény;
- Gazdaságbiztonsági Tartalékban vagy Állami Céltartalékban lévő készletek tárolását végző létesítmény.

A rendelet egy esetet emel ki európai létfontosságú rendszerelem kijelölésére:

Növényi genetikai erőforrásokat megőrző génbank akkor jelölhető ki európai létfontosságú rendszerelemnek, ha egy esetleges katasztrófahelyzet közvetlenül veszélyeztetné az egyedi és pótolhatatlan biológiai alapok megtartását, és a létfontosságú létesítmény legalább harmincezer, szőlő és gyümölcsstermő növények esetén legalább ötezer megőrzött tétellel rendelkezik.

A kijelölt létfontosságú rendszerelem biztonsági összekötő személynek az Lrtv.vr.-ben előírt képesítési követelményein kívül az adott létesítmény tevékenységéhez köthető végzettséggel is rendelkeznie kell, úgy mint mezőgazdasági, állatorvosi, élelmiszer kereskedelmi, logisztikai, vagy élelmiszer biztonsági képesítéssel.

2019-ben a rendelet 7. §-a módosult, ettől kezdve a Nemzeti Élelmiszerlánc-biztonsági Hivatalon kívül a vármegyei kormányhivatalok is lefolytathatják agrárgazdasági ágazat tekintetében a létfontosságú rendszerelem helyszíni ellenőrzését, élelmiszerlánc-biztonsági és állategészségügyi, illetve növény- és talajvédelmi feladatkörében eljárva.²²¹

2020-ban több kiegészítés és módosítás került a rendeletbe. Bekerült a sertés tartását végző létesítmények, illetve nem csak a kereskedelemmel, hanem a logisztikai feladatokkal foglalkozó létesítmények köre is. Külön pontban bekerült a rendeletbe az agrárgazdaság ágazatban rendkívüli esemény fogalma és mutatói.²²²

Az agrár kormányrendelet nem tartalmaz utasítást vagy feladatot az alapvető szolgáltatást nyújtó szereplők, vagy az Lrtv.vr. 3. mellékletét képező alapvető szolgáltatások jegyzékének vizsgálatára.

541/2013. (XII. 30.) Korm. rendelet a létfontosságú vízgazdálkodási rendszerelemek és vízlétesítmények azonosításáról, kijelöléséről és védelméről

A kormányrendelet a víz ágazat tekintetében javaslattevő hatóságként a területileg illetékes vízügyi igazgatóságot, a nemzeti és európai létfontosságú rendszerelem kijelölő hatóságként,

²²¹ 360/2019. (XII. 30.) Korm. rendelet 128. §.

²²² 375/2020. (VII. 30.) Korm. rendelet

valamint a helyszíni ellenőrzések lefolytatására jogosult hatóságként pedig a létesítmény szerint illetékes vízügyi hatóságot jelöli meg.

Pontjaiban részletesen meghatározza a létfontosságúként kijelölendő rendszerelemek ágazati kritériumait, és azok küszöbértékeit a következő területekre lebontva:

- ivóvíz-szolgáltatás:
 - felszíni ivóvízbázisként üzemeltetett tározó,
 - felszíni és felszín alatti vízbázisra telepített víztisztító mű,
 - ivóvíztároló medence,
 - közműves ivóvízellátást biztosító víziközmű-rendszer,
 - gazdasági célú ivóvízhasználatot végző üdítőital, ásványvíz gyártó,
- szennyvízelvezetés és -tisztítás:
 - szennyvíztisztító telep,
 - közműves szennyvízelvezetést és -tisztítást biztosító víziközmű-rendszer,
- vízkárelhárítás:
 - kiemelt jelentőségű vízilétesítmény,
 - elsőrendű árvízvédelmi vízilétesítmény.

Az európai létfontosságú rendszerelemként való kijelölés kritériumait hasonló területek alapján tárgyalja, melyekben kiemelt rész, ha Magyarországon kívül még egy szomszédos állam is érintett lehet.

2020-ban kiegészítésként került be kormányrendeletbe, hogy amennyiben egy közműves ivóvíz szolgáltató teljesíti az ágazati követelményeket, abban az esetben a az Lrtv.vr. alapján alapvető szolgáltatást nyújtó szereplőként is azonosítani kell. Ehhez kapcsolódóan a kormányrendelet új pontban fejt ki a víz ágazatra vonatkozó rendkívüli esemény fogalmát.²²³

2021-ben pontosították a vízgazdálkodási létesítmény üzemeltetője által foglalkoztatott biztonsági összekötő személy végzettségét, mely szükség szerint szakági mérnöki, vagy „biztonsági összekötő személy” szakirányú végzettséget jelent.²²⁴

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

²²³ 375/2020. (VII. 30.) Korm. rendelet

²²⁴ 375/2021. (VI. 30.) Korm. rendelet

Az egészségügyi kormányrendelet a pontos értelmezés érdekében bevezeti a közepes és magas biztonsági kategóriákat, illetve a mikrobiológiai vagy egyéb biológiai anyag, valamint toxin fogalmát és az ehhez kapcsolódó kutatáshoz, fejlesztéshez, gyártáshoz, kísérletezéshez szükséges műszaki-technológiai támogatás fogalmát.

Javaslattevő hatóságokként több szervezetet is megjelöl, a hozzájuk tartozó alapfeladatoktól függően:

- Országos Kórházi Főigazgatóság,
- Országos Mentőszolgálat,
- Országos Vérellátó Szolgálat,
- országos tisztifőorvos,
- Országos Gyógyszerészeti és Élelmezés-egészségügyi Intézet,
- Nemzeti Egészségbiztosítási Alapkezelő.

Az egészségügyi kormányrendelet kijelölő hatóságként nem konkrét szervet, szervezetet, hanem az egészségügyért felelős minisztert jelöli meg, illetve elrendeli az adott azonosítási, kijelölési folyamatra egy 9 tagból álló döntés-előkészítő bizottság létrehozását. A bizottság tagjait a miniszter, illetve a különböző egészségügyi alapfeladatokért felelős államtitkárok delegálják, megbízásuk három évre szól.

Nemzeti létfontosságú rendszerelemek kijelölésének ágazati kritériumait, és azok küszöbértékeit a következő területekre vonatkoztatva adja meg:

- aktív fekvőbeteg-ellátó, illetve annak telephelyei (kórházak),
- mentésirányítási központok,
- Állami Egészségügyi Tartalék nyilvántartó és tároló rendszerei,
- országos vér- és transfuziológiai készleteket nyilvántartó és tároló rendszerei,
- közepes vagy magas biztonsági szintű laboratóriumok,
- referencialaboratóriumok,
- gyógyszer-nagykereskedelmi tevékenységet végző gazdálkodó szervezetek.

A kormányrendelet értelmében európai létfontosságú rendszerelemek ágazati kritériumai hasonló területekre vonatkoznak, de maga a rendszerelem magasabb küszöbértékeket teljesít.

A rendelet létfontosságú rendszerelem azonosítási vizsgálatra kötelez minden kórházat, mentésirányítást végző szervezetet, Állami Egészségügyi Tartalék kezelőt, állami vérvérvétel

kezelőt és minden olyan laboratóriumot, mely a 21/2013. (I. 30.) Korm. rendelet²²⁵ alapján bejelentésre kötelezett, valamint azon gyógyszer-nagykereskedelmi tevékenységet végző szervezetet, melyek teljesítik az ágazati kritériumokban megadott rájuk vonatkozó küszöbértékeket.

A biztonsági összekötő személy vonatkozásában a kormányrendelet az egészségügyi ágazat az adott szakterületekre vonatkozó szakképzettséget ír elő, a „biztonsági összekötő személy” szakképzettség nem jelenik meg a követelmények között.

A kormányrendelet az Üzemeltetési Biztonsági Terv elkészítésére is tartalmaz kiegészítő rendelkezéseket. Az egészségügyi szakterületek vonatkozásában kapcsolódó résztervek elkészítését követeli meg, úgy mint:

- a közművek kiváltására, alternatív működtetésére vonatkozó tervet,
- a szükséges, elengedhetetlen szolgáltatások biztosítására vonatkozó tervet,
- az élelmezési tervet,
- a gyógyszerek, fogyóeszközök, vér- és vérkészítmények pótlási tervét,
- mikrobiológiai vagy egyéb biológiai anyag, valamint toxin kijutása esetén alkalmazandó válságtervet,
- beléptetés regisztrálására, az illetéktelen személy belépésének megakadályozására vonatkozó tervet,
- kommunikációs tervet.

Ellenőrzést lefolytató szervként a kórházak és laboratóriumok tekintetében a népegészségügyi feladatkörében eljáró fővárosi és vármegyei kormányhivatalt, a többi szakterület vonatkozásában az egészségügyért felelős miniszter alá tartozó ellenőrzési feladatokat ellátó szervezeti egységet jelöli meg.

2020-ban jelentős módosítás és kiegészítés került az egészségügyi kormányrendeletbe is. A módosítások lekövezték a szervezeti változásokat és újabb fejezeteket iktattak be. Így új fejezetet képez az egészségügyi ágazatban minősített rendkívüli események fogalma és típusai.

Új fejezetként került be az alapvető szolgáltatásokkal kapcsolatos jelentős zavar mértéke, mely hasonlóan az előzőekhez, egészségügyi szakterületenként adja meg a küszöbértékeket. A rendelkezés szerint minden kórház, mentésirányítási központ, Állami Egészségügyi Tartalék

²²⁵ 21/2013. (I. 30.) Korm. rendelet a bakteriológiai (biológiai) és toxin-fegyverek kifejlesztésének, előállításának és tárolásának megtiltásáról és e fegyverek megsemmisítéséről szóló egyezményből eredő nyilatkozattételi kötelezettségek végrehajtásáról és az ellenőrzés rendjéről

kezelő szervezet, vérkészlet kezelő szervezet és gyógyszer nagykereskedelmi gazdálkodó szervezet mely létfontosságú rendszeremmé lett kijelölve, egyben egészségügyi ágazatba tartozó alapvető szolgáltatást nyújtó szereplőként is azonosítandó.

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

A pénzügyi ágazat 2015-ben adta ki Lrtv. által megkövetelt kormányrendeletet. A jogszabály szűk terjedelemben rendelkezik a pénzügyi ágazat kötelezően kijelölendő szereplőiről, mely szerint a javaslattevő, valamint a helyszíni ellenőrzést lefolytató szervezet a Magyar Nemzeti Bank, mint felügyelet. Kijelölő hatóságként a pénz-, tőke- és biztosítási piac szabályozásáért felelős minisztert jelöli meg.

A minisztert a kijelölés folyamatában egy hat tagból álló döntéshozó bizottság segíti, melynek elnökét a miniszter kéri fel, tagjait pedig az általa vezetett minisztérium kormánytisztviselői közül jelöli ki. A bizottság tagjainak legalább egy éves szakmai gyakorlattal kell rendelkezniük a pénzügyi ágazat valamely területén.

A nemzeti vagy európai létfontosságú rendszerem azonosításának és kijelölésének kritériumaként a Lrtv.vr.-ben meghatározott horizontális kritériumokra hivatkozik. A rendelet szerint létfontosságú rendszeremként azonosítandó:

- állami tulajdonban lévő szakosított hitelintézet,
- pénzügyi, befektetési szolgáltatást végző intézmények fizetéseképtelensége esetén kártalanítási funkciót betöltő, magyarországi székhelyű betétbiztosítási vagy befektetés-biztosítási rendszer,
- készpénzellátás folyamatosságát alapvetően elősegítő, Magyarországi székhellyel rendelkező vállalkozás,
- Magyarországi székhellyel rendelkező, legalább 10%-os piaci részesedéssel rendelkező hitelintézet,
- fizetési, illetve értékpapír-elszámolási rendszerekben történő teljesítés véglegességéről szóló 2003. évi XXIII. törvény 9. §-a szerinti eljárásban a Magyar Nemzeti Bank által kijelölt rendszerüzemeltető,
- hatékony tőkeáramlás, tőkeértékelés, az árfolyam és egyéb kockázat megosztása érdekében a tőzsdei termékek keresletét és kínálatát koncentráló, azok kereskedését

lebonyolító, a nyilvános árfolyam-alakulást elősegítő magyarországi székhellyel rendelkező vállalkozás

amennyiben az intézet vagy szervezet vonatkozásában a horizontális kritériumok bekövetkezésének legalább egy lehetősége fennáll. A jogszabály külön pontban rendelkezik a Magyar Nemzeti Bank nemzeti és európai létfontosságú rendszerelemmé történő kijelölhetőségéről is.

A biztonsági összekötő személy részére felsőfokú közgazdasági, műszaki, informatikai, rendészeti, katasztrófavédelmi vagy jogi végzettséget ír elő.

2020-ban két új pont került a kormányrendeletbe, melyek röviden bevezetik a pénzügyi ágazatra vonatkozó, alapvető szolgáltatásokkal kapcsolatos jelentős zavar és rendkívüli esemény lehetséges fajtáit. Ezen zavarok és események a normál ügymenet, a bank- és fizetési titok, az informatikai rendszer adatkezelés, számlavezetés, elektronikus banki ügyintézés sérülésére, illetve bizonyos időre történő leállítására vonatkoznak.

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

A honvédelmi ágazat által kiadott kormányrendelet elveiben eltér az eddig tárgyalt ágazati rendeletektől. Egyedüli módon arra is lehetőséget ad, hogy más ágazatokhoz tartozó rendszerelemek honvédelmi érdekből történő kijelölését a honvédelmi ágazat kezdeményezze. A honvédségi szervek kezdeményezhetik saját üzemeltetésű, honvédségi rendszerelemek és más ágazatok által üzemeltetett, ágazaton kívüli rendszerelemek azonosítását és kijelölését is honvédségi létfontosságú rendszerelemként.

A kormányrendelet a honvédelmi ágazaton belüli létfontosságú rendszerelemekkel kapcsolatban javaslattevő hatóságként, kijelölő hatóságként, nyilvántartó hatóságként, helyszíni ellenőrzést lefolytató szervként és az ellenőrzést koordináló szervként is a Honvédelmi Minisztériumot (a továbbiakban: HM) jelöli meg. Kiemeli, hogy az elektronikus információs hálózatok, hadiipari gyártás és szolgáltatás tekintetében figyelembe kell venni a kapcsolódó felügyeleti hatóságok véleményét.

A biztonsági összekötő személy képesítési követelményeiként a honvédelmi ágazathoz tartozó rendszerelemnél katonai felsőfokú végzettséget és legalább 2 éves szakmai tapasztalatot ír elő

a rendelet, honvédelmi ágazaton kívüli rendszerelem tekintetében pedig az illetékes ágazatra vonatkozó szakképzettséget.

A nemzeti létfontosságú rendszerelemek honvédelmi ágazati kritériumai olyan létesítményekre, infrastruktúrára, eszközökre vagy szolgáltatásokra vonatkoznak, melyek kiesése a honvédelmi ágazat működésképtelenségét, súlyos zavarát vagy képességvesztését okozzák és kiemelten szerepelnek az országvédelmi tervekben, a Befogadó Nemzeti Támogatás feladataiban, a NATO magyarországi szövetségi rendszerében vagy a NATO Válságreagálási Rendszerrel összhangban álló Nemzeti Intézkedési Rendszerben. Ebbe a körbe tartozhatnak azon elemek is, melyek stratégiai fontosságú gyártó, javító, tároló, elosztó, ellátási vagy egyéb kapacitást képviselnek és nem helyettesíthetők a készenlétfokozás rendszerét szabályozó tervekben meghatározott időn belül.

Az ágazaton belüli honvédelmi létfontosságú rendszerelemek ellenőrzését éves ellenőrzési tervhez köti, azzal a kitéttel, hogy minden rendszerelem legalább 5 évente ellenőrzésre kerüljön. Az ágazati ellenőrzést koordináló szerv a helyszíni ellenőrzésbe a HM vagyonfelügyeleti és védelemgazdasági szervezeteit, a Magyar Honvédség illetékes szervezeti egységeit, illetve az ellenőrizendő rendszerelemhez kapcsolódó egyéb felügyeleti szerveket is bevon. Fontos pont, hogy az ellenőrzés során megállapított hiányosságok megszüntetésére irányuló intézkedésekről az üzemeltetőnek 60 napon belül tájékoztatnia kell az ágazati ellenőrzést koordináló szervet.

A kormányrendelet külön pontban tartalmazza a honvédelmi ágazaton kívüli honvédelmi létfontosságú rendszerelemek azonosításának, kijelölésének és ellenőrzésének szabályait. Két esetet különböztet meg a rendelet honvédelmi létfontosságú rendszerelemként történő kijelölésre.

Első esetben a rendszerelem még nem lett kijelölve létfontosságú rendszerelemként más ágazat által, de honvédelmi szempontból kijelölése indokolt. Ebben az esetben javaslattevő hatóságként, kijelölő hatóságként, ellenőrzést koordináló szervként, valamint nyilvántartó hatóságként is a HM jár el.

Második esetben a rendszerelem már kijelölésre került más ágazatban, de az adott ágazat kritériumai szerinti kijelölés nem biztosítja megfelelő szinten a honvédelmi érdekek maradéktalan érvényesülését. Ebben az esetben egy új fogalmat vezet be a kormányrendelet, az ún. kettős kijelölés fogalmát. Kettős kijelölés esetén a honvédelmi ágazat kijelölő hatósága is kijelöli külön határozatban a rendszerelemet, illetve a honvédelmi ágazat is nyilvántartásba

veszi. Kettős kijelölésű létfontosságú rendszerem helyszíni ellenőrzését a honvédelmi ágazat és az illetékes ágazat kijelölt szervei összehangolva hajtják végre. Fontos megjegyezni, hogy a nemzeti szabályozás nem enged – a honvédelmi ágazat kivételével – kettős kijelölést.

Az elmúlt években a honvédelmi ágazati kormányrendelet több ízben is módosításra került. Több apró változtatás a jogszabályi környezet változásait hivatott lekövetni, de bekerült a rendeletbe a honvédelmi létfontosságú rendszeremet érintő rendkívüli esemény és a honvédelmi létfontosságú elektronikus információs rendszerem fogalma is. Mivel a Lrtv.vr. 2020-ban történt módosítása már részletesen tartalmazza az Üzemeltetői Biztonsági Terv felépítését, ezért a honvédelmi ágazati rendeletből ezek az ágazati kiegészítő követelmények kikerültek.

2020-ban egy fontos kiegészítés került a rendeletbe.²²⁶ Honvédelmi létfontosságú rendszeremet gyorsított eljárásban is ki lehet jelölni, akár a honvédelmi ágazaton belüli vagy kívül eső rendszerem esetén is. Az eljárás megindításának nem feltétele az üzemeltető által elkészített azonosítási jelentés, helyette a javaslattevő hatóság egyszerűsített adatközlést kér az ágazati kritériumok teljesüléséről, melyet az üzemeltetőnek 3 napon belül vissza kell küldeni. 2022-ben ez a fejezet kiegészült azzal is, hogy az ilyen módon kijelölt létfontosságú rendszerem fokozott nemzeti és szövetségi védelmének megtervezéséhez és végrehajtásához a honvédelmi ágazat adatokat szolgáltat a honvédségi és NATO szervek részére.²²⁷

A honvédelmi ágazati kormányrendelet az európai létfontosságú rendszeremekkel kapcsolatban nem tartalmaz rendelkezést.

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

A 2017-ben kiadott kormányrendelet hatálya alá tartoznak:

- az internet-hozzáférési szolgáltatás és internet-infrastruktúra;
- az elektronikus hírközlési szolgáltatások, elektronikus hírközlő hálózatok;
- a műsorszórás;
- a postai szolgáltatások;

²²⁶ 375/2020. (VII. 30.) Korm. rendelet 84. §.

²²⁷ 409/2022. (X. 24.) Korm. rendelet 20. §.

- kormányzati elektronikus információs rendszerek.

A rendelet hatálya nem vonatkozik a zárt célú elektronikus információs rendszerekre, mint például a honvédelmi célú elektronikus információs rendszerek, valamint a kísérleti, kutatási, oktatási céllal működtetett rendszereire.

Az ágazati kijelölő hatóságként a 2017-ben megjelent kormányrendelet a postaügyért felelős minisztert határozta meg, de a 2020-ban bevezetett módosítások óta az ágazatba besorolt rendszerelemek nemzeti és európai létfontosságú rendszerelemként történő kijelölésére a Nemzeti Média- és Hírközlési Hatóság jogosult.²²⁸ A kijelölő hatóság feladatát döntés-előkészítő bizottság segíti. A postaügyért felelős miniszter a postai szolgáltatások alágazat nemzeti létfontosságú rendszerlemeinek és európai létfontosságú rendszerlemeinek kijelölése és a kijelölés visszavonása során javaslattevő hatóságként jár el.

A kormányrendelet az infokommunikációs ágazathoz tartozó nemzeti létfontosságú rendszerelemek ágazati kritériumainak meghatározásakor olyan infokommunikációs szolgáltatásokat vesz figyelembe, melyek országos lefedettségűek, a teljes lakosság nagy részénél elérhetőek, illetve honvédelmi vagy közigazgatási feladatok ellátásában kiemelten szükségesek. Európai létfontosságú rendszerelemek tekintetében az ágazati kritériumok olyan postai, infokommunikációs, közigazgatási rendszerekre vonatkozhatnak, melyek nemzetközi viszonylatban, egy vagy több tagállammal való együttműködésben, illetve terrorelhárítási, katasztrófavédelmi feladatokban jelennek meg.

Az infokommunikációs ágazatban a biztonsági összekötő személy képesítési követelményeit az üzemeltető is megállapíthatja, de a kormányrendelet minimum 5 év szakmai tapasztalatot ír elő. A postai szolgáltatások tekintetében a biztonsági összekötő személy szakirányú végzettségének kell tekinteni a jogi végzettséget is.

2020-as módosítás folyamán több új fejezettel is kiegészült az infokommunikációs kormányrendelet.²²⁹

Új fejezetként került be, hogy az internet-hozzáférést, elektronikus hírközlést, műsorszórást szolgáltatók, amennyiben elérik az éves nettó 1 milliárd forint árbevételt, azonosítási jelentés beadására kötelezettek. A Lrtv.vr. alapján előírt azonosítási jelentés tartalmát ki kell egészíteni az üzemeltető teljes hálózati infrastruktúrájának bemutatásával, illetve egy elemzéssel, mely arra vonatkozik, hogy az adott üzemeltető egyes rendszerlemeit mely más elektronikus

²²⁸ 375/2020. (VII. 30.) Korm. rendelet

²²⁹ 375/2020. (VII. 30.) Korm. rendelet

hírközlési szolgáltatók veszik igénybe. Ez a pont első lépése lehet egy átfogóbb ágazati belső interdependencia vizsgálatnak.

Ugyancsak új fejezetként került be a kormányrendeletbe 2020-ban a jelentős zavar mértékének, az azokhoz kapcsolódó küszöbértékeknek a meghatározása, illetve a rendkívüli események definiálása.

161/2019. (VII. 4.) Korm. rendelet a közlekedési létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

A közlekedési ágazati kormányrendelet az első fejezetében pontosítja, hogy üzemeltetőként a közutak kezelőjét, repülőterek és légiforgalmi földi berendezések, hajózási létesítmények, logisztikai központok üzemeltetőjét, valamint a vasúti pályahálózat-működtető társaságokat kell érteni.

A közlekedési létfontosságú rendszeresemények ágazati kijelölő hatósága és a helyszíni ellenőrzést lefolytató szerve tekintetében a kormányrendelet elkülöníti az alágazatokat, mely alapján:

- a közúti közlekedés alágazat tekintetében az útügyi közlekedési hatóság,
 - a vasúti közlekedés alágazat tekintetében a vasúti közlekedési hatóság,
 - a légiközlekedés alágazat tekintetében a légiközlekedési hatóság,
 - a víziközlekedés alágazat tekintetében a hajózási hatóság,
 - a logisztikai központok alágazat tekintetében az útügyi közlekedési hatóság jár el.
- Kivételt képeznek azok a logisztikai létesítmények, melyeknek vasúti kapcsolata van, ebben az esetben a vasúti közlekedési hatóságot jelöli meg a kormányrendelet.

A közlekedési kormányrendelet javaslattétő hatóságot nem jelöl meg, így az azonosítási eljárást vagy maga az üzemeltető, vagy az adott kijelölő hatóság kezdeményezheti. Illetve a honvédelmi ágazati kormányrendelet alapján akár a honvédelmi javaslattétő hatóság.

Európai létfontosságú rendszeresemények kijelölésének ágazati kritériumaiként minden alágazat tekintetében fontos szempont, hogy az adott közlekedési rendszeresemény olyan hálózat része, melynek kiesése nemzetközi viszonylatban is fennakadásokat okoz. Példaként ide lehet sorolni a transzeurópai úthálózat törzshálózatának közúti és vízi részeit, a gyorsforgalmi utak hídjait, nemzetközi személy és áruforgalom lebonyolítását végző közúti és vasúti határátkelőhelyeket, nemzetközi kereskedelmi repülőtereket, intermodális terminálokat.

Nemzeti létfontosságú rendszerelemek kijelölésének ágazati kritériumai tekintetében a kormányrendelet hasonlóan fogalmaz mint az európai rendszerelemek tekintetében, de a nemzeti érdekeket emeli ki. A kormányrendelet megfogalmazása szerint így a közlekedési ágazat minden európai létfontosságú rendszereleme, amely Magyarország területén került kijelölésre, egyben nemzeti létfontosságú rendszerelem is. Ezeken felül nemzeti létfontosságú rendszerelemként jelölhetőek ki a megyei jogú városok közötti magasabb osztályú utak, a megyei jogú városok közötti forgalomirányító rendszerei, a Duna hídjai, az országos vasúti törzshálózat alagútjai, hídjai, támfalai, a felszín alatti vasút és tartozékai, légiforgalmi irányítás rendszere, valamint magas forgalmú kikötők.

2020-ban új fejezetként került be a kormányrendeletbe az alapvető szolgáltatásokkal kapcsolatos jelentős zavar mértékének, az azokhoz kapcsolódó küszöbértékeknek a meghatározása, illetve a rendkívüli események definiálása.

Az új fejezetek részletes adatai, valamint a kormányrendelet ágazati kritériumai alapján az üzemeltetők pontosan be tudják azonosítani, hogy az általuk kezelt rendszerelem potenciálisan létfontosságú, illetve alapvető szolgáltatást nyújtó rendszerelem-e. Ezek alapján a kormányrendelet záró rendelkezésében, a rendelet kihirdetésétől számított 90 napot ad az üzemeltetők részére az azonosítási jelentésük benyújtására.

Korábbi, mára hatálytalan információbiztonsági jogszabályok

Fontos megemlíteni a mára már hatálytalan, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt és kapcsolódó rendeleteit^{230, 231, 232, 233}, melyek a nemzeti elektronikus adatvagyon és az ezt kezelő információs rendszerek biztonságával foglalkoztak, ennek jogi alapjait teremtették meg. Ennek okán kiemelt figyelmet

²³⁰ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

²³¹ 187/2015. (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

²³² 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól

²³³ 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

fordítottak a létfontosságú rendszerelemekre, illetve az ezekhez kapcsolódó létfontosságú információs rendszerek biztonságára.

A 2013. évi L. törvény először adta meg az elektronikus információbiztonság alapvető követelményeit, az elektronikus információs rendszerek biztonsági osztályba sorolásának alapjait, a szervezetek biztonsági szintjének meghatározásához szükséges alapokat. Így a szervezetek képesek voltak besorolni saját elektronikus információs rendszereiket és a besorolás alapján kialakítani a védelmüket. Bár ez a feladat igen sok kötelezettséget rótt az üzemeltetőkre.

A NIS megjelenésével a 2013. évi L. törvény is kiegészült az alapvető szolgáltatást nyújtó szolgáltatók fogalmával és a Kormány az alapvető szolgáltatást nyújtó szolgáltatók információs rendszereit érintő biztonsági események és fenyegetések kezelése érdekében két eseménykezelő központot hozott létre, a honvédelmi célú rendszerek és a törvény hatálya alá eső más szervek, szervezetek rendszerei vonatkozásában. A 2013. évi L. törvény részletesen megadja a köztük lévő kapcsolatot és a működésük alapjait, de a feladat- és hatáskörök, valamint a biztonsági események kezelésének szabályait már a 271/2018. (XII. 20.) Korm. rendelet tartalmazza. A honvédelmi célú elektronikus információs rendszereket érintő biztonsági események és fenyegetések kezelésére a Katonai Nemzetbiztonsági Szolgálatot, a nem honvédelmi célú, alapvető szolgáltatást nyújtó szolgáltatók, valamint a bejelentés-köteles szolgáltatást nyújtó szolgáltatók elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelésére pedig a Nemzetbiztonsági Szakszolgálatot jelöli ki.

A 2013. évi L. törvény a legújabb technológiai fejlesztéseket hivatott lekövetni a 2021-es kiegészítéssel, mely fejezet a matematikailag valószínűsíthetően igazolható, kvantumszámítógép által megvalósított támadás ellen, a hagyományos kriptográfiai alkalmazáson felüli poszt-quantum megoldást nyújtó titkosításról rendelkezik. Előremutató módon szabályozza a poszt-quantumtitkosítás alkalmazását, meghatározza az alkalmazás általános szabályait, az erre kötelezett szervezetek védelmi kötelezettségeit, valamint a poszt-quantum szolgáltatást nyújtó szervezetekkel szembeni követelményeket. A fejezet a megfelelés tanúsítását és a hatósági felügyeletet is rendezi, felismerve a kvantumszámítástechnika jövőbeni kockázatait.

2. SZÁMÚ MELLÉKLET

Képzési program a kritikus szervezet fizikai védelmének oktatásához (MINTA)

1. A képzés megnevezése: Kritikus szervezet fizikai védelmének alapjai, területei, aktualitásai

2. A képzés kódja: FV-01

3. A képzésért felelős:

- *szervezés, végrehajtás, ellenőrzés:* Minta Gyula; (Vezetési Osztály, Ellenálló képességért felelős vezető; Tel.: +1-234-5678; e-mail: minta1@szervezet.com);
- *végrehajtás, értékelés:* Fizi Béla; (Védelmi Osztály, Fizikai Védelmi Csoport, csoportvezető; Tel.: +1-234-6789; e-mail: minta2@szervezet.com);

4. Célcsoport: Kritikus szervezet állandó munkavállalói

A képzésen a fizikai védelemben nem érintett munkavállalók 2 évente vesznek részt. Az új belépő, fizikai védelemben érintett munkavállalók a *Szervezet fizikai védelmének elemei, működése* (FV-02) c. képzés előfeltételeként vesznek részt ezen a képzésen.

5. Képzési előfeltétel: Új belépő állandó munkavállalók szervezeti ismereti képzése (ÚMSZ-01)

6. A képzési órák száma és típusa

A képzés 60% elméleti és 30% gyakorlati órát tartalmaz. A kontakt órák mellett önképzésre javasolt óraszám megadható.

A képzés szervezője a 10. pontban javasolt óraszámoktól eltérhet, figyelembe véve a képzésen résztvevők munkakörét, felkészültségét.

7. A képzés szakmai tartalma: Tájékoztatót adni a szervezet tagjai számára a kritikus szervezetek fizikai védelmének elveiről, gyakorlati sajátosságairól, a szervezettel kapcsolatos fizikai védelmi intézkedések aktualitásairól.

8. Elérendő kompetenciák:

Tudása:

- Ismeri a fizikai védelem alapelveit.
- Ismeri szervezet fizikai védelmének főbb elemeit.
- Tisztában van a fizikai védelem munkakörökre vonatkozó befolyásoló hatásával.
- Tisztában van a fizikai biztonsági incidens esetén szükséges teendőivel.

Képességei:

- képes a munkavállalók részére készített fizikai védelmi intézkedések értelmezésére.

Autonómiája és felelőssége:

- Szakmai feladatainak elvégzése során figyelemmel van a kritikus szervezet fizikai védelmének elveire, szabályaira, felelősségteljesen együttműködik más szakterület munkavállalóival.
- Felelősséget vállal, szintjének megfelelő döntéseket hoz a fizikai védelem szinten tartása érdekében.
- Fizikai biztonsági incidens esetén együttműködik a fizikai védelem munkatársaival, segíti kollégáit a szükséges teendők végrehajtásában.

9. A képzés tananyagának leírása, tematika:

1. Az átfogó védelem

1.2. *Ellenálló képesség*

Ellenálló képesség fogalma, elemei. Kritikus szervezetek ellenállóképességére vonatkozó jogszabályok.

1.2. *Átfogó védelem rendszere*

Az átfogó védelem elemei, egymásra épülésük, az elemek fő feladatai.

1.3. *Az átfogó védelem megvalósítása*

A kombinált, az integrált és az átfogó védelem megvalósításának részletei, az elemek egymáshoz kapcsolásának lehetőségei.

2. Fizikai védelem kialakítása

2.1. Fizikai védelem elvei

A fizikai védelem helye az átfogó védelemben. A fizikai védelem alapelvei, részei, jellemzői.

2.2. Létesítmény megközelíthetősége

Biztonsági zónák fogalma, elvei, kialakításuk jellemzői.

2.3. Élőerős őrzés-védelem

Az élőerős őrzés-védelem résztvevői, működésük jogszabályi alapjai, módszerei. Feladatuk, jogköreik, kötelességeik.

2.4. Fizikai védelem technikai eszközei

Az elektronikai és mechanikai biztonságtechnikai eszközök.

3. A szervezet fizikai védelme

3.1. A védelmi tervek, a Fizikai Védelmi Terv

A védelmi tervek helye a dokumentációs hierarchiában, a fizikai védelmi terv helye a rendszerben. A Fizikai Védelmi Terv részletes felépítése.

3.2. A szervezet fizikai védelmének felépítése

A szervezet fizikai védelmének működési jellemzői, fizikai védelmi intézkedések és azok végrehajtásának jellemzői.

3.3. A szervezet fizikai védelmének aktuális helyzete

Aktuális biztonsági kérdések a fizikai védelem tükrében. Új eszközök, módszerek, technológiák a szervezet fizikai védelmében.

10. A képzés javasol óraszámja (Elmélet + Gyakorlat)

Tárgykör	Témakör	Munkakör			
		vezetői	admin. beosztott	fizikai beosztott	Védelmi munkakör
1.	1.1.	4+0	1+0	1+0	4+0
	1.2.	2+0	-	-	2+0
	1.3.	4+0	-	-	2+0
2.	2.1.	2+0	-	-	1+0
	2.2.	2+2	1+2	2+2	4+4
	2.3.	4+2	1+0	2+0	4+4
	2.4.	2+2	2+2	2+2	4+4
3.	3.1.	2+2	1+0	1+0	2+4

	3.2.	2+0	1+0	1+0	4+4
	3.3.	4	2	2	4

11. Az órákon való részvétel követelményei, az elfogadható hiányzások mértéke, a távolmaradás pótlásának lehetősége: A tanórák minimum 60%-án a részvétel kötelező. Hiányzás esetén a résztvevő köteles a mulasztott óra anyagát beszerezni, abból önállóan felkészülni.

12. Ismeretek ellenőrzésének rendje: az oktató a leadott tananyagból szóban visszaellenőrizheti a megszerzett tudást, interaktív módszerek segítségével ellenőrizheti az ismereteket.

13. Az értékelés megszerzésének feltételei:

Az órákon való részvétellel a képzés teljesítettnek tekinthető.

14. Irodalomjegyzék:

Kötelező irodalom:

1. 2024. évi LXXXIV. tv. a kritikus szervezetek ellenálló képességéről
2. 474/2024. (XII. 31.) Korm. rendelet a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról
3. Szervezeti Ellenálló Képességi Terv (kivonat a munkavállalók részére)
4. Szervezeti Fizikai Védelmi Terv (kivonat a munkavállalók részére)

Ajánlott irodalom:

1. Szervezeti Örutasítás

3. SZÁMÚ MELLÉKLET

Kohéziós táblázat

	TUDOMÁNYOS PROBLÉMA	HIPOTÉZIS	CÉLKITŰZÉS	KUTATÁSI MÓDSZER	KÖVETKEZTETÉS	HIPOTÉZIS IGAZOLÁSA/ELVETÉSE	ÚJ Tudományos EREDMÉNY
1.	A kritikus szervezetek azonosításának és kijelölésének alapját képező jelenlegi jogi szabályozás fejlett, meghatározza a végrehajtás kereteit, problémát jelent azonban, hogy az azonosítási és kijelölési folyamatok gyakorlati végrehajtásához nem biztosít egységes módszertani támogatást. A hiányosságok a jogszabályok eltérő alkalmazását és a folyamatok végrehajtásának alacsony hatékonyságát eredményezik.	Feltételezem, hogy a jogi szabályozás megfelelő módosításával a kritikus szervezetek és infrastruktúrák azonosítási, kijelölési folyamatának és rezilienciájának hatékonysága növelhető.	Olyan módosítási javaslatok megfogalmazása a nemzeti jogszabályok tartalmára, melyek a kritikus szervezetek és infrastruktúrák azonosítási és kijelölési folyamatának szabályait közelebb hozzák a gyakorlati végrehajtáshoz, törvény és kormányrendelet szintű szabályokkal támogatják a végrehajtás folyamatát.	A releváns nemzeti jogszabályok és a kijelölési folyamat összehasonlító és rendszerszintű elemzése, az eredmények felhasználásának vizsgálata.	A releváns nemzeti jogszabályok meghatározzák a kijelölési folyamat kereteit, de nem adnak módszertant a kritikus szervezetek részére, így a gyakorlati végrehajtás nem egységes.	Az 1. hipotézis a jogszabályok elemzésével és az azonosítási és kijelölési folyamat, valamint a kijelölést követő feladatok vizsgálatával igazolható.	Azonosítottam a kritikus szervezetek és kritikus infrastruktúrák kijelölési folyamatában és támogatásában lehetséges fejlesztési irányokat, melyek alapján javaslatot tettem a hatályos jogi szabályozók tartalmi módosítására.
2.	Sem a hatóságok által kiadott szabályozók és minták, sem az üzemeltetők által alkalmazott sablonok és eljárások nem vizsgálják kellő mértékben az ágazaton belüli és az ágazatok közötti, több típusú, mélyebb interdependenciát, nem veszik figyelembe az interdependencia komplex jellemzőit, így nem alkalmasak részletes, mélyebb eredmények kialakítására.	Feltételezem, hogy az interdependencia, mint a kapcsolat egy bizonyos állapota rendelkezik olyan tulajdonságokkal, dimenziókkal, melyek elkülöníthetők egymástól, így a vizsgálatuk standardizálható és jól mérhető.	Az interdependencia elkülöníthető dimenzióinak és jellemzőinek feltárása.	Hazai és nemzetközi szakirodalom elemzése. Valós veszélyhelyzetben végrehajtott feladatok tapasztalatainak feldolgozása.	Az interdependencia több olyan dimenzióval bír, melyek minden kritikus szervezet esetén fellelhetők, jól elkülöníthetők egymástól és különböző módszerekkel elemezhetők.	A 2. hipotézis a kritikus szervezetek okmányaiban rögzített kockázatelemzések vizsgálatával és a feltárt interdependencia dimenziók elemzésével igazolható.	Meghatároztam a kritikus szervezetek és infrastruktúrák interdependenciájának dimenzióit, figyelemmel a kritikus szervezetek és infrastruktúrák jellemzőire.
3.	Sem a hatóságok által kiadott szabályozók és minták, sem az üzemeltetők által alkalmazott sablonok és eljárások nem vizsgálják kellő mértékben az ágazaton belüli és az ágazatok közötti, több típusú, mélyebb interdependenciát, nem veszik figyelembe az interdependencia komplex jellemzőit, így nem alkalmasak részletes, mélyebb eredmények kialakítására.	Feltételezem, hogy az interdependencia dimenzióinak meghatározását követően olyan	Javaslatot tenni az interdependencia vizsgálatának egységes gyakorlati módszerére.	Azonosítási, kijelölési dokumentumok és végrehajtott függőségi vizsgálatok	Az interdependencia dimenzióit figyelembe vevő, egységes gyakorlati módszerrel végrehajtott	A 3. hipotézis az Ellenálló Képességi Tervben alkalmazott függőségi vizsgálatok és a feltárt interdependencia	Kidolgoztam a kritikus szervezetek és infrastruktúrák interdependencia vizsgálatának gyakorlatban alkalmazható módszerét.

		egységes vizsgálati módszertan hozható létre, mely részletesebb és pontosabb függőségi elemzést eredményez, valamint alapja lehet az egységes országos interdependencia térkép kialakításának.		eredményeinek elemzése. Kijelölt kritikus szervezetek valós kockázatelemzésének vizsgálata, valós veszélyhelyzetben végrehajtott elemzésekből levont tapasztalatok feldolgozása.	elemzés részletes és több szintű eredményt ad.	dimenziók összehasonlító elemzésével igazolható.	
4.	A kritikus szervezetek és infrastruktúrák fizikai védelmének kialakítása sok esetben jelentős mértékben függ a kritikus szervezetek eltérő humán erőforrás jellemzőitől és a anyagi lehetőségeitől, melyek következtében a kezelésükben lévő infrastruktúrák és létesítmények fizikai védelme többségében nem éri el a szükséges védelmi szintet.	Feltételezem, hogy a fizikai védelem hatékonysága növelhető a minden részletre kiterjedő tervezéssel, a szükséges védelmi szint elérhető a humán és anyagi erőforrások előre tervezett optimalizálásával.	Javaslatot tenni a kijelölt kritikus szervezetek és az infrastruktúrák üzemeltetői részére a megfelelő Fizikai Védelmi Terv elkészítéséhez, figyelemmel a kapcsolódó védelmi tervekkel való összhangjára.	Az átfogó és a fizikai védelemmel kapcsolatos szakirodalom és jogszabályok elemzése, kijelölt kritikus szervezetek valós fizikai védelmi terveinek vizsgálata.	Az átfogó védelemre figyelemmel kialakított egységes Fizikai Védelmi Terv elősegíti a humán erőforrás és az anyagi lehetőségek optimalizált és hatékony felhasználását a fizikai védelem megfelelő szintjének kialakításában és megvalósításában.	A 4. hipotézis a fizikai védelem elméleti lehetőségeinek és a kritikus szervezetek megvalósított fizikai védelmének összehasonlításával igazolható.	Kidolgoztam a kritikus szervezetek és kritikus infrastruktúrák jellemzőit figyelembe vevő fizikai védelmi terv elkészítéséhez szükséges metodikát és a Fizikai Védelmi Terv tartalmi elemeit.
5.	A modern védelmi módszerek, technológiai és műszaki megoldások fejlődése ellenére a kritikus szervezetek működésében továbbra is az emberi tényező jelenti a legnagyobb kockázatot, mivel a nem megfelelő felkészültség, védelmi tudatosság és szervezeti ismeret jelentősen csökkentheti a védelmi rendszerek hatékonyságát	Feltételezem, hogy a kritikus szervezetek üzemeltetői nem rendelkeznek a megfelelő tudással az azonosítási és kijelölési folyamat, valamint a megfelelő védelmi intézkedések végrehajtásához.	Javaslatot tenni a kritikus szervezetek ellenálló képességének fejlesztésére, a szervezet vezetői és munkáltatói részére kialakított szervezeten belüli felkészítési rendszer kialakításával.	Fegyveres szervek belső felkészítési rendszerének elemzése, az elvek kritikus szervezetek belső képzésébe való adaptálhatóságának vizsgálata.	A szervezetek belső képzésének kialakításával erősíthető a munkavállalók rendszerben való gondolkodása és a védelmi tudatosságuk, mely növeli a kritikus szervezetek rezilienciáját a humán erőforrás fejlesztésén keresztül.	Az 5. hipotézis személyes interjúk, dokumentumelemzések és képzési rendszerek vizsgálata és adaptációja alapján igazolható.	Kidolgoztam a kritikus szervezetek személyi állományának belső felkészítésére vonatkozó képzési alapelveket, metodikát és a hozzá kapcsolódó képzési program mintát.

	és a szervezetek ellenálló képességét.						
6.	A kritikus szervezetek belső felkészítési rendszerének kialakítása és folyamatos működtetése jelentős anyagi és szervezett humánerőforrás-ráfordítást igényel, amely megfelelő támogató és ellenőrző elemek hiányában hosszú távon csökkenti a képzések hatékonyságát, valamint a megszerzett tapasztalatok és ismeretek szervezeti szintű hasznosulását.	Feltételezem, hogy támogató elemek nélkül a belső felkészítési rendszerek nem hatékonyak, eredményeik hasznosítása, a tapasztalatok visszaforgatása hosszabb távon nem történik meg, így erőforrást vonnak el, de a szervezet rezilienciáját nem növelik.	Kidolgozni a szervezetek belső felkészítési rendszerének főbb támogató elemeit.	Szakirodalmi elemzés, a fegyveres szervek hasonló támogató elemei adaptációjának vizsgálata.	A dokumentációs hierarchia és a felkészítési rendszer ellenőrzési elemeinek alkalmazása a költségek növekedése nélkül is képesek a felkészítési rendszer hatékonyságának fokozására.	A 6. hipotézis a vállalatigazgatás témában már korábban végrehajtott elemzések szakirodalmának vizsgálatával és a Magyar Honvédség hasonló rendszereinek adaptálásával igazolható.	Meghatároztam a kritikus szervezetek belső felkészítését támogató dokumentációs hierarchia és ellenőrzési rendszer kialakításának alapelveit.