Doktori (PhD) értekezés

Ronyecz Lilla

- 2026-

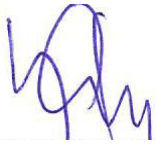
NEMZETI KÖZSZOLGÁLATI EGYETEM
KATONAI MŰSZAKI DOKTORI ISKOLA

Ronyecz Lilla

Létfontosságú rendszerek és létesítményekkel kapcsolatos kockázat- és következményelemző módszerek kutatása és fejlesztése

Doktori (PhD) értekezés

Tudományos témavezetők:



.....	.....
Dr. Kátai-Urbán Lajos	**Dr. Bognár Balázs**
tű. ezredes PhD.	**tű. dandártábornok PhD.**

BUDAPEST, 2026.

TARTALOMJEGYZÉK

BEVEZETÉS

1. A KUTATÁSI TÉMA AKTUALITÁSA

A tudományos kutatásom elsősorban a kritikus infrastruktúrák védelmének és azzal összefüggő kockázatelemzésének műszaki és alkalmazhatósági követelményeinek meghatározására, valamint a műszaki megoldások kidolgozására irányul. A kritikus szervezetek védelmének effektív és hatékony ellátása egyaránt igényli a kritikus infrastruktúrák hibrid fenyegetések és dominóhatások elleni feladatok ellátásához szükséges módszerek alkalmazását.

A kritikus szervezetek és infrastruktúrák védelmének elsődleges célja a lakosság és anyagi javak védelme, valamint a lakosság ellátásához szükséges szolgáltatások üzemfolytonosságának fenntartása. A központi államigazgatási szerveknél, valamint a kritikus infrastruktúrák működtető gazdálkodó szervezeteknél több mint egy évtized óta foglalkoznak a kritikus infrastruktúrák védelmével, készítenek kockázatelemzést és végzik el a hatósági munkát.

A kritikus szervezetek és infrastruktúrák számos rendszerből, illetve alrendszerből áll, amelyek komplex rendszerként foghatók fel. Ezek a rendszerek, alrendszerek kölcsönös függésben, szoros kölcsönhatásban vannak egymással, így bármelyikében bekövetkezett változás potenciálisan átgyűrűzik a többi rendszerbe, alrendszerbe, melynek következtében láncreakciók indulhatnak be.

Ez azt is jelentheti, hogy valamely alrendszert ért támadás vagy bármely más jellegű negatív behatás káros hatások folyamatát indíthatja be több rendszer, alrendszer vonatkozásában. Ha mindezek következtében a kritikus társadalmi feladatok ellátásához nélkülözhetetlen rendszerelemek részben, vagy egészben működésképtelenné válhatnak, szükségessé válik azok fokozott és preventív védelme a szolgáltatás, rendszer vagy infrastruktúra üzembiztonságának, üzemfolytonosságának növelése érdekében.

Ennek értelmében a kritikus szervezetek védelme napjaink egyik legfontosabb biztonsági feladata. Az ezzel összefüggő kockázatelemzés nem csupán technikai eljárás, hanem stratégiai alapja annak, hogy ezek a szervezetek ellenállóak maradjanak váratlan, komplex fenyegetésekkel szemben. A kritikus infrastruktúrák biztosítják a napi élet alapvető működését, úgy, mint a víz, az energia, az egészségügy, és a pénzforgalom. Ha ezen rendszerek megszakadnak, az súlyos következményekkel járhatnak az életminőségre, a gazdaságra és a lakosságra, így kirajzolódik, hogy a kritikus szervezetek rezilienciája elengedhetetlen az alapvető szolgáltatások üzemfolytonosságának fenntartásához. [1]

A biztonságpolitikai környezet felgyorsult változásával a kockázatok is folyamatosan változnak, nem csak a hagyományos fizikai veszélyek, hanem az új fenyegetések is növekednek, mint a kibertámadások, és a hibrid fenyegetések. A kritikus szervezetek kiesése nemcsak működési zavarokat, hanem jelentős gazdasági károkat is okozhat.

A téma aktualitását jól mutatja a fokozódó geopolitikai feszültség, a nemzetközi környezet instabilitása, a hibrid hadviselés, a klímaváltozás hatásai, a gyakori és egyre súlyosabb természeti jelenségek, melyek plusz kockázati tényezőt jelentenek a kritikus infrastruktúrák számára. Emellett a téma kutatását és fejlesztését indokolja a technológia gyorsulása, a digitalizáltabb és összekapcsolt rendszerekkel, aminek révén nő a kockázatok komplexitása. A 2022. decemberében hatályba lépő *az Európai Parlament és a Tanács 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről* (a továbiakban: CER Irányelv), valamint a magyarországi implementációjának eredményeként bevezetett *kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény* (a továbbiakban: Kszetv.) jól mutatja, hogy újra kell gondolni a korábban létfontosságú rendszerelemeknek nevezett kritikus infrastruktúrák védelmét, és alkalmazkodni szükséges a folyamatosan megjelenő újabb kihívásokhoz. [2]

A kritikus szervezetek védelmének és kockázatelemzésének folyamatos fejlesztése szükségszerű stratégiai elem, ezáltal garantálható, hogy a kulcsfontosságú infrastruktúrák és szolgáltatások rendelkezésre álljanak válsághelyzetekben is. Az új és változó fenyegetések, a technológiai összefonódottság, valamint a jogszabályi követelmények mind azt erősítik, hogy a kockázatelemzés nem egyszeri feladat, hanem folyamatos integrált eljárás legyen a kritikus szervezetek működésében. Leszögezhető tehát, hogy a kritikus szervezetek védelmének szakterülete és a hozzá kapcsolódó műszaki technikai eszközrendszer fejlesztése egyre jobban előtérbe kerül és a fejlesztési lehetőségek feltárása napjaink kiemelt kérdésévé vált. Egyértelmű tehát, hogy ennek a területnek a kutatása időszerű kutatási feladattá vált.

2. A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

Az értekezés aktualitásának bemutatásából kiderült, hogy külön tudományos problémaként jelentkezik a kritikus szervezetek és infrastruktúrák védelmében jelentős szerepet játszó kockázatelemzés alkalmazott műszaki technikai eszközrendszerének kutatása és fejlesztése. A folyamatosan változó biztonságpolitikai helyzetre tekintettel, a lehetséges konfliktusforrások, fenyegetések, támadások megfelelő kezelése érdekében összehangoltan kell alkalmazni a katonai és a nem katonai eszközöket, a kormányzati és civil szervezetek képességeit, valamint a nemzeti erő más formáit is.

A jövőbeli konfliktusokra történő felkészülés érdekében szükséges fokozni a rendszerelemek fizikai és kiber védelmét, illetve törekedni kell a támadásokkal szembeni, lehető legteljesebb ellenállóképességük növelésére. Az ellenálló képesség növeléséhez szorosan hozzájárul a kockázat és következményelemzés annak érdekében, hogy a szervezetek és a hatóságok minél hatékonyabban tudjanak felkészülni és kezelni a veszélyeket és azok hatásait. Az egységes megvalósítás rendszerének elengedhetetlen eleme a vizsgálati módszertan kialakítása, és a tapasztalatok birtokában dinamikusan fejlődő korszerűsítése.

A kritikus szervezet és infrastruktúra védelmének újragondolása szükségessé teszi a megfelelő műszaki, technológiai, kommunikációs, és jogszabályi feltételek meglétét, amelyhez kapcsolódó eszközrendszer, eljárásrend és módszertan kutatása és fejlesztése kiemelt kutatási feladatot jelent, amelynek részelemei a következők lehetnek:

1. A kritikus szervezetek fenyegetettsége napjainkban jelentősen átalakult, főként a geopolitikai instabilitás, a technológiai fejlődés és a digitális sérülékenységek miatt, így a védelmi rendszerek naprakészen tartása és fejlesztése a nemzetközi előírások és gyakorlati tapasztalatok figyelembevételével indokolttá vált.
2. A magyarországi kritikus szervezetek kockázatelemzése jelenleg jellemzően szervezeti és nemzeti szinten zajlik, így hiányzik az ágazati szintű átfogó kockázati kép. Ez különösen problémás a dominóhatások és az ágazatközi függőségek feltérképezésekor, például az energia-, víziközmű-, és közlekedési rendszerek kölcsönhatásai esetében, így annak kialakítása külön módszertan kialakítását igényli.
3. A kritikus szervezetek feladatainak ellátásában részt vevő hatóságok (ellenőrző, nyilvántartó, kijelölő, szakhatóság), és a kritikus szervezetek vezetői, valamint az ellenálló képességért felelős vezetők közötti kommunikáció gyakorisága igen szerteágazó, annak nincs jogszabályban foglalt útja, módja, így egy módszertan, eljárásrend kialakításának igényét alapozza meg, mivel az információszolgáltatásnak nem szabad kizárólag strukturált jelentésekre korlátozódnia. A vezetők egyre inkább igénylik az interaktív fórumokat, szakmai egyeztetéseket és a kétirányú kommunikáció lehetőségét, ahol a tapasztalatmegosztás és közvetlen visszacsatolás is megvalósulhat.

Az általam azonosított kutatási problémák megoldásának alapját képezi az iparbiztonsági műszaki technikai eszközrendszer kialakításának fogalmi és rendszertani elemzése és értékelése, amely kutatói munka, különös tekintettel a közelmúlt jelentős kritikus infrastruktúrákat érintő veszélyeire, pandémiás válsághelyzetekre még várat magára.

A kutatási hipotéziseimet és célkitűzéseimet a fentiekben bemutatott tudományos problémák megoldása érdekében dolgoztam ki.

3. KUTATÁSI HIPOTÉZISEK

Az értekezés kidolgozását megelőzően az alábbi hipotéziseket állítottam fel:

1. Feltételezésem szerint jelentős összefüggést van a kritikus szervezetek és infrastruktúrák rezilienciája és egy mindenre kiterjedő, a kritikus infrastruktúra sajátosságait részletesen figyelembe vevő kockázatelemzés között. Ennek alapján időszerűvé vált a kritikus infrastruktúrák védelmét meghatározó kockázatelemzés és a jelenleg is zajló konfliktusok, kritikus infrastruktúrákat ért támadások hatásainak elemzése, értékelése, Feltételezem, hogy a kritikus szervezetek közötti kölcsönös függőségek kritikus pontjai és töréspontjai meghatározzák a rendszerszintű kockázatok terjedését.
2. Feltételezésem szerint a kritikus szervezeteket és infrastruktúrákat veszélyeztető tényezők felméréséhez és az ellenálló képesség növeléséhez szükséges egy ágazati kockázatelemzés elvégzése, ami kiemeltem vizsgálja a rendszerelemek közötti interdependenciát.
3. Feltételezésem szerint jelenleg az ellenállóképességért felelős vezetők nem rendelkeznek kellő információval a kockázatelemzés teljes körű felülvizsgálatához és elkészítéséhez. Míg a rendszerelem környezetében fellelhető veszélyeket tudják azonosítani, azonban a külső támadás, hibrid fenyegetés okozta fenyegetettség mértékét nem tudják önállóan megállapítani, mivel ilyen információval nem rendelkeznek.

4. KUTATÁSI CÉLKITŰZÉSEK

A kutatási célkitűzéseimet - a tudományos problémák meghatározásánál már ismertetett – három fő kutatási részterületen fogalmazom meg:

1. A kutatás során elemzem és értékelem a kritikus szervezetek védelmének intézményi és szabályozási keretrendszerét, különös tekintettel a jelenkori biztonságpolitikai környezetre és annak hatásaira a kritikus infrastruktúrák védelmére. A vizsgálat kiterjed a szabályozás kialakulásának időszakában azonosított fenyegetésekre, valamint a kritikus szervezeteket érő aktuális kockázatokra és támadási mintázatokra. Feldolgozom és rendszerezem a kritikus infrastruktúrák fenyegetettségére, sebezhetőségére és interdependenciáira vonatkozó szakirodalmat, majd elemezni kívánom a kritikus szervezetek közötti kölcsönös függőségek kritikus pontjait és lehetséges töréspontjait, amelyek meghatározzák a rendszerszintű kockázatok terjedését.

Célom, hogy a kutatás eredményeképpen feltárjam a kritikus szervezetek védelmének fejlesztési irányait, valamint azokat a mechanizmusokat, amelyek a reziliencia növelését és a rendszerszintű kockázatok mérséklését szolgálhatják.

2. A kutatásom célja egy olyan ágazati kockázatelemzési keretrendszer kialakítása, amely egységes, összehasonlítható és módszertanilag megalapozott módon támogatja a kritikus szervezetek kockázatkezelését. Ennek érdekében összehasonlító elemzést végzek több ország kockázatelemzési gyakorlatáról, különös tekintettel az alkalmazott módszerekre. A dolgozatban kidolgozom az ágazati kockázatelemzés módszertani keretét, amely tartalmazza az értékelési folyamat lépéseit, és a kockázati kritériumok rendszerét. Ezzel párhuzamosan felépítem az adatfeldolgozási és elemzési módszertant, amely biztosítja a különböző ágazatokból származó adatok integrálhatóságát és a rendszerszintű kockázatok vizsgálatát. A kutatás célja tehát egy olyan tudományosan megalapozott és gyakorlati alkalmazásra is alkalmas modell létrehozása, amely hozzájárul a nemzeti ellenállóképesség növeléséhez.
3. A kutatásom célja a kritikus szervezetek és a hatóságok közötti kommunikáció hatékonyságának értékelése, valamint a kockázatelemzések elkészítéséhez szükséges információáramlás javítására alkalmas módszertani keret kidolgozása. Ennek érdekében összehasonlító elemzést végzek a különböző kockázatelemzési gyakorlatok között, több szempont alapján. A vizsgálatot esettanulmányokon alapuló elemzésekkel egészítem ki, amelyek feltárják a kommunikációs hibák, adathiányok és visszacsatolási problémák működési következményeit. A cél végül egy olyan, tudományosan megalapozott információáramlási és jelentési modell kialakítása, amely mind a kritikus szervezetek, mind a hatóságok kockázatkezelési tevékenységét hatékonyabban támogatja.

5. KUTATÁSI MÓDSZEREK

A kutatásom során az alábbi kutatási módszereket használtam fel:

1. A kutatási célkitűzéseimhez illeszkedően alkalmaztam az általánosan elfogadott kutatási módszereket, úgymint analízis, szintézis, indukció és dedukció.
2. Kellő körültekintéssel és a teljesség igényére törekedve a kutatómunkám megalapozása érdekében a kutatási problémákat szem előtt tartva megfelelő mértékben dolgoztam fel a nemzetközi, az európai uniós, valamint a hazai jogi szabályozást. Különös tekintettel a releváns külföldi és magyar szakirodalom értékelő-elemző vizsgálatára.

3. Elemző módszereket alkalmazása, amelynek szerves részét képezik a kritikus infrastruktúrákkal összefüggő módszertan értékelésében, illetve az ebből eredő következtetések levonása alapján javaslatok megfogalmazása.
4. Külföldi műszaki megoldások és jó gyakorlat tanulmányozása, a hazai műszaki technikai megoldásokkal történő összehasonlító elemzése.
5. Részvétel nemzetközi és hazai szakmai konferenciákon, ahol a dolgozat elkészítéséhez is szükséges adatokat gyűjtöttem össze.
6. Konzultáció a kutatott témában az ellenállóképességért felelős vezetőkkel, elismert hazai kritikus infrastruktúra szakemberekkel.

6. RELEVÁNS SZAKIRODALOM ÁTTEKINTÉSE

A kutatási célkitűzéseim megvalósításához elengedhetetlen a kutatási feladataimmal kapcsolatos nemzetközi és magyarországi jogi szabályozás, valamint a mértékadó szakirodalom rövid áttekintése. Az értekezés tartalmi fejezeteiben elvégzem a nemzetközi és hazai jogi szabályozásnak, illetve a témához kapcsolódó mértékadó szakirodalomnak az elemzését.

A kritikus szervezetekkel és infrastruktúrákkal kapcsolatos védelem területén meghatározó nemzetközi jogi norma az Európai Parlament és a Tanács által kiadott korábban említett CER Irányelv, valamint a kritikus szervezetek kiberbiztonságának alapjait lefektető az *Európai Parlament és aTanács (EU) 2022/2555 irányelve (2022. december 14.) 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 hatályon kívül helyezéséről* (a továbbiakban: NIS 2 Irányelv). [3]

A magyarországi szabályozás alappillére a korábban említett Kszetv. és végrehajtási rendelete *a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról szóló 474/2024. (XII. 31.) Korm. rendelet*, valamint külön jogszabályban szabályozza az *ország védelme és biztonsága szempontjából jelentős szervezeteket és infrastruktúrákat a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény* (a továbbiakban: Vbö.) V/A fejezetében, és annak végrehajtási rendeletében *az ország védelme és biztonsága szempontjából jelentős szervezetek ellenálló képességéről szóló 475/2024. (XII. 31.) Korm. rendelet* (a továbbiakban: Vbö. Vhr.). Ezen jogszabályok foglalják magukba a kritikus szervezetek kijelölésének, védelmének, ellenőrzésének és a komplex gyakorlatok lefolytatásának menetét, részletszabályait. [4]

A kritikus infrastruktúrák szakterületén minden ágazat hatósága rendelkezik belső szabályzóval, dokumentumokkal. A nemzeti kockázatelemzés és a nemzeti stratégia részletszabályait a *Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti kockázatértékeléséről szóló 1191/2025. (VI. 5.) Korm. határozat (a továbbiakban: nemzeti kockázatelemzési határozat),* valamint *Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti stratégiájáról szóló 1192/2025. (VI. 5.) Korm. határozat (a továbbiakban: Nemzeti stratégiai határozat)* tartalmazza. [5]

A kritikus infrastruktúrák kockázatelemzésével kapcsolatos első mértékadó szakirodalom a Georgios Giannopoulos, Roberto Filippini, Muriel Schimmer szerzőpáros által írt kockázatértékelés módszertanaival összefüggő írása megvizsgálta a kritikus infrastruktúrák kockázatelemzési módszereit, bemutatta a kockázatértékelési módszerek jelenlegi állását az EU-ban és világszerte. [6] Az első rész megjelenését követően 2015-ben megjelent a Marianthi Theocharidou, Georgios Giannopoulos szerzőpáros által kiadott II. tanulmány [9].

A témában részletes NATO kézikönyv is született *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency* címen, ami széleskörűen elemzi a kritikus infrastruktúrák fizikai és kiber védelmét, aminek tartalmát fontos elemezni és értékelni, továbbá meg kell vizsgálni az *Európai Unió és a NATO „EU-NATO Task Force on the resilience of critical infrastructure című* 2023-as értékelő jelentését. Emellett meg kell vizsgálni az Amerikai Egyesült Államok Belbiztonságának *„National Infrastructure Protection Plan Risk Management Framework"*című keretrendszerét tartalmazó domunemtumát. [7]

Nem lehet elmenni a külföldi szakirodalomban *Marianthi Theoharidou Risk assessment methodology for interdependent critical infrastructures* című 2011-es cikkén, ami egy olyan kockázatelemzési keretrendszert mutat be, amely külön hangsúlyt helyez a kritikus infrastruktúrák közötti függőségek feltárására. A szerző kiemeli, hogy a hagyományos kockázatértékelési módszerek nem elegendők, mert nem képesek kezelni az ágazatok közötti láncreakciós hatásokat. A tanulmány ezért komplex, több szintű értékelési megközelítést javasol, amely rugalmasan alkalmazható különböző infrastruktúra rendszerekre. [6]

Enrico Zio *Challenges in the vulnerability and risk analysis of critical infrastructures* című cikkének tanulmányozása elengedhetetlen a kutatásom során, hiszen Zio cikke a kritikus infrastruktúrák sebezhetőségének és kockázatának elemzésével kapcsolatos főbb tudományos és gyakorlati kihívásokat tárgyalja. Hangsúlyozza, hogy a komplex rendszerek hálózatos működése, a bizonytalanság és a sztochasztikus hatások kezelése különösen nehéz feladat.

A tanulmány fejlett matematikai és modellezési módszerek szükségességére hívja fel a figyelmet a reális döntéstámogatás érdekében. [8]

A hazai szakirodalom vizsálata során meg kell említeni Cimmer Zsolt, Kátai-Urbán Lajos és Vass Gyula 2015-ös *Veszélyes üzemekkel kapcsolatos üzemazonosítási szabályozás értékelése-hazai szabályozás* című tudományos cikkét. A tanulmány a veszélyes üzemek hazai azonosítási rendszerét elemzi, különös tekintettel a Seveso-irányelv alkalmazására. A szerzők rámutatnak a szabályozás gyakorlati nehézségeire és az üzemazonosítás következetlenségeire. A cikk módosítási javaslatokat fogalmaz meg a hatékonyabb és egységesebb kockázatkezelés érdekében. [9]

Emellet elemezni szükséges Angyal István és Mógor Judit *A létfontosságú rendszerek védelmére vonatkozó szabályozás fejlesztése* című 2022-es cikkét, hiszen a szerzők áttekintik a magyar kritikus infrastruktúra védelmi szabályozás fejlődését és hiányosságait. A cikk rámutat arra, hogy a szabályozási környezet folyamatos frissítést igényel az új fenyegetések és technológiai változások miatt. Kiemelik az állami irányítás és a szolgáltatói szféra közötti együttműködés fejlesztésének szükségességét. [10]

Szintén érdemes górcső alá venni Mógor Judit és Angyal István *A kritikus infrastruktúrák ellenálló képesség fejlesztését célzó szabályozás mérföldkövei* című cikkét, ami a kritikus infrastruktúrák rezilienciájának szabályozási aspektusait elemzi történeti megközelítésben. A szerzők bemutatják a reziliencia központi szerepét a kockázatcsökkentésben és az üzemmenet-folytonosság biztosításában. Hangsúlyozzák, hogy a jövőbeni szabályozásoknak a megelőzés mellett az adaptációs képességek erősítésére is nagy hangsúlyt kell helyezniük. [11]

Értékelni szükséges Sáfár Brigitta és Kállai Krisztina *A rezíliencia elméletek, mint az egyén és a közösségek alapvető képességének vizsgálata a krízishelyzetek és természeti katasztrófák kapcsán című 2024*-es cikkét, mivel a tanulmány a reziliencia fogalmát vizsgálja pszichológiai és társadalmi szempontból, különösen válsághelyzetek és természeti katasztrófák kontextusában. A szerzők bemutatják, hogyan járul hozzá a reziliencia az egyének és közösségek alkalmazkodóképességéhez és mentális stabilitásához. A cikk hangsúlyozza a közösségi támogatás és a tudatos felkészítés szerepét a katasztrófák hatásainak csökkentésében. [12]

7. AZ ÉRTEKEZÉS FELÉPÍTÉSE, ELHATÁROLÁSOK

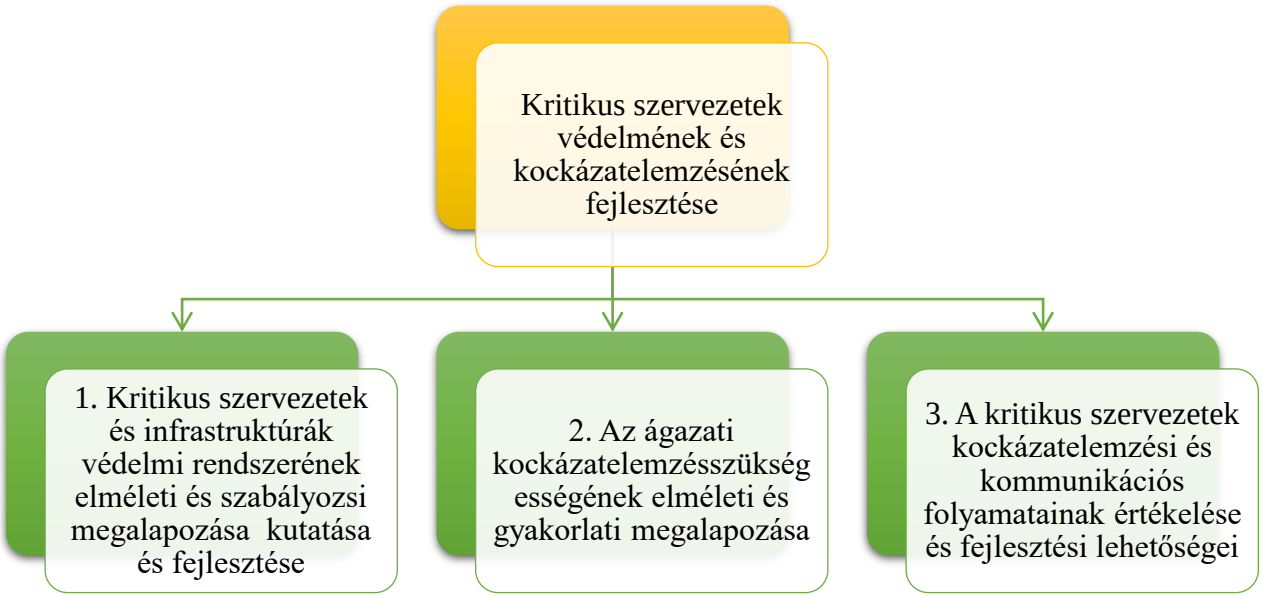
Az első fejezetben összefoglaló és rendszerező tanulmány keretében vizsgálom a kritikus szervezetek és infrastruktúrák védelmi rendszerével kapcsolatos elméleti kérdéseket.

A tudományos rendszerező és elemző munkám része feldolgozni a kritikus szervezetek védelmének intézményi és szabályozási hátterének elemzését, megvizsgálni a kritikus szervezetek fenyegetettségét, valamint meghatározni a képességbeli hiányokat és a lehetséges műszaki fejlesztési lehetőségeket a kritikus infrastruktúrák védelmével összefüggésben.

Az értekezés második fejezetében megvizsgálom egy ágazati kockázatelemzés szükségességét, ennek érdekben értékelem a kritikus infrastruktúrák védelmének és kockázatelemzésének nemzetközi gyakorlatait, tanulmányozom a kritikus szervezetek kockázatelemzésének hazai és külföldi irodalmát, és megvizsgálom, milyen lehetséges módszertan alapján lehetne alkalmazni egy ágazati kockázatelemzést. Javaslatot teszek a módszertan alkalmazására, valamint kidolgozom az alkalmazni kívánt metódust.

Az értekezés harmadik fejezetében feldolgozom a kockázatelemzéssel összefüggő tapasztalatokat, tanulmányozom a kritikus szervezetek vezetői, az ellenálló képességért felelős vezető és a hatóságok közötti kommunikációt és javaslatot dolgozom ki annak fejlesztési lehetőségére, továbbá módszertant és eljárásrendet dolgozom ki egy kockázati jelentés kialakítására és bevezetésére, az ellenálló képességért felelős vezetők interjújának értékelése alapján.

A tudományos célkitűzéseim alapján a doktori értekezést három egymásra épülő tartalmi fejezetre bontva dolgozom ki, amelyet az 1. ábra szemléltet:



1. ábra: *Doktori disszertáció felépítése, Készítette: a Szerző.*

Jelen értekezésben végzett kutatásaim kapcsán elsősorban az alábbi elhatárolási szempontokat veszem figyelembe:

- A kutatási téma interdiszciplináris jellegéből adódik, hogy a kutatásaim során több érintett szakterület, kritikus szervezetek ágazatainak (energia, víz, katasztrófavédelmi, közlekedés, biztonságpolitika stb.) sajátosságait kizárólag a célkitűzésemnek megfelelő mértékben áll módomban elemezni.
- Kutatásom ugyan nemzetközi példákból merít, de nem tartozik célkitűzéseim közé a határon átnyúló kritikus szervezetek és infrastruktúrák és azok hatásainak vizsgálata, a határokon átnyúl együttműködés lehetőségeinek elemzése.
- A CER Irányelv és a NIS 2 Irányelv szorosan kapcsolódik a kritikus szervezetek védelméhez, azonban a kritikus szervezetek kibervédelmét csak olyan mértékben vizsgálom, amely összhangban van a célkitűzéseimmel.
- Az értekezést a békeidőszaki és nem a háborús időszaki eseményekre történő felkészüléssel összefüggésben készítettem el. Ez utóbbi kérdéskör vizsgálata – annak összetettsége miatt – további kutatás tárgya lehet.

A kutatás előkészítését és lefolytatását jelentősen támogatta, hogy szakmai feladataimból fakadóan részt vettem a CER Irányelv honvédelmi szempontú hazai véleményezési folyamatában, valamint az implementációt előkészítő munkacsoport kezdeti ülésein, továbbá részt vettem nemzetközi és hazai szakmai konferenciákon, ahol nyílt forrásokból és interjúk segítségével lehetőségem nyílt adatokat és információt gyűjteni a nemzetközileg alkalmazott eszközökről és felmérni a hazai tapasztalatokat.

Ezen túl több mint nyolc éve foglalkozom kritikus infrastruktúrák védelmének honvédelmi aspektusaival és látok el hatósági tevékenységet. Így gyakorlati tapasztalatokkal és háttér információval is rendelkezem a szakterületi képességek rendelkezésre állásának helyzetéről.

Kutatómunkámat nehezítette, hogy kritikus szervezetek ágazatainak, a NATO és európai uniós kockázatelemzéssel és kritikus infrastruktúrák védelmével összefüggő vizsgálataim során kizárólag a nyilvános forrásokból beszerzett adatokat használhattam fel.

A kutatásaimat 2026. január 31-én zártam le.

1. A KRITIKUS SZERVEZETEK ÉS INFRASTRUKTÚRÁK VÉDELMI RENDSZERÉNEK ELMÉLETI ÉS SZABÁLYOZÁSI MEGALAPOZÁSA, KUTATÁSA ÉS FEJLESZTÉSE

A modern társadalmak működését egyre összetettebb, egymással szorosan összefüggő technológiai, gazdasági és infrastruktúrális rendszerek biztosítják. E rendszerek egyes elemei – az úgynevezett kritikus szervezetek és infrastruktúrák – működésük révén alapvető szolgáltatásokat nyújtanak az állampolgárok, a gazdasági szereplők, valamint az állami intézmények számára. Ezek sérülékenysége vagy meghibásodása nemcsak gazdasági és társadalmi zavarokat, hanem közbiztonsági és nemzetbiztonsági kockázatokat is generálhat. Éppen ezért a kritikus szervezetek védelme kiemelt jelentőséggel bír mind nemzeti, mind uniós szinten.

A 21. század kihívásai – mint a digitalizáció térnyerése, a kibertérben jelentkező fenyegetések, a globális járványok, a klímaváltozás következményei vagy akár a geopolitikai instabilitás – rávilágított arra, hogy a kritikus szervezetek védelme nem csupán technikai kérdés, hanem stratégiai és rendszerelméleti megközelítést igényel. A védelmi rendszer hatékonysága nagyban függ annak strukturális felépítésétől, szabályozottságától, az érintett szereplők együttműködéséről, valamint attól, mennyire képes rugalmasan reagálni a gyorsan változó kockázati környezetre.

Jelen értekezés alapvető célja annak feltárása, hogy a hazai védelmi rendszer – különös tekintettel a kritikus szervezetek kockázatelemzése – mennyiben alkalmas a jelenlegi és jövőbeli fenyegetettségek kezelésére. Ennek érdekében az első fejezet célja egy általános hatáselemzés elvégzése, amely a rendszer működésének vizsgálatán túl feltárja annak strukturális és működésbeli hiányosságait, kritikus pontjait, valamint azonosítja a lehetséges fejlesztési irányokat.

A fejezet középpontjába tehát egy kérdés áll: miként működik jelenleg a kritikus szervezetek védelmi rendszere Magyarországon, milyen eredményeket mutat fel, hol mutatkoznak gyengeségek, és hogyan reagál a változó környezeti feltételekre. Az elemzés több szinten történikm áttekinti a szabályozási keretet, a szervezeti és intézményi szereplőket, megvizsgálja a működési folyamatokat, az együttműködés és kommunikáció minőségét, valamint a technikai és humán erőforrásokat.

A fejezet továbbá megalapozza a kutatás további részeit azzal, hogy azonosítja a főbb problématerületeket és beavatkozási pontokat. E megállapítások mentén fogalmazódnak meg azok a kutatási kérdések és fejlesztési javaslatok, amelyek az értekezés későbbi fejezeteibe részletesebben kidolgozásra kerülnek. Ezzel a fejezet betölti hármas funkcióját, azaz feltáró elemzést végez, értékelést ad a meglévő rendszer működéséről, és javaslatokat készít elő egy fejlesztési keretrendszer számára. A következő alfejezetben először a fogalmi és szabályozási háttér kerül értékelésre, majd a védelmi rendszer működésének elemzése következik. Ezt követi a hiányosságok részletes feltárása, végül pedig a lehetséges fejlesztési irányok azonosítása, figyelembe véve a nemzetközi jó gyakorlatokat.

A disszertáció tárgyi hatálya azokra a kritikus szervezetekre és infrastruktúrákra terjed ki, amelyek a Kszetv. törvény alapján a nemzeti létfontosságú funkciók működőképességét biztosítják. A vizsgálat az első fejezetben az energia-, a közlekedési (vasúti, közúti, légi és vízi), a digitális és a világűr infrastruktúrák körére fókuszál, kiemelten azok műszaki és kockázatelemzési sajátosságaira. Ezen ágazatok működésében meghatározó a kiber és fizikai rendszerek jelenléte, a magas szintű technológiai függőség és az erős interdependencia, amelyek miatt egyes komponensek meghibásodása több ágazatra kiterjedő dominóhatásokat idézhet elő. A kutatás ezért azokra a rendszerjellemzőkre, sérülékenységekre és függőségekre koncentrál, amelyek kockázatelemzési szempontból meghatározzák a kritikus szervezetek ellenállóképességét, és alapot adnak a későbbi fejlesztési javaslatok megalapozásához.

1.1 A kritikus szervezetek védelmének intézményi és szabályozási hátterének elemzése

A kritikus szervezetek védelmének vizsgálata során elengedhetetlen a kulcsfogalmak pontos definiálása és azok egységes értelmezése. E fogalmak nem csupán a szakpolitikai és jogszabályi környezetben bírnak meghatározó szereppel, hanem a kutatás értelmezési keretét is kijelölik, befolyásolva az alkalmazott módszertant és a lehetséges következtetéseket.

1.1.1 A kritikus szervezetek védelméhez kapcsolódó fogalmi és értelmezési keretek

1.1.1.1 A kritikus szervezetek védelméhez kapcsolódó szabályozás értékelése műszaki és rendszerszintű szempontok alapján

A kritikus infrastruktúrák fogalma az idők során jelentős fejlődésen ment keresztül, tükrözve a társadalmi, gazdasági és technológiai változásokat, valamint a fenyegetések és kockázatok alakulását. Az infrastruktúrák alapvető fontosságának felismerése és azok védelmének szükségessége nem újkeletű, de a kritikus infrastruktúrák modern koncepciója a 20. század végén kezdett formálódni és azóta folyamatosan bővül és mélyül.

A Kszetv. hazai szinten új keretet teremt a kritikus szervezetek ellenálló képességének és a kapcsolódó kockázatmenedzsment folyamatok szabályozására. [13] A kritikus infrastruktúrák a 3. §-a alapján „*olyan eszköz, létesítmény, építmény, berendezés, hálózat, rendszer vagy ezek része, amely az alapvető szolgáltatás nyújtásához szükséges*.” [13] Ez például lehet egy erőmű, ivóvízhálózat, adatközpont vagy vasúti vezérlőrendszer. A kritikus szervezetek emellett alapvető szolgáltatást nyújtó szervezetek, valamint elengedhetetlenek az ország társadalmi, gazdasági stabilitásához és a biztonság, a környezet, a közegészségügy, a védelmi képességek és a nemzeti ellenálló képességi rendszer fenntartásához. A kritikus szervezetek a kritikus infrastruktúrákat birtokolják, üzemeltetik, vagy irányítják, illetve felelősek annak fenntartásáért, működéséért. Például az áramszolgáltató vállalat, amely üzemelteti az elektromos hálózatot.

Fontos tisztázni, hogy a kritikus szervezet mindig valamilyen kritikus infrastruktúrához kapcsolódik, annak működtetője, fenntartója vagy tulajdonosa. A védelem közvetlen tárgya az infrastruktúra, de a felelősségi és intézkedési kötelezettségek a szervezetet terhelik.

Emellett az alapvető szolgáltatások a kritikus szervezet által biztosított szolgáltatás, amelynek működése nélkülözhetetlen Magyarország társadalmi és gazdasági stabilitásának megőrzéséhez, valamint a nemzet biztonságának, környezetének védelméhez, a közegészségügy működéséhez, a védelmi képességek fenntartásához és a nemzeti ellenálló képességi rendszer működéséhez. Ilyen az országos sürgősségi betegellátás, az Országos Mentőszolgálat által nyújtott mentési szolgáltatás, a villamosenergia-átvitel és – elosztás, azaz a MAVIR Zrt. rendszerirányítása, vagy az MVM Zrt. elosztóhálózat üzemeltetése.

A Kszetv. értelmében az ellenálló képesség egy adott kritikus szervezet vagy infrastruktúra azon komplex képességét jelenti, hogy egy váratlan rendkívüli eseményt – legyen az természeti, technológiai, emberi eredetű vagy szándékos támadás – képes megelőzni, felismerni, kezelni, a hatásait enyhíteni, illetve az azt követő működését helyreállítani. Ez a képesség nem statikus állapot, hanem egy folyamatosan fejlesztendő rendszerszintű készség, amely szervezeti, technológiai, humán és szabályozási elemeket egyaránt magába foglal. Például egy áramszolgáltató képes-e egy hirtelen kibertámadás után gyorsan visszaállítani az ellátást, vagy egy kórház informatikai rendszere túléli-e egy áramszünet vagy zsarolóvírus támadás hatásait és képes-e adatvesztés nélkül újraindulni. [13]

A kockázat fogalma és a kockázatalapú gondolkodás bővebben került bevezetésre a Kszetv.-ben. A kockázat a veszteségek, zavarok és kiesések lehetőségét jelenti, amelyet egyrészt a potenciális esemény bekövetkezésének valószínűsége, másrészt annak hatásának súlyossága határozza meg.

A modern biztonsági szemlélet nem csupán az események elkerülésére törekszik, hanem a kockázat alapú gondolkodás alkalmazására. A döntéshozók előre azonosítják a releváns kockázatokat, elemzik azok természetét, értékelik a kezelhetőségüket, majd megalapozott stratégiákat dolgoznak ki azok kezelésére. A Kszetv. részletesen szabályozza a kockázatkezelés folyamatát, amely négy alapvető lépésből áll:

1. A kockázatazonosítás azon tényezők felismerése, amelyek veszélyeztethetik a szervezet működését vagy céljainak elérését. Például elöregedett adatmentési infrastruktúra, amely kritikus adatok elvesztéséhez vezethet.
2. A kockázatelemzés a kockázat természetének megértése, a következmények, a valószínűségek és a forgatókönyvek vizsgálata. Például mi történik, ha 24 órára leáll a vízellátás egy megyeszékhelyen.
3. A kockázatértékelés annak eldöntése, hogy az adott kockázat elfogadható-e, vagy szükséges-e beavatkozás. Például a leállás kockázata nem elfogadható, mert életveszélyes következményekkel járhat.
4. A kockázatkezelés intézkedések és erőforrások tervezett alkalmazása a kockázat csökkentésére, elkerülésére vagy enyhítésére. Például tartalék generátorok telepítése, ügyeleti protokoll bevezetése. [13]

A kockázati fogalmak mellett a rendkívüli esemény és a kölcsönös függés is megjelenik a Kszetv.-ben. A törvény egyik újdonsága a rendkívüli esemény fogalmának kiterjesztése, nem csupán akkor tekinthető egy esemény rendkívülinek, ha az egy szolgáltatás kiesését okozza, hanem akkor is, ha annak elhárításához más, külső szereplő beavatkozása válik szükségessé. Ez a meghatározás felismeri azt a kölcsönös függőséget, amely a különböző kritikus ágazatok (energia, közlekedés, egészségügy, hírközlés stb.) között fennáll – az egyik rendszer sérülékenysége dominóhatást válthat ki a többiekben. Például egy regionális áramszünet miatt leáll az ivóvíz szolgáltatás, amit a vízmű nem tud egyedül elhárítani, így a katasztrófavédelem és az energiaszolgáltató összehangolt fellépésére van szükség. [13]

Emellett a Kszetv. számos a kritikus szervezetek védelmével összefüggő fogalmat határoz meg. Az ellenálló képességi mátrix olyan elemzési eszköz, amely a kritikus infrastruktúrát érintő kockázatokat, azok hatását, gyakoriságát és a szervezet kitettségét rendszerezetten jeleníti meg. A mátrix célja, hogy átláthatóvá tegye a kockázatok jelentőségét, valamint kijelölje a kezelésükre szolgáló beavatkozási pontokat.

Tartalmazza a maradványkockázatok azonosítását is, ezáltal támogatva a szervezet tudatos kockázati toleranciaszintjének meghatározását. A mátrix a kockázatkezelési döntéshozatal központi dokumentuma. [13]

Az ellenálló képességi terv a kritikus szervezet működésének védelmét biztosító átfogó dokumentum, amely kockázatkezelési, riasztási, fizikai védelmi és helyreállítási intézkedéseket foglal magában. Tartalmazza a rendkívüli események megelőzésének és kezelésének folyamatát, valamint az alapvető szolgáltatás újraindításának alternatív megoldásait. A terv kijelöli a kritikus munkakörök feladatait, az ehhez kapcsolódó oktatási és gyakorlati követelményeket is. Ezáltal a szervezet felkészültségének alapdokumentuma, amely a reziliencia operatív megvalósítását biztosítja. [13]

A horizontális kritérium olyan ágazattól független szempont, amely alapján egy szervezet, létesítmény vagy eszköz kritikusnak minősíthető. A kritérium figyelembe veszi a kölcsönös függőségeket, a kritikus kitettséget, az alternatív ellátási lehetőségeket és az ellátási láncban betöltött szerepet. Lényege, hogy ne csak ágazati logika mentén lehessen kijelölni kritikus infrastruktúrát, hanem rendszerszintű megfontolások alapján is. Ez elősegíti a komplex, több ágazatot érintő kulcselemek azonosítását. Az ágazati kritérium olyan, a Kszetv. 1. mellékletében meghatározott ágazathoz kötődő szempont, amely alapján egy szervezet, eszköz vagy létesítmény elengedhetetlennek minősíthető Magyarország társadalmi és gazdasági stabilitása, valamint a biztonság, környezetvédelem, közegészségügy, védelmi képességek és nemzeti reziliencia fennmaradása szempontjából. A fogalom célja az ágazatspecifikus sajátosságok figyelembevétele a kritikus szervezetek és infrastruktúrák kijelölése során, mivel egyes szolgáltatások jelentősége és sérülékenysége erősen ágazatspecifikus. Az ágazati kritériumok meghatározása lehetővé teszi, hogy a kijelölési folyamat ne csak általános, hanem ágazati mélységű szakmai elvek alapján történjen. Ennek eredményeként a védelem és a kockázatkezelés célzottabbá és hatékonyabbá válik az adott szektor saját működési logikájához igazodva. [13]

A Vbö. I. fejezetében meghatározza az ország védelme és biztonsága szempontjából jelentős infrastruktúrák és szervezetek különböző alcsoportjait, attól függően, hogy mely kijelölő hatóság jelölte ki őket, és hogy a kijelölés honvédelmi ágazaton belül vagy azon kívül történt. A fogalmak rendszere megkülönbözteti a kizárólag honvédelmi ágazatban kijelölt elemeket, a kettős (honvédelmi és általános) kijelölésű infrastruktúrákat és szervezeteket, valamint azokat, amelyeket csak a honvédelmi ágazati hatóság jelölt ki más ágazatban.

A cél, hogy az alapvető szolgáltatások folytonosságához és az ország biztonságához nélkülözhetetlen szervezetek és infrastruktúrák pontos kategorizálásban jelenjenek meg, külön kezelve a honvédelmi jelentőségű szereplőket. Ez a differenciált rendszer biztosítja, hogy a védelem, a felügyelet és az ellenállóképesség fejlesztése a kijelölés jellegéhez igazodó, célzott módon valósulhasson meg. [14]

1.1.1.2 A kritikus szervezetek védelméhez kapcsolódó alapfogalmak műszaki és funkcionális elemzése

A kritikus szervezetek és infrastruktúrák azonosítása a jogi keretrendszer mellett a műszaki szakirodalmi megközelítésekben is központi jelentőségű. A rendszerek fejlődése, a hálózatok összekapcsoltsága, a digitális irányítórendszerek mint például Industrial Control System (a továbbiakban: ICS), és SCADA szerepe, valamint a rendszerszintű sebezhetőségek megjelenése szükségessé tette, hogy a kritikus fogalmakat ne csak jogi, hanem mérnöki és rendszerelméleti szempontból is értelmezzük. [15]A következőkben elemzem a Kszetv.-ben definiált fogalmak műszaki tartalmait, valamint összevetem a jogi megközelítéssel. Az ágazati kritériumok műszaki értelmezésben olyan hálózati, fizikai és technológiai szempontokat jelentenek, amelyek alapján az adott ágazat létfontosságú elemei azonosíthatók. Míg jogi oldalról ezek a társadalmi jelentőség és kapcsolódó kötelezettségek alapján kerülnek meghatározásra, a műszaki szakirodalomban a rendszerek topológiája, a függőségek és a redundancia hiánya kerül előtérbe. A villamosenergia hálózat átviteli pontjai, a távközlési maghálózat gerince vagy a vízkivételi művek fő vezérlői példák olyan technikai elemekre, amelyek ágazati szempontból kritikusnak minősülnek.

Az alapvető szolgáltatás fogalma műszaki megközelítésben olyan szolgáltatást jelöl, amely rendkívül magas rendelkezésre állást, meghibásodás tűrést és redundáns architektúrát igényel. Nemzetközi modellek pl. a megbízhatósági elmélet szerint ezek mögött összetett fizikai és információs rendszerek állnak, amelyek működését rendszerfolyamatok és szolgáltatási szintek határozzák meg. A jogi definiálás társadalmi nélkülözhetetlenségre épül, míg a műszaki szemlélet a hibakövetkezmények, a késleltetés, a kiesési idők és a működésbiztonsági paraméterek oldaláról közelíti meg a kérdést.

Az ellenálló képesség a műszaki szakirodalomban mérhető, dinamikus rendszerjellemző, amely a rendszer zavarokra adott válaszreakcióját, alkalmazkodóképességét és helyreállítási idejét foglalja magában. A reziliencia négy fő dimenziója a robusztusság, az erőforrás-mobilizáció, a rugalmasság és a helyreállítási kapacitás. Mérőszámai között szerepelhet például a helyreállítási idő a redundanciafok vagy a sérülés utáni teljesítménygörbe alatti terület.

A jogi meghatározás feladat- és kötelezettség orientált, míg a műszaki megközelítés a rendszer viselkedésének időbeli és strukturális modellezésére épül. Ezzel szorosan összefügg az ellenálló képességi terv, amely mérnöki logikában a működésbiztonsági és üzemfolytonossági dokumentumok gyűjtőfogalma. A dokumentum tipikusan tartalmazza a hálózati redundanciák biztosítását, az alternatív üzemmódokat, a tartalékkapacitásokat, az incidenskezelési protokollokat és a kiberbiztonsági integrációkat. Míg a jogi fogalom szervezeti és eljárási szintű, a műszaki változat konkrét rendszertervhez kötött, részletes technikai folyamatleírásokkal. [16]

A horizontális kritérium mérnöki megközelítésben olyan rendszerszintű, ágazattól független jellemzőt takar, amely kritikus szerepet jelöl ki a hálózat működésében. Tipikus példák az interdependenciák, a központi csomópontok, a szűk keresztmetszetek, a redundancia hiánya vagy az ellátási láncban betöltött egyedüli szerepkör. Míg a jogi definíció célja az ágazaton átívelő kijelölési logika megteremtése, a műszaki értelmezés a rendszerelméleti sebezhetőségekre és a láncreakciók kockázatára épít. A kritikus infrastruktúra a műszaki szakirodalomban információs és fizikai rendszerek komplex hálózatát jelenti, amelyek működését számottevően befolyásolja a topológia, a sebezhetőségi pontok elhelyezkedése, és a függőségi hálózatok szerkezete. Míg a jogi szabályozás társadalmi jelentőség alapján jelöl ki infrastruktúrát, a műszaki elemzések a rendszer komplexitását, hibaterjedési mintáit és redundanciafokát vizsgálják.

A kritikus szervezet műszaki értelmezésben olyan operátor vagy üzemeltető, amely felelős a szolgáltatás technológiai, üzemviteli és információs és fizikai működéséért. A szakirodalom hangsúlyozza, hogy a kritikus szervezet működése nem csupán adminisztratív, hanem rendszerarchitektúrához kötött, humán erőforrás, működési eljárások, beszerzési láncok egyaránt meghatározzák. A műszaki megközelítés tehát az operátori szerepet, nem pedig a jogi besorolást tekinti elsődlegesnek. A rendkívüli esemény műszaki értelmezése szélesebb spektrumot ölel fel, mint a jogi. Minden olyan rendszerállapot változást ide sorol, amely eltérést okoz a normál működéstől, azaz meghibásodást, külső fizikai behatást, kiber incidenst, üzemzavart vagy irányítórendszeri hibát. A nemzetközi gyakorlatban az incidenskezelést szabványos modellek vezérlik, amelyek az esemény életciklusát, tehát az észlelést, az elemzést, a reagálást, a helyreállítást definiálják. A jogi fogalom csak a bizonyos következményszintet elérő eseményeket tekinti rendkívülinek, a műszaki megközelítés ezzel szemben az alacsony intenzitású zavarokat is elemzi, mert ezek gyakran kritikus előjelei nagyobb hibáknak. [17]

Végül a fogalmak műszaki értelmezése szorosan összefügg a kockázatkezelési paradigmával, amely a kritikus infrastruktúrák működését meghatározza.

A mérnöki szakirodalom egyértelműen megkülönbözteti a veszélyt, a fenyegetést, a sebezhetőséget és a kitettséget és a kockázatot ezek függvényeként írja le. Az ISO 31000 és az ISO 22301 szabványok, valamint a veszélyes üzemekben alkalmazott módszerek a Hazard and Operability Study (a továbbiakban: HAZOP), a Fault Tree Analysis (a továbbiakban: FTA), az Event Tree Analysis (a továbbiakban: ETA), a Bow-Tie jól illeszkednek a kritikus infrastruktúrák vizsgálatához, mivel képesek a rendszerhibák, a dominó események és üzemzavarok strukturált feltárására. A kritikus infrastruktúrák sajátossága, hogy egyszerre kell kezelni fizikai, kiber- és működési kockázatokat, amelyek egymást erősítő módon jelenhetnek meg.

Összességében a Kszetv. fogalmai szilárd jogi keretet biztosítanak, a műszaki megközelítés pedig ezeket rendszerelméleti, mérnöki és üzemeltetési kontextusba helyezi. A két szemlélet együtt ad teljes képet arról, hogy a kritikus infrastruktúrák sérülékenysége, védelme és ellenálló képessége hogyan értelmezhető a gyakorlatban. A jogi kijelölések így műszaki tartalommal egészülnek ki, és biztosítják, hogy a kritikus elemek nemcsak szabályozási, hanem rendszertechnikai szempontból is azonosíthatók és védhetők legyenek.

1.1.1.3 Kockázatkezelés műszaki értelmezése a kritikus szervezetek és infrastruktúrák rendszerszemléletű megközelítésében

A műszaki szakirodalomban a kockázatkezelés olyan rendszerezett, ciklikus folyamat, amely a veszélyek azonosítására, a kockázatok számszerűsítésére, a megelőző és védelmi intézkedések meghatározására, valamint a működés folytonosságának biztosítására irányul. A kritikus infrastruktúrák működése során a kockázatkezelés különösen összetett feladat, mivel a rendszerek információs és fizikai jellegűek, magas fokú összekapcsoltsággal és jelentős interdependenciákkal rendelkeznek. A műszaki megközelítés elsősorban kvantitatív, modellezésre épülő módszereket alkalmaz, amelyek lehetővé teszik a hibaterjedések, dominójelenségek és működési zavarok előrejelzését.

A veszély a rendszer fizikai vagy technológiai tulajdonságából fakadó potenciális károkozó tényező. A mérnöki környezetben ilyen lehet egy túlnyomás egy csővezetékben, egy forgógép kopása, egy transzformátor túlmelegedése vagy egy fizikai vagy információs rendszer protokollsebezhetősége. A fenyegetés ezzel szemben szándékos vagy célzott cselekmény is lehet, például kibertámadás az ICS vezérlés ellen. [18] A veszély és a fenyegetés együtt alakítja ki azt a környezetet, amelyben a rendszer sebezhetősége értelmezhető. [19]A sebezhetőség a rendszer olyan gyenge pontja, amelyen keresztül a veszély vagy fenyegetés reálisan kárt okozhat.

A kritikus infrastruktúrák esetében a sebezhetőségek gyakran hálózati vagy irányítástechnikai jellegűek ritka redundancia, elavult SCADA-protokollok, titkosítás nélküli kommunikáció, vagy földrajzilag koncentrált erőforrások. [20]

A kitettség azt mutatja meg, hogy a rendszer mennyire van ténylegesen jelen a veszélyzónában például egy árvízvédelmi létesítmény árvízszinthez való közelsége, vagy egy alállomás kibertámadási felülete. Kritikus infrastruktúráknál a fizikai és kiberkitettség gyakran együttesen jelenik meg, ami komplex kockázati mintázatot eredményez. A kockázat a bekövetkezés valószínűsége és a következmény súlyossága közötti kapcsolat, azaz a kockázat egyenlő a hatás és valószínűség szorzatával. A kritikus rendszerekben a következmény lehet szolgáltatás kiesés, kapacitáscsökkenés, hálózati instabilitás vagy interdependenciából fakadó dominóhatás [21]. A műszaki szakirodalom és a veszélyes üzemekben alkalmazott módszerek alapján a kockázatkezelés az alábbi lépésekre bontható: [22]

A kockázatazonosítás fázisban történik a veszélyek, fenyegetések, hibamódok, működési zavarok feltérképezése. A kritikus infrastruktúráknál az alábbi módszereket alkalmazzák:

- A HAZOP (Hazard and Operability Study) részletes, csomóponti szintű veszélyelemzés vegyi üzemekben, ivóvízművekben, energetikai rendszerekben. Például egy víztisztító telepben a klóradagoló állomás HAZOP-ja feltárja a túladagolási, szelepmeghibásodási vagy áramkimaradásból eredő működésképtelenségeket. [23]
- A FMEA/FMECA (Failure Mode and Effects Analysis / Criticality Analysis) eszköz- vagy rendszerkomponens szintű hibaelemzés. Például transzformátorvédelmi relék hibamódjainak vizsgálata villamosenergia-hálózatban. [24]
- A Kiber-Hazard elemzés ICS rendszerekre– protokollsebezhetőségek, hozzáférési utak, SCADA-logika hibái. [25]

A kockázatértékelés a kockázatok számszerűsítése többféle módszerrel történhet:

- Az FTA (Fault Tree Analysis) logikai hibafa elemzés a lehetséges meghibásodási ok-okozati láncolatok modellezésére. Tipikus alkalmazása, ha egy atomerőmű hűtőrendszerének meghibásodási valószínűségének becslése. [26]
- Az ETA (Event Tree Analysis) eseményfák segítségével előre jelezhető, hogyan terjed egy induló hiba különböző következményirányokba. [27]
- A Monte Carlo-szimuláció valószínűségi következmény modellek összetett kritikus infrastruktúrákra. [28]
- A hibamodellek (elektromos hálózat → telekommunikáció → víz → közlekedés) Ezek alkalmasak láncreakció szerű meghibásodások. [29]

A kockázatkezelés során a műszaki intézkedések célja a valószínűség vagy a következmény csökkentése:

- redundancia növelése (tartalék ágak, bypass útvonalak, tartalék generátorok),
- robusztus irányítórendszerek (SCADA-biztonság),
- automatikus leválasztó és védelembe kapcsoló rendszerek,
- földrajzi diverzifikáció (elosztott infrastruktúra),
- kiberbiztonsági védelem (titkosítás, hozzáférés-kezelés).

A monitoring és visszacsatolás folyamatában a folyamatos felügyelet, hibadetektálás és anomáliaelemzés (AI-alapú rendszerek, sensor fusion technikák) elengedhetetlenek a kritikus infrastruktúrák biztonságához. Például az okos elektromos hálózatok valós idejű terheléseloszlási monitorozása, amely előre jelzi a túlterhelést és megelőzi a kimenő ágak lekapcsolását.

A veszélyes üzemekben alkalmazott módszerek sok tekintetben megegyeznek a kritikus infrastruktúrák vizsgálati technikáival. Magyarországon a SEVESO üzemek kockázatértékelési gyakorlata számos olyan elvet használ, amely a kritikus infrastruktúrákra is átültethető [9]:

- HAZOP → működéskritikus létesítmények folyamatbiztonsága.
- Bow-Tie elemzés → ok–következmény összekapcsolása.
- Quantitative Risk Assessment (a továbbiakban: QRA) → valószínűségi következmény-becslés.
- Eszkalációs eseményláncok elemzése → kaskádhibák előrejelzése CI-hálózatokban. [29]

Ezek jól illeszkednek a kritikus infrastruktúrák technikai sajátosságaihoz, különösen ott, ahol informatikai és fizikai rendszerek integráltan működnek.

A kritikus infrastruktúrák kockázatkezelése műszaki szemléletben multidiszciplináris folyamat, amely a fizikai, technológiai és kiberfenyegetések együttes vizsgálatára épül. A kockázatkezelési ciklus nem csupán a veszélyek azonosításából áll, hanem magában foglalja a hibarendszerek modellezését, a hálózati interdependenciák vizsgálatát, valamint olyan veszélyes üzemi módszerek adaptálását, amelyek bizonyítottan alkalmasak összetett rendszerek hibafolyamatainak feltárására. A műszaki szakirodalmi megközelítés így kiegészíti a jogi kereteket, és megteremti a kritikus infrastruktúrák rezilienciájának mérhető, tervezhető és fejleszthető alapjait.

1.1.2 A kritikus szervezetek védelmének szabályozási környezete – elemző és értékelő megközelítés

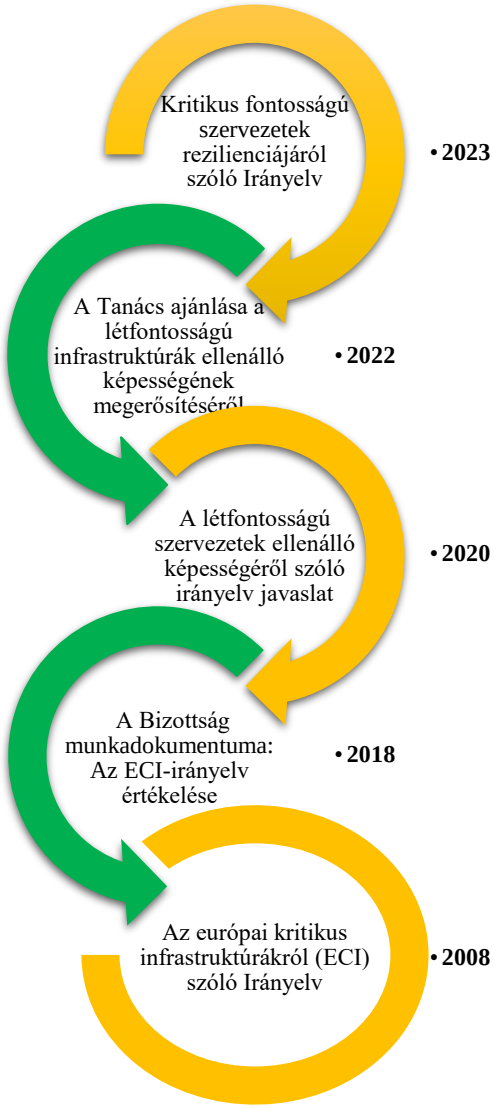
A kritikus szervezetek védelme nem csupán nemzeti érdek, hanem szorosan kapcsolódik az Európai Unió (a továbbiakban: EU) közös biztonsági, digitális és infrastrukturális politikáihoz. Az uniós szinten meghatározott szabályozási keretek célja, hogy a tagállamok egységes alapelvek mentén, összehangolt módon biztosítsák a kritikus szervezetek és infrastruktúrák védelmét, figyelembe véve a határokon átnyúló kockázatokat és interdependenciákat.

A jelenlegi uniós szabályozás központi eleme a NIS 2 Irányelv [3], amely a hálózati és információs rendszerek biztonságáról szól, és 2023-ban vált kötelezően átültetendővé a tagállamok nemzeti jogrendjébe. A NIS2 Irányelv célja, hogy növelje az EU egészének kiberellenálló képességét, különös tekintettel a létfontosságú szolgáltatásokat nyújtó szervezetekre. Az irányelv új követelményeket vezet be a kockázatkezelés, incidensjelentés, hatósági ellenőrzés és szankcionálás terén, és jelentősen kiszélesíti az érintett ágazatok körét. [3]

A nemzetközi térben a NATO és az ENSZ is egyre hangsúlyosabban foglalkozik a kritikus szervezetek és infrastruktúrák védelmével. Ezek a szervezetek főként ajánlásokat, irányelveket és jó gyakorlatokat tesznek közzé, amelyek a tagállamok belső szabályozásának kiegészítő elemei lehetnek – különösen a kiberfenyegetések, a hibrid támadások, valamint a természeti katasztrófák elleni felkészülés terén. A nemzetközi és uniós szabályozás közös jellemzője, hogy egyre inkább a reziliencia-alapú megközelítést helyezik előtérbe, szemben a kizárólag védelmi vagy reaktív szemlélettel. Ez azt jelenti, hogy a rendszereknek nemcsak ellen kell állniuk a támadásoknak, hanem képesnek kell lenniük a gyors helyreállításra, a zavarok lokalizálására, valamint a működés folyamatos fenntartására is – még krízishelyzetekben is.

A CER irányelv 2023. január 16-án lépett hatályba, a nemzeti jogszabályi környezetbe történő átültetési határideje 2024. október 17 volt. [30] A CER Irányelv hatályba lépésével és az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló a TANÁCS 2008/114/EK Irányelvnek [31] (a továbbiakban: ECI Irányelv) hatályon kívül helyezésével olyan változások következtek be az akkori nevén létfontosságú rendszerelemek védelmében, amelyek újragondolják az egész rendszer felépítését és célkitűzéseit. A CER Irányelv jelentős hangsúlyt fektet a modern kockázatok kezelésére, mint például a kibertámadások, természeti katasztrófák, járványok és a hibrid fenyegetések, emellett kibővíti az ágazatok körét, beleértve az energetikai, szállítási, banki, pénzügyi piac infrastruktúráit, egészségügyi, ivóvíz- és szennyvízkezelési, digitális

infrastruktúrákat, közlekedést, élelmiszerellátást, közigazgatást és gyártást. Emellett a CER Irányelv kötelezi a tagállamokat arra, hogy kockázatértékeléseket végezzenek és folyamatosan frissítsék azokat. Az érintett kritikus szervezetek kötelesek jelenteni minden olyan eseményt, amely jelentős hatással lehet az infrastruktúrájukra, és veszélyeztetheti az ellátásbiztonságot. A tagállamoknak együtt kell működniük az EU szerte működő partnereikkel, valamint meg kell osztaniuk az információkat és a jó gyakorlatokat. Az irányelv ösztönzi a közös megközelítések és szabványok kialakítását, hogy a rezilienciát egységes szinten lehessen kezelni EU szerte. Ezen felül a CER Irányelv kiemelt figyelmet fordít a kibertámadások elleni védelemre, és megköveteli, hogy a kritikus szervezetek fejlesszék informatikai rendszereik biztonságát, és alakítsanak ki hatékony válaszintézkedéseket a digitális fenyegetések ellen [30].



2. ábra: *Az Európai Uniós szabályozás kialakulásának mérföldkövei*

Készítette: a Szerző, forrás: [3-6]

A CER Irányelvvel kapcsolatos jogharmonizáció 2023-ban kezdődött meg. Ezáltal a korábban hatályban lévő jogszabályok hatályukat veszítették, azaz a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (a továbbiakban: Lrtv.), [32] a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet (a továbbiakban: Lrtv. Vhr.) [33] és az ágazati rendeletek.

3. ábra: CER Irányelv implementálásának lépései, Készítette: a Szerző, forrás: [30]

A törvényjavaslat benyújtásának időpontját 2024. októberre datálták. A CER Irányelv értelmében nem csak új szabályozást kellett létrehoznia a tagállamoknak, hanem el kell készíteniük a kritikus szervezetek rezilienciájára vonatkozó stratégiát. A stratégiának tartalmaznia kell a kritikus szervezetek rezilienciájának fokozására irányuló célkitűzéseket különös tekintettel a határokon átnyúló és kölcsönös függőségekre, a stratégia végrehajtásában részt vevő szervezetek körét, a reziliencia fokozására irányuló intézkedések leírását, a kritikus szervezetek azonosítását szolgáló eljárás leírását, a kritikus szervezetek védelmében szerepet játszó szervezetek közötti együttműködés erősítését célzó intézkedéseket, főbb hatóságok jegyzékét. A tagállamoknak négyévente frissíteniük kell stratégiáikat, és az elfogadást követő három hónapon belül továbbítaniuk kell azokat az Európai Bizottságnak, beleértve a jelentős frissítéseket is [30].

A stratégiát követően szükséges elkészíteni a nemzeti kockázatelemzést, amely egy tervezési dokumentum a kritikus szervezetek és infrastruktúrák ellenálló képességének támogatása érdekében.

A nemzeti kockázatelemzés elkészítése során figyelembe kell venni az ágazatokat, Magyarország nemzeti katasztrófakockázat-értékelését, az általános és ágazatspecifikus kockázatokat, valamint a meglévő uniós normák alapján készített kockázatelemzéseket. A nemzeti kockázatelemzés tartalmát a kritikus szervezetnek figyelembe kell vennie a saját kockázatelemzésének elkészítése során, valamint az ellenálló képességi intézkedéseinek megtételéhez. A nemzeti kockázatelemzés újdonságként jelenik meg a kritikus infrastruktúrák és szervezetek védelmében [34].

A jogszabályok implementálása során az eddigiektől eltérően a törvény végrehajtási rendelete és az ágazati specifikumokat szabályozó rendeletek nem külön korm. rendeletben kerültek megjelenítésre, hanem egy rendeletben összpontosulnak. Kivételt képez ez alól a honvédelmi ágazat, ahol továbbra is külön jelennek meg a specifikus szabályok. A fentiek alapján megállapítható, hogy a CER Irányelv a kritikus infrastruktúrák, kritikus szervezetek védelmét egy holisztikusabb és adaptívabb megközelítés keretében szabályozza, ami a globális biztonsági környezet változásainak megfelelően alakul.

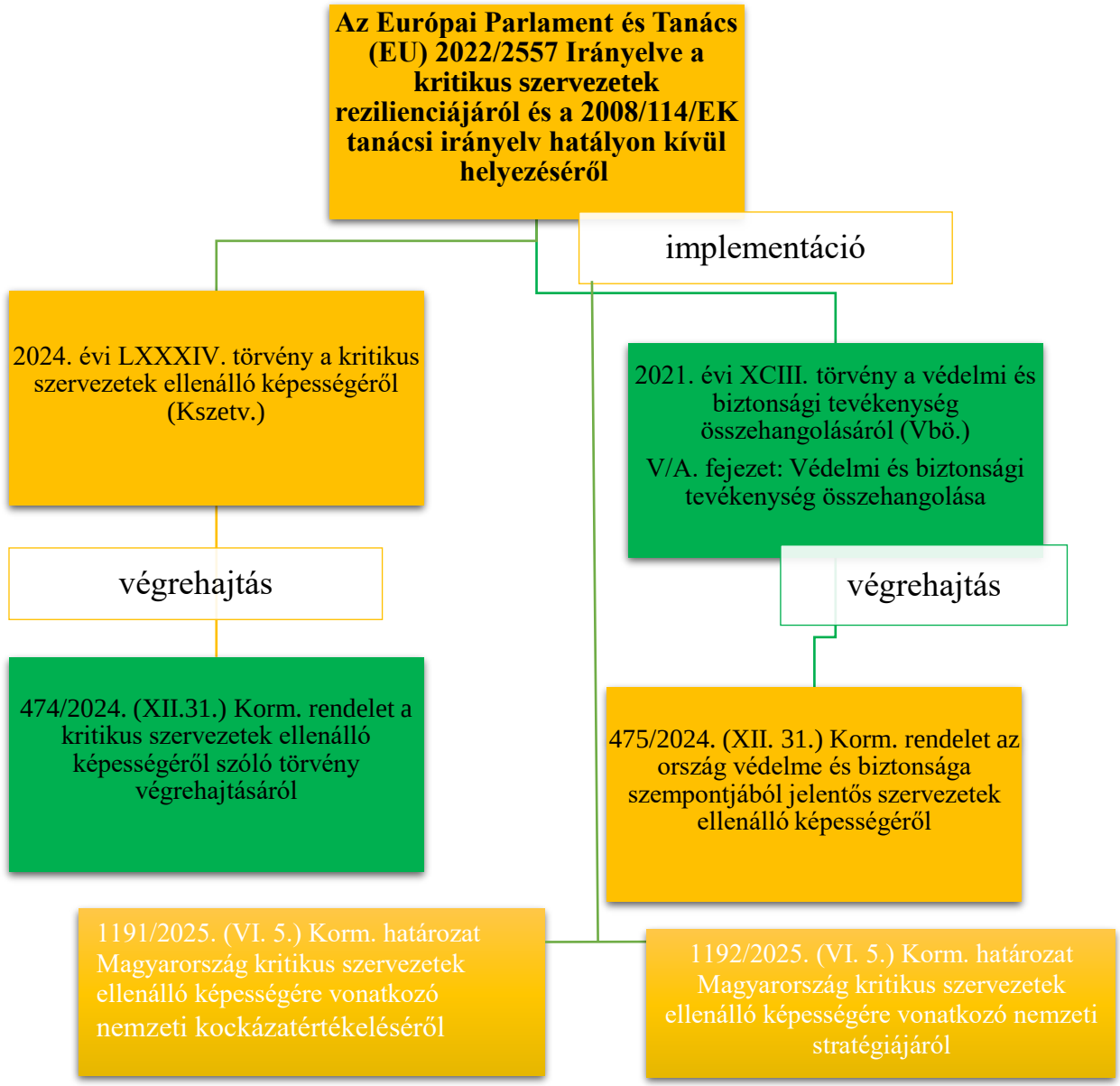
1.1.3 A kritikus szervezetek védelmének hazai szabályozási környezete

Magyarország Alaptörvényében a kritikus infrastruktúrákkal kapcsolatos közvetlen szabályozás nem található. Az Alaptörvény inkább általános elveket és kereteket határoz meg, amelyek közvetve érinthetik a kritikus infrastruktúrák védelmét és biztonságát [35].

A vonatkozó rendelkezések közé tartoznak:

1. Állampolgárok védelmével összefüggésben az Alaptörvény kimondja, hogy Magyarország védi állampolgárait, ami magában foglalhatja az infrastruktúrák védelmét, amelyektől az állampolgárok mindennapi élete függ.
2. Nemzetbiztonsági kérdéssel összefüggésben a magyar állam működése a hatalom megosztásának elvén alapszik, és az állam jogosult kényszer alkalmazására az Alaptörvény és a jogszabályok érvényre juttatása érdekében, amely magában foglalhatja a kritikus infrastruktúrák védelméhez szükséges intézkedéseket.
3. Nemzetközi együttműködéssel összefüggésben Magyarország közreműködik az európai egység megteremtésében EU tagállamaként, és részt vesz a közös európai biztonsági intézkedésekben, amelyek kiterjednek a kritikus infrastruktúrák védelmére is.

Ezek az általános rendelkezések biztosítják a keretet a részletesebb törvények és rendeletek számára, amelyek specifikusan szabályozzák a kritikus infrastruktúrák védelmét [35].



4. ábra: Kritikus szervezetek jogszabályi háttere, Készítette: a Szerző, 2025.

Az ábra a kritikus szervezetek ellenálló képességének uniós és hazai szabályozási rendszerét, valamint az implementáció és végrehajtás logikai láncolatát mutatja be. A folyamat kiindulópontja a CER Irányelv, amely meghatározza a kritikus szervezetek rezilienciájának új kereteit, és hatályon kívül helyezi a korábbi ECI Irányelvet. Ennek hazai implementációja két fő törvényen keresztül valósul meg, egyrészt a Kszetv.szabályozását rögzíti, másrészt a Vbö. összehangolását szabályozza, különösen annak V/A. fejezete révén. A törvényi szint alatt helyezkednek el a végrehajtási rendeletek a Kszetv. végrehajtását biztosító kormányrendelet, valamint a Vbö. Vhr.

A szabályozási struktúrát tovább erősítik a 2025-ben kiadott kormányhatározatok az 1191/2025. (VI. 5.) határozat, amely a kritikus szervezetek ellenálló képességére vonatkozó nemzeti kockázatértékelést írja elő (a továbbiakban: nemzeti kockázatelemzési határozat), illetve az 1192/2025. (VI. 5.) határozat, amely a nemzeti reziliencia-stratégia kereteit határozza meg (a továbbiakban: nemzeti stratégiai határozat). Az ábra így teljeskörűen szemlélteti, hogyan épül egymásra az uniós irányelv, a hazai implementáció, a végrehajtási rendeletek és a stratégiai szintű kormányhatározatok rendszere.

Láthatjuk tehát, hogy a kritikus szervezetek és infrastruktúrák védelmére irányuló hazai szabályozás az elmúlt években jelentős átalakuláson ment keresztül összhangban az EU-s Irányelvekkel, különösen a CER Irányelve és a NIS 2 Irányelv kapcsán [3]. A szabályozási környezet jelenlegi alapját a Kszetv., valamint a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról szóló 474/2024. (XII.31.) Korm. rendelet (Kszetv. Vhr.) [36] képezik. Emellett kiemelt szerepet tölt be a Vbö. [14], különösen annak V/A fejezete, amely a kritikus szervezetek és infrastruktúrák védelmére vonatkozó alapelveket és szervezeti együttműködést szabályozza.

- A Kszetv. célja, hogy növelje azon kritikus szervezetek ellenállóképességét, amelyek szolgáltatásai alapvetően szükségesek az alapvető társadalmi, gazdasági funkciók, közszolgáltatások, vagy éppen a közbiztonság fenntartásához. A törvény meghatározza a kritikus szervezetek kijelölésének feltételeit, az ágazati és horizontális hatóságok szerepét, a felügyelet gyakorlásának módját, valamint a szervezetek azon kötelezettségeit, amelyek az ellenálló képességük fejlesztését célozzák. A törvény külön figyelmet fordít a kockázatkezelési gyakorlatok bevezetésére, az incidenskezelés szabályaira, valamint a jelentéstételi és együttműködési kötelezettségekre. [13]
- A Kszetv. Vhr. a törvény végrehajtási szabályait tartalmazza. A rendelet pontosítja a kritikus szervezetek kijelölésének eljárási rendjét, a kockázatértékelés követelményeit, valamint az ellenőrzések és hatósági beavatkozások kereteit. Meghatározza továbbá az egyes ágazati koordinációs szereplők feladatait, így például a belügyminiszter és az ágazati miniszterek közötti felelősségmegosztást. [36]
- Az ország védelme és biztonsága szempontjából jelentős szervezetek ellenálló képességéről szóló 475/2024. (XII. 31.) Korm. rendelet (a továbbiakban: Vbö. Vhr.) kifejezetten a kijelölési eljárás rendjét és technikai részleteit szabályozza. Ez a rendelet kulcsfontosságú abból a szempontból, hogy a kritikus szervezetek azonosítása és nyilvántartásba vétele objektív, egységes és transzparens módon történjen. A kijelölés

alapjául szolgáló szempontok között megjelennek az ellátási láncok közötti függőségek, az informatikai rendszerek védelmének szintje, valamint a működési zavarokból eredő lehetséges társadalmi és gazdasági következmények. [4]

- A hazai szabályzás beágyazottságát és horizontális koordinációját Vbö. V/A fejezete biztosítja, amely kritikus szervezetek és infrastruktúrákkal kapcsolatos különleges szabályokat tartalmazza. A fejezet lefekteti a stratégiai szintű együttműködés alapjait a központi államigazgatási szervek, ágazati irányító hatóságok, valamint a szolgáltatók között. A szabályozás előírja a rendszeres kockázatelemzést, a közös szcenárióalapú gyakorlatokat, valamint a nemzeti kockázati térkép folyamatos frissítésének kötelezettségét. [14]

A kritikus szervezetek ellenálló képességének megerősítése érdekében 2025-ben két, egymással szorosan összefüggő stratégia határozatot fogadott el.

A *nemzeti kockázatelemzési határozat*, [37] valamint *a nemzeti stratégiai határozatok* [5] egymásra épülnek, míg az első határozat elsősorban a veszélyeztetettség átfogó és rendszeres értékelésének keretrendszerét határozza meg, addig a második ezen eredményekre építve a hosszú távú ellenállóképesség-fejlesztés irányvonalait rögzíti. Mindkét határozat közvetlenül a Kszetv. végrehajtásának részét képezi, és szorosan illeszkedik az EU vonatkozó szabályozási környezetéhez, különös tekintettel a CER Irányelv és a NIS2 követelményeire.

A nemzeti kockázatértékelési határozat célja egy olyan strukturált, a nemzeti szinten releváns veszélyforrásokat és azok lehetséges hatásait szisztematikusan feltáró dokumentum létrehozása, amely megalapozza a kritikus szolgáltatások zavartalan fenntartásához szükséges védelmi és alkalmazkodási intézkedéseket. A kormányhatározat nem csupán adminisztratív kötelezettséget ró a szereplőkre, hanem elvárja, hogy az érintett szervezetek saját belső kockázatelemzési és döntéstámogató folyamataikat is ennek megfelelően strukturálják. A határozat deklaráltan figyelembe veszi a társadalmi, gazdasági, környezeti és technológiai interdependenciákat, valamint az új típusú fenyegetések, például a hibrid támadások vagy az éghajlatváltozással összefüggő rendkívüli események rendszerszintű hatásait.

Ezzel párhuzamosan a nemzeti stratégiai határozat az ellenálló képesség nemzeti szintű fejlesztési irányait határozza meg, hangsúlyt fektetve az ágazatközi koordinációra, a szereplők közötti információmegosztás erősítésére és a szolgáltatásbiztonság középpontba állítására. A stratégia nem kizárólag állami szereplőkre vonatkozik, hanem egyértelműen számol a magánvállalatokkal, különösen a technológiai, energia- és pénzügyi infrastruktúrák működtetőinek felelősségével is.

A nemzeti stratégiai határozat kiemelt célként határozza meg, hogy a kritikus és jelentős szervezetek a kockázatokra nem reaktívan, hanem proaktív módon válaszoljanak, amelyhez egységes fogalmi és módszertani kereteket is biztosít. Ezzel a stratégia előmozdítja az ellenállóképesség rendszerszintű szemléletének elterjesztését, és megalapozza a periodikus, minőségbiztosított visszaméréseken nyugvó fejlesztési ciklusok kialakítását. A stratégia és a kockázatelemzés együttes alkalmazása biztosítja, hogy Magyarország ne csupán megfeleljen a nemzetközi szabályozási elvárásoknak, hanem proaktívan képes legyen saját szervezeti és infrastrukturális rendszerének robusztusságát fokozni. A rendszeres felülvizsgálat, az ágazatok közötti együttműködés ösztönzése, valamint a köz- és magánszféra közötti felelősségmegosztás tudatosítása révén e dokumentumok nemcsak normatív, hanem strukturáló erejű szakpolitikai eszközként is értelmezhetők.

A szabályozásban megjelenik biztonsági dokumentumként az ellenállóképességi terv. A kritikus szervezetek ellenállóképességének kialakítása és fenntartása több, egymásra épülő hazai jogszabály alapján történik. A Kszretv. meghatározza az ellenállóképességi terv kötelező tartalmi elemeit, amelyek a megelőzés, a reagálás és a helyreállítás teljes spektrumát lefedik. A törvény rögzíti, hogy a terv a kritikus szervezet működésének biztonságát, folytonosságát és a rendkívüli események kezelését szolgáló technikai, szervezeti és információbiztonsági intézkedéseket foglalja össze. A tervnek tartalmaznia kell a kritikus infrastruktúrák fizikai és kiberbiztonsági védelmét, a riasztási és kommunikációs eljárásokat, a külső szervekkel való együttműködés rendjét, valamint az alternatív és tartalékmegoldások meghatározását, amelyek biztosítják az alapvető szolgáltatás minimális szintű fenntartását. [13]

A jogszabály kifejezetten előírja, hogy az ellenállóképességi terv kockázatelemzésre épüljön**.** A kockázatelemzés keretében a kritikus szervezetnek azonosítania kell a rendszereit érintő veszélyeket, fenyegetéseket, sebezhetőségeket és függőségeket, a kockázatokat valószínűség és hatás alapján értékelnie kell, valamint meg kell határoznia a kockázatcsökkentő intézkedéseket. A kockázatértékelésnek ki kell terjednie fizikai, kiber-, humán és ellátási lánc kockázatokra, továbbá azokra az interdependenciákra, amelyek más ágazatok működését befolyásolhatják. [14]

A Vbö. kiegészítő keretet biztosít az ellenállóképességi tervezéshez azáltal, hogy meghatározza az állami és ágazati vezetők feladatait, a koordináció rendjét, valamint a védekezési és reagálási szerepköröket.

A törvény előírja, hogy a kritikus szervezetek felkészülése nemcsak szervezeti, hanem rendszerszintű szempontok alapján is történjen, így a tervben szerepelniük kell a különböző hatóságok, ágazati szereplők és infrastruktúra üzemeltetők közötti együttműködési protokolloknak is. [14]

A Vbö. és a Kszetv. végrehajtási rendeletei részletezik az ellenállóképességi terv formai és eljárási követelményeit. Előírják a terv struktúráját, a kötelező kockázatelemzési mellékleteket, az éves felülvizsgálat és ötéves mélyreható aktualizálás rendjét, valamint a szervezetekre vonatkozó adatszolgáltatási kötelezettségeket. A kockázatelemzéshez kapcsolódóan a rendeletek megkövetelik a rendkívüli események küszöbértékeinek meghatározását, a riasztási lánc feltüntetését, a kritikus erőforrások listáját, valamint a rendszerszintű függőségek és kitettségek elemzését. [4]

A végrehajtást támogató kormányhatározatok meghatározzák a stratégiai állami feladatokat, a koordinációs fórumok működését, valamint a kritikus infrastruktúrák ellenállóképességének fejlesztéséhez szükséges intézkedéseket. [5] Ezek a dokumentumok kiemelik a kockázatelemzés és az ellenállóképességi tervezés kapcsolatát a nemzeti reziliencia rendszerével, valamint előírják a gyakorlatok, oktatások és képzések rendszeres megszervezését, amelyek az ellenálló képességi terv végrehajtásának alapfeltételei. [37]

A hazai szabályozás tehát egységes keretet ad az ellenállóképességi tervek elkészítéséhez, amelynek központi eleme a kockázatkezelési folyamat integrálása. A kockázatelemzés szolgáltatja azokat az adatokat, amelyek alapján a szervezet meg tudja határozni a védelmi prioritásokat, az alternatív működési módokat, a kulcserőforrások biztosítási igényeit és a gyors helyreállítási protokollokat. Emiatt az ellenállóképességi terv a kockázatelemzés gyakorlati megvalósítása, olyan dokumentum, amely a kockázati eredményekből operacionalizálható folyamatokat, műszaki intézkedéseket és szervezeti szabályokat hoz létre.

Összességében a hazai szabályozás az elmúlt időszakban szorosabban integrálta a kritikus szervezetek és infrastruktúrák védelmét a nemzeti kockázatkezelés területén. A hangsúly eltolódott a reaktív védekezésről a proaktív ellenállóképesség-fejlesztés irányába, a rendszer működőképességének fenntartására válsághelyzetben is. Ennek ellenére a szabályozás gyakorlati alkalmazása, az együttműködési mechanizmusok hatékonysága, valamint az ágazati szereplők közötti interoperabilitás továbbra is fejlesztendő területként jelenik meg, különösen az interdependens rendszerek és a digitális fenyegetések növekvő jelentősége miatt.

1.1.4 A szabályozási követelmények hazai implementációjának aktuális állapotáról

A Kszetv. alapján a kijelölési folyamatok megkezdődtek, nem minden szervezet vagy infrastruktúra kapott végleges státuszt. Az új rendszerhez történő alkalmazkodás igényli a szervezetek részéről a belső folyamatok, dokumentációk, kockázatelemzés kialakítását, ez mind időigényes feladat. A kisebb szervezetek, önkormányzatok esetén lehetnek erőforrás problémák a megfelelés biztosításához, személyzet, szakértelem, költségek. A korábbi indokolások is említik, hogy az önkormányzati szintnél nehezebb a komplex kockázatmenedzsment bevezetése.

A kijelölési folyamat 2024 végén indult, és 2025-ben fokozatosan haladt előre az ágazati szervezetek körében. 2025. júniusában hirdették ki a nemzeti kockázatértékeléssel és a nemzeti stratégiával összefüggő korm. határozatokat. A kijelölési és felügyeleti rendszer több szinten működik. A központi koordinációért a BM OKF felel, amely az ágazati hatóságokkal együttműködésben végzi a kijelölési eljárásokat és az éves beszámoltatást. A hazai implementáció tapasztalatai alapján több strukturális nehézség is kirajzolódik. Az erőforráshiány különösen a kisebb regionális szolgáltatók esetében hiányzik a megfelelő szaktudás és pénzügyi háttér a kockázatelemzés és a reziliencia-tervezés végrehajtásához. A szabványosítás hiánya az ágazatok között eltérő módszertanok alkalmazása nehezíti az összehasonlíthatóságot és a nemzeti szintű visszacsatolást. A monitoring-rendszerek kialakulatlansága a legtöbb szervezet még a kezdeti fázisban van az indikátor alapú teljesítménymérés és a visszacsatolási mechanizmusok kiépítésében. E tapasztalatok ugyanakkor jelzik, hogy a jogszabályi és intézményi keret már nem csupán elméleti, hanem fokozatosan gyakorlati szintre kerül, a szervezetek többsége kijelölte az ellenálló képességért felelős vezetőt, és megkezdte az éves reziliencia beszámolók elkészítését, amelyeket a BM OKF értékel

A szervezeteknek tehát az alábbi kötelezettségeik vannak jelenleg:

- Ellenálló képességért felelsős vezető kinevezése és adatainak bejelentése határidő szerint.
- Ellenálló képességi terv készítése, a törvény szerinti tartalommal és formai követelményekkel, az elektronikus benyújtás és vizsgálat kötelező.
- Rendszeres gyakorlatok, komplex ellenőrzések, ahol a hatóság és a kijelölt szervezet együtt végzi az ellenálló képességi gyakorlatot. [36]

Összességében elmondható, hogy a kritikus szervezetek implementációja Magyarországon 2025-re előrehaladott, de még nem teljesen lezárt folyamat. Az implementáció jól mutatja, hogy a stratégiai elvek, úgymint a kockázat alapú megközelítés és a reziliencia fókuszú tervezés alkalmazható a gyakorlatban, azonban a szabályozásból fakadó kötelezettségek, gyakorlatok további erőfeszítést igényelnek.

1.1.5 Irodalmi áttekintés a magyar szabályozási környezet és fogalmi fejlődés tükrében

A kritikus infrastruktúrák és kritikus szervezetek védelmének magyarországi szabályozása szorosan kapcsolódik az Európai Unió és a nemzetközi szervezetek által kialakított fogalmi, intézményi és módszertani keretekhez. A hazai fogalom- és szabályozásfejlődés ezért csak úgy értelmezhető, ha egyben tekintjük a nemzetközi szakirodalom és a nemzetközi szakpolitikai dokumentumok irányvonalait is. Az Európai Bizottság hivatalos portáljai, a *Joint Research Centre (a továbbiakban: JRC)* kritikus infrastruktúravédelmi publikációi, valamint az European Union Agency for Cybersecurity (a továbbiakban: *ENISA),* az Organisation for Economic Co-operation and Development (a továbbiakban: *OECD)* és a *NATO* vonatkozó jelentései mind olyan keretrendszereket kínálnak, amelyekhez a magyar szabályozás fokozatosan igazodott. [38]

A hazai szakirodalom – különösen Angyal István és Mógor Judit munkái rámutatnak arra, hogy a magyar kritikus infrastruktúra szabályozás első hullámában a hangsúly elsősorban az infrastruktúra elemek azonosításán és fizikai védelmén volt, miközben az ágazatok közötti interdependenciák és a kiberfizikai sérülékenységek csak részben jelentek meg. Angyal és Mógor 2022-es elemzése kiemeli, hogy a korábbi modell csak korlátozottan volt összehangban az uniós elvárásokkal, különösen az EPCIP program, az ECI Irányelv és az EU-s kritikus infrastruktúra védelmi ajánlások által képviselt, hálózatalapú gondolkodással. [10] Az általuk felvetett kritikák az integrált kockázatalapú megközelítés, a fizikai és informatikai fenyegetettségek együttes kezelése, az ágazatközi koordináció hiánya erősen rezonálnak a nemzetközi szakirodalomban megjelenő megállapításokkal. [20]

Angyal István 2024-es írása ezen az alapon már kifejezetten a kritikus szervezet kategóriájának bevezetését és a Kszektv. szerkezetét vizsgálja, amely a korábbi kritikus infrastruktúra szemléletről a szolgáltatásnyújtó szervezetekre helyezi át a fókuszt. [39] Ez a megközelítés jól illeszkedik a CER-irányelv logikájához, ahol az „entity” – mint szolgáltatást biztosító szervezet – válik a szabályozás alanyává, és ahol a védelmi kötelezettség kockázatértékelési, ellenállóképesség fejlesztési és incidenskezelési elvárásokban konkretizálódik. Ezt a gondolkodásmódot erősítik az Európai Bizottság *CER-dokumentumai,* a *NIS Cooperation Group* iránymutatásai, valamint az ENISA rendszeresen frissített *Threat Landscape* és *Critical Entities* jelentései. [38]

A hazai reziliencia szakirodalom – például Sáfár Brigitta és Kállai Krisztina szervezeti rezilienciát vizsgáló munkái – kifejezetten a nemzetközi reziliencia elméletek (Linkov, Hollnagel, Bruneau stb.) irányvonalához kapcsolódnak.

Ezek a tanulmányok hangsúlyozzák, hogy a kritikus szervezetek védelme nem redukálható a hagyományos, eseményorientált biztonságmenedzsmentre, hanem multidimenzionális rendszerszemléletet igényel, amely figyelembe veszi a technológiai, szervezeti, társadalmi és interdependencia-eredetű sérülékenységeket is. [40]

A külföldi szakirodalom, különösen az olyan folyóiratokban megjelenő tanulmányok, mint az *International Journal of Critical Infrastructure Protection,* a *Reliability Engineering & System Safety*, a *Safety Science* vagy a *Journal of Contingencies and Crisis Management*, további támpontokat adnak a hazai szabályozás értelmezéséhez. Ezek a publikációk – amelyekhez a disszertáció a nemzetközi tudományos adatbázisok (Scopus, Web of Science, ScienceDirect, SpringerLink) segítségével kapcsolódik – rendre azt mutatják, hogy a kritikus infrastruktúra védelem fejlődése világszinten is a fizikai védelemtől a kockázatalapú, majd a rezilienciaalapú megközelítés irányába mozdult el.

Mindezek alapján a magyar szabályozási környezet fejlődése a nemzetközi trendekbe illeszkedő, de sajátos nemzeti jellegzetességeket is hordozó folyamatként értelmezhető. A Kszetv. és a kapcsolódó kormányrendeletek nemcsak honosítják a CER-irányelv elvárásait, hanem a hazai biztonságpolitikai, intézményi és kockázatkezelési gyakorlatba is beépítik a nemzetközi szakirodalom és szakmai platformok által kimunkált elveket. [30]

1.1.6 A kritikus szervezetek és infrastruktúrák védelmének történeti fejlődése, vizsgálata

A kritikus infrastruktúrák és kritikus szervezetek védelmének történeti fejlődése Európában több, jól azonosítható biztonságpolitikai sokkhatás és az azokra adott intézményi-szabályozási válasz mentén rajzolódik ki. A 2001. szeptember 11-i terrortámadás, majd a 2004-es madridi és a 2005-ös londoni robbantások rávilágítottak arra, hogy a modern európai társadalmak működése egy szűk körű, de rendkívül kritikus infrastruktúrahálózattól függ, amelynek sérülése aránytalanul nagy társadalmi és gazdasági hatásokkal járhat. A madridi és londoni események különösen azt mutatták meg, hogy a közlekedési, kommunikációs és biztonsági rendszerek reagáló és együttműködési képessége még nem volt kellőképpen összehangolt.

E válaszkeresés eredménye volt az European Programme for Critical Infrastructure Protection (a továbbiakban: EPCIP) Európai Unió EPCIP programjának kialakítása, amelyet az Európai Bizottság tematikus dokumentumai és konzultációs anyagai (Green Paper, Fehér Könyv jellegű anyagok) alapoztak meg. A *JRC* szakmai anyagai, valamint az *EU Council* dokumentumai együttesen jelölték ki azokat az irányokat, amelyek mentén a tagállamoknak ki kellett alakítaniuk saját kritikus infrastruktúra védelmi rendszereiket.

Ezzel párhuzamosan jött létre a CIWIN (Critical Infrastructure Warning Information Network) mint információmegosztó és korai figyelmeztető platform, amelynek célja a tagállami tapasztalatok, incidensek és legjobb gyakorlatok rendszeres cseréje volt. Több mint 20 évvel ezelőttre vezethető vissza az európai szabályozás igényének felmerülése azon kritikus infrastruktúrák tekintetében, amelyek hatással vannak egy adott ország vagy térség működésére, emellett számos mérföldkővel találkozhatunk az EU-ban, melyek hatással voltak a szabályozás kialakulására. [41]

Első és legismertebb mérföldköve a 2004. március 11-én történt madridi robbantás. A támadás során mindösszesen 10 pokolgépet robbantottak fel Madrid főbb pályaudvarain, és főbb vasútvonalakon a legforgalmasabb reggeli időszakban. A robbantás áldozatainak száma 191 főre tehető és közel 1900 sebesültről beszélhetünk. A támadás hatására Európa rádöbbent, hogy már nem egy óceán választja el a terrrorizmustól, hanem az Európába is befészkelte magát. A célirányos, gyors lefolyású támadássorozat váratlanul érte a reagáló egységeket, így lassú, koordinálatlan beavatkozás volt tapasztalható a kárelhárítás és felszámolás során. Ennek eredményeként Európa bizalmatlanná vált, így az európai állampolgárok biztonsága egyre fontosabbá vált, ezáltal a tagállamok és az EU nagy hangsúlyt fektetett a nemzetközi együttműködés megerősítésére, az ENSZ, az Amerikai Egyesült Államok és harmadik országok bevonásával. Az együttműködés keretében megkezdték a terrortámadások elleni reagálóképesség felmérését a tagállamok körében, valamint felmerült egy átfogó stratégia létrejöttének igénye a kritikus infrastruktúrák és a lakosság védelme érdekében. [9]

A közös munka eredményeképpen 2004-ben javaslatot tettek egy európai program létrejöttére. Az EPCIP az EU által indított program, amelynek célja a tagállamok kritikus infrastruktúráinak védelme és biztonságának növelése volt. [42] Az EPCIP keretében az EU olyan irányelveket és stratégiákat dolgozott ki, amelyek segítették az infrastruktúrák védelmét a különféle fenyegetésekkel szemben, beleértve a természeti katasztrófákat, terrorista támadásokat és kibertámadásokat. [38] A program elősegítette a tagállamok közötti együttműködést, az információmegosztást és a legjobb gyakorlatok cseréjét, valamint támogatást nyújtott a nemzeti kritikus infrastruktúra védelmi terveik kidolgozásához és végrehajtásához. Az EPCIP keretében létrehozták az Európai Kritikus Infrastruktúra kijelölési mechanizmust is, amely azonosítja azokat az infrastruktúrákat, amelyek működése elengedhetetlen az EU egészének biztonsága és jóléte szempontjából [39].

Alig egy év elteltével újabb robbantás rázta meg Európát, 2005. július 7-én a londoni metróhálózatot érte támadás. Az öngyilkos merénylet során négy robbanás történt, három a londoni metróhálózatában és egy a buszon. A reggeli csúcsforgalomban összesen 52 ember halt meg és közel 700-an sérültek meg. A robbantások jól szervezettek, célirányosak és kiterjedtek voltak, továbbá a robbantók alkalmazkodtak a kialakult helyzethez, mivel a negyedik bombát is a metróhálózatban szerették volna felrobbantani, azonban az meghiúsult, így egy elemeletes buszt vettek célba. Hasonlóan a madridi robbantáshoz, ebben az esetben is váratlanul érte a hatóságokat a támadás, a reagálásuk több esetben hiányos volt, azonban erre az időszakra tömegközlekedési korlátozásokat vezetek be. [45]

A robbantást követően az EU a fenyegetések csökkentésére irányuló fellépést részesítette előnyben, emellett fontosnak tartotta a kommunikáció és a reagálóképesség korszerűsítését a tagállamok között, figyelembe véve az országok sajátosságait. Világossá vált, hogy az események minél hatékonyabb kezelése, valamint kiszűrése érdekében nemzetközi és tagállami gyakorlatok végrehajtására is lenne szükség. Elsősorban a szolgáltatás célú infrastruktúrák védelmének növelése volt a cél, így a megelőzésre, a fejlesztésre és a gyakorlásra helyezték a hangsúlyt.

Az újbóli támadás hatására egy konzultációs időszak vette kezdetét. Ekkor fogadta el a Bizottság az európai program zöld könyvét, amely a kritikus infrastruktúrák védelmét szorgalmazta. A dokumentum lehetőségeket fogalmazott meg arra vonatkozóan, hogy a Bizottság milyen módon konstruálná a kritikus infrastruktúrák védelmére vonatkozó európai programot, valamint a kritikus infrastruktúrák figyelmeztető információs hálózatot, azaz a Critical Infrastructure Warning Information Network-öt, a CIWIN-t. A 2004 és 2008-as év közötti események hatására az Európai Unió javaslatokat, irányokat, programokat, fogalmazott meg a kritikus infrastruktúrák védelmével kapcsolatban, melyet egy dokumentumba foglaltak össze [38]. Ennek alapján jött létre 2008-ban a korábban is említett ECI Irányelv.

Az ECI Irányelv iránymutatást fogalmazott meg a tagállamok számára a kritikus infrastruktúrák azonosítására és kijelölésére vonatkozóan és kiemelten kezelte az energia és a közlekedési ágazatot. [31] A folyamat jogi szempontból az ECI Irányelv elfogadásában csúcsosodott ki, amely a kritikus infrastruktúrák védelmének első, kifejezetten jogi kötelezettségeket rögzítő európai kerete. Az irányelv még elsősorban az energia- és közlekedési ágazatra fókuszált, és a kritikus infrastruktúra fogalmát infrastruktúra-objektumokhoz kötötte.

Ezt követően – részben az ENISA, a NIS Cooperation Group, az OECD és a NATO különböző jelentéseire, valamint a JRC kutatásaira építve – fokozatosan erősödött az a felismerés, hogy a védelemnek nemcsak az objektumokra, hanem a szolgáltatásokra, ellátási láncokra és a szervezeti működésre is ki kell terjednie. [46]

A 2010-es évektől kezdődően a szabályozás és a szakmai diskurzus súlypontja a kibertér és a kiber-fizikai rendszerek sérülékenységére, az ellátási láncok globális kitettségére, valamint az interdependens infrastruktúrahálózatok rendszerszintű kockázataira helyeződött át. A NIS Irányelv, majd a NIS2 és végül a CER Irányelv már egy olyan fejlődési szakasz termékei, amelyben a kritikus szervezetek védelme a fizikai és kiberbiztonság integrált kezelésére, a reziliencia mérésére és fejlesztésére, valamint a tagállamok közötti koordinációra épül. E folyamatot kísérik végig olyan szervezetek elemzései, mint az *ENISA*, az *OECD* reziliencia jelentései, a *NATO* kritikus infrastruktúrákat érintő iránymutatásai, valamint a *ESA* űrinfrastruktúrákra vonatkozó kockázatelemzései. A külföldi tudományos szakirodalom – különösen Zio, Theoharidou, Ouyang, Kröger és más szerzők munkái – a történeti fejlődést a módszertani megoldások tükrében is leírják, a komponensszintű megbízhatósági elemzéstől eljutunk a hálózat- és rendszeralapú kockázatelemzésig, majd a reziliencia-indexekkel dolgozó modellekig. [47] Ezek a tanulmányok a kritikus infrastruktúrák védelmét egyre inkább nemzeti és nemzetközi összefüggésben, ágazatközi kapcsolatokkal átszőtt rendszerként értelmezik.

A magyar szabályozás történet ebbe a fejlődési ívbe illeszkedik, a korai kritikus infrastruktúra felfogástól a létfontosságú rendszerelemek és szolgáltatások védelmén át jut el a kritikus szervezetek rezilienciáját középpontba állító Kszektv.-ig és kapcsolódó rendeletekig. A hazai intézményrendszer – különösen a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban BM OKF), az ágazati hatóságok (pl. MEKH, NMHH), valamint a nemzeti kiberbiztonsági struktúrák – fokozatosan építik be a nemzetközi ajánlásokat és szakmai platformok által közvetített elveket. Így a kritikus szervezetek védelmének történeti vizsgálata nemcsak események és jogszabályok soraként, hanem a nemzeti és nemzetközi tudományos-szakmai diskurzusba beágyazott fejlődési folyamatként értelmezhető.

1.2 A kritikus szervezetek és infrastruktúrák aktuális fenyegetettségi környezetének elemzése

A szabályozás kialakulását követően számos olyan esemény történt, mely megváltoztatta Európa és a világ biztonságpolitikai helyzetét. A biztonságpolitikai és társadalmi környezet változása még jobban rávilágított a kritikus szervezetek sérülékenységére és azok védelmének fontosságára. Napjaink helyzete több szempontból is figyelemre méltó.

1.2.1 A COVID-19 világjárvány hatásainak értékelése és az infrastruktúrákra gyakorolt hatásainak elemzése

Modern világunk nagymértékben függ az egymásra épülő infrastruktúrák komplex rendszerének működésétől. Egy infrastruktúra meghibásodása súlyos és messzemenő hatást gyakorolhat más infrastruktúrákra, és veszélyeztetheti az egész rendszer működését. Míg bizonyos infrastruktúrákat rendkívül kritikusnak tekintenek, és függőségeikkel és védelmükkel széleskörűen és évtizedek óta foglalkoznak, másokat kevésbé vagy egyáltalán nem tekintenek kritikusnak, és alig vitatják őket. A COVID-19 világjárvány soha nem látott terhelést okozott az infrastruktúrák működésében, és feltárta, hogy a folyamatban lévő és hosszan tartó válság során más infrastruktúrák válnak rendkívül kritikussá, mint egy hirtelen, de rövid távú válság idején [40].

Az infrastrukturális rendszerek kölcsönösen függenek egymástól, ha egy rendszerben zavar vagy meghibásodás lép fel, az átterjedhet más rendszerekre, és ezt követően sokszorosára erősítheti annak hatását, és további rendszerekre is kihathat. Az infrastruktúrák közötti kapcsolatok folyamatos növekedése és összetettségének növekedése miatt a teljes rendszeren belüli kölcsönös függőségek is tovább nőnek, ami miatt a rendszer fogékonyabbá válik a zavarokra [20]. Egy kritikus infrastruktúra (pl. közegészségügyi rendszer) több ágazatból áll, hálózatokkal és komponensekkel, amelyek csomópontokban összekapcsolódnak. Ezáltal komplex hálózat jön létre, amelynek jellemzői határozzák meg, hogy a kritikus infrastruktúra rendszerhibáinak hatásai hogyan és milyen intenzitással terjednek át a függő alrendszerekre és a társadalomra. A múltbeli események feljegyzései jól mutatják, hogy a kritikus infrastruktúrák meghibásodásának milyen súlyos és messzemenő hatásai lehetnek. Példának említhető az osztrák élelmiszerágazat, mivel a határzárás következtében a kelet-európai betakarítási munkások nem léphettek be az országba. A megfelelő munkások hiánya veszélyeztette a betakarítást, és ezzel a szezon élelmiszertermelését. A szociális és elosztórendszerek ágazatán belül hiány volt az idősgondozókból, akik a határzár és a közlekedés hiánya miatt nem tudtak a munkahelyükre utazni, mivel a lakosság nagy része otthonról dolgozott, jelentősen megnőtt az információs és kommunikációs szolgáltatásokra nehezedő terhelés. [40] A kapcsolatok túlterhelésének elkerülése érdekében a nagy szolgáltatók, például a YouTube és a Netflix úgy döntöttek, hogy ideiglenesen csökkentik a videó minőségét, hogy tehermentesítsék az internetes vonalakat. Ez csak néhány példa a COVID-19 világjárvány kritikus infrastruktúrák rendszereire gyakorolt hatásaira [41].

A következmények messzemenőek és hosszan tartóak voltak. Az azonban bizonyosan kijelenthető, hogy a helyzet rávilágított a kritikus infrastruktúrákra és azok hatásaira, valamint a modern világunk összekapcsolódásaira minden eddiginél alaposabban történő kutatásának fontosságára. [42]

Egyrészt a koronavírus járvány több szempontból is rávilágított a védelem fontosságára. A kórházak leterheltségével fontossá vált az üzemfolytonosság biztosítása, így a járvány rávilágított a nélkülözhetetlen munkavállalók fontosságára a társadalom működésében. Az élelmiszer és boltok ellátási láncának fenntartása is nagy problémát jelentett bizonyos országokban a tömegesen előforduló pánikvásárlások következtében, így néhány esetben a boltok nem tudták kielégíteni a vásárlói igényeket. A koronavírus járvány a korlátozások és gazdasági hatások a termelési és ellátási láncok töredezését okozták, így több létfontosságú infrastruktúra ágazat működését veszélyeztette, zavart keltve a lakosság ellátásában.

A COVID-19 világjárvány révén a terrortámadásokon és természeti katasztrófákon túl egy újabb formáját ismerhettük meg a kritikus infrastruktúrák sebezhetőségének.

1.2.2 Az orosz-ukrán konfliktus kritikus szervezetekre és infrastruktúrákra gyakorolt hatásainak elemzése

A COVID–19 világjárványt követően Európában olyan biztonsági környezet alakult ki, amelyben a létfontosságú szolgáltatások biztosítása és a kritikus infrastruktúrák működőképessége kiemelt figyelmet kapott. A 2022-ben kirobbant orosz–ukrán fegyveres konfliktus tovább erősítette ezt a tendenciát, mivel számos nemzetközi szakmai szervezet – köztük az Európai Bizottság, az EU IPCR Mechanizmusa, a JRC, az OECD és az ENISA – elemzései rámutattak, hogy a fegyveres konfliktusok során több ágazat és alágazat működése kerülhet tartós terhelés alá. A hangsúly ugyanakkor a szakpolitikai és infrastrukturális hatások vizsgálatára helyeződik, nem pedig a konfliktusban részt vevő felek politikai vagy katonai értékelésére. [43]

A nemzetközi források – például a JRC *Technical Reports on Critical Infrastructure Resilience in Conflict Settings,* az ENISA *Threat Landscape,* az OECD *Systemic Resilience* jelentései, valamint az UN OCHA és a Világbank infrastrukturális értékelései – több olyan ágazatot azonosítanak, amelyek a háborús környezetben különösen sérülékennyé válhatnak. Ezek közé tartozik mindenekelőtt az energiaágazat, például a villamosenergia-hálózatok, az alállomások, az erőművek, a távvezetékek, mivel az energiaellátás meghatározó szerepet játszik más ágazatok működésében, és bármilyen hosszabb kiesése rendszerszintű hatásokkal járhat.

Ezzel párhuzamosan a vízellátás és szennyvízelvezetés infrastruktúrái is érintettek lehetnek, hiszen vízkezelő telepek, szivattyúállomások vagy elosztóhálózatok sérülése ellátási zavarokat okozhat. A Világbank és az UNICEF elemzései alapján a szolgáltatás folytonosságának fenntartása válságkörnyezetben kiemelkedő kihívás, különösen a nagyvárosi és ipari térségekben. [44]

A közlekedési ágazat szintén kritikus szerepet tölt be. A nemzetközi szakirodalom a konfliktus során érintett számos alágazatot azonosít: [45]

- vasúti infrastruktúra: pályák, váltók, biztosítóberendezések, logisztikai csomópontok,
- közúti infrastruktúra: hidak, kulcsfontosságú útszakaszok, csomópontok,
- légi közlekedés infrastruktúrái: repülőterek, irányító rendszerek,
- vízi közlekedés: kikötők, hajózsilip-rendszerek, folyami infrastruktúra.

A JRC és az OECD elemzései hangsúlyozzák, hogy a közlekedési hálózatok működése mind humanitárius, mind ellátási lánc szempontból meghatározó, így bármilyen kapacitáscsökkenés jelentős rendszerterhelést okozhat.

A digitális infrastruktúrák, különösen az elektronikus hírközlési hálózatok, az adatközpontok, az internetes gerinchálózatok és a vészhelyzeti kommunikációs rendszerek, a fegyveres konfliktusok idején fokozottan sérülékenyek. Az ENISA jelentései szerint a hálózati infrastruktúrákra nehezedő nyomás, az esetleges fizikai károsodás, valamint a megnövekedett kiberfenyegetettség együttese komplex kihívások elé állítja a szolgáltatókat és a hatóságokat. [46]

A nukleáris létesítményekkel kapcsolatos nemzetközi értékelések – például az International Atomic Energy Agency (a továbbiakban: IAEA) monitoringjelentései – külön is kiemelik, hogy a nagy energiaigényű és magas kockázati profilú infrastruktúrák működése konfliktushelyzetben fokozott felügyeletet igényel, a biztonság és a védettség fenntartása érdekében. Az energiaellátó rendszerekhez kapcsolódó tengeri és tenger alatti infrastruktúrák (pl. gázvezetékek, tenger alatti kábelek) biztonságára a NATO, az EU Critical Maritime Infrastructure Protection munkacsoportja és több európai szakmai szervezet is felhívta a figyelmet. A 2022-ben és 2023-ban azonosított tengeri incidensek rávilágítottak arra, hogy a víz alatti létfontosságú rendszerelemek sérülése több országot érintő ellátási zavarokat is okozhat.

A nemzetközi szakirodalom tehát azt mutatja, hogy fegyveres konfliktusok során nem egyetlen ágazat, hanem ágazatok és alágazatok összekapcsolt rendszere válik érintetté.

Különösen az alábbiak:

- villamosenergia-termelés és elosztás,
- vízellátó rendszerek,
- közlekedési infrastruktúrák (vasút, közút, hidak, repülőterek, kikötők),
- kommunikációs és digitális hálózatok,
- egészségügyi ellátórendszer infrastruktúrái,
- nagykapacitású ipari létesítmények,
- határátkelőhelyek és logisztikai csomópontok.

Az ágazati sérülékenységi mintázatok alapján a nemzetközi szakirodalom egybehangzóan megállapítja, hogy az energiaellátás, a közlekedési hálózatok, a digitális infrastruktúrák és az alapellátási rendszerek a konfliktuskörnyezetben különösen kritikus szerepkört töltenek be. [47]

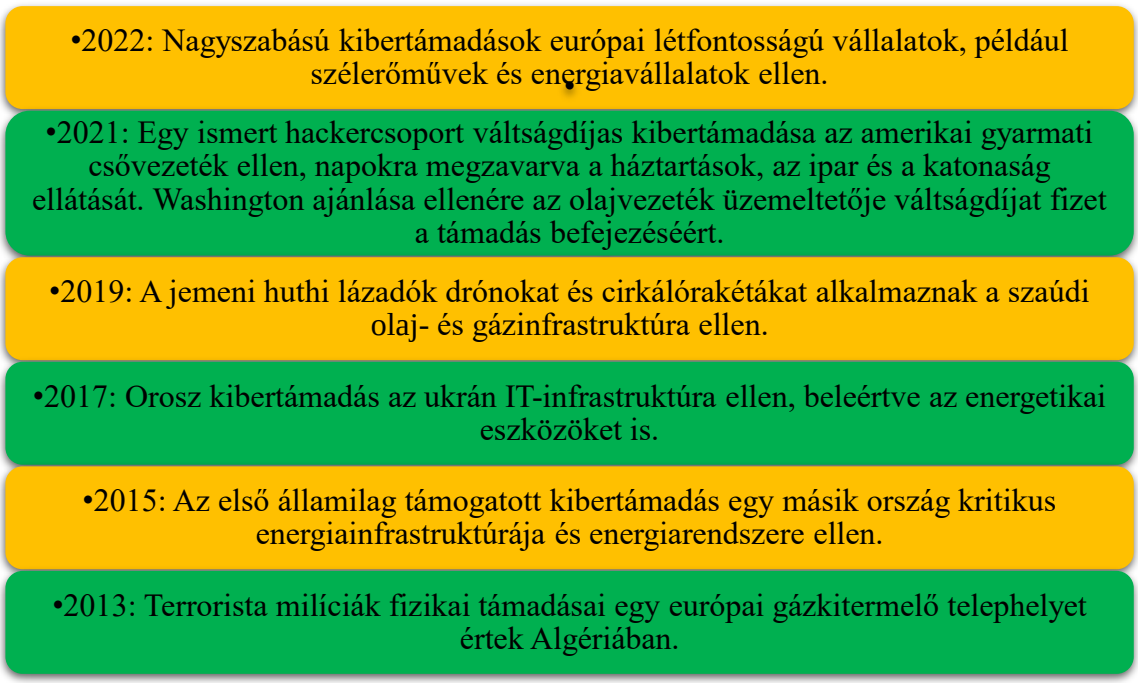
1.2.3 További komplex és hibrid fenyegetések értékelése

A kiberbiztonság és a kritikus szervezetek és infrastruktúrák védelmének kérdése világszerte jelentős aggodalomra ad okot. A fenyegető szereplők, köztük az államilag támogatott csoportok és bűnszervezetek, egyre inkább a kritikus infrastruktúra ágazatait veszik célba, többek között az energiát, a közlekedést, a vízrendszereket és az egészségügyet. Számos taktikát, technikát és eljárást alkalmaznak, beleértve az adathalászatot, a zsarolóprogramokat és az ellátási lánc támadásait, hogy megzavarják a szolgáltatásokat, érzékeny információkat lopjanak el, és esetlegesen fizikai károkat okozzanak.

Az Egyesült Államokban 2021. májusában történt Colonial Pipeline incidens egy jelentős infrastrukturális támadás példája 2021. első felétől. Ez a ransomware támadás az Egyesült Államok egyik legnagyobb üzemanyag-vezetékének ideiglenes leállását eredményezte, ami széles körű üzemanyaghiányt és növekedést okozott. [48]

2022-ben Németországban a vasúthálózatot kiszolgáló optikai kommunikációs kábeleket két különböző ponton vágták el egy „rosszindulatú és célzott” akció során. Ez hosszan tartó vonatkimaradásokhoz vezetett, még a nemzetközi kapcsolatokat is érintve. [57]

A közelmúltban történt fizikai támadások rávilágítottak az európai kritikus infrastruktúrát fenyegető növekvő hibrid fenyegetésekre. 2023. januárban a NATO és az EU megállapodott abban, hogy szorosabb együttműködést folytatnak a biztonság- és védelempolitika terén, beleértve a rezilienciával és a kritikus infrastruktúrákkal foglalkozó közös munkacsoport létrehozását.



5. ábra: Támadások az energia infrastruktúra ellen, Készítette: a Szerző [28-29]

Az Európai Bizottság újonnan javasolt tanácsi ajánlása arra szólította fel a tagállamokat, hogy végezzenek új kockázatértékeléseket, és gyorsítsák fel az EU létfontosságú elemei ellenálló képességének erősítésére irányuló munkát. A kritikus infrastruktúra védelmének megerősítése három kiemelt területet ölel fel:

- a készenlétet,
- a reagálást, és
- a nemzetközi együttműködést, kiemelten a készenlétet.

A dokumentum nagyobb szerepet javasolt a Bizottságnak a fenyegetések kezelésében, valamint az EU tagállamok és harmadik országok közötti együttműködés javításában, különösen a transznacionális létfontosságú infrastruktúrák terén. Ez magában foglalja a felülvizsgált hálózat- és információbiztonsági irányelv szerinti közös és összehangolt kockázatértékelések elvégzését, amely az e kihívásokkal kapcsolatban tavaly májusban elért politikai megállapodáson alapul [34].

Az ajánlás arra is kötelezte a tagállamokat, hogy alkalmazzák mind a felülvizsgált változatot, mind a kritikus szervezetek ellenálló képességéről szóló irányelvet. Ez utóbbi célja, hogy megerősítse az államok azon képességét, hogy megvédjék létfontosságú intézményeiket számos biztonsági kockázattól, és javítsák a terrortámadásokra vagy természeti katasztrófákra adott válaszokat. A kritikus infrastruktúrák tengeralattjárói védelmét illetően azonban központi jelentőségű az EU-n belüli párbeszéd a legjobb gyakorlatokról állami szinten – mivel a kábelvédelem a tengerbiztonság, a kiberbiztonság, az óceánirányítás és az infrastruktúra-politikák egymást átfedő területeire hivatkozik. Ez az EU és a NATO, valamint az EU és az Egyesült Királyság közötti szorosabb együttműködéshez is vezethet, mivel ez valamennyi fél érdeke, és nem megoldható egyetlen kormány vagy szervezet által.

Az Európa elleni felfokozott hibrid hadviselés és a transzatlanti víz alatti internetkábelek megfelelő reagálása érdekében az EU nemcsak új rendeleteket, irányelveket és hálózati biztonsági koncepciókat kell elfogadnia. A víz alatti kritikus infrastruktúrák ellenállóbbá tétele érdekében az EU-t arra kényszerítik, hogy stratégiai tartalékot hozzon létre elegendő internet-, kommunikációs- és tápkábelekből, valamint hajókból ezek gyors javítása érdekében. A növekvő geopolitikai konfliktusok idején a reziliencia fokozása a kritikus infrastruktúra védelmének és a nyugati elrettentésnek is elengedhetetlen részévé válik a nagyhatalmak és más agresszorok által az infrastruktúrák szabotázsra irányuló erőfeszítésekkel szemben [46]. Az orosz-ukrán konfliktus egyik tanulsága éppen az volt, hogy a háborús stratégák mennyire tudatosan és célzottan támadták a kritikus infrastruktúrákat, hogy destabilizálják az ellenséges állam működését és társadalmát. A konfliktus során a vízforrások, az energiaellátó rendszerek és a kommunikációs hálózatok szándékos tönkretétele egyértelműen megmutatta, hogy a kritikus infrastruktúrák védelme mind békeidőben, mind háborús helyzetben is alapvető fontosságú.

1.2.4 A kritikus szervezetek és infrastruktúrák fenyegetettségével kapcsolatos szakirodalom kritikai áttekintése, értékelése

Az elmúlt évek kritikus szervezetek védelmével foglalkozó szakirodalma egyértelműen rávilágít arra, hogy a fenyegetettségek szervezeti, technológiai és külső, geopolitikai dimenzióban is jelentősen erősödtek. Kárász Balázs 2025-ben megjelent tudományos cikkében kifejezetten a humán tényező szerepét emeli ki az információs infrastruktúra védelmében. A szervezetek nem csak technológiai eszközöket igényelnek, hanem tudatos, jól képzett, szabályozási és fenyegetéstudatos munkavállalókat is. A tanulmány hangsúlyozza, hogy a társadalmi és emberi tényezők, például belső fenyegetések vagy alacsony biztonsági kultúra kritikus sebezhetőségi forrásként jelennek meg. [49]

Egy másik 2025-ben megjelent tudományos cikk alapján, a fenyegetés reziliencia elméletét mutatja be, amely nem egy-egy fenyegetéshez szabott megközelítést hirdet, hanem olyan moduláris, redundancián és diverzitáson alapuló rendszereket javasol, melyek képesek megőrizni működésüket előre nem látható válsághelyzetekben is. [50]

Bures 2022-es cikkében az IoT-komponensek sebezhetőségére fókuszál, különös tekintettel a fizikai rendszerek (pl. energiaellátás, közlekedés) digitális hálózatra kapcsolt eszközeinek támadhatóságára. Az IoT elemzés rámutat, hogy ezeket a heterogén rendszereket gyakran sérülékeny csomópontok jellemzik, melyek meghibásodása kritikus teljesítményzavarokat okoznak. [51]

1.3 A kritikus szervezetek és infrastruktúrák védelmének fejlesztési irányai

A fenti kritikus szervezeteket ért támadások, konfliktusok rávilágítottak arra, hogy azok védelmét folyamatosan felül kell vizsgálni és igazodnia kell a gyorsan kialakuló biztonságpolitikai helyzethez, az esetleges támadásokhoz. Az alfejezet során célom olyan innovatív javaslatokat megfogalmazni, amik hozzájárulnak a védelem folyamatos fejlesztéséhez és rugalmasságának fokozásához.

A kritikus szervezetek védelme komplex és interdiszciplináris feladat, amely magában foglalja a kockázatértékelést, a sebezhetőségi elemzést, a védekezési stratégiák kidolgozását és a gyors reagálási képességek fejlesztését. Az állami és üzemeltetők szereplőinek együttműködése, a nemzetközi kooperáció, valamint a folyamatos technológiai innovációk mind hozzájárulnak ahhoz, hogy a kritikus infrastruktúrák védelme hatékony és eredményes legyen, ezáltal biztosítva a társadalom és az állam zavartalan működését.

A kritikus szervezetek meghibásodása súlyos negatív hatásokat gyakorolhat az alapvető kormányzati műveletekre, a létfontosságú közszolgáltatásokra, valamint a szövetséges országok és a tagállamok gazdasági tevékenységeire. Ezek a zavarok alááshatják a katonai műveleteket is, beleértve a kiképzési gyakorlatokat, a telepítési, megerősítési és fenntarthatósági erőfeszítéseket. A rendszerek közötti bonyolult kölcsönös függőségek azt jelentik, hogy a kritikus szervezetek és infrastruktúrák egy-egy területén bekövetkező zavar dominó vagy egymást erősítő hatásokat válthat ki. Például az áramellátás megszakadása negatívan befolyásolhatja a közszolgáltatásokat és az alapvető javak biztosítását. Ezek a zavarok az összekapcsolt hálózatok és egyes esetekben a több országot átfogó infrastruktúrák miatt átléphetik az országhatárokat. [52]

Az infrastruktúrákat különböző természeti és ember okozta tényezők egyaránt megzavarhatják. A gazdaságok és társadalmak egyre növekvő kölcsönös függősége azt jelenti, hogy az ilyen zavarok széles körű, több ágazatra és akár nemzetközi határokat is érintő hatásokkal járhatnak. Az infrastruktúrák különösen érzékenyek a szándékos támadásokra vagy a véletlen meghibásodásokra. Számos infrastrukturális eszköz nagy területen helyezkedik el, és egyesek könnyen hozzáférhetőek. A támadók a kritikus infrastruktúrát "puha célpontnak" tekinthetik, amely különösen érzékeny a hibrid taktikákra, amelyek lehetővé teszik, hogy az ilyen támadások hihető tagadás mellett történjenek. Ezek a szándékos támadások stratégiailag is időzíthetők, hogy maximalizálják a bomlasztó hatásukat.

Az orosz-ukrán konfliktus bebizonyította, hogy a kritikus infrastruktúrát többféle módszerrel lehet célba venni, beleértve a kémkedést, a hírszerzést, a fizikai támadásokat, az ellenséges felderítést, a hibrid és kibertevékenységeket, valamint a függőségek kihasználását vagy a teljes elkobzást. A tapasztalatok megmutatták, hogy még a nagyszabású támadásoknak is ellen lehet állni, hangsúlyozva a rugalmas infrastruktúra és az alapvető szolgáltatások folyamatos biztosítása létfontosságú szerepét egy nemzet védelmi képességében.

A konfliktus hatására világossá vált, hogy a konfliktus résztvevői a kritikus infrastruktúrára, mint célpontra összpontosítanak. Emellett a terrorszervezetek továbbra is fenyegetik a kritikus infrastruktúrákat, többször is támadtak közlekedési rendszereket a szövetséges államokon és a tagállamokon belül. Ezenkívül a természeti katasztrófák és a szélsőséges időjárási események jelentős kockázatot jelentenek az infrastruktúra fizikai károsítása és a szolgáltatások megzavarása révén. E kihívások gyakorisága és súlyossága várhatóan növekedni fog az éghajlatváltozás miatt, amely növeli a tengerszint emelkedésének, a változó időjárási mintáknak és a gyakoribb szélsőséges időjárási eseményeknek való kitettséget.

A növekvő stratégiai verseny korszakában kulcsfontosságú a stratégiai sebezhetőségek és függőségek azonosítása és kezelése, amelyeket az ellenfelek kihasználhatnak. A kulcsfontosságú technológiai és ipari ágazatok, a kritikus infrastruktúra, valamint a stratégiai anyagok és ellátási láncok feletti külföldi ellenőrzés lehetővé teheti az ellenséges szereplők számára, hogy érzékeny információkat gyűjtsenek a NATO és az EU műveleteiről, potenciálisan megzavarják a kritikus infrastruktúrához való hozzáférést, vagy akadályozzák az általuk nyújtott szolgáltatásokat [53].

A tengerfenék egyre nagyobb stratégiai jelentőségű területté vált a tenger alatti infrastruktúrára való támaszkodás, valamint a hibrid fenyegetésekkel és fizikai károkkal szembeni védelmének egyedi kihívásai miatt.

1.3.1 Ágazati sajátosságok és kockázati specifikumok elemzése

A korábban bemutatott jogszabályi és intézményi környezet jól mutatja, hogy a rezilienciára vonatkozó európai és hazai követelmények egyre inkább a kockázatok rendszerszintű, ágazatokon átívelő megértésére épülnek. Ennek megfelelően a kritikus szervezetek fejlesztési irányait csak úgy lehet értékelni, ha az elemzés egyszerre veszi figyelembe a műszaki működés sajátosságait, az ágazati sérülékenységeket, valamint a módszertani kereteket, amelyek meghatározzák a kockázatok azonosítását, elemzését és kezelését.

Az ágazati specifikumok vizsgálata során kiemelt jelentőséggel bír a kockázatelemzés technikai alapjainak feltárása, hiszen az energia-, közlekedési, digitális infrastruktúrák és világűr infrastruktúrái olyan összetett rendszerek, amelyekben a hibák, meghibásodások és támadások láncreakciót, úgynevezett dominóhatást eredményezhetnek. A kockázatelemzés nem csupán a fenyegetések katalogizálását jelenti, hanem a kritikus elemek működésének fizikai, informatikai és szervezeti összefüggéseinek mély feltárását. Ezért a fejezet az ágazati részeknél nagyobb hangsúlyt helyez a műszaki jellegű megállapításokra, különös tekintettel azokra az elemzési módszerekre, amelyek az adott infrastruktúrák sajátosságaihoz igazodnak. [62]

A fejlesztési lehetőségek értékelése nem lehet kizárólag elméleti, szükség van a magyarországi környezetre jellemző példák és tapasztalatok beépítésére is. A hazai esettanulmányok például nagyobb energetikai üzemzavarok, távközlési kimaradások vagy közlekedési rendszerhibák lehetővé teszik, hogy az ágazati kockázatok ne csupán elméleti konstrukciók legyenek, hanem a gyakorlatban is értékelhető, bizonyítható sérülékenységeket tárjanak fel. Ez a megközelítés biztosítja, hogy a fejezet valódi tudományos eredményt hozzon létre, amely az ágazati kockázatok összehasonlításán és a közös mintázatok azonosításán keresztül támogatja a magyar reziliencia keretrendszer fejlesztését.

A következő alfejezetek ezért egyrészt bemutatják a négy kiemelt ágazat működési logikáját és technikai felépítését, másrészt részletesen elemzik azokat a kockázati tényezőket, amelyek meghatározzák az infrastruktúrák védelmi fejlesztésének irányait. Ezen alfejezet az ágazati specifikumokra építve azonosítja a fő műszaki sérülékenységeket, míg az ezt követő alfejezet a hazai és nemzetközi szakirodalomra, valamint a magyarországi gyakorlatra támaszkodva vázolja fel a kockázatalapú fejlesztési lehetőségeket. Ez a két rész együttesen adja meg azt a rendszerszintű alapot, amelyre a kritikus szervezetek rezilienciájának jövőbeni kiépítése épülhet.

1. Energia ágazat.

Az ágazat jellemzői: Az energia ágazat létfontosságú, mivel minden más ágazatot működtet, az egészségügytől a pénzügyekig. Az energiaellátásban bekövetkező zavarok azonnali és súlyos következményekkel járhatnak számos területen, ami rávilágít a robusztus és ellenálló energia infrastruktúra szükségességére. A stabil energiaellátás a gazdaságok és társadalmak működésének alapvető feltétele, különböző energiaforrások és kereskedelmi kapcsolatok révén. Az energia biztonsága azonban egyre nagyobb kihívást jelent a jelenlegi geopolitikai környezetben, mivel ellenséges szereplők és stratégiai versenytársak káros tevékenységeket folytatnak a kibertérben, manipulálják az energiaszállításokat, és gazdasági kényszert alkalmaznak. A katonai tevékenységek nagymértékben függnek a polgári energiahálózatoktól és ellátástól, ami tovább hangsúlyozza a kritikus energia infrastruktúra és ellátási láncok biztonságának szükségességét.

A Nord Stream gázvezetékek szabotázsa rávilágít az energia infrastruktúra sérülékenységére. Az orosz-ukrán konfliktus következtében megnövekedett az ellátási hiány kockázata, ami felhívta a lakosság figyelmét az esetleges mindennapi életet érintő károkra. Az energia infrastruktúra kiterjedtsége (csővezetékek, elektromos kábelek), megnehezíti annak folyamatos megfigyelését vagy védelmét így egyetlen támadás is súlyos károkat okozhat. Az infrastruktúra hálózatos jellege miatt egy helyi zavarból más területekre is átterjedő hatások lehetnek, továbbá az infrastruktúra elhelyezkedésére vonatkozó információk általában nyilvánosan elérhetők. Az energia infrastruktúra digitalizálásába történő jelentős beruházások pedig potenciálisan növelik az ilyen infrastruktúrák kiber támadásokkal szembeni sérülékenységét. Az óceán alatti energia infrastruktúra különösen sérülékeny, hiszen kiterjedt, és nehéz megfigyelni, valamint megvédeni [52]. Például a cseppfolyósított földgáz (a továbbiakban: LNG) használatának növekedése és az LNG-terminálok kiépítése új kihívásokat hoz az infrastruktúra védelme terén.

A megújuló energiaforrások növekvő használata és az elektrifikáció elősegítheti a rezilienciát azáltal, hogy növeli a források sokféleségét és az autonómiát, ám az új, távoli és szétszórt energiaforrások védelme újabb kihívásokat jelent. A megújuló energiaforrások nagyban függnek a NATO-n és az EU-n kívüli ellátási láncoktól, ami potenciális sebezhetőségeket hozhat magával.

Az energiaágazat különleges jellemzői, mint például a valós idejű követelmények, a dominóhatás lehetősége és a különböző technológiák egyidejű fenntartásának szükségessége, egyedi intézkedéseket igényelnek a reziliencia biztosítása érdekében [52].

A villamosenergia rendszer technológiai felépítése és kritikus pontjai: A villamosenergia ellátás négy fő alrendszerből tevődik össze, a termelés, átviteli hálózat, elosztó hálózat és a fogyasztó oldali kritikus szempontok. Ezek közül több pont egyedi műszaki sérülékenységet hordoz, mint például az alállomások és transzformátorok túlterhelődése, meghibásodása, a kondenzátorbankok és védelmi relék hibái, a SCADA/ICS rendszerek kibertársadalmának való kitettség, valamint az átviteli vezetékek időjárásfüggő sérülékenysége. A villamosenergia rendszer elemzése során kulcsfontosságú az a kritérium, amely előírja, hogy a hálózat egy eleme meghibásodása esetén a rendszereknek továbbra is stabilan kell működnie. E kritérium nélkül nem teljesülne a széles körű, láncreakciót okozó üzemzavar veszélye. Hazai esettanulmányt tekintve a MAVIR éves rendszerjelentései alapján Magyarországon a nyári csúcsterhelések idején több alállomás közelíti meg a kapacitáshatárt, ami növeli a túlmelegedésből fakadó üzemzavarok és kiesések kockázatát. [63]

A földgázellátási rendszer sajátosságai és sérülékenysége: A földgázágazat műszaki struktúrája a nemzetközi betáplálási pontokból, a nagynyomású átviteli hálózatokból és az elosztói hálózatok és tárolókból áll. A kritikus műszaki pontjai közé tartoznak a kompresszorállomások, vezeték korróziók és a hegesztési pontok hibái, a nyomásszabályozók meghibásodása, a szenzorhibák a felügyeleti rendszerekben, valamint a szállítási útvonalak geopolitikai sérülékenysége. Magyarország egyedülállóan nagy kapacitású föl alatti gáztárolókkal rendelkezik, amely csökkenti a külső hatásokat, ugyanakkor a tárolók töltése és kitárolása komplex műszaki kockázatokat hordoz, úgy mint kompresszorok, nyomásingadozás, szezonális terhelés. Az Failure Mode and Effects Analysis (a továbbiakban: FMEA) a villamosenergia rendszerben általánosan alkalmazott módszer olyan tipikus meghibásodási módok azonosítására, mint például transzformátor fölmelegedése, reléhibák, távvezeték-földzárlatok. A FMEA különösen alkalmas műszaki eredetű kockázatok rangsorolására. Az energiaágazat kiemelten függ az informatikai működéséről, a közlekedési infrastruktúráktól és a víziközművektől. A Rinaldi–Peerenboom-féle modell alapján a villamosenergia-rendszer a legkritikusabb forrási infrastruktúra, amelynek kiesése dominóhatást indít el. [20]

Magyarországi gyakorlatot érintő esettanulmányként említhető meg az országos távközlési zavar, ami a villamosenergia termelő egységek adatszolgáltatási kiesését okozza. Az elmúlt években több rövid idejű esemény történt, amelyek megmutatták, hogy a digitális és energetikai rendszerek összefonódása egyre kritikusabb. Az időjárás okozta vezetékhibák a széllökések és jégképződés több helyen vezetékszakadást és alállomási túlterhelést okoztak. Az energia ágazat ágazatainak főbb sérülékenységi pontjai ez alapján:

- erős hálózati összefonódás, ami nagyfokú dominóhatás kockázatát eredményezi,
- műszaki eszközpark elöregedése, a transzformátorok és vezetékek esetében,
- SCADA/ICS kibertámadási kitettség,
- időjárásfüggés fokozódása a klíma változás okán,
- az interdependenciák számának növekedése, összetett rendszerszintű kockázatok. [63]

1. táblázat: Villamosenergia hálózat műszaki sérülékenységei és kritikus hálózati elemei

Készítette: a Szerző, 2025. [65]

Hálózati elem	**Tipikus meghibásodási mód**	**Sérülékenység jellege**	**Következmény**
Transzformátor	Túlmelegedés, olajszivárgás, tekercs hiba	Fizikai, üzemviteli	Kapacitáscsökkenés, hálózati instabilitás
Alállomási kapcsolóberendezések	Kontaktushiba, reléhiba	Műszaki, elektromos	Áramszünet lokális/kiterjedt formában
Távvezetékek	Jég- és szélterhelés, mechanikai szakadás	Időjárási, fizikai	Fogyasztók nagykörű kiesése
SCADA/ICS rendszerek	Ransomware, manipuláció, adatvesztés	Kiberbiztonsági	Irányíthatóság elvesztése, hibás kapcsolások
Harmadik országokból érkező importkapacitás	Kínálati sokkok, fizikai megszakadás	Ellátásbiztonsági	Ellátási zavar, frekvenciaesés
Erőművi egységek	Turbina-hiba, gázellátási zavar	Fizikai, ellátási lánc	Termelési kapacitás kiesése

2. Közlekedés:

A közlekedési ágazat kulcsfontosságú az áruk, a személyek és a szolgáltatások mozgásához. Támogatja a globális ellátási láncokat és más kritikus infrastruktúrákat, például a sürgősségi szolgáltatások és a logisztika működését.

A közlekedési infrastruktúra elengedhetetlen társadalmaink, gazdaságaink és haderőink működéséhez. Ez a kiterjedt hálózat magában foglalja a közutakat, vasutakat, belvízi utakat, repülőtereket, tengeri és belvízi kikötőket, amelyek lehetnek állami tulajdonban, magántulajdonban vagy a köz- és magánszféra közötti partnerségek keretében kezeltek.

Az üzemképes közlekedési infrastruktúra fenntartása kritikus fontosságú, különösen a transzeurópai közlekedési hálózatban azonosított infrastruktúrák esetében, amelyek az Európán átívelő és a szomszédos országokba irányuló szállítás fő ütőereként szolgálnak.

E hálózat kiterjedtsége ellenére, amely számos alternatív útvonalat és intermodális szállítási megoldást kínál, bizonyos kulcsfontosságú csomópontok, mint például a főbb repülőterek, tengeri kikötők és fő vasúti csomópontok, pótolhatatlanok és létfontosságúak mind a polgári, mind a katonai műveletek szempontjából. A közelmúlt természeti katasztrófái megmutatták, hogy e kulcsfontosságú pontokon bekövetkező zavarok jelentősen befolyásolhatják az elérhetőséget és a műveleteket.

A tömegközlekedési infrastruktúra gyakori célpontja volt a terrortámadásoknak, ami fokozott biztonsági intézkedéseket tett szükségessé. Az, hogy ezt az infrastruktúrát továbbra is hozzáférhetővé kell tenni a nyilvánosság számára, korlátozza a védelem megvalósítható mértékét. A közlekedési infrastruktúra, beleértve a repülőtereket és a tengeri kikötőket is, egyre inkább ki van téve a kibertámadásoknak, amelyek súlyos gazdasági károkat okozhatnak és megzavarhatják a katonai tevékenységeket.

A hadseregnek a polgári és kereskedelmi közlekedési eszközökre, például a tengeri kikötőkre, repülőterekre és a szárazföldi intermodális összeköttetésekre való támaszkodása kulcsfontosságú a gyors bevetés és a folyamatos műveletekhez Európa szerte. A kulcsfontosságú csomópontok, különösen a nagyobb tengeri kikötők és repülőterek meghibásodása mélyreható következményekkel járhat mind a polgári, mind a katonai logisztikára nézve.

A közlekedési ágazat és más kritikus ágazatok, például az energia és a digitális infrastruktúra közötti kölcsönös függőségek egyre nőnek. A közlekedés fokozódó villamosítása tovább növeli az elektromos hálózattól, akkumulátoroktól és a kapcsolódó infrastruktúrától való függőséget, míg a szénhidrogénvezetékektől való függőség továbbra is jelentős marad. Emellett a közlekedési infrastruktúra digitalizálódása miatt nagyobb mértékben függ a digitális rendszerektől, és sebezhetőbbé válik a kiberfenyegetésekkel szemben. A közlekedési infrastruktúra az űrrendszerektől is függ, különösen a helymeghatározás, a navigáció és az időzítés terén, a kikötői műveletek pedig a globális navigációs műholdrendszerekre támaszkodnak a konténerek kirakodásának irányítása érdekében.

Összefoglalva, bár a közlekedési infrastruktúra szerves részét képezi a különböző ágazatoknak és a nemzetvédelemnek, sebezhetősége különösen a kibertámadásokkal és fizikai zavarokkal szemben fokozott védelmet és az érdekelt felek közötti koordinációt tesz szükségessé az ellenálló képesség és megbízhatóság biztosítása érdekében [52].

A villamosenergia rendszer technológiai felépítése és kritikus pontjai: A közlekedési ágazat különösen a vasúti, légi és közúti irányítási rendszerek összetett, egymásra épülő alrendszerekből áll, amelyekben a technológiai, humán és infrastruktúra elemek közötti interakciók egyaránt befolyásolják a működés biztonságát. A közlekedés szerepe a kritikus infrastruktúrák működésében kettős, egyrészt független ágazatként biztosítja az emberek és áruk mobilitását, másrészt kiszolgáló infrastruktúraként alapvető feltétele a karbantartási, logisztikai és ellátási lánc folyamatoknak más kritikus ágazatokban pl. energia, egészségügy, digitális rendszerek. Ennek következtében a közlekedési ágazat sérülékenységei nemcsak közvetlen biztonsági kockázatokat hordoznak, hanem láncszerű, többszintű hatásokkal járó rendszerszintű kockázatokat is.

A vasúti közlekedés műszaki rendszere négy fő komponensből áll a biztosítóberendezésekből pl. váltók, jelzők, sináramkörök, a forgalomirányításból pl. központi rendszerek, távvezérlés, az energiaellátásból felsővezetékek, alállomások, és a járműtechnikából pl. mozdonyok, fékrendszerek, fedélzeti diagnosztika. A legnagyon sérülékenységet a váltóhibák pl. fagy, szennyeződés, mechanikai hiba hatására, a biztosítóberendezések meghibásodása, jelzőrendszer leállása, a kommunikációs hálózat hibái, valamint az alállomási áramszünet jelentik. Hazai példákból merítendő a 2023-az MÁV informatikai rendszerének leállása, ahol több ezer járatot érintő késés és leállás, teljes kommunikációs rendszer kimaradás volt tapasztalható. Emellett 2021 telén váltóhiba volt tapasztalható, ami országos fennakadásokat, műszaki hibákat és időjárási hatások kombinációját okozta. [66]

A légi közlekedés rendszereiben a légi forgalomirányítás rendkívül technológiafüggő rendszer, amely több, egymásra épülő alrendszert használ, úgymint radarrendszerek, kommunikációs hálózatok, irányítói munkaállomások, navigációs infrastruktúra. Legfőbb sérülékenysége a légiforgalmi irányítás informatikai rendszereinek meghibásodása, a repülőtéri infrastruktúra leállása és az elektromos ellátás zavara. A repülőtér üzemfolytonosságát veszélyeztetheti az energiabetáplálási zavarok, a radar kiesése és a földi kiszolgálási rendszer hibái.

A modern közúti infrastruktúra jelentős mértékben támaszkodik a forgalomirányítási rendszerekre, a szenzorokra és a változtatható jelzőtáblákra. Tipikus műszaki sérülékenységek lehetnek a központi szerverek meghibásodása, a távközlési hálózat kiesése és az áramellátási zavarok, jelzőlámpák és kijelzők működésképtelensége. A vízi közlekedés biztonságát befolyásoló legfontosabb tényezők a navigációs rendszerek megbízhatósága, a hajózóút-jelzések és mederfenntartási munkák minősége, valamint a folyamatos monitoring.

Magyarország vízi közlekedése különösen sérülékeny a klímaváltozásból eredő hidrológiai szélsőségekkel szemben. Az egyre gyakoribb rendkívül alacsony vízállások, amelyek az elmúlt években többször is előfordultak a Dunán, jelentős korlátozásokat okoztak a hajóforgalomban, különösen a teherhajók merülési korlátai miatt. A vízállás csökkenésével összefüggő forgalomkorlátozások nemcsak logisztikai fennakadásokat eredményeznek, hanem ellátási lánc kockázatokat is, különösen a gabona- és olajszállítmányok esetében. Ezen túlmenően, az extrém magas vízállás vagy az árvizek a kikötők infrastruktúrájában, partvédelmi műtárgyakban és rakodóberendezésekben okozhatnak komoly károkat.

A közlekedési ágazat fő sérülékenységi:

- technológiai függőség, magas fokú amortizáció, hiba esetén rendelkezésre állási kockázat.
- kiber és fizikai rendszerek összefonódása, vasúti és légiforgalmi irányítás különösen érzékeny a támadásokra,
- humán tényező dominanciája, döntéshozatali hibák, túlterheltség, információs túltengés,
- interdependencia a digitális és energiaágazattal, energia nélkül nincs jelzés, nincs kommunikáció, nincs forgalomirányítás,
- klímaváltozás hatásai, gyorsabban változó időjárási mintázatok, vasúti infrastruktúra fokozott terhelése. [67]

A közlekedési ágazat reziliencia profilja a három nagy közlekedési alrendszer összehasonlításából a következő megállapítások vonhatók le:

- a vasút a leginkább infrastruktúra függő rendszer, a műszaki meghibásodás domináns,
- a légi közlekedés a leginkább információfüggő rendszer, kommunikációs és digitális kockázatok dominálnak,
- a közút a leginkább környezeti hatásfüggő rendszer, az időjárási és forgalmi kockázatok dominálnak. [68]

Ez a három eltérő sérülékenységi profil jól mutatja az ágazat heterogenitását, és alátámasztja, hogy fejlesztések csak kockázatalapú, alrendszer-specifikus megközelítéssel lehetnek hatékonyak. [69]

2. táblázat: Közlekedési ágazat műszaki sérülékenységei
Készítette: a Szerző, 2025.

Infrastruktúra elem	Tipikus meghibásodás / sérülékenység	Sérülékenység típusa	Következmény / Hatás	Hazai relevancia
Vasúti váltók	Befagyás, mechanikai hiba, szennyeződés	Fizikai, időjárási	Késések, vonatmegállások	Télen rendszeres váltóhibák
Biztosítóberendezések	Reléhiba, jelzőhiba, szoftverhiba	Műszaki, informatikai	Üzemzavar, leállás	MÁV 2023 IT-incidens
GSM-R kommunikáció	Mobilhálózati zavar, frekvenciainterferencia	Kiber + kommunikációs	Forrászavar, irányítási nehézség	Vasúti forgalomirányítás érzékeny
Légi navigációs rendszerek	Kalibrációs hiba, jelvesztés	Műszaki	Korlátozott megközelítés	Budapest Airport
Légiforgalmi irányítási rendszerek	Szerverhibák, adatvesztés	Informatikai	ATC műveletek korlátozása	Időszakos kimaradások
VJT/VAR közúti jelzők	Túlmelegedés, hálózati hiba	Fizikai + energia	Információhiány, torlódás	Autópálya ITS hibák
Közlekedésirányító központok	Szoftverfrissítési hiba, adatbázis-hiba	Kiber, IT	Több város érintett fennakadás	Budapest közlekedési rendszer
Hidak és alagutak infrastruktúrája	Szerkezeti károk, korrózió	Fizikai	Kapacitáskorlátozás	Lánchíd, alagút felújítások

3. Digitális infrastruktúra:

A digitális infrastruktúra a modern kommunikációs rendszerek gerince, amelyek nélkülözhetetlenek a társadalom és a gazdaság működéséhez. Mivel a digitális infrastruktúrára való támaszkodás egyre nő, különösen a kritikus kormányzati kommunikációban, különösen válsághelyzetekben, ennek jelentősége tovább növekszik.Az információs és kommunikációs szolgáltatások támogatásához sokféle infrastrukturális elemre van szükség, többek között földalatti és tenger alatti üvegszálas kábelekre, cellás bázisállomásokra és műholdakra. Bár a redundanciát általában beépítik a kommunikációs hálózatokba, továbbra is alapvető fontosságú, hogy készenléti tervekkel rendelkezzenek, például az elsődleges, alternatív, vészhelyzeti és vészhelyzeti lehetőségek meghatározásával.

Egyes infrastruktúrális csomópontok, mint például az adatközpontok és a tenger alatti kábelek különösen kritikusak és nehezen pótolhatók, ami a potenciális ellenfelek számára értékes célpontokká teszi őket. A tenger alatti kommunikációs kábelek különösen fontosak, mivel a világ internetes forgalmának 95%-át ezeken keresztül bonyolítják le. Kiterjedt hosszúk és a felügyeletükkel kapcsolatos kihívások miatt ezek a kábelek vonzó célpontok lehetnek. Több tenger alatti kábel egyidejű megszakítása jelentős kockázatot jelentene mind a tagállamok, mind a szövetségesek számára, mivel a javítási lehetőségek korlátozottak, és e kábelek távoli elhelyezkedése késleltetheti a javítást. [70]

Az 5G hálózatok megjelenése tovább növelte a digitális infrastruktúra jelentőségét, mivel ezek a hálózatok egyre inkább a köz- és gazdasági funkciók szempontjából létfontosságú szolgáltatások gerincét alkotják, például az energia, a közlekedés, a banki szolgáltatások, az egészségügy és az ipari vezérlőrendszerek. Az 5G hálózatok széles körű használata és a következő generációs hálózatokra való jövőbeli támaszkodás fokozza bármely széles körű zavar lehetséges következményeit. Az 5G-hálózatok ráadásul új sebezhetőségeket is bevezetnek, ami erősebb biztonsági és ellenálló képességi intézkedéseket tesz szükségessé. A külső beszállítóktól származó hálózati berendezésekre és szolgáltatásokra való támaszkodás szintén szükségessé teszi a stratégiai kockázatok gondos értékelését, különösen olyan harmadik országok tekintetében, amelyek biztonsági törvényei és vállalati gyakorlatai kockázatot jelenthetnek a szövetségesek és a tagállamok biztonságára nézve. [71]

Mivel a digitális infrastruktúra nagy része a vállalatok tulajdonában és üzemeltetésében van, egyre inkább felismerik, hogy biztosítani kell a biztonságot és az ellenálló képességet. Különösen a kormányok és a fegyveres erők függnek nagymértékben a magánkézben lévő digitális infrastruktúrától, ami rávilágít arra, hogy jobban meg kell érteni és ellenőrizni kell, hogy hol tárolják és dolgozzák fel az adatokat. Bár a kormányok és a hadsereg által használt digitális infrastruktúra egy része állami tulajdonban van és állami üzemeltetésben, ugyanilyen fontos annak ellenálló képességének javítása, és a meglévő közszféra jogszabályai és politikái potenciálisan a katonai területre is alkalmazhatók.

Továbbá a digitális infrastruktúra ellátási láncok globális jellege sebezhetővé teszi őket a véletlenszerű, akár időjárási események vagy emberi hiba miatti, akár politikai, katonai, pénzügyi vagy bűnügyi indíttatású, szándékos zavarokkal szemben. A NATO-n vagy az EU-n kívülről beszerzett létfontosságú komponensek nem feltétlenül tartják be ugyanazokat a biztonsági vagy adatvédelmi előírásokat, ami sebezhetőséget jelenthet a szövetségesek vagy a tagállamok hálózataiban [52].

A digitális infrastruktúra technológiai felépítése és kritikus pontjai: A digitális infrastruktúra a modern társadalom „láthatatlan gerince”, amely adatátviteli hálózatokból, adatközpontokból, felhőszolgáltatásokból, távközlési rendszerekből és alapvető internetes protokollszolgáltatásokból áll. A kritikus szervezetek működésében a digitális infrastruktúra azért tekinthető különösen sérülékenynek, mert rendszerszintű, sokszor nem redundáns pontokra épül, körzeti adótornyok, adatközpontok, és ezek kiesése aránytalanul nagy hatást gyakorol a többi kritikus ágazatra.

A digitális infrastruktúra sajátossága, hogy egyszerre kell kezelnie a fizikai komponensek sérülékenységét kábelek, aktív eszközök, energiaellátás és a kiberfenyegetésekből eredő sérülékenységeket mint az adatintegritás, a hozzáférés, a rendelkezésre állás veszélyeztetettsége.

A fizikai és digitális sérülékenységek egymást erősítő hatása miatt a digitális infrastruktúra az egyik legkomplexebb ágazat a kockázatelemzés szempontjából. A hálózati struktúra több szinten épül fel, amelyek jelenthetik a kritikus pontjait is, azaz a gerinchálózatból, a hozzáférési hálózatból, az adatközpontok és felhőszolgáltatókból, és a DNS és routing infrastruktúrából. A fentiek közül több komponens egyedi sérülékenységet hordoz, az optikai kábelek akaratlan ásás, rongálás, árvíz, tűz esetén regionális internetkiesést okozhat. Az adatközpontoknál egy esetleges hűtési hiba, tűz, energiaellátás kimaradását okozhatja.

Fizikai infrastruktúra sérülékenysége közé sorolható az optikai kábelek sérülése, az adatközpontok hűtéri hibái, valamint a mobil bázisállomások nagy energiaszükséglete. Kiber sérülékenysége közé sorolható a DDos támadások nagy sávszélességű szolgáltatók ellen, a Ransomware támadások felhőszolgáltatókon vagy vállalati végpontok, a Zero-day sérülékenység hálózati eszközökben, és az adatintegritási incidensek. Az interdependencia okozta sérülékenység energiaellátási kiesést, ezáltal mobilhálózat és adatközpontok azonnali leállását okozza, amennyiben a kritikus eszközpart kiszállítása kiesik közlekedési fennakadásokat okoz, továbbá egy telekommunikációs szolgáltató hibája országos lefedettségű zavart okozhat. Magyarországon 2022-ben országos mobilhálózat túlterhelődött, a szerveroldali frissítési hiba és forgalmi csúcs együttesen okozták a többórás kiesést. Az optikai kábelvágás miatt több alkalommal térségi internetszünet következett be, építési munkák következtében több település teljes internet kapcsolata szűnt meg órákra. Az adatközpont hűtési hibája miatt a túlmelegedés több szolgáltatás kimaradását okozta. [72]

Az infokommunikációs ágazat fő műszaki sérülékenységei:

- erős koncentráció a gerinchálózati csomópontoknál, egy hiba több régiót is érinthet,

- magas függőség a folyamatos energiaellátástól, energia nélkül a digitális infrastruktúra percek alatt leáll.
- redundanciahiány a vidéki térségekben, egyetlen optikai útvonaltól való függés,
- felhőszolgáltatói függés, centrális sérülékenység, nemzeti hatással,
- kiber-fizikai kölcsönhatások komplexitása, a kiberincidensek fizikai leállást eredményezhetnek,
- gyorsan változó fenyegetési környezet, a zero-day sérülékenységek, új támadási technikák.

A digitális infrastruktúra kockázati profilja a négy vizsgált ágazat közül a legnagyobb kiberkitettségű, a leggyorsabban változó, és a leginkább interdependens. Egyetlen incidens könnyen átterjed az energia- és közlekedési rendszerekre, ami azt jelenti, hogy a digitális infrastruktúra a magyar rezilienciarendszer egyik legkritikusabb csomópontja. [26]

3. táblázat: Digitális infrastruktúrák műszaki sérülékenységei
Készítette: a Szerző, 2025.

Infrastruktúra elem	**Meghibásodás / sérülékenység**	**Sérülékenység típusa**	**Következmény / Hatás**	**Hazai relevancia**
Optikai gerinchálózat	Kábelvágás, árvízkár, tűzkár	Fizikai	Regionális internetszünet	Építési kábelvágások
Adatközpontok	Hűtési hiba, UPS-kiesés	Műszaki, energia	Szolgáltatás-leállás	Magyar DC-események 2021–23
Mobil bázisállomások	Áramkimaradás, fizikai rongálás	Energia + fizikai	Mobilhálózati kiesés	Többórás kiesések 2022
Routerek, switch-ek (core–aggregation)	Firmware-hiba, túlterhelés	Informatikai	Hálózatleállás, csomagvesztés	ISP jelentések
DNS infrastruktúra	DNS poisoning, szerverhiba	Kiber	Tartományszintű kiesés	Több országos DNS-lassulás
BGP routing	BGP hijack, route leak	Kiber	Internet-hozzáférés sérülése	Regionális esettanulmányok
Felhőszolgáltatói platformok	Szoftverfrissítés, adatvesztés	Informatikai	Digitális szolgáltatások leállása	európai uniós szolgáltatók hibái
IoT és kritikus ipari eszközök	Sebezhetőségek, jelszivárgás	Kiber-fizikai	SCADA-lánc támadhatóság	Energia–víziközmű rendszerek

4. Világűr:

Az űrinfrastruktúra egyre fontosabb, mivel olyan kritikus szolgáltatásokat nyújt, mint a műholdas kommunikáció, a navigáció és a földi megfigyelés. Ezek a szolgáltatások a katonai műveletektől kezdve a katasztrófaelhárításon át a globális helymeghatározó rendszerekig mindenhez nélkülözhetetlenek. Az űrinfrastruktúra magában foglalja mind az űrbe telepített eszközöket, mind a földi rendszereket, beleértve az adat- és rádiófrekvenciás kapcsolatokat, amelyek mindegyike ki van téve különböző, ember okozta és természeti kockázatoknak. Ezek az eszközök olyan szervezetek tulajdonában és üzemeltetésében vannak, mint az EU (pl. Galileo, Copernicus, IRIS), a tagállamok, a szövetségesek és egyre inkább a kereskedelmi vállalkozások.

A stratégiai riválisok és a potenciális ellenfelek olyan fejlett űrellenes képességeket fejlesztenek ki, amelyek veszélyeztetik a NATO és az EU űrben való működési képességét, és potenciálisan megzavarhatják vagy megsemmisíthetik a kritikus űrszolgáltatásokat. Az ilyen fenyegetések mind a polgári, mind a katonai infrastruktúrát károsíthatják, amelytől más alapvető szolgáltatások függnek. Emellett az űrinfrastruktúra olyan egyedi kihívásokkal is szembesül, mint az űrszemét, amely károkat okozhat és csökkentheti a pályák használhatóságát, valamint az űridőjárás, amely hatással lehet a műholdak működésére és a földi hálózatokra.

Számos kritikus ágazat, köztük az energia, a közlekedés, a pénzügyek és a digitális infrastruktúra nagymértékben támaszkodik az űrből származó adatokra és szolgáltatásokra. Az űrágazat fejlődésével és a hozzáférés bővülésével az e szolgáltatásokban bekövetkező zavarok jelentősen befolyásolhatják a tagállamok és a szövetségesek ellenálló képességét, csökkentve a szolgáltatások hatékonyságát és növelve a költségeket. Az ilyen zavarokkal szembeni ellenálló képességet redundanciával lehet fokozni, a tagállamok, a szövetségesek és az EU képességeinek űradatai és szolgáltatásai egymást kiegészítő szerepet töltenek be [52]. Ezek az ágazatok egyedi kihívásokkal szembesülnek, például a kiberbiztonsági fenyegetésekkel, fizikai támadásokkal és sebezhetőségekkel, amelyek összekapcsolt jellegükből adódnak. E kihívások kezelése alapvető fontosságú ezen ágazatok, és ezen keresztül az egész kritikus infrastruktúra ellenálló képességének megerősítéséhez.

Az említett ágazatspecifikus tényezők rávilágítanak az ágazatok közötti szoros fizikai és digitális összefonódásokra, ideértve azokat az ágazatokat is, amelyek nem képezik jelen elemzés tárgyát például egészségügy, vízellátás, agrárgazdaság. [52] A különböző infrastruktúrák közötti erős kölcsönös függőség miatt egy adott ágazatban bekövetkező zavarok láncreakció szerűen más ágazatok kritikus infrastruktúráit is érinthetik.

Ezeknek az összefüggéseknek a mélyebb megértése kulcsfontosságú ahhoz, hogy előre jelezhessük a lehetséges láncreakciókat, meghatározhassuk a mérséklésükre szolgáló intézkedéseket, és elősegíthessük a hatékony, egymást kiegészítő polgári és katonai reagálást [54].

A világűr technológiai felépítése és kritikus pontjai: A világűr ágazat különösen a műholdas kommunikáció, navigáció, Föld megfigyelés, űridőjárási monitoring és műholdas adatátvitel, egyre inkább a modern államok kritikus infrastruktúrájának önálló pillérévé válik. Bár Magyarország nem rendelkezik saját teljes műholdflottával, a világűr ágazat mégis közvetlenül érinti a hazai kritikus szervezetek működését, mivel a legtöbb szolgáltatás európai vagy globális rendszerek (pl. Galileo, EGNOS, Copernicus, Starlink) révén biztosított. A világűr infrastruktúrák sajátossága, hogy az ágazat extrém mértékben technológia intenzív, ugyanakkor a felhasználók nagy része nincs tudatában annak, hogy mindennapi szolgáltatásaik, mint például a navigáció, az időszinkronizáció, a kommunikáció, a meteorológiai előrejelzés, és a mezőgazdasági adatgyűjtés közvetetten a műholdak rendelkezésre állására épülnek. A műholdas rendszerek sérülékenysége ezért nemcsak űrtechnológiai kérdés, hanem nemzetbiztonsági és ágazatközi kockázatkezelési problémakör is. Az ágazat három fő technológiai rétegre osztható a műholdrendszerekre, mint a kommunikációs, navigációs, megfigyelő műholdak és az új generációs, több ezer eszközből álló megfigyelő konstellációk, mint a Starlink vagy OneWeb. Másik réteg a földi kiszolgáló infrastruktúra, az irányítóközpontokkal, a földi átjátszóállomásokkal és az adatfeldolgozókkal. A harmadik pedig a felhasználói szegmens, a közlekedési, mezőgazdasági és mobilhálózati időszinkronjai, a műholdas internet eszközei és a földmegfigyelési adatot használó rendszerek. [74]

A műholdas rendszerek sérülékenységei három fő kategóriába sorolhatók. Az első a fizikai és űrbeli kockázatok, ahol számolni kell az űrszemét ütközési kockázatával, a mikro meteorit becsapódásával, a műholdak élettartamának csökkenésével a sugárzás miatt, valamint a pályakarbantartási hibákkal és pályaeltérésekkel. Tehát a részleges vagy teljes műhold kiesés, navigációs hibákat és kommunikációs zavarokat okozhatnak.
A második kategória az űridőjárás okozta kockázatok, ezen belül is a napkitörések, geomágneses viharok, a rádiózavarás, ás a töltött részecskék okozta elektronikai meghibásodás. Ennek következtében a zavar keletkezhet a közlekedési ágazatban, a műholdak átmeneti kiesésével lehet számolni, az elektromos áramkörök meghibásodásával és a a villamosenergia-hálózatok, transzformátorok túlterhelődésével.

A harmadik fő kategória a kiber és kommunikációs sérülékenység, ezen belül is a műholdirányítás elleni kibertámadás, a jelszórási zavarás vagy megtévesztés, a földi irányítóközpont elleni támadás és az adatlopás műholdas kommunikációból. [75] Bár Magyarország nem üzemeltet saját navigációs műholdakat, az alábbi területek közvetlenül érintettek, úgymint a navigáció és légi közlekedés, intelligens forgalomirányítás, a mobilhálózatok időszinkronja, az árvízmodellezés, az erdőtűz monitoring, szárazsági indexek, továbbá a műholdas kommunikáció szerepe tartalék infrastruktúraként, mint a Starlink rendszerek alkalmazása extrém helyzetekben (pl. természeti katasztrófák után). [76]

Az infokommunikációs ágazat fő műszaki sérülékenységei:

- erősen centralizált erőforrások, egyetlen műhold vagy irányítóállomás kiesése nagy hatású esemény,
- kettős kitettség, az űrbeli objektum fizikai javítása nehézkes vagy lehetetlen, ezért a kibertámadások hatása fokozott,
- űridőjárási bizonytalanság, a naptevékenység növekedésével a következő években magasabb kockázati szint várható,
- magas interdependencia szint más kritikus ágazatokkal
    - navigáció (közlekedés),
    - időszinkron (digitális rendszerek),
    - meteorológiai adatok (víziközművek, mezőgazdaság),
    - kommunikáció (biztonsági szervezetek),
- a megfigyelő műholdak konstellációi gyors növekedése új típusú kockázatot hoz
    - ütközések valószínűsége nő,
    - pályaszabályozás nehezül,
    - megfigyelés és követés erőforrásigénye nő.

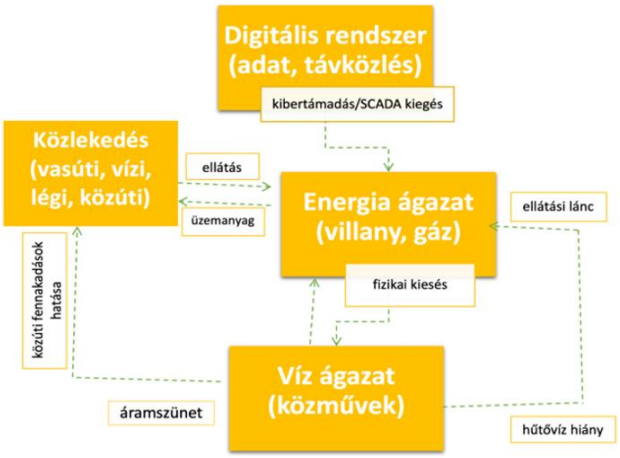
A világűr ágazat kockázati profilja a többi vizsgált ágazathoz képest a legösszetettebb, térben nem lokalizált, a legmagasabb kitettséggel rendelkezik, a legmagasabb fokú technológiai függésű, és interdependenciái a legerősebbek a digitális és közlekedési ágazatokkal. A műholdas infrastruktúrák sérülése ezért még részleges esetben is olyan ágazatokban okoz zavart, amelyek a napi működéshez elengedhetetlenek Magyarországon pl. mobilhálózat, pénzügyi időszinkron, légi forgalom. [77]

4. táblázat: Világűr ágazat műszaki sérülékenységei

Készítette: a Szerző, 2025.

Infrastruktúra elem	Tipikus sérülékenység / meghibásodás	Sérülékenység típusa	Következmény	Nemzetközi / hazai relevancia
Műholdak (LEO/MEO/GEO)	Ütközés űrszeméttel, sugárzási hiba	Fizikai, környezeti	Műhold-kiesés, adatvesztés	ESA–NOAA figyelmeztetések
GNSS rendszerek (GPS, Galileo)	Jamming, spoofing, integritásvesztés	Kiber + rádiófrekvenciás	Navigációs hiba	Kelet-európai GPS-zavarások
Űridőjárás – napvihar (CME)	Geomágneses vihar	Környezeti	Navigációs, kommunikációs zavar	2024-es erős naptevékenység
Földi irányítóközpontok	IT-rendszerhiba, kibertámadás	Informatikai	Műholdvezérlés akadozása	EU SST program
Gateway és antennarendszerek	Mechanikai sérülés, időjárási kár	Fizikai	Jelvesztés, adatátviteli zavar	Regionális szolgáltatói hibák
LEO konstellációk	Pályaszabályozási hibák, tömeges ütközési kockázatok	Fizikai + üzemeltetési	Tömeges műhold-kiesés	Starlink, OneWeb növekedés
Földmegfigyelés (Copernicus)	Adatfeldolgozó központ hiba	Informatikai	Késleltetett katasztrófavédelmi adat	Árvízmodellezésben fontos
Űrkommunikációs rendszerek	Rádiózavarás, antennahiba	Műszaki	Katonai/pol-civ kommunikáció sérülése	NATO figyelmeztetések

A lenti grafikus ábra a Rinaldi–Peerenboom-féle infrastruktúra-függőség modell adaptációja, magyarországi energia-, közlekedési és digitális rendszerekre illesztve. [20] Az energia és a digitális infrastruktúra esetében az áramkimaradás azonnali szolgáltatásmegszakadást okoz a mobilhálózatokban, adatközpontokban. A digitális infrastruktúra és az energia ágazatnál a SCADA/ICS rendszerek kiesése hibás kapcsolási utasításokat vagy túlterhelést eredményezhet. A közlekedés és energia ágazatnál a súlyos közúti vagy vasúti fennakadások megakadályozzák a transzformátorok, alkatrészek, tartalék generátorok szállítását. Az energia és víz ágazat kapcsolatánál az áramszünet hatására a szivattyútelepek leállnak, ami befolyásolja az erőművi hűtőrendszereket.



6. ábra: Interdependencia grafikon
Készítette: a Szerző, 2025.

A víz és energia ágazatnál pedig az extrém alacsony vízállás esetén a folyóvízi erőművek termelése drasztikusan csökkenhet. Ez a modell jól mutatja, hogy az energiaágazat központi, támogató infrastruktúra, amely szinte minden más ágazat működését meghatározza. A tipikus kockázati kategóriákat bemutató összehasonlító mátrix lehetővé teszi az egyes ágazatok fizikai, műszaki meghibásodásnak, sérülékenységének és kockázatainak egységes szempontrendszer szerinti értékelését.

5. táblázat: Tipikus kockázati kategóriákat összehasonlító mátrix, Készítette: a Szerző, 2025.

Kockázati kategória	**Energiaágazat**	**Közlekedési ágazat**	**Digitális infrastruktúra**	**Világűr**
Fizikai műszaki meghibásodás	Transzformátor-hiba, alállomási kiesés	Váltóhiba, jelzőberendezés meghibásodása	Adatközponti hűtési hiba, kábelvágás	Műholdkomponens meghibásodás, pályaeltérés
Kiberkockázat	SCADA támadás, ransomware	Vasúti irányítás, ATC rendszer támadása	DDoS, ransomware, BGP hijack	Műholdirányítás hackelése, jamming/spoofing
Időjárási és környezeti extrémumok	Hőhullám, jegesedés, vihar	Vihar, árvíz, fagy miatti meghibásodás	Fizikai infrastruktúrára ható időjárás	Napkitörés (CME), geomágneses vihar, űridőjárás
Ellátási lánc sérülékenység	Gázimport, transzformátor-ellátás	Járműalkatrész-ellátás, logisztikai zavar	Mikrochip-hiány, felhőszolgáltató függés	Üzemeltetői monopóliumok, kilövési infrastruktúra függés
Emberi tényező	Hibás kapcsolási utasítás	Irányítói hiba, túlterheltség	Konfigurációs hiba, rossz frissítés	Hibás pályaszámítás, hibás irányítási parancs

Kockázati kategória	Energiaágazat	Közlekedési ágazat	Digitális infrastruktúra	Világűr
Interdependencia-kockázat	Energia nélkül minden rendszer leáll	Energia- és digitális függés	Energia- és GNSS-függés	Navigációs, időszinkron és kommunikációs függés
Geopolitikai kockázat	Energiaszállítási útvonalak, szankciók	Légtérzárak, közúti/vasúti határzár	Nemzetközi internetgerinc kapcsolatok	Űreszközök katonai célponttá válása, GNSS hadászati befolyás
HILP események (ritka, de nagy hatású)	Országos áramszünet, nagyfeszültségű kiesés	ATC teljes leállása, közlekedési rendszer összeomlása	Országos DNS/BGP támadás	Extrém napvihar, tömeges műhold-kiesés

A négy vizsgált ágazat reziliencia profilját bemutató összehasonlító táblázat szemlélteti az ágazatok közötti eltéréseket a reziliencia erősségeket, kritikus függőségeket, és fejlesztési prioritásokat.

6. táblázat: Összehasonlító táblázat a négy ágazat reziliencia profiljáról

Készítette: A Szerző, 2025

Ágazat	Legfőbb sérülékenységek	Reziliencia erősségek / enyhítő tényezők	Kritikus függőségek	Kockázatok jellemző mintázata	Reziliencia fejlesztési prioritások
Energia	Elöregedett eszközpark, hálózati túlterhelés, kiber-fizikai sérülékenység, importfüggőség	Erős szabályozási háttér (N-1), diverzifikált termelési mix, nagy tárolókapacitás	Digitális irányítás, közlekedés (alkatrész-logisztika), víziközművek	Energia → minden más ágazat: gyors dominóhatás	Hálózati redundancia növelése, SCADA védelem erősítése, ellátási lánc rugalmasságának növelése
Közlekedés	Műszaki meghibásodások, humán hiba, időjárási extrémumok, IT-függőség	Kiterjedt szabványrendszer (RAMS, ICAO), tartalékirányítási rendszerek	Energia, digitális kommunikáció, GNSS	Közlekedés ↔ energia: logisztikai lánc; közlekedés ↔ digitális: irányításfüggés	ITS és forgalomirányító rendszerek kibervédelme, időjárási adaptáció, redundancia növelése

Ágazat	Legfőbb sérülékenységek	Reziliencia erősségek / enyhítő tényezők	Kritikus függőségek	Kockázatok jellemző mintázata	Reziliencia fejlesztési prioritások
Digitális infrastruktúra	Kiberkitettség (DDoS, ransomware), fizikai SPOF pontok, felhőfüggés, kábelvágások	Gyors helyreállítási képesség, multipath routing, virtualizáció	Energia, világűr (GNSS időszinkron), fizikai hozzáférési pontok	Digitális → energia/ közlekedés: irányítási rendszerleállás	Redundáns útvonalak, adatközponti kapacitásvédelem, BGP/DNS védelem, 5G reziliencia
Világűr	Űrszemét, napviharok, RF-zavarás, irányító rendszerek kiberkockázata	Több műholdas konstelláció, ESA/EU SST monitoring, GNSS integritásvédelem	Digitális infrastruktúra, közlekedés, energiaidőszinkron	GNSS hiba → digitális → közlekedés: többlépcsős kaszkádhatás	Jamming/spoofing elleni védelem, űridőjárási monitoring, földi redundanciák (terresztriális alternatívák)

A rezilienciaprofilok összehasonlítása rámutat, hogy bár mindegyik ágazat sajátos technológiai és működési logikával rendelkezik, a sérülékenységek nagy részét az egymásra épülő függőségek alakítják. Az energiaágazat támogató szerepe miatt vezérlő eleme a rendszernek, a digitális infrastruktúra biztosítja az irányítást és adatáramlást, a közlekedési ágazat fizikai és információs függőségei miatt különösen érzékeny a zavarokra, míg a világűr infrastruktúrái a navigáció és időszinkron révén olyan háttérszolgáltatásokat nyújt, amelyek kiesése többszintű dominóhatást generálhat. Ez a komplex függőségi háló indokolja, hogy a reziliencia fejlesztése komplex ágazaton átívelő rendszerszintű megközelítést igényel, amely egyaránt figyel a műszaki, kiber, ellátási lánc és interdependencia eredetű sérülékenységekre. [20]. A vizsgált ágazatok az energia, a közlekedési, a digitális és a világűr infrastruktúra elemzése egyértelműen rámutat arra, hogy mindegyik rendszer erősen technológiafüggő, ugyanakkor eltérő módon sérülékeny a fizikai, kiber és környezeti hatásokkal szemben. Az energiaágazat esetében a legkritikusabb tényezők a hálózati topológia, az elöregedő eszközpark és a kibertámadások fizikai következményeket is kiváltó hatása, míg a közlekedési alágazatok (vasút, légi, közút, vízi) elsősorban a komplex irányítási rendszerük, a humán tényezők és az időjárási extremitások miatt sérülékenyek. A digitális infrastruktúra ezzel szemben a legerősebb kiberkitettséggel rendelkezik, és működése intenzíven függ a folyamatos energiaellátástól, egyetlen optikai útvonal vagy adatközpont meghibásodása széles körű dominóhatást indíthat el.

A világűr ágazat sérülékenységei pedig részben környezeti eredetűek (űrszemét, napviharok), részben technológiai és kiber jellegűek, amelyek a műholdas kommunikáció, az időszinkron és a földmegfigyelési adatok révén közvetlen hatást gyakorolnak a többi kritikus infrastruktúrára. [78]

A négy ágazat összehasonlítása azt mutatja, hogy a modern kritikus rendszerek közös jellemzője a magas fokú interdependencia, amely miatt egy-egy alrendszer meghibásodása nemcsak lokális üzemzavarokat, hanem gyorsan terjedő, rendszerszintű hatásokat is kiválthat. Az energiaágazat szerepe miatt kulcsszereplő minden más infrastruktúra működésében, a digitális rendszerek központi szerepe a kommunikációban és irányításban szintén nélkülözhetetlenné teszi őket. A közlekedés és a világűr ágazat pedig olyan kapcsolatokkal rendelkezik (logisztikai ellátás, navigációs rendszerek), amelyek a rendszerek közötti függőségi hálót még komplexebbé teszik. A sérülékenységek és függőségek közös értékelése így elengedhetetlen a kritikus szervezetek rezilienciájának növeléséhez, és megerősíti a kockázatalapú, ágazatközi szemlélet szükségességét a magyar szabályozási és szervezeti gyakorlatban.

1.3.2 A kritikus szervezetek és infrastruktúrák védelmének fejlesztési lehetőségei a szakirodalom tükrében

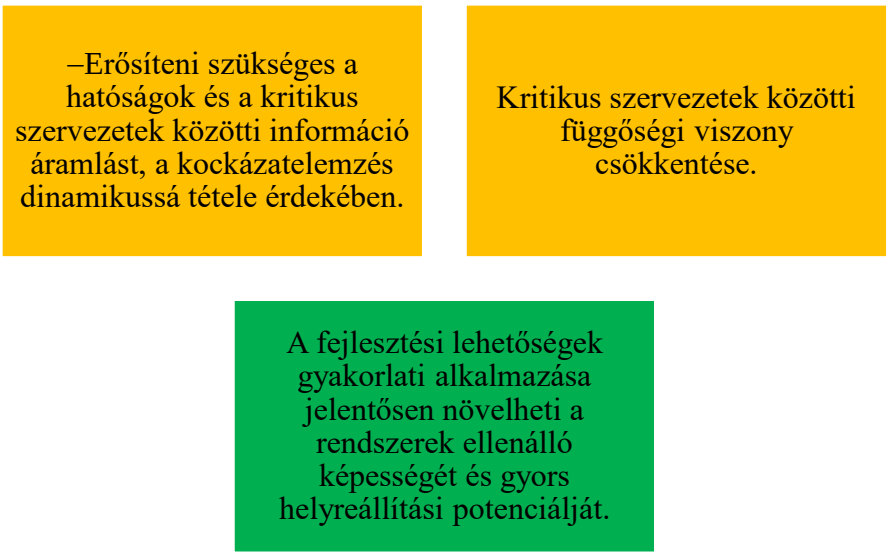
A különböző források a fenyegetettségek fényében számos fejlesztési irányt és javaslatot kínálnak, amelyek strukturálisan és technológiailag is előrelépést jelenthetnek. Kárász Balázs 2025-ben megjelent tudományos cikkben a humán tényezők integrációját javasolja, tudatos képzési programok, szimulációs gyakorlatok és incidenskezelési protokollok lefektetésével. Ezáltal csökkenthető a belső sebezhetőség és erősíthető a belső biztonsági kultúra. [49] Egy másik 2024-ben megjelent tudományos cikkben generatív AI és LLM- alapú támadásfelderítési és támadásmegelőzési rendszereket fogalmaz meg, automatizált támadás-szimulációk, valós idejű adatformálás, adaptív védelem kialakításával. [55] Tump a fenyegetésfüggetlen reziliencia elvének bevezetését szorgalmazza, redundáns infrastruktúrák, diverzifikált rendszerelemek, modul rendszerű védelem, rugalmas építmények kialakításával. [50]

A kritikus szervezetek védelmében alkalmazott kockázatelemzés folyamatos fejlesztésre szorul, mivel a fenyegetettségek gyorsan változnak, egyre komplexebbek, és sokszor nem lineáris hatásokat eredményeznek. A kritikus szervezetek védelmének megalapozott stratégiai tervezése a hagyományos kockázatelemzési módszerek megújítását igényli.

A globalizált és digitalizált működési környezet új típusú fenyegetéseket eredményez, amelyekre kizárólag dinamikus, komplexitást kezelni képes elemzési keretrendszerekkel lehet reagálni.

Az alábbiakban összefoglalom a legfontosabb, napjainkban releváns fejlesztési lehetőségeket a kockázatelemzés területén, kifejezetten a kritikus infrastruktúrák és szervezetek szempontjából:

- Az első kiemelt fejlesztési irány a kockázatelemzéssel függ össze. A dinamikus kockázatelemzési modellek a hagyományosan alkalmazott statikus kockázati mátrixok és hatás valószínűség alapú értékelések nem alkalmasak teljes mértékben a gyorsan változó, sokszor ismeretlen fenyegetések kezelésére. A kritikus szervezeteknek képesnek kell lenniük érzékelni a változásokat, megragadni a lehetőségeket és folyamatosan adaptálódni. [56] Ennek érdekében erősíteni szükséges a hatóságok és a kritikus szervezetek közötti információ áramlást, a kockázatelemzés dinamikussá tétele érdekében.
- A fejezetben bemutatott fenyegetettségi környezet komplexitása szükségessé teszi olyan dinamikus, interdependenciákat is kezelő elemzési eszközök fejlesztését, amelyek képesek a többágazatos kockázatok és dominóhatások vizsgálatára. Ennek érdekében a hagyományos, statikus kockázatértékelési megközelítések kiegészítése válik szükségessé.



7. ábra: Legfontosabb fejlesztési lehetőségek

Készítette: a Szerző, 2025.

A kritikus szervezetek és infrastruktúrák védelmének fejlesztésével foglalkozó szakirodalom az elmúlt két évtizedben fokozatosan elmozdult a hagyományos, eseménycentrikus biztonsági megközelítésektől a rendszerszintű, kockázat- és rezilienciaalapú megközelítések irányába. A korai munkák döntően egy-egy ágazat például az energiaellátás vagy a távközlés műszaki biztonságára összpontosítottak, míg az újabb tanulmányok már az interdependens infrastruktúra hálózatok sérülékenységével és a komplex kockázatterjedési mechanizmusokkal foglalkoznak. [81]A fejlesztési lehetőségeket bemutató irodalom ezért ma már nem pusztán védelmi intézkedésekről beszél, hanem a kockázatelemzési módszertanok fejlesztését, a műszaki redundancia és diverzifikáció erősítését, valamint a reziliencia mérését és menedzselését tekinti központi kérdésnek. [8]

A műszaki kockázatelemzés klasszikus eszköztárából az FMEA, a hibafa-elemzés az eseményfa-elemzés és a megbízhatósági alapú módszerek továbbra is meghatározóak a kritikus infrastruktúrák védelmi fejlesztésében. Ezek a technikák különösen az energia- és közlekedési ágazatban terjedtek el, ahol az egyes berendezések meghibásodása kvantitatív módon becsülhető, és a fejlesztési döntések például redundancia beépítése, karbantartási stratégiák módosítása ezen elemzések eredményeire támaszkodnak. [82] A vasúti és légi közlekedési rendszerekben a vizsgált szakirodalom részletesen bemutatja, hogyan vezetnek a megbízhatósági modellek a rendszerszintű kockázatcsökkentési intézkedések azonosításához, például redundáns jelző- és biztosítóberendezések, tartalék irányítóközpontok és hibadiagnosztikai rendszerek formájában. [83]

A klasszikus, lineáris kockázatelemzési módszerek ugyanakkor korlátozottan alkalmasak a nagy kiterjedésű, hálózatként viselkedő infrastruktúrák vizsgálatára. Erre a problémára válaszul jelent meg a hálózatelméleti és gráf-alapú megközelítések irodalma, amely a kritikus infrastruktúrákat csomópontok rendszerének tekinti, és olyan mutatókkal dolgozik, mint a csomóponti fokszám, központiság, sebezhetőségi index vagy hálózati hatékonyság. [29] Ezek a modellek lehetővé teszik, hogy a fejlesztési lehetőségeket például új csomópontok létrehozása, alternatív betáplálási útvonalak kialakítása, kulcselemek fokozott védelme hálózati sérülékenységcsökkentés szempontjából is értékeljük. Az ilyen jellegű elemzések különösen az energia- és digitális hálózatok esetében relevánsak, ahol a kritikus meghibásodási pont kiküszöbölése, illetve az alternatív útvonalak biztosítása kulcsfontosságú fejlesztési irány. [84]

A kockázatelemzési módszertanok fejlődésének másik fontos iránya a valószínűségi és sztochasztikus modellek alkalmazása, amelyek Bayes-hálók, Markov-modellek vagy Monte Carlo szimulációk formájában jelennek meg a szakirodalomban.

Ezek a módszerek lehetővé teszik a bizonytalanságok kezelése mellett olyan forgatókönyvek vizsgálatát is, amelyek több, egymást követő eseményből állnak, így különösen alkalmasak a dominóhatások modellezésére. A fejlesztési lehetőségek szempontjából az ilyen modellek előnye, hogy nemcsak a jelenlegi kockázati szintet tudják jellemezni, hanem különböző védelmi vagy redundancia-bővítési intézkedések várható hatását is képesek számszerűsíteni, támogatva ezzel a költség–haszon alapú döntéshozatalt. [6]

A kritikus infrastruktúrák védelmének fejlesztési irányaival foglalkozó irodalom egyre hangsúlyosabban emeli ki, hogy a hagyományos kockázatcsökkentés önmagában nem elegendő, mivel a komplex, interdependens rendszerek esetében mindig marad egy nem elhanyagolható bizonytalansági tartomány. Erre válaszul alakult ki a reziliencia-centrikus megközelítés, amely nem csupán a bekövetkezés valószínűségének csökkentésére törekszik, hanem a rendszer ellenálló képességét, alkalmazkodó képességét és helyreállítási képességét is vizsgálja [85] A fejlesztési lehetőségek itt már nem kizárólag a védelem megerősítéséről szólnak, hanem olyan architekturális és üzemviteli megoldásokról, mint például a decentralizáció, a moduláris rendszerkialakítás, a rugalmas terhelésátcsoportosítás vagy a több szinten értelmezett tartalékok. [86]

A reziliencia mérésének és értékelésének irodalma a műszaki és kockázatelemzési dimenziót kifejezetten mérőszámokkal és reziliencia-indexekkel igyekszik megragadni. Linkov és szerzőtársai többdimenziós reziliencia-értékelési keretrendszere például az infrastruktúrák robusztusságát, redundanciáját, erőforrás-átcsoportosítási képességét és adaptivitását együttesen vizsgálja, míg más szerzők az időbeli viselkedést – a teljesítmény-idő görbe alakulását – veszik alapul, és a zavar előtti, alatti és utáni állapotokat hasonlítják össze. Ezek a megközelítések lehetővé teszik, hogy a fejlesztési lehetőségeket ne csak intézkedés-listaként, hanem reziliencia-szint növekedésével járó, mérhető beavatkozásokként értékeljük. [87]

Az interdependenciákra épülő fejlesztési javaslatok azt hangsúlyozzák, hogy a kritikus infrastruktúrák védelme akkor tekinthető hatékonynak, ha figyelembe veszi a többi ágazattal fennálló kölcsönös függőségeket. Rinaldi 2001-es modellje, valamint az OECD rendszerszintű rezilienciajelentései alapján készült tanulmányok azt mutatják, hogy a villamosenergia-rendszer, a digitális infrastruktúra és a távközlés olyan kulcsfontosságú infrastruktúra-csomópontok, amelyek meghibásodása több ágazatban is egyidejű zavarokat válthat ki. A fejlesztési lehetőségek itt nemcsak a saját ágazaton belüli redundancia növelését jelentik, hanem az ágazatközi koordináció, az információmegosztási mechanizmusok, a közös kockázatelemzési gyakorlatok és ágazatközi gyakorlatok erősítését is. [88]

Az energiaágazatot vizsgáló műszaki–kockázatelemzési irodalom kiemeli például az N-1 kritérium és a hálózati stabilitásmodell alapvető szerepét a fejlesztési döntésekben, de egyre gyakrabban jelennek meg olyan megoldásjavaslatok is, mint a decentralizált termelési struktúrák, a mikrorácsok, a megújuló energiaforrások integrációja és a fogyasztói oldal rugalmasságán alapuló megoldások. Ezek a fejlesztések egyfelől növelik a rendszer robusztusságát az egyedi meghibásodásokkal szemben, másfelől csökkentik az importkitettséget és a rendszerszintű nagy zavarok valószínűségét. [89]

A közlekedési ágazatban a fejlesztési lehetőségeket bemutató irodalom szintén a műszaki–kockázati megközelítések és a reziliencia összekapcsolására törekszik. A vasúti RAMS-előírások, a légi közlekedés gyakorlata és a közúti ITS-rendszerek kockázatelemzése mind olyan keretek, amelyek a kritikus csomópontok, irányítási rendszerek, kommunikációs hálózatok és humán tényezők célzott fejlesztését támogatják. Az újabb irodalom a klímaváltozás közlekedési infrastruktúrára gyakorolt hatásait – például szélsőséges időjárási eseményeket, hőhullámokat, árvizeket – is integrálja a kockázatelemzésbe, és ennek megfelelően javasol adaptív infrastruktúrafejlesztést, rugalmas üzemviteli protokollokat és valós idejű monitoring rendszereket. [83]

A digitális infrastruktúrák védelmének fejlesztésével foglalkozó szakirodalom középpontjában a kibertér-specifikus kockázatelemzés és a kritikus információs infrastruktúrák védelme áll. A NIST Cybersecurity Framework, az ENISA ajánlásai és a különböző nemzeti kiberstratégiák mind azt hangsúlyozzák, hogy a fejlesztés kulcsa a kockázatalapú, réteges, a folyamatos monitoring, az incidenskezelés és a helyreállítási képesség. A műszaki kockázatelemzési irodalom egyre inkább foglalkozik a felhőalapú infrastruktúrák, az adatközpontok és a nagy forgalmú gerinchálózatok sérülékenységeivel, és olyan fejlesztési irányokat javasol, mint a topológiai redundancia, BGP- és DNS-védelem, valamint a szolgáltatói diverzifikáció. [90]

A világűr ágazatot érintő műszaki–kockázatelemzési irodalom – amely a GNSS, a műholdas kommunikáció és a Föld-megfigyelés kritikus szerepére hívja fel a figyelmet – az űrszemét és a műholdrendszerek kiberbiztonsága köré szerveződik. Az ESA, EASA és ENISA jelentései egyaránt hangsúlyozzák, hogy a műholdas rendszerek védelmi fejlesztése nemcsak orbitális manőverezésre és űrkövetésre, hanem kiberbiztonsági erősítésre, jelzavarás elleni védelemre, valamint a földi redundáns rendszerek kialakítására is kiterjed.

A fejlesztési lehetőségek között egyre fontosabb helyet foglalnak el az úgynevezett „terresztriális back-up” megoldások, amelyek alternatív navigációs, kommunikációs vagy időszinkronizációs képességet biztosítanak GNSS-kiesés esetén. [38]

Összességében a nemzetközi műszaki és kockázatelemzési szakirodalom abba az irányba mutat, hogy a kritikus szervezetek és infrastruktúrák védelmének fejlesztése csak integrált, többdimenziós kockázatelemzési keretben értelmezhető. A komponensszintű megbízhatósági elemzések, a hálózati és interdependencia-alapú modellezés, a kiberkockázati keretrendszerek és a reziliencia-centrikus megközelítések olyan, egymást kiegészítő nézőpontokat adnak, amelyek együttes alkalmazása alapozhatja meg a kockázatalapú fejlesztési stratégiákat. A magyar kritikus szervezetek szempontjából ez azt jelenti, hogy a jövőbeni fejlesztési irányoknak nemcsak a hazai szabályozási követelményekhez, hanem ezekhez a nemzetközileg elfogadott, műszaki kockázatelemzési gyakorlatokhoz is igazodniuk kell.

1.4 Összegzés

A jogszabályi környezet vizsgálata révén megállapítható, hogy Magyarországon a kritikus szervezetek védelmének új jogszabályi környezete 2025-re előrehaladott fejlettségi szintet ért el. A kockázatalapú megközelítés, valamint a rezilienciára építő tervezés már megjelent a szabályozásban és több szervezet működési gyakorlatában. Ugyanakkor az implementáció még nem tekinthető teljesnek, mivel a gyakorlati alkalmazás, az együttműködési mechanizmusok hatékonysága és az ágazati szereplők közötti interoperabilitás továbbra is fejlesztendő. Az eredmények azt mutatják, hogy a kritikus szervezetek biztonságának növelése érdekében a hagyományos kockázatelemzési keretrendszer célszerű egy adaptív, rendszerszintű szemlélettel kibővíteni, amely képes kezelni az egymástól függő infrastruktúrák összetett működését.

Különösen fontos felismerés, hogy a fizikai és digitális infrastruktúrák közötti összefonódások miatt egyetlen ágazatban bekövetkező zavar más területeken is láncreakció jellegű összeomlást idézhet elő. Ebből következően a védekezési és helyreállítási kapacitás növelése szempontjából elengedhetetlen olyan elemzési és tervezési módszerek bevezetése, amelyek képesek előre jelezni az ágazatok közötti hatáshullámokat. A kutatási eredmények alapján javasolt egy ágazati szintű kockázatelemzés és kockázati jelentés integrálása a CER Irányelv alapján kialakított új rendszerbe, amely várhatóan csökkentené a láncreakciós jellegű zavarok kockázatát, valamint megerősítené a polgári és katonai reagáló mechanizmusok összehangoltságát. Ennek bevezetése nemcsak az ellenálló képességet növelné, hanem a kritikus rendszerek gyorsabb helyreállítását is elősegítené egy jövőbeli válsághelyzet során.

1.5 Részkövetkeztetések az 1. fejezethez

1. A kritikus szervezetek és infrastruktúrák jogszabályi vizsgálatával összefüggésben az alábbi megállapításokat teszem:
    a. Az újonnan megjelenő törvény és a hozzá tartozó kormányrendeletek egyik legfontosabb újítása a kockázatalapú gondolkodásmód intézményesítése. Kötelező nemzeti kockázatértékelést, ellenállóképességi tervet és kockázatkezelési intézkedéseket ír elő, és ezekhez módszertani támogatást is nyújt. A 2012-es szabályozás sokkal inkább statikus védelmi elemekre és listákra épített, kevésbé ösztönözve a dinamikus kockázatmenedzsmentet.
    b. A szabályozás a kritikus szervezetek fogalmát helyezi előtérbe. Ez a szemléletváltás lehetővé teszi, hogy ne csupán fizikai rendszerelemekre, hanem működési egységekre, szolgáltatásokra és azok irányítására is kiterjedjen a védelem. Az új definíció rugalmasabb és jobban leképezi a valós szervezeti működést, különösen a szolgáltatási láncok és digitális infrastruktúrák tekintetében.
    c. Az új törvény középpontjába az ellenálló képesség fejlesztését állítja, amely nemcsak a megelőzésre, hanem a reagálásra, alkalmazkodásra és helyreállításra is kiterjed. Ez a szemlélet az EU reziliencia alapú megközelítését követi, és messze túlmutat a korábbi törvény által sugallt pusztán fizikai védelem logikáján.
    d. A szakpolitikai javaslatok ennek megfelelően a többágazatos, összehangolt kockázatelemzési gyakorlatok megerősítésére irányulnak. Indokolt az olyan elemzési módszerek szélesebb körű alkalmazása, amelyek a hálózati összefüggéseket és a szolgáltatás-folytonosságot is értékelik (pl. reziliencia indexek, hálózatszimulációk, RAMS és kiber és fizikai kockázati modellek). A nemzetközi jó gyakorlatok alapján javasolt a digitális és világűrinfrastruktúrák időszinkronizációs függéseinek vizsgálata, a közlekedési alágazatok kritikus csomópontjainak részletes feltérképezése, valamint az energiaágazat vezérlőrendszereinek (SCADA/ICS) megerősítése. Az európai uniós szakmai platformok – ENISA, JRC, NIS Cooperation Group – által közzétett trendek és fenyegetésértékelések rendszeres integrálása hozzájárulhat a nemzeti kockázatértékelés módszertani harmonizációjához és a reziliencia fejlesztéséhez.

2. A kritikus szervezetek és infrastruktúrák fenyegetettségének vizsgálatával kapcsolatban az alábbi megállapításokat teszem:
    a. A kritikus szervezetek fenyegetettsége napjainkban jelentősen átalakult, főként a geopolitikai instabilitás, a technológiai fejlődés és a digitális sérülékenységek miatt.
    b. A kritikus infrastruktúrák célponttá váltak a hibrid hadviselésben. A fizikai támadások mellett kibertérben zajló akciók pl. zsarolóvírusok, adatlopások, dezinformációs kampányok is veszélyeztetik a létfontosságú szolgáltatásokat.
    c. A hagyományos, statikus védelmi modellek már nem elegendőek. Hangsúlyossá vált a dinamikus képességek fejlesztése, úgymint a gyors újratervezés, visszaállítási stratégiák, kockázatérzékeny döntéshozatal. A szervezeteknek olyan rugalmas és tanulóképes védelmi rendszert kell kialakítaniuk, amely képes adaptálódni a gyorsan változó fenyegetettségi környezethez.
    d. A digitális, világűr-, közlekedési és energiaágazatok összehasonlító elemzése egyértelművé teszi, hogy ezek a rendszerek egymástól erősen függő, kiber és fizikai hálózatokként működnek, amelyek sérülése vagy kapacitáscsökkenése egyszerre több ágazatot érintő zavarokat idézhet elő. A nemzetközi szakirodalom arra mutat rá, hogy a modern kockázati környezetben a kritikus infrastruktúrákat már nem lehet elszigetelten vizsgálni, a digitális hálózatok meghibásodása befolyásolja az energiairányítást és a közlekedési folyamatokat, a rendszerek sérülékenysége kihat a navigációra és hálózati időszinkronra, míg az energiaellátás kiesése a többi ágazat működésének alapfeltételeit veszélyezteti. Mindezek alapján szükséges a hálózatalapú megközelítések, a dominóhatások és az interdependenciák módszeres feltérképezése.
3. A kritikus szervezetek védelmének fejlesztésével kapcsolatban az alábbi megállapításokra és javaslatokra jutottam:
    a. A kutatás eredményei arra utalnak, hogy a jelenlegi, statikus és időszakos kockázatelemzések nem képesek megfelelően lekövetni a gyorsan változó fenyegetettségi környezetet, ezért a gyakorlatban célszerű lenne dinamikus elemzési modell kialakítása, amely valós idejű információkra, visszacsatolásokra és prediktív elemzésekre épül.

Az eredmények egyértelműen mutatják, hogy fontos megvizsgálni a továbbiakban a kockázati jelentés bevezetésének szükségességét, az ahhoz kapcsolódó eljárásrendek bevezetésének szükségszerűségét.

b. A feltárt geopolitikai veszélyek és kihívások rávilágítottak arra, hogy a különböző ágazatok közötti kölcsönös technológiai, logisztikai és informatikai függőségek súlyosbítják a rendszerszintű sebezhetőségeket.
c. Az elemzés során feltárt eredmények rámutattak arra, hogy szükséges lenne megvizsgálni egy ágazatok közötti kritikus kapcsolódási pontokat és az ezekből eredő hatáshullámokat is vizsgáló kockázatelemzés szükségességét, ami mérhetően növelné az egész védelmi rendszer rezilienciáját. Így javasolt annak további vizsgálata.

2. AZ ÁGAZATI KOCKÁZATELEMZÉS SZÜKSÉGESSÉGÉNEK ELMÉLETI ÉS GYAKORLATI MEGALAPOZÁSA

Az ágazati kockázatelemzés kulcsfontosságú a kritikus szervezetek és infrastruktúrák védelmében, mivel minden ágazat egyedi kihívásokkal és fenyegetésekkel szembesül. Az ágazati kockázatelemzés segítségével azonosíthatók azok a sebezhetőségek és potenciális kockázatok, amelyek specifikusan az adott ágazatra jellemzőek.

Ez az elemzés lehetővé teszi a döntéshozók számára, hogy célzott védelmi intézkedéseket hozzanak, amelyek figyelembe veszik az adott ágazat sajátosságait, a kölcsönös függőségeket és az interakciókat más ágazatokkal. Emellett az ágazati kockázatelemzés segít előre látni azokat a láncreakciókat, amelyek egy adott ágazat zavarai esetén más ágazatban is problémákat okozhatnak. Így biztosítható, hogy a védelmi intézkedések holisztikusak legyenek, és a különböző ágazatok együttműködésével hatékonyabb védelmet nyújtsanak a kritikus infrastruktúrák számára.

Az ágazati kockázatelemzés alapvető fontosságú ahhoz, hogy a kritikus szervezet és infrastruktúra védelme célzott, hatékony és a teljes rendszert átfogó legyen, minimalizálva a sebezhetőségeket és a potenciális zavarok következményeit. Ahhoz, hogy egy ágazati kockázatelemzést beültessük a hazai védelmi rendszerbe, szükséges elemezni és értékelni a külföldi tapasztalatokat. Ennek alapján összegyűjtöttem és értékeltem több európai uniós és EU-n kívüli országban alkalmazott kritikus szervezetek védelmével kapcsolatos eljárásokat, metódust, hogy ezt követően azokat be tudjam építeni a hazai javaslatba.

2.1 A kritikus szervezetek és infrastruktúrák kockázatelemzésének nemzetközi modelljeinek és gyakorlatainak összehasonlító elemzése

A kritikus szervezetek és infrastruktúrák védelme napjaink biztonságpolitikai környezetében kiemelt jelentőséggel bír, hiszen ezek a rendszerek nemcsak az állam működésének alapfeltételeit biztosítják, hanem a társadalom mindennapi életének folyamatos hátterét is adják. A globálisan változó fenyegetettségi környezet, a digitalizációból fakadó sérülékenységek, az ellátási láncok összetettsége, a természeti katasztrófák gyakoriságának növekedése és a geopolitikai bizonytalanságok szükségessé teszik a nemzetközi tapasztalatok és bevált gyakorlatok vizsgálatát.

A nemzetközi példák elemzése különösen fontos a magyar szabályozási és kockázatkezelési rendszer fejlesztése szempontjából, hiszen a CER Irányelv új követelményeket támaszt a tagállamokkal szemben, amelyeket célszerű olyan országok gyakorlatával összevetni, amelyek hasonló kihívásokkal szembesülnek, illetve előrehaladott reziliencia rendszerrel rendelkeznek.

A vizsgálat első csoportját Kanada, az Egyesült Államok és az Egyesült Királyság alkotja. Ezek az országok a kritikus infrastruktúrák védelmében évtizedek óta élen járnak, fejlett kockázatelemzési módszertannal, kiforrott ágazati együttműködési mechanizmusokkal és a nemzeti szintű reziliencia politikák gazdag tapasztalatanyagával. A NATO és a transzatlanti együttműködésben betöltött szerepük, valamint a sokszereplős kormányzási modelljük különösen értékes összehasonlítási alapot biztosít a reziliencia szervezés és információmegosztás terén.

A második vizsgált országcsoport Lengyelország, Csehország, Ausztria, Németország és Szlovénia, amelyek Magyarországhoz térségben és igazgatási rendszerükben is közelebb állnak. Ezek az államok az uniós CER keretrendszerrel azonos jogi és stratégiai kötelezettségek mentén szervezik a kritikus szervezetek védelmét, emellett számos olyan történelmi, gazdasági és biztonsági sajátossággal is rendelkeznek, amelyek a magyar modellhez hasonlóvá teszik őket. Így összehasonlításuk lehetőséget ad a regionális jó gyakorlatok feltárására és arra, hogy láthatóvá váljanak az eltérések az implementáció és a végrehajtás szintjén.

Az összehasonlítás szempontjai ágazatspecifikus megközelítések, a minden veszélyre kiterjedő kockázatértékelési módszertan, az együttműködés és információmegosztás rendszere, a nemzeti ágazatközi fórumok működése, valamint az útmutatás és támogatás formái olyan területeket fednek le, amelyek meghatározzák a kritikus szervezetek rezilienciájának gyakorlati működését. Ezek a dimenziók jól összehasonlíthatók a különböző országok között, és közvetlenül kapcsolódnak a CER Irányelv által előírt kötelezettségekhez. A kiválasztott szempontok lehetővé teszik, hogy ne csupán a jogi kereteket, hanem a gyakorlati megvalósítás minőségét, a kormányzási mechanizmusok fejlettségét, valamint az állam és a szolgáltatók közötti együttműködés hatékonyságát is értékelni lehessen. [30]

Az alábbi táblázatban láthatóak a kiválasztott országokkal kapcsolatos, általam összesített adatok, azok értékelése és a fontosabb információk: [57]

7. táblázat: *A kritikus szervezetek és infrastruktúrák Kanadában, Készítette: a Szerző.*

Kanada	Kanadában a kritikus szervezetek és infrastruktúrák ágazati kockázatértékelésének gyakorlata egy szélesebb körű nemzeti stratégia része, amelynek célja az alapvető rendszerek és szolgáltatások ellenálló képességének növelése. A kanadai kormány a kanadai közbiztonságon keresztül létrehozta a kritikus szervezetek és infrastruktúrák védelmének keretrendszerét, amely a szövetségi, tartományi, területi és önkormányzati kormányok, valamint a magánszféra érdekelt felei közötti együttműködést hangsúlyozza. [7]
Fontosabb szempontok:	Ágazatspecifikus megközelítések: Kanada kritikus szervezetek és infrastruktúrák tíz kulcsfontosságú ágazatra oszlik, köztük az energia és közművek, az információs és kommunikációs technológia, a pénzügyek, az egészségügy, az élelmiszeripar, a vízügy, a közlekedés, a biztonság, a kormányzat és a feldolgozóipar. Ezen ágazatok mindegyike felelős a saját kockázatértékelésének elvégzéséért, a működésükre vonatkozó konkrét fenyegetésekre és sebezhetőségekre összpontosítva. Ez az ágazatspecifikus megközelítés lehetővé teszi az egyes infrastruktúra típusok egyedi kockázatait kezelő, személyre szabott stratégiák kidolgozását.
	Minden veszélyre kiterjedő kockázatértékelési módszertan: Ez magában foglalja mind a természeti, mind az ember által okozott fenyegetéseket, például a kiberfenyegetések, a terrorizmus és a természeti katasztrófák azonosítását. A cél a kritikus szolgáltatásokat megzavaró kockázatok megértése és mérséklése. Ezt a módszert a különböző ágazatokban alkalmazzák a potenciális kockázatok átfogó értékelésének biztosítása érdekében.
	Együttműködés és információmegosztás: A kanadai közbiztonság ösztönzi a folyamatos együttműködést és információcserét a kritikus infrastruktúrákban érdekelt felek között. Ez magában foglalja a bevált gyakorlatok, a veszélyekkel kapcsolatos információk és a kockázatértékelési módszerek megosztását. [58]
	Nemzeti ágazatközi fórum: Az ágazati kockázatértékelések javítása érdekében Kanada létrehozta a Nemzeti Ágazatközi Fórumot, amely a kritikus szervezetek és infrastruktúrák egyes ágazatainak képviselőit tömöríti, hogy megvitassák a közös kockázatokat és függőségeket. Ez a fórum támogatja az integrált kockázatkezelési stratégiák kidolgozását, amelyek figyelembe veszik az ágazatok közötti kölcsönös függőségeket és a dominóhatásokat.
	Útmutatás és támogatás: A kanadai kormány iránymutatást és eszközöket biztosít az ágazatok számára a kockázatértékelések elvégzéséhez. Ezek közé tartozik a Critical Infrastructure Resilience Tool (CIRT), amely segít a szervezeteknek a kockázatok azonosításában és értékelésében, valamint a Regional Resilience Assessment Program (RRAP), amely helyszíni értékeléseket végez a kritikus infrastruktúrák ellenálló képességének értékelése céljából.

Konklúzió	Az ágazati kockázatértékelések kulcsfontosságúak Kanada kritikus infrastruktúrák védelmére vonatkozó megközelítésében, mivel lehetővé teszik az egyes ágazatokon belüli sebezhetőségek és fenyegetések célzott elemzését. Az ágazatspecifikus kockázatok és kölcsönös függőségek megértésével Kanada hatékonyabb védelmi és ellenálló képességi stratégiákat tud végrehajtani, ezáltal biztosítva a kanadaiak számára az alapvető szolgáltatások folyamatos biztosítását. [59]

8. táblázat: *A kritikus szervezetek és infrastruktúrák védelme az Amerikai Egyesült Államokban Készítette: a Szerző,2025.*

Amerikai Egyesült Államok	Az Egyesült Államokban a kritikus szervezetek és infrastruktúrák ágazati kockázatértékelései alapvető részét képezik a kritikus infrastruktúrák védelmére vonatkozó országos megközelítésnek. Ezt a megközelítést a Belbiztonsági Minisztérium (DHS) koordinálja a Kiberbiztonsági és Infrastruktúrabiztonsági Ügynökségen (CISA) keresztül, amely szövetségi, állami, helyi, és területi kormányzatokkal, valamint a magánszféra érdekelt feleivel együttműködve dolgozik. [60]
Az ágazati kockázatértékelések legfontosabb gyakorlatai:	Ágazatspecifikus ügynökségek és ágazati kockázatkezelési ügynökségek (SRMA): Az Egyesült Államok kritikus szervezetei és infrastruktúrája 16 ágazatra oszlik, mint például az energia, a kommunikáció, a víz és a közlekedési rendszerek. Minden ágazathoz tartozik egy-egy ágazati kockázatkezelési ügynökség (SRMA), amely egy olyan szövetségi ügynökség, amely az adott ágazat kockázatkezelési tevékenységeinek koordinálásáért felelős. Például az Energiaügyi Minisztérium az energiaágazat SRMA-ja, míg a Közlekedési Minisztérium a közlekedési rendszerek ágazatáért felelős. Ezek az ügynökségek vezetik az ágazati kockázatok felmérésére irányuló erőfeszítéseket, és stratégiákat dolgoznak ki a kockázatok mérséklésére. [61]
	Nemzeti Kockázatkezelési Központ (NRMC): A CISA Nemzeti Kockázatkezelési Központja központi szerepet játszik a különböző ágazatokban végzett kockázatértékelések koordinálásában. Stratégiai kockázatkezelési támogatást nyújt, elemzi az ágazatok közötti kölcsönös függőségeket, és olyan kockázatok enyhítésén dolgozik, amelyek egyszerre több ágazatot is érinthetnek. [62]
	Minden veszélyt figyelembe vevő kockázatértékelési megközelítés: Kanadához hasonlóan az Egyesült Államok is a "minden veszélyt" figyelembe vevő kockázatértékelési megközelítést alkalmazza. Ez a módszertan a potenciális veszélyek széles körét veszi figyelembe, beleértve a természeti katasztrófákat, a terrorizmust, a kiberfenyegetéseket és a világjárványokat. Ágazatspecifikus kockázatértékeléseket végeznek annak megértése érdekében, hogy ezek a veszélyek hogyan hathatnak a kritikus szervezetekre és infrastruktúrára, és hogy megfelelő kockázatcsökkentési stratégiákat dolgozzanak ki.
	Nemzeti infrastruktúra-védelmi terv (NIPP): A 2013-as NIPP felvázolja, hogy a kritikus szervezetek és infrastruktúrák közösségének kormányzati és magánszférán belüli résztvevői hogyan működnek együtt a kockázatok

	kezelése, valamint a biztonság és az ellenálló képesség elérése érdekében. Ez magában foglalja az ágazatspecifikus tervek (SSP-k) alkalmazását, amelyeket az egyes ágazatok a NIPP keretrendszerével összhangban dolgoznak ki. Az SSP-k irányítják az ágazat erőfeszítéseit a kockázatok azonosítása, a prioritások meghatározása és a védelmi intézkedések végrehajtása terén.
	Ágazatspecifikus tervek (SSP-k): Minden egyes kritikus szervezet és infrastruktúra ágazat saját ágazatspecifikus tervet dolgoz ki a NIPP keretrendszer részeként. Ezek a tervek az egyes ágazatok egyedi jellemzőihez és kockázataihoz igazodnak, és részletezik, hogyan kell elvégezni a kockázatértékeléseket, milyen veszélyeket kell figyelembe venni, és hogyan kell koordinálni a többi ágazattal és érdekelt féllel.
	Információmegosztó és elemző központok (ISAC): Ez egy olyan nonprofit szervezet, amely összegyűjti, elemzi és megosztja a fenyegetésekkel kapcsolatos információkat a tagjai között. Ezek a központok kritikus szerepet játszanak a kockázatértékelések elvégzésében és annak biztosításában, hogy az ágazatspecifikus kockázatokról minden érintett érdekelt fél tudomást szerezzen.
	Kockázati és sebezhetőségi értékelések: A CISA kockázat- és sebezhetőségi értékeléseket végez a kritikus infrastruktúrák sebezhetőségének azonosítása és a kockázatok csökkentésére irányuló konkrét intézkedések ajánlása céljából. Ezek az értékelések az egyes ágazatok sajátos igényeihez igazodnak, és a biztonság és az ellenálló képesség fokozása érdekében használható információkat. [63]
Konklúzió	Az Amerikai Egyesült Államokban az ágazati kockázatértékelések kulcsfontosságúak, mivel lehetővé teszik a sebezhetőségek és fenyegetések célzott, ágazatspecifikus megértését. Az ilyen értékelések elvégzésével az Egyesült Államok rangsorolhatja az erőforrásokat, fokozhatja az érdekelt felek közötti koordinációt, és hatékonyabb védelmi intézkedéseket dolgozhat ki a kritikus infrastruktúráknak a veszélyek széles körével szembeni biztosítására. Ezek a gyakorlatok biztosítják, hogy az Egyesült Államok kritikus infrastruktúrája rugalmas maradjon, és képes legyen ellenállni mind a jelenlegi, mind az újonnan megjelenő fenyegetéseknek, ezáltal védve a gazdaságot, a nemzetbiztonságot és a közbiztonságot.

9. táblázat: *Kritikus infrastruktúrák védelme az Egyesült Királyságban*
Készítette: a Szerző, 2025.

Egyesült Királyság	Az Egyesült Királyságban a kritikus infrastruktúrák ágazati kockázatértékelései szerves részét képezik a nemzeti biztonság és ellenálló képesség biztosítását célzó országos megközelítésnek. Az Egyesült Királyságban a gyakorlatot több minisztérium és ügynökség koordinálja, a felügyeletet pedig a Kabinetiroda és a Nemzeti Infrastruktúra Védelmi Központ (Centre for the Protection of National Infrastructure, CPNI) látja el.

Az ágazati kockázatértékelések legfontosabb gyakorlatai:	Nemzeti kritikus infrastruktúra kijelölése: Az Egyesült Királyság 13 kulcsfontosságú ágazatban, többek között az energia, a víz, az egészségügy, a közlekedés és a kommunikáció területén határozza meg a kritikus nemzeti infrastruktúrákat. Ezeket az ágazatokat az állam működéséhez nélkülözhetetlennek tekintik, és védelmük a nemzetbiztonsági erőfeszítések során prioritást élvez. Minden egyes ágazat felelős a kockázatértékelések elvégzéséért, hogy azonosítsák a működésükre jellemző sebezhetőségeket és fenyegetéseket. [64]
	Ágazati ellenálló képességi tervek (SRP-k): Az Egyesült Királyságban minden egyes kritikus infrastrukturális ágazatnak ki kell dolgoznia egy ágazati ellenálló képességi tervet. Ezek a tervek, amelyeket az egyes ágazatok vezető minisztériuma felügyel, felmérik az ágazatot fenyegető kockázatokat, és stratégiákat vázolnak fel e kockázatok mérséklésére. Az SRP-ket évente felülvizsgálják és frissítik annak biztosítása érdekében, hogy tükrözzék az aktuális fenyegetettségi helyzetet és az ágazat működésében bekövetkezett változásokat.
	Minden veszélyt figyelembe vevő megközelítés: Az Egyesült Királyságban más országokhoz, például az Egyesült Államokhoz és Kanadához hasonlóan a kockázatértékelés "minden veszélyt figyelembe vevő" megközelítését alkalmazzák. Ez azt jelenti, hogy az ágazati kockázatértékelések a potenciális veszélyek széles körét veszik figyelembe, beleértve a természeti katasztrófákat, a terrorizmust, a kibertámadásokat és a világjárványokat. Ez az átfogó megközelítés biztosítja, hogy a kritikus infrastruktúrát érintő valamennyi lehetséges kockázatot értékelik és kezelik.
	Nemzeti Infrastruktúra Védelmi Központ (CPNI): A CPNI központi szerepet játszik abban, hogy iránymutatást és támogatást nyújtson a CNI-ágazatoknak a biztonsági intézkedésekkel és a kockázatkezeléssel kapcsolatban. A CPNI szorosan együttműködik az ágazati partnerekkel a kockázatértékelések elvégzése és az egyes ágazatok sajátos igényeihez igazított biztonsági intézkedések kidolgozása érdekében. A CPNI az általános nemzeti ellenálló képesség javítása érdekében megkönnyíti az ágazatok közötti információcserét is.
	Közös kockázatértékelés és tervezés: Az Egyesült Királyság hangsúlyozza a különböző ágazatok közös kockázatértékelését és tervezését a kölcsönös függőségek és a dominóhatások kezelése érdekében. Ez az együttműködésen alapuló megközelítés biztosítja, hogy az egyik ágazat zavarai ne legyenek aránytalan hatással a többi ágazatra. A kabinetirodán belül a polgári vészhelyzetekkel foglalkozó titkárság koordinálja ezeket az erőfeszítéseket, biztosítva a kockázatok nemzeti szintű kezelését.
	Nemzeti Kockázati Nyilvántartás (NRR): Az Egyesült Királyság kormánya nemzeti kockázati nyilvántartást vezet, amely felvázolja az országot fenyegető főbb kockázatokat, beleértve a kritikus infrastruktúrákkal kapcsolatos kockázatokat is. Ez a nyilvántartás az ágazati kockázatértékelésekhez nyújt tájékoztatást, áttekintést nyújtva a legjelentősebb fenyegetésekről és azok lehetséges hatásairól. Az NRR-t

	rendszeresen frissítik a felmerülő kockázatok tükrözése érdekében, és mind az állami, mind a magánszférabeli szervezetek használják a kockázatkezelési stratégiáik irányításához. [65]
	Kiberbiztonsági fókusz: Az Egyesült Királyság ágazati kockázatértékeléseiben jelentős hangsúlyt fektet a kiberbiztonságra, tekintettel a digitális infrastruktúrától való növekvő függőségre. A Nemzeti Kiberbiztonsági Központ (NCSC) a CPNI-vel együtt dolgozik a kritikus infrastruktúrát érintő kiberkockázatok felmérésén és a szilárd védelmi intézkedések kidolgozásán. A kiberbiztonsági kockázatértékelések szerves részét képezik az Egyesült Királyságban a kritikus infrastruktúrákra vonatkozó átfogó kockázatkezelési folyamatnak.
Konklúzió	Az Egyesült Királyság ágazati kockázatértékelésekre vonatkozó megközelítése létfontosságú a kritikus infrastruktúrák ellenálló képességének biztosítása szempontjából. Részletes és ágazatspecifikus kockázatértékelések elvégzésével az Egyesült Királyság azonosítani tudja a sebezhetőségeket, előre látja a potenciális fenyegetéseket, és hatékony kockázatcsökkentési stratégiákat tud végrehajtani. Ez a gyakorlat segít megvédeni azokat az alapvető szolgáltatásokat, amelyektől a lakosság és a gazdaság függ, miközben az ország általános nemzetbiztonságát is fokozza. [66]

A három nagy országot követően megvizsgáltam öt, európai uniós ország kritikus szervezetekkel kapcsolatos védelmét, köztük olyat is, ami Magyarországhoz merőben hasonlít. Az alábbi táblázatok a lengyel, a cseh, az osztrák, a német, és a szlovén gyakorlatot foglalják össze. A fókuszban az ágazati megközelítések, a kockázatértékelési módszertanok, az együttműködési mechanizmusok és az alkalmazott iránymutatások állnak.

10. táblázat: *Kritikus szervezetek védelme Lengyelországban, Készítette: a Szerző, 2025.*

Lengyelor-szág	Lengyelországban a kritikus szervezetek és infrastruktúrák védelme a Nemzeti Kritikus Infrastruktúra Védelmi Program része. A Belbiztonsági Kormányzati Központ (Rządowe Centrum Bezpieczeństwa – RCB) koordinálja az államigazgatási szervek, a tartományi és helyi hatóságok, valamint a vállalatok közreműködését, és meghatározza a program céljait, prioritásait a kritikus szervezetek ellenálló képességének növelése érdekében.
Az ágazati kockázatérték elések legfontosabb gyakorlatai:	Ágazatspecifikus megközelítés: Kritikusnak minősülnek az energiával, az üzemanyaggal és energiahordozókkal kapcsolatos rendszerek, a kommunikációs rendszerek, az infokommunikációs hálózatok, a pénzügyi rendszerek, az élelmiszer-ellátás, a vízellátás, az egészségügy, a közlekedés, a mentő- és katasztrófavédelmi rendszerek, a közigazgatás folyamatos működését biztosító rendszerek, valamint a vegyi és radioaktív anyagok előállítására, tárolására vagy szállítására szolgáló létesítmények. Ezek az ágazatok saját kockázatértékelést végeznek, figyelembe véve az adott területre jellemző fenyegetéseket.
	Minden veszélyre kiterjedő kockázatértékelés:

	Az RCB kétévente készíti el a nemzeti biztonsági fenyegetések jelentését, amely azonosítja és elemzi az országot fenyegető mintegy ötven kockázatot. A jelentésre épül a Nemzeti Válságkezelési Terv és a miniszterek, központi hivatalok és vajdák válságkezelési tervei. A kockázatértékelés mind a természeti veszélyeket (árvizek, viharok, járványok), mind az emberi eredetű fenyegetéseket (szabotázs, terrorizmus, kibertámadások) figyelembe veszi.
	Együttműködés és információmegosztás: A program előírja az információcsere és a közös tervezés mechanizmusait az állami és az vállalatok között. A kormányzati és ágazati munkacsoportok tapasztalatokat, veszélytérképeket és kockázatértékelési módszereket osztanak meg, az üzemeltetőknek jelenteniük kell a működési zavarokat, és részt kell venniük a közös gyakorlatokban. [67]
	Útmutatás és támogatás: A Nemzeti Kritikus Infrastruktúra Védelmi Program útmutatókat dolgoz ki az ágazatok számára a kockázatértékeléshez és a védelem fejlesztéséhez. A RCB képzéseket szervez, támogatja a kockázatbecslő eszközök bevezetését, és gondoskodik arról, hogy a védelmi intézkedések összehangoltak legyenek az európai uniós irányelvekkel.
Konklúzió	Lengyelország rendszere az állami irányítás és a magánszféra együttműködésén alapul. A széles körű ágazati lista és a rendszeres, minden veszélyre kiterjedő kockázatértékelés elősegíti a kulcsfontosságú szolgáltatások védelmét. A magyar gyakorlat számára tanulságos az RCB koordináló szerepe, illetve az, hogy a kockázatértékelést a válságkezelési terv részévé tették. [68]

11. táblázat: Kritikus szervezetek védelme Csehországban, Készítette: a Szerző, 2025.

Csehország	A 2025. augusztus 19-én hatályba lépett 266/2025. számú törvény – a kritikus szervezetek rezilienciájáról – a korábbi válságkezelési törvény helyébe lépett és az uniós CER irányelv átültetését szolgálja. A törvény a fizikai létesítmények helyett az alapvető szolgáltatások koncepciójára épít, és jelentősen bővíti a szabályozott ágazatokat.
Az ágazati kockázatért-ékelések legfontosabb gyakorlatai:	Ágazatok és alapvető szolgáltatások: A törvény meghatározza az energia (villamos energia, távhő, olaj, gáz, hidrogén), a közlekedés (légi, vasúti, vízi, közúti, közösségi), a banki szolgáltatások, a pénzügyi piac infrastruktúrái, az egészségügy, az ivóvíz és szennyvíz, a digitális infrastruktúra (hírközlő hálózatok, hitelesítési és elektronikus azonosítási szolgáltatások), a közszolgáltatások, az űrágazat, az élelmiszer-termelés, a feldolgozás és a forgalmazás, valamint a biztonság (tűz- és polgári védelem, közrend, állami anyagtartalékok) területét, mint alapvető szolgáltatásokat.
	Kockázatértékelési kötelezettségek: Az alapvető szolgáltatást nyújtó szervezeteknek három hónapon belül adatot kell szolgáltatniuk az illetékes minisztériumnak és a belügyminisztériumnak az általuk nyújtott szolgáltatásokról. Azok, akiket a Belügyminisztérium kritikus szervezetként jelöl ki, kilenc hónapon belül kötelesek átfogó kockázatértékelést készíteni minden veszélyre kiterjedően,

	majd tíz hónapon belül reziliencia tervet kell kidolgozniuk a technikai, szervezeti és ellenőrzési intézkedésekről.
	Együttműködés és információmegosztás: Az egyes ágazatok felügyeletét az illetékes minisztériumok és a Cseh Nemzeti Bank látják el. Az alapvető szolgáltatást nyújtó szervezetek kötelesek adatot szolgáltatni a nemzeti kockázatértékeléshez, az információáramlás központi szerve a Belügyminisztérium, amely a kritikus szervezetek listáját vezeti és koordinálja az ágazatok közötti kapcsolatokat. [69]
	Útmutatás és szankciók: A törvény az előző szabályozás hiányosságait orvosolja azzal, hogy szankciókat vezet be a kötelezettségek elmulasztásáért. Az EU NIS2 és CER irányelveinek végrehajtása miatt jelentősen bővül a szabályozott vállalatok köre és követelményrendszere.
Konklúzió	A cseh szabályozás az alapvető szolgáltatások szemléletét helyezi előtérbe, és kötelező kockázatértékelési és reziliencia-terv készítését írja elő. A magyar rendszer számára tanulságos lehet az, hogy a jogszabály részletes határidőket, felelősségi köröket és szankciókat rendel a kritikus infrastruktúra védelméhez. [70]

12. táblázat: *Kritikus szervezetek védelme Ausztriában, Készítette: a Szerző 2025.*

Ausztria	Ausztriában a Kritikus Infrastruktúrák Védelmének Osztrák Programja (APCIP) kormányzati felelősségi kör részeként kezeli a kritikus létesítmények védelmét. A program kiindulópontja, hogy az infrastruktúrák működését természeti katasztrófák, műszaki balesetek, emberi mulasztás, bűncselekmények, terrorizmus és kiberfenyegetések egyaránt veszélyeztethetik, ezért átfogó, minden veszélyre kiterjedő szemléletre van szükség.
Az ágazati kockázat-értékelések legfontosabb gyakorlatai:	Ágazatok: Ausztria nemzeti programja tizenhárom kritikus ágazatot különít el: az energia, az információs és a kommunikációs technológia, a víz, az élelmiszer, az egészség, a pénzügy, a közlekedés, a vegyipar, a kutatás, az alkotmányos intézmények, a szociális rendszer, az elosztórendszer és a kutató-mentő szolgálatok.
	Kockázatértékelés: Az APCIP az „all-hazards” megközelítést alkalmazza, amely figyelembe veszi a természeti, technológiai és emberi eredetű veszélyeket. A program célja az ágazatok közötti kölcsönös függőségek feltérképezése és a kockázatok rangsorolása. Bár nincsenek egységesített eszközök, az osztrák kormány ösztönzi a kockázatértékelési módszerek harmonizálását és az európai normákhoz való igazodást.
	Együttműködés és információmegosztás: A program a szövetségi kancellária égisze alatt zajlik, és hangsúlyt fektet a minisztériumok, a tartományok, az önkormányzatok és a magán-üzemeltetők közötti partnerségre. Közös munkacsoportok és fórumok működnek, amelyek a függőségek és a dominóhatások elemzését, illetve a legjobb gyakorlatok megosztását célozzák. [71]
	Útmutató és támogatás:

	Az APCIP keretében különböző útmutatók és ágazatspecifikus kockázatértékelési kézikönyvek készültek. A kormány támogatja a képzéseket és gyakorlatokat, és részt vesz az uniós kockázatértékelési kezdeményezésekben.
Konklúzió	Ausztria széles ágazati listája és a minden veszélyre kiterjedő szemlélete mintául szolgálhat. A program hangsúlyt helyez a kölcsönös függőségek elemzésére, a különböző szintű kormányzatok összehangolására és a magánszereplők bevonására. [72]

13. táblázat: *Kritikus szervezetek védelme Németországban, Készítette: a Szerző, 2025.*

Németország	Németországban a kritikus infrastruktúrák védelme a belügyi tárca felügyelete alatt a nemzetbiztonsági politika központi eleme. A fő felelősség az infrastruktúra-üzemeltetőké, de a szövetségi kormány és a tartományok szabályozási és támogatási keretet biztosítanak. A védendő létesítményeket olyan veszélyek fenyegetik, mint a természeti katasztrófák, a terrorizmus, a szabotázs és az emberi hiba.
Az ágazati kockázat-értékelések legfontosabb gyakorlatai:	Ágazatok: A KRITIS-szabályozás nyolc ágazatot határoz meg: energia, víz, élelmiszer, egészségügy, közlekedés, hulladékgazdálkodás, informatika és távközlés, valamint pénzügyi és biztosítási ágazat. A NIS2 irányelv és a KRITIS kerettörvény tervezett végrehajtása új ágazatokat (például űrkutatás, vegyipar, digitális szolgáltatások, kutatás) is bevon, és a szabályozott szervezetek számát 2000-ről mintegy 30 000-re emeli.
	Minden veszélyre kiterjedő kockázatértékelés: A Szövetségi Polgári Védelmi és Katasztrófavédelmi Törvény alapján a szövetségi kormány a tartományokkal együtt évente országos kockázatelemzést készít. 2012 óta külön elemzések készültek az árvizekről, rendkívüli járványokról, téli viharokról, viharhullámokról, radioaktív és vegyi anyagok kibocsátásáról, aszályról és földrengésről. A kockázatelemzés eredményei integrált cselekvési terv kidolgozásához vezetnek, amely a veszélyek folyamatos azonosításán, elemzésén, értékelésén és kezelésén alapul.
	Együttműködés és információmegosztás: A szövetségi belügyminisztérium koordinálja a tárcák közötti együttműködést. A Szövetségi Polgári Védelmi és Katasztrófavédelmi Hivatal (BBK) fejleszti a stratégiai irányvonalakat, szervezi a képzéseket, és figyelmeztetési rendszert üzemeltet (például a NINA okostelefon-alkalmazást) a lakosság tájékoztatására. A civil-katonai együttműködés és a több mint 1,8 millió önkéntes részvétele erősíti a rendszer rugalmasságát. [73]
	Útmutatás és következmények: A KRITIS-szabályozás előírja, hogy az üzemeltetők korszerű információbiztonsági irányítási rendszert (ISMS) és üzletmenet-folytonossági rendszert (BCMS) vezessenek be, jelentsék az incidenseket és két évente független auditnak vessék alá rendszereiket. A NIS2 végrehajtása tovább szigorítja a követelményeket.
Konklúzió	Németország kiegyensúlyozott rendszert hozott létre, amely ötvözi a kormányzati irányítást a szolgáltatók felelősségével. A rendszeres, ágazatonkénti és országos kockázatértékelések, az

	erős szabályozás és a társadalmi szereplők bevonása fokozza a rezilienciát. A magyar gyakorlat számára releváns lehet az ISMS/BCMS kötelező bevezetése és a NINA-hoz hasonló lakossági riasztórendszerek alkalmazása. [74]

14. táblázat: *Kritikus szervezetek védelme Szlovéniában, Készítette: a Szerző, 2025.*

Szlovénia	A 2017-ben elfogadott Kritikus Infrastruktúra Törvény (ZKI) meghatározza a kritikus infrastruktúra fogalmát és a védelmét szolgáló kötelezettségeket. A törvény szerint kritikusnak minősülnek az energiaellátáshoz (villamosenergia, kőolajtermékek, földgáz), a közlekedéshez (vasutak, kikötők, repülőterek), az élelmiszerlánchoz, az ivóvízhez, az egészségügyhöz, a pénzügyi szolgáltatásokhoz, a környezetvédelemhez, valamint az elektronikus információs és kommunikációs rendszerekhez kapcsolódó létesítmények.
Az ágazati kockázat-értékelések legfontosabb gyakorlatai:	Ágazati felelősség: Minden kritikus ágazat élén egy „ágazati vezető” (a vonatkozó minisztérium vagy a Szlovén Nemzeti Bank) áll, aki kijelöli a kritikus infrastruktúra elemeket és felügyeli a védelmi intézkedéseket.
	Kockázatértékelési kötelezettség: A tulajdonosoknak és üzemeltetőknek úgynevezett kritikus infrastruktúra tervezési dokumentumot kell készíteniük, amely leírja az aktuális állapotot, azonosítja és értékeli a kockázati forrásokat, és meghatározza a megelőző és elhárító intézkedéseket. A dokumentumot az illetékes minisztérium hagyja jóvá. Az üzemeltetőknek állandó és kiegészítő védelmi intézkedéseket kell végrehajtaniuk, és évente jelentést kell készíteniük a zavarokról és a megtett lépésekről.
	Útmutató a kockázatértékeléshez: A Honvédelmi Minisztérium „Útmutató a kritikus infrastruktúra működéséhez kapcsolódó kockázatértékeléshez” című dokumentuma részletezi, hogy az üzemeltetőknek be kell mutatniuk az infrastruktúra állapotát, fel kell térképezniük az összes potenciális kockázati tényezőt, és értékelniük kell a valószínűséget, a súlyosságot és az üzleti folyamatokra gyakorolt hatást. Az iránymutatás lehetővé teszi, hogy a szervezetek nemzetközi kockázatkezelési szabványokra és korábbi fenyegetés-értékelésekre támaszkodjanak.
	Együttműködés és információmegosztás: A törvény előírja az államigazgatási szervek és az üzemeltetők közötti rendszeres adatcserét. Az ágazatok közötti koordinációt az ágazati vezetők biztosítják, és a beszámolók alapján évente nemzeti szintű elemzés készül. [75]
Konklúzió	Szlovénia modellje az ágazatok szerinti felelősségi rendszerre és a részletes kockázatértékelési kötelezettségre épül. Az éves jelentési kötelezettség és a honvédelmi tárca által kiadott útmutató biztosítja, hogy a kockázatok azonosítása és kezelése egységes szempontok szerint történjen. A magyar gyakorlat számára hasznos lehet az ágazatonkénti vezető kijelölése és a részletes értékelési útmutató alkalmazása.

A kritikus infrastruktúrák és szervezetek működési zavara a lakosság biztonságát és a gazdasági stabilitást egyaránt veszélyeztetheti. A veszélyek sokfélesége a természeti katasztrófák, a terrorizmus, a szabotázs, a kibertámadások miatt a védelmi intézkedések egyik alapköve a kockázatelemzés. A lengyel válságkezelési törvény szerint a kritikus infrastruktúra olyan rendszerek és létesítmények összessége, amelyek nélkülözhetetlenek az állam működéséhez és a lakosság ellátásához. Mindezek funkcionális fenntartása érdekében a nemzeti és ágazati szinten egyaránt strukturált kockázatelemzési gyakorlatok alakultak ki. E gyakorlatok célja a fenyegetések azonosítása, a sérülékenységek értékelése, valamint a kockázatok valószínűségének és lehetséges hatásainak számszerűsítése, hogy megalapozott döntések szülessenek a megelőzés, a védelem és a helyreállítás érdekében. [76]

A nemzeti szintű, „minden veszélyre kiterjedő” kockázatelemzések a legátfogóbb kereteket adják. Lengyelországban a kormányzati krízismenedzsment rendszer részeként kétévente készül „Jelentés az országos biztonsági fenyegetésekről”, amely mintegy ötven kockázatot azonosít, ez a jelentés a Nemzeti Válságkezelési Terv alapját képezi. A dokumentum a veszélyek teljes spektrumát lefedi, a természeti katasztrófáktól a társadalmi feszültségekig, és meghatározza a megelőző és reagáló intézkedések prioritási sorrendjét. Hasonló gyakorlat létezik Németországban, ahol a szövetségi kormány 2012 óta évente országos kockázatelemzéseket végez, például az árvizek, a rendkívüli járványok, a viharhullámok, a radioaktív és a vegyi kibocsátások, az aszály és a földrengés kapcsán. Az eredmények integrált cselekvési tervhez vezetnek, amely a folyamatos kockázatazonosításra és -kezelésre épül. Ezek a horizontális elemzések képezik a kritikus infrastruktúrák védelmének stratégiai hátterét, és támogatják a kormányzati döntéshozatalt.

Az új uniós szabályozások és a nemzeti jogszabályok egyre inkább előtérbe helyezik az ágazati, illetve vállalati szintű kockázatelemzéseket. A cseh jogszabályok például előírják, hogy az alapvető szolgáltatást nyújtó szervezeteknek kilenc hónapon belül részletes kockázatértékelést kell végezniük, amely minden lehetséges veszélyt, fenyegetést, sérülékenységet és lehetséges hatást vizsgál, ezt követően tíz hónapon belül reziliencia tervet kell készíteniük. [77] A célzott kockázatelemzés az egyes ágazatok sajátosságaihoz igazodó intézkedéseket tesz lehetővé, legyen szó az energiatermelés, a közlekedés, az egészségügy vagy a pénzügyi szolgáltatások területéről. Szlovéniában a jogszabályi környezet egy külön kritikus infrastruktúra tervezési dokumentum elkészítését írja elő minden üzemeltető számára, amelyben az aktuális állapot leírása mellett fel kell térképezni az összes potenciális kockázati forrást, értékelni kell azok valószínűségét és súlyosságát, valamint meg kell határozni a megelőző és elhárító intézkedéseket.

E dokumentumot az illetékes minisztérium hagyja jóvá, és a szervezetek éves jelentési kötelezettséggel tartoznak a zavarokról és a megtett intézkedésekről. A kockázatelemzések módszertanát tekintve az all-hazards megközelítés mellett egyre több helyen alkalmaznak szcenárió alapú, kvantitatív és kvalitatív módszereket, amelyek a kritikus infrastruktúrák közötti függőségeket, a dominóhatás lehetőségét és a kibertér jelentette fenyegetéseket is vizsgálják. Ausztria például az APCIP keretében mind a természeti, mind a technológiai és emberi eredetű veszélyeket figyelembe veszi, miközben ösztönzi a módszerek harmonizálását.

Németországban a KRITIS-szabályozás nemcsak a kockázatelemzések elvégzését írja elő, hanem követelménnyé teszi az információbiztonsági irányítási rendszerek és az üzletmenet-folytonossági rendszerek bevezetését, valamint az incidensek bejelentését és a kétévenkénti auditot. Ezek a megközelítések azt jelzik, hogy a kockázatelemzés a kritikus szolgáltatások menedzsmentjének integrált elemévé vált, amely a megfelelőség, a stratégiai tervezés és a reziliencia folyamatos javítását szolgálja.

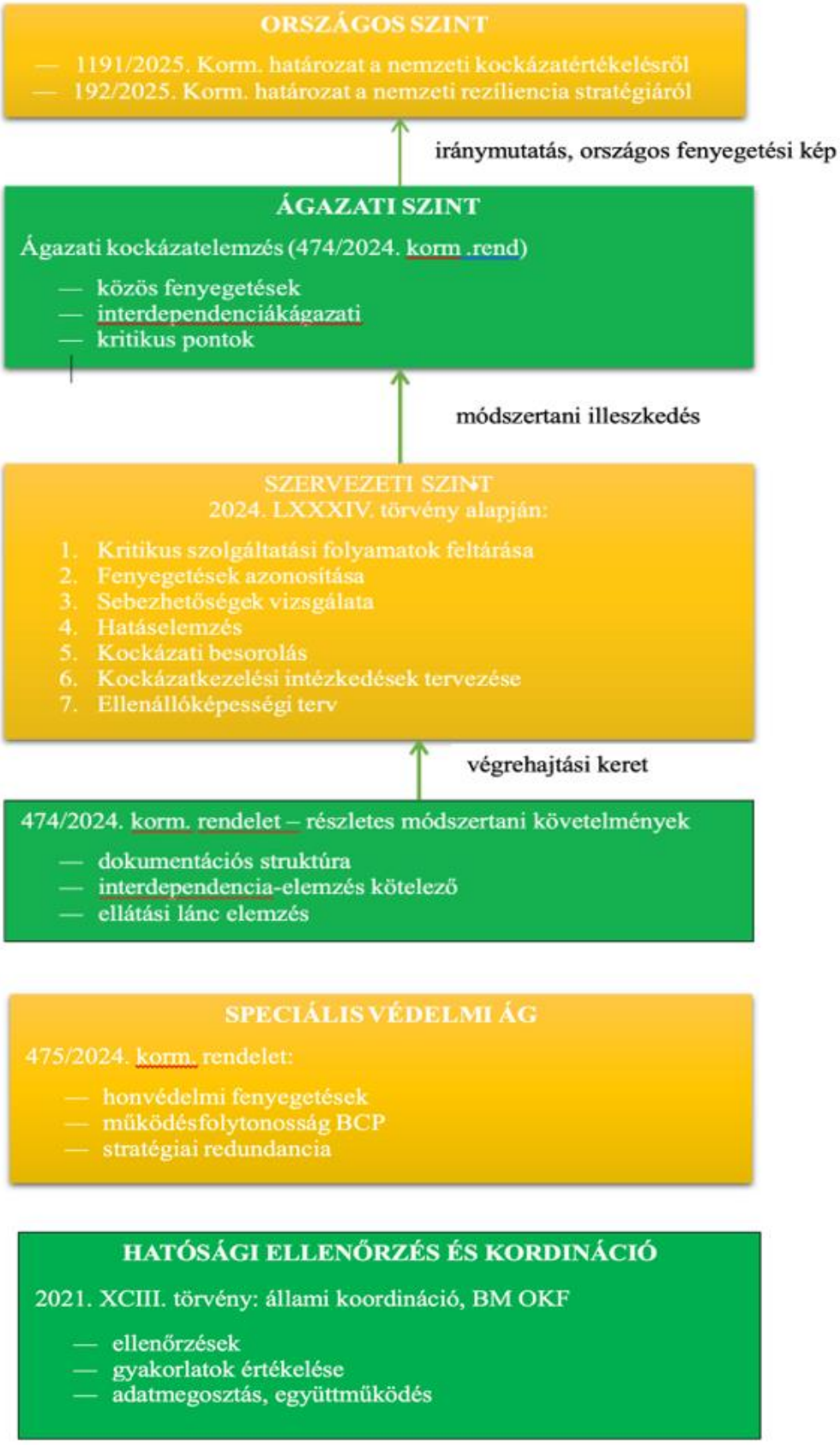
2.2 A jogszabályi környezet által meghatározott kockázatelemzési követelmények elemzése

A Kszetv. egységes, több szintű kockázatértékelési rendszert ír elő a kritikus szervezetek és infrastruktúrák számára. A rendszer csúcsszintjén a Kormány által elfogadott nemzeti stratégia és a négyévente felülvizsgált, hivatalos kormányhatározattal közzétett nemzeti kockázatértékelés áll, amelyek iránymutatást adnak a szervezeti szintű értékelésekhez, beleértve az országhatáron átnyúló kölcsönös függőségek figyelembevételét is. A nemzeti kockázatértékelés egy tervezési dokumentum, amely az ágazatokra, a nemzeti katasztrófakockázat-értékelésre, és az általános kockázatokra épül. A dokumentum kötelező referenciapont a kritikus szervezetek saját kockázatértékelése és ellenálló-képességi intézkedései számára. Szervezeti szinten a jogszabály előírja, hogy a kritikus szervezet a belső és külső környezet alapján azonosítja, értékeli és kezeli mindazon kockázatokat, amelyek az alapvető szolgáltatás folyamatosságát befolyásolhatják. Az értékelésnek ki kell terjednie a kötelező általános és ágazati kockázatokra, valamint a szervezet által feltárt egyéb kockázatokra, az eredményt ellenálló képességi mátrixban kell rendszerezni. E kockázatelemzés az ellenálló képességi terv (üzemfolytonossági és helyreállítási intézkedéseket is tartalmazó dokumentum) alapja, amelyet a kijelölő hatóság formanyomtatványán kell benyújtani, éves rendes, illetve meghatározott esetekben soron kívüli felülvizsgálattal. [13]

A végrehajtási részletszabályokat a Kszetv. Vhr. konkretizálja. Ez rögzíti többek között, hogy a kockázatértékelést és a mátrixot az általános kijelölő hatóság által közzétett módszertani segédlet és ellenálló-képességi mátrix szerint kell elkészíteni, a kritikus szervezetnek 24 órás

felügyeleti rendszert kell fenntartania, a szervezeti egységek félévente részjelentést, évente átfogó jelentést készítenek az ellenálló-képességért felelős vezetőnek, az ellenálló képességi tervet minden év január 31-ig felül kell vizsgálni és ha szükséges elektronikusan meg kell küldeni a hatóságnak, továbbá komplex ellenálló-képességi gyakorlatokat és stressztesztet is előír, amelyek eredményei beépítendők az éves értékelő jelentésbe. [36] A jelentési kötelezettségek közül kiemelendő a rendkívüli események bejelentése, a törvény órában mérhető határidőkkel írja elő a bejelentést a katasztrófavédelem ügyelete és az illetékes hatóságok felé, a lezárást követően az ellenálló-képességért felelős vezető részletes zárójelentést nyújt be a kijelölő és ágazati hatóságoknak, illetve ahol releváns, az energetikai kijelölő hatóságnak, amelyek továbbítják azt a nemzeti eseménykezelő központnak. A kontrollált rendkívüli eseményekről éves összesítő jelentés készül.

A Vbö. szabályozásként biztosítja a védelmi és biztonsági tevékenységek összehangolását. A törvény kijelöli a kockázatalapú koordináció állami kereteit, valamint rögzíti az információmegosztási és együttműködési kötelezettséget a nemzetbiztonsági, védelmi és ágazati szereplők között. E keretrendszer nélkülözhetetlen ahhoz, hogy a kritikus szervezetek kockázatelemzései összhangban legyenek az országos védekezési mechanizmusokkal. A Vbö. Vhr. az ország védelme és biztonsága szempontjából jelentős szervezetekre vonatkozó külön szabályokat rögzíti. Ezek a szervezetek eltérő fenyegetési környezetben működnek, ezért kockázatelemzésüknek a honvédelmi jellegű fenyegetésekre, hibrid hadviselési mintázatokra és stratégiai rendszerek zavarára is ki kell terjednie. A rendelet egy védelmi rezilienciamodellt vezet be, amely nagy hangsúlyt helyez a redundanciára, a műveleti folytonosságra és a stratégiai tartalékok fenntartására. [14] A nemzeti kockázatértékelési határozat országos szintű fenyegetési kategóriákat, sérülékenységi területeket és prioritásokat jelöl ki, amelyek irányadóak a szervezeti és ágazati kockázatelemzések számára. A nemzeti kockázatértékelés egyfajta makroszintű viszonyítási alapként funkcionál, biztosítva, hogy a különböző ágazatok elemzései ne térjenek el egymástól módszertani vagy tartalmi szempontból. [37] A nemzeti stratégiai határozat Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti stratégiáját rögzíti. A stratégia a megelőzés, felkészülés, reagálás és helyreállítás négyes reziliencia szerkezetére épül, és hangsúlyozza, hogy a kockázatelemzés nem statikus dokumentum, hanem folyamatos fejlesztést igénylő, iteratív folyamat. A stratégia kiemeli az interdependenciák kezelésének szükségességét is, amely a modern infrastruktúrák rendszerszintű sérülékenységének egyik legkritikusabb tényezője. [5]



8. ábra: A kritikus szervezetek kockázatkezelési folyamatának és jogszabályi kapcsolódásainak rendszere Magyarországon Készítette: a Szerző, 2025.

Az ábra a magyar kritikus szervezetek és infrastruktúra védelem jogszabályi rendszerére épülő kockázatkezelési folyamat fő szintjeit és azok kapcsolódásait mutatja be. A folyamat legfelső rétegét az országos dokumentumok, a nemzeti kockázatértékelés és a nemzeti reziliencia stratégia alkotják, amelyek meghatározzák az országos szintű fenyegetéseket, prioritásokat és reziliencia célokat. Ezek adják a keretet az ágazati kockázatelemzések számára, amelyek a közös fenyegetések, az infrastruktúra függőségek és az ágazati sérülékenységi pontok feltárását végzik.

A szervezeti szintű kockázatértékelés a Kszektv. alapján a kritikus szolgáltatási folyamatok, fenyegetések, sebezhetőségek és hatások elemzésére épül, amelyből az ellenállóképességi terv készül. A végrehajtási rendeletek határozzák meg az alkalmazandó módszertant, míg a védelmi jelentőségű infrastruktúrákra külön szabályok vonatkoznak. A teljes rendszer koordinációját és ellenőrzését a Vbö. biztosítja, így az ábra egy egymásra épülő, több szintű, összehangolt kockázatkezelési modellt ábrázol. [13]

A 16/2025. (VI. 6.) HM utasítás speciális szerepet tölt be, meghatározza az ország védelme és biztonsága szempontjából jelentős infrastruktúrák azonosítását, ellenőrzését és nyilvántartását. Ez az utasítás biztosítja, hogy a honvédelmi ágazat saját kockázati és sérülékenységi adatai beépüljenek az országos reziliencia rendszerbe. A nyilvántartási kötelezettség révén stabil adatbázist hoz létre a fenyegetések, sérülékenységek és biztonsági események rendszerszintű értékeléséhez. [112]

Átmenetileg a kijelölési eljárások első körét 2025. április 30-ig kellett megindítani, ami a régi létfontosságú rendszerelemekről való átállást szolgálja. Emellett egyes honvédelmi érdekből jelentős szervezetekre külön kormányrendelet állapít meg többletkötelezettségeket (pl. éves tervfelülvizsgálat és speciális ellenőrzések. Összességében elmondható, hogy a magyar kritikus infrastruktúra védelem új szabályozási rendszere komplex, többszintű és egymásra épülő kockázatelemzési követelményeket határoz meg. A törvényi szint biztosítja az alapelveket és felelősségi kereteket, a végrehajtási rendeletek pontos módszertani elvárásokat szabnak, a kormányhatározatok stratégiai iránymutatást adnak, a honvédelmi utasítás pedig a speciális ágazati igényeket integrálja. Ez a struktúra illeszkedik a nemzetközi szakirodalomban megjelenő reziliencia modellhez, amely a kritikus infrastruktúrákat dinamikus, hálózatos, egymásra utalt rendszerekként értelmezi. A kockázatelemzés így nem csupán jogszabályi kötelezettség, hanem a nemzeti biztonság és ellátásbiztonság egyik legfontosabb garanciája. [36]

2.3 A kritikus szervezetek kockázatelemzésének elméleti és módszertani háttere a szakirodalom tükrében

2.3.1 A hazai szakirodalom kritikai áttekintése

A hazai szakirodalomban Mógor Judit és Angyal István, valamint Szénási Imre tanulmányai jól érzékeltetik, hogy a kritikus szervezetek kockázatelemzése a korábbi, szigetszerű megközelítésektől a rendszerszintű, szabályozás-vezérelt és interdependenciákra érzékeny modellek felé tolódott. Mindkét munka középpontjában az a felismerés áll, hogy a kritikus szolgáltatások védelme nem oldható meg pusztán szervezeti keretek között, ágazati és ágazatközi koordinációt, egységesített módszertant és az adatok intézményesített megosztását igényli.

Mógor és Angyal az európai és a friss hazai keretrendszerekből kiindulva a reziliencia és a nemzeti kockázatértékelés összekapcsolását hangsúlyozza. Értelmezésében a kockázatelemzés nem önmagáért végzett adminisztratív aktus, hanem prioritásképzésre alkalmas döntéstámogató eszköz, amely a fenyegetettség, sérülékenység, kitettség és következmény dimenzióit egységes indikátorrendszerbe rendezi. Külön figyelmet kap a szabályozói megfelelés és a jelentési fegyelem, az ágazatok közti összehasonlíthatóság érdekében szerinte standardizált metrikákra, súlyozási elvekre és auditálható adatfolyamatokra van szükség. A szerzők a gyakorlatba ültetés feltételei közé sorolja az adathozzáférés rendezését, a kis és közepes szolgáltatók kapacitásfejlesztését, illetve az ágazatközi gyakorlatok és stressztesztek bevezetését. [10]

Szénási az intézményi és kormányzási logikát tárja fel, kik a felelősek a kritikus infrastruktúra védeleméért, hogyan szerveződik a kompetenciamegosztás a kormányzaton belül, milyen eljárások biztosítják a helyzetértékelés és a beavatkozás összehangolását. A tanulmány erőssége, hogy rámutat az irányítási és információs asszimmetriákra, különösen a töredezett adatvagyon, az eltérő érettségű szervezetek és a beszállítói láncok átláthatatlansága miatt, valamint az interdependenciák kezelési nehézségeire (energia–víz–közlekedés). Szénási szerint a hatékony kockázatelemzés feltétele egy stabil kormányzati architektúra, világos mandátummal, visszacsatolási mechanizmusokkal és a valós idejű monitoring irányába tett lépésekkel, enélkül a módszertani fejlesztések nem skálázhatók rendszer szintre. [78]

A három szerző nézőpontja komplementer: Mógor és Angyal a tartalmi, módszertani, Szénási az intézményi, folyamat oldali feltételeket konkretizálja. Közös metszetük az all-hazards szemlélet, az ágazatközi függések explicitté tétele, és az, hogy az értékelésből prioritás és intézkedés portfólió szülessen, ne csak kockázati listák.

Mindketten felvetik a standardizált indikátorkészlet szükségességét, ugyanakkor arra is figyelmeztetnek, hogy a túlságosan bonyolult módszertan magas adatigénnyel könnyen kizárja a kisebb szereplőket.

Módszertani tanulságként Mógor és Angyal írása legitimálja az indikátor alapú, súlyozott kockázatértékelést, továbbá a stressztesztek és szcenáriók szerepét a bizonytalanság kezelésében. Szénási elemzése ehhez képest a végrehajtás sikerfaktorait részletezi, adat- és információs kormányzás, hozzáférési szabályok, titokvédelem, a felügyeleti és szolgáltatói szerepek összehangolása, és a beszállítói láncokból fakadó külső függések beemelése a rendszeres kockázati ciklusba. A szerzők implikált kutatási hiányokat is azonosítanak, egységes súlyozási szempontrendszer hiánya ágazati szinten, hálózati/rendszerkockázati metrikák (centralitás, dominó-modellek) korlátozott alkalmazása, valós incidens adatokra épített visszatesztek (AUC/Brier) ritkasága, továbbá a kisebb szolgáltatók bevonásának operatív akadályai. [11]

Az ágazati kockázatelemzés bevezetésének hazai relevanciáját mindkét munka megerősíti. Mógor és Angyal a jogszabályi megfelelés és a stratégiai koherencia felől indokolja az egységes értékelési kereteket, Szénási az intézményi kapacitások és együttműködési protokollok oldaláról teszi egyértelművé, hogy a kockázatelemzés csak kormányzási hordozó közegben tud hatékonyan működni. [10]

Összegzésképpen a szerzők munkái együtt egy kettős szükségletet rajzolnak ki a magyar kritikus szervezetek kockázatelemzésében, a szabályozás- és evidencia-alapú, indikátorokkal és súlyokkal operáló módszertani standardot, valamint a kormányzási és adat-infrastruktúrát, amely garantálja a végrehajtás minőségét, az adatok megoszthatóságát és az ágazatközi koordinációt. A disszertációdban javasolt keretrendszer ezekre a hiányokra ad koherens, implementálható megoldást, és jó alapot teremt a nemzeti kockázatértékelés és a reziliencia gyakorlati megerősítéséhez.

2.3.2 A nemzetközi szakirodalom összehasonlító elemzése

A nemzetközi szakirodalom közös kiindulópontja, hogy a kritikus infrastruktúrák kockázatkezelése rendszerszintű megközelítést és interdependenciákra érzékeny módszertant igényel. A klasszikus, a területet azóta is meghatározó tanulmány Rinaldi, Peerenboom és Kelly a függés- és kölcsönös függés-típusok taxonómiáját adja, és felhívja a figyelmet a dominóhatások, a láncreakciók és rejtett kapcsolatok szerepére, ez a gondolkodásmód indította el a hálózat-alapú elemzések hullámát az energia-, víz-, telekommunikációs és pénzügyi hálózatokban. [20]

Az Európai Bizottság Közös Kutatóközpontja (JRC) átfogó módszertani összegzései a fenyegetettség, a sérülékenység, a következmény hármasára épülő, indikátor alapú kereteket ajánlanak, amelyek ágazati szinten is alkalmazhatók. A JRC szerint a módszertan kiválasztása mindig a döntési kontextushoz igazítandó (kvalitatív, félkvantitatív vagy kvantitatív), és külön figyelmet kell fordítani a normalizálásra, súlyozásra és a bizonytalanságkezelésre. [79]

A kiberfenyegetettségi dimenziót az EU szinten ENISA Threat Landscape jelentések adják hozzá: az éves ETL a fő támadási mintázatokat, aktorokat és technikákat rendszerezi, ágazat specifikus kitekintésekkel pl. pénzügyi ágazat. Ezek a jelentések mára döntéstámogató támponttá váltak az ágazatokban. [80]

Az OECD a reziliens infrastruktúra-kormányzás oldaláról egészíti ki a képet, a 2025-ös anyagok a kormányzási pillérekre, az infrastruktúra indikátorokra és a klíma reziliencia szempontokra teszik a hangsúlyt. A fő üzenet, hogy az ágazati kockázatelemzés csak akkor skálázható országos szintre, ha azt átlátható irányítási és mérési rendszer hordozza a szabványosított indikátorok, a beszámolási rend, és összehasonlíthatóság. [81]

Az Egyesült Királyság NCSC Cyber Assessment Framework (a továbbiakban: CAF) keretrendszere a létfontosságú szolgáltatók számára nyújt kimenet orientált önértékelési és felügyeleti mércét. A CAF a kritikus funkciók védelmére koncentrál, 4 célra és 14 elvre tagolva, folyamatosan frissül. [82]

Az Egyesült Államokban a NIST SP 800-30 a kockázatfelmérés közös nyelve, a formális kockázatmodellre, a likelihood–impact becslésre és a kockázatkezelési ciklushoz kötött folyamatra épít. Bár információbiztonsági fókuszú, módszertani megoldásai a kockázati tényezők, a skálák, a bizonytalanság jól transzferálhatók ágazati kritikus infrastruktúra környezetbe. [83] A tágabb amerikai kormányzási keretet a National Infrastructure Protection Plan (a továbbiakban: NIPP 2013) és a CISA Cross-Sector Cybersecurity Performance Goals (a továbbiakban: CPG) adják. Előbbi a partnerség alapú, kockázat arányos védelem és az információmegosztás struktúráját rögzíti, utóbbi pedig priorizált, ágazatközi minimumcélokat fogalmaz meg. Ezek együtt azt illusztrálják, hogyan fordítható le a módszertan végrehajtható követelményekké különböző ágazatokban. [84]

Tematikusan a külföldi irodalom négy közös módszertani erőssége rajzolódik ki.

- Indikátor- és súlyozás-alapú értékelés: a JRC/NIST/NCSC anyagok következetesen igénylik a mérhető indikátorokat és transzparens súlyozást, a döntési kontextushoz illesztett normalizálással.

- Interdependencia-modellezés: Rinaldi taxonómiája óta a hálózat alapú és input–output szemlélet vált rendszerszintű kockázatoknál.
- Bizonytalanság és trendek kezelése: az ENISA-jelentések éves ciklusa és a stressztesztek gyakorlata dinamikus, élő kockázati képet ad.
- Kormányzási beágyazás: az OECD/NIPP a skálázhatóság feltételeként a szerepek, mérés, beszámolás tisztázását hangsúlyozza. [85]

A legfrissebb fejlemények ráerősítenek az ágazati szemlélet szükségességére, az ENISA szerint 2023–2024-ben nőtt a diszruptív támadások száma és komplexitása, a geopolitikai kitettségek és beszállítói láncok miatt pedig az ágazatközi terjedés is gyorsult, pl. pénzügyi ágazat célzottsága. Ezek az eredmények közvetlenül beépülnek a tagállami és ágazati kockázati keretekbe. [86]

Šarūnienė tanulmánya egy átfogó, több ágazatra kiterjedő kockázatelemzési keretrendszert mutat be, amely a kritikus infrastruktúrák interdependenciáit helyezi előtérbe. A szerző hangsúlyozza, hogy a modern infrastruktúrák hálózatos jellege miatt a kockázatok nem értékelhetők izoláltan, mivel az ágazatok közötti kölcsönhatások önálló sérülékenységi forrásokat teremtenek. A cikk a veszélyazonosítás, hatáselemzés és valószínűségi értékelés integrált megközelítését alkalmazza, kiegészítve a kritikus elemek működéskiesésének modellezésével. Fontos megállapítása, hogy az ágazati kockázatelemzés csak akkor hatékony, ha figyelembe veszi a külső függőségeket és a láncreakció jellegű szolgáltatás kimaradásokat. [120]

Ali Aghazadeh, Marianna Lezzi és Mahdad Pourmadadkar közös tanulmánya a kritikus infrastruktúrák kiber rezilienciájának kockázatelemzését helyezi előtérbe, és egy multidiszciplináris keretrendszert javasol a fizikai és kiber fenyegetések integrált értékelésére. A szerzők rámutatnak, hogy a kritikus infrastruktúra rendszere digitalizációja újfajta sebezhetőségeket hozott létre, amelyek sok esetben nagyobb hatást gyakorolnak a működés folytonosságára, mint a hagyományos fizikai veszélyek. A cikk részletesen tárgyalja a kiber fenyegetések valószínűségének becslési módszereit, a rendszer redundanciáját befolyásoló tényezőket és a sérülékenységeket csökkentő technikai intézkedéseket. A módszertan külön előnye, hogy egyaránt alkalmazható energia-, víziközmű- és közlekedési infrastruktúrákra. A tanulmány hangsúlyozza, hogy a kiber reziliencia értékelése nem választható el a működési rezilienciától, mivel a két terület erősen egymásra utalt. [121]

Papamichael 2024-es tanulmánya a kritikus infrastruktúrák védelméhez kapcsolódó kockázatértékelési folyamat gyakorlati nehézségeit és módszertani korlátait elemzi, különös tekintettel azokra a tényezőkre, amelyek a szakértők döntéshozatalát befolyásolják. A szerző kiindulópontja, hogy a kritikus infrastruktúrák védelmi rendszerében a kockázatelemzés a leginkább meghatározó funkció, ugyanakkor az ágazatok közötti módszertani eltérések, a különböző szervezeti kultúrák és az információhiány jelentősen torzíthatják a kockázati képet. A cikk empirikus interjúkra és esettanulmányokra épít, amelyekből kiderül, hogy a szakemberek gyakran nem egységes kockázati definíciókat használnak, ami az ágazati kockázatelemzés eredményeinek összehasonlíthatóságát is akadályozza. Papamichael hangsúlyozza, hogy a kritikus entitások működési környezete egyre inkább transznacionális fenyegetésekkel terhelt, például kiber incidensekkel, ellátási lánc zavarokkal vagy régión átnyúló infrastrukturális függőségekkel, amelyek komplexitása meghaladja a hagyományos lineáris elemzési kereteket. [111]

A tanulmány egyik legfontosabb megállapítása, hogy a kockázatértékelés sikere döntően azon múlik, mennyire képes a folyamat integrálni a különböző tudásterületeket és ágazatok közötti együttműködést. Papamichael szerint a jelenlegi kritikus infrastruktúra módszertanok gyakran túlságosan technikai fókuszúak, és kevés figyelmet fordítanak a szervezeti döntéshozatal működésére, a bizonytalanság kezelésére és a kommunikációs aszimmetriákra. A cikk kritikusan elemzi azokat az eseteket, amikor a kockázatértékelés formalitássá válik, és nem tükrözi a tényleges fenyegetéseket vagy az interdependenciákból fakadó másodlagos hatásokat. Ennek kapcsán a szerző felveti a standardizált, EU-szinten is összehangolt módszertan szükségességét, különösen a kritikus szervezetek keretrendszerben, ahol a szolgáltatásnyújtás folytonosságát több, egymástól függő rendszer teljesítménye határozza meg. Papamichael javaslata egy olyan adaptív kockázatelemzési modell bevezetése, amely képes kezelni a többtényezős bizonytalanságot, a dinamikusan változó fenyegetési környezetet és a szakterületek közötti tudásmegosztás hiányosságait. A tanulmány így fontos hozzájárulást jelent mind a módszertani vitákhoz, mind a gyakorlati kritikus infrastruktúra védelem fejlesztéséhez, és jól illeszthető a kritikus szervezetek rezilienciájának vizsgálatához. [111]

Lubis tanulmánya a kritikus infrastruktúrák rezilienciájának mérhetőségére koncentrál, és új mérőszámokat javasol a kulcsfontosságú rendszerek működőképességének értékeléséhez. A cikk kiemeli, hogy a reziliencia gyakran elvont fogalom marad, ha nem kapcsolódik számszerűsíthető indikátorokhoz, például helyreállítási időhöz, redundancia fokhoz vagy szolgáltatásbiztonsági szintekhez.

A szerző többlépcsős értékelési keretet javasol, amely a fenyegetések, sebezhetőségek és rendszerképességek együttes vizsgálatán alapul. A módszertan alkalmazható ágazati és szervezeti kockázatelemzésben egyaránt, és jól illeszkedik a kritikus entitások reziliencia követelményeihez. A cikk hozzájárul a kockázatelemzés objektív alapokra helyezéséhez. [122]

Zubair A. Baig, és Sherali Zeadally tanulmánya egy átfogó kiberbiztonsági kockázatértékelési keretrendszert mutat be, amely a kritikus infrastruktúrák digitális védelmére összpontosít. A szerzők áttekintik a kritikus infrastruktúra rendszerekben előforduló tipikus kiber fenyegetéseket, például SCADA rendszerek sérülékenységeit, hálózati támadásokat és belső fenyegetéseket. A módszertan hangsúlyt fektet a sebezhetőségek priorizálására és a védekező kapacitások optimalizálására. A cikk egyik fontos megállapítása, hogy a kockázatelemzés hatékonysága nagymértékben függ a valós idejű monitorozástól és a gyors reagálás képességétől. Ez a megközelítés jól illeszkedik a modern kritikus infrastruktúra rendszerek követelményeihez. [123]

Sean S. Baggott és Joost R. Santos 2020-as cikkében egy strukturált kockázatelemzési keretrendszert kínál, amely egyszerre értékeli a fizikai és kiber fenyegetések hatását a kritikus infrastruktúrákra. A szerzők egy olyan integrált modellt mutatnak be, amely a veszélyek, sérülékenységek és potenciális következmények sztochasztikus elemzésére épül. A tanulmány külön figyelmet fordít a költséghatékonysági szempontokra, vagyis arra, hogyan választhatók ki optimálisan a védelmi intézkedések. A modell jól alkalmazható energiainfrastruktúrák, közlekedési hálózatok és víziközművek esetében. A cikk értéke abban rejlik, hogy világosan bemutatja a kiber és fizikai integráció kihívásait. [124]

Ayeni és Oluwagbenga 2024-es tanulmánya a kritikus infrastruktúrák rezilienciájának értékelésére és fejlesztésére összpontosít, és modern, átfogó szemléletet képvisel a működésbiztonság és a szolgáltatásfolytonosság vizsgálatában. A szerzők kiemelik, hogy a kritikus infrastruktúrák egyre összetettebb és kölcsönösen egymásra utalt rendszerekből állnak, amelyek működését egyszerre befolyásolják természeti, technológiai, humán és kiber fenyegetések. A cikk egyik központi érve, hogy a reziliencia nem azonos a hagyományos védelemmel vagy a kockázatok csökkentésével, sokkal inkább azt fejezi ki, hogy a rendszer mennyire képes alkalmazkodni, fennmaradni, regenerálódni és gyorsan helyreállni különböző zavarok után. Ezt a reziliencia felfogást a szerzők többdimenziós modellbe illesztik, amely a felkészülés, megelőzés, reagálás és helyreállítás teljes ciklusát integrálja. [125] A szerzők hangsúlyozzák, hogy a reziliencia csak akkor növelhető hatékonyan, ha a kritikus szervezetek átfogó képet kapnak saját sebezhetőségeikről, beleértve az ágazati és ellátási lánc függőségeket

is. A cikk gyakorlati példákat mutat be energia és víziközmű infrastruktúrák esetében, amelyek igazolják, hogy a reziliencia fokozása gyakran szervezeti és stratégiai beavatkozást is igényel, nem csupán technikai fejlesztést. Ayeni és Oluwagbenga szerint nagy kihívást jelent, hogy a döntéshozók sokszor kizárólag a fenyegetések valószínűségére koncentrálnak, miközben a reziliencia kulcsa a rendszerképességek növelése és a működésfolytonosság alternatíváinak kiépítése. A tanulmány jól rávilágít arra, hogy a kritikus infrastruktúra védelem nem működhet pusztán kockázatcsökkentésre épülő modellként, hanem szükség van olyan holisztikus megközelítésre, amely a rendszer teljes életciklusát és az ágazatok közötti kapcsolatrendszert is vizsgálja. [125]

A szerzők végkövetkeztetése egyértelmű, a reziliencia értékelése és fejlesztése a kritikus infrastruktúrák fenntartható működésének előfeltétele, és a jövőbeli védelmi rendszerek egyik legmeghatározóbb pillére lesz. Ez a megközelítés kiválóan illeszthető a kritikus szervezetek koncepciójához, amely a szolgáltatás nyújtásának folyamatát és a szervezet teljes működési képességét helyezi középpontba. A tanulmány így mind elméleti, mind gyakorlati szempontból értékes hozzájárulás a reziliencia kutatásokhoz és a kritikus infrastruktúrák védelmének fejlesztéséhez. [125]

Roshanaei cikke a kritikus infrastruktúra védelem stratégiai kihívásait tárgyalja, és a reziliencia koncepcióját a kritikus infrastruktúra rendszerek központi elemének tekinti. A tanulmány szerint a modern infrastruktúrák egyre kevésbé képesek ellenállni az összetett, többtényezős fenyegetéseknek, ezért a kockázatkezelésnek a teljes rendszer rugalmasságát kell fejlesztenie. A szerző elemzi a politikai, technológiai és szervezeti korlátokat, amelyek akadályozzák a reziliencia megvalósítását. A cikk hangsúlyozza a többágazatú koordináció szükségességét, és rámutat, hogy a legnagyobb veszélyt az interdependenciák alulértékelése jelenti. [126]

Hemme elemzése arra világít rá, hogy a kritikus infrastruktúrák karbantartása nem pusztán üzemeltetési kérdés, hanem nemzetbiztonsági jelentőségű tényező. A szerző részletesen tárgyalja, hogyan vezet a rendszerek elhanyagolása sérülékenységekhez, és hogyan növeli a fizikai és kiber fenyegetések sikerességének valószínűségét. Hemme hangsúlyozza, hogy a kritikus infrastruktúrák tekintetében a preventív karbantartás ugyanolyan fontos, mint a hagyományos védelmi intézkedések. További fontos megállapítás, hogy a fenntartható infrastruktúra védelemhez hosszú távú beruházási és tervezési szemlélet szükséges. A cikk releváns történeti és stratégiai hátteret nyújt a kritikus infrastruktúra védelméhez. [127]

Ouyang 2014-es átfogó tanulmánya a kritikus infrastruktúrák közötti interdependenciák modellezésének és szimulációjának legfontosabb kutatási irányait foglalja össze, és máig alapműnek számít a témában. A szerző kiindulópontja, hogy a kritikus infrastruktúrák egymástól való függései nem csupán működési sajátosságot jelentenek, hanem a rendszerszintű sérülékenység elsődleges forrásai. Működési zavarok ugyanis gyakran nem az adott ágazat belső hibáiból erednek, hanem abból, hogy egy másik ágazatban bekövetkező kiesés dominóhatásszerű következményekhez vezet. Ouyang részletesen osztályozza a függőségek típusait úgy, mint fizikai, kiber-információs, földrajzi és logikai, és bemutatja, hogy ezek különböző kombinációi hogyan alakítják egy kritikus szervezet tényleges kockázati profilját. [29]

A cikk egyik legerősebb hozzájárulása a különböző modellezési megközelítések szisztematikus összehasonlítása. A szerző bemutatja a hálózatelméleti modelleket, a rendszer-dinamikai keretrendszereket, az „agent-based" szimulációkat, valamint a hibatérképező (fault tree és event tree) módszereket, kiemelve mindegyik előnyeit és korlátait. Ouyang rámutat, hogy nincs univerzális modell, a választott módszer meghatározza, milyen típusú interdependenciák és hatásmechanizmusok tárhatók fel. A tanulmány azt is hangsúlyozza, hogy a szimulációk eredményeit gyakran korlátozza az adat elérhetőség és az ágazatok közötti információmegosztás hiánya, ami megnehezíti a valóság hű leképzését. Ennek ellenére a modellezés továbbra is az egyik legfontosabb eszköz a rendszerszintű kockázatok előrejelzésében és a komplex hatásláncok feltárásában.

Ouyang végkövetkeztetése, hogy a modern kritikus infrastruktúra védelem csak akkor lehet hatékony, ha a kockázatelemzés folyamatában figyelembe veszik a többágazatú kölcsönhatásokat és az interdependenciák nemlineáris működését. A szerző szerint a jövőben olyan hibrid modellekre van szükség, amelyek egyesítik a hálózatelmélet, a dinamikus szimuláció és a kockázatelemzés eszközeit, valamint képesek kezelni a bizonytalanságot és az felmerülő rendszerjelenségeket. A cikk rendkívül fontos elméleti hátteret nyújt a kritikus szervezetek és ágazatok közötti kapcsolatok értelmezéséhez, és erős alapot ad az ágazati kockázatelemzés modern, integrált megközelítéséhez is. [29]

Rinaldi, Peerenboom és Kelly 2001-es úttörő munkája meghatározó szerepet játszott a kritikus infrastruktúrák közötti interdependenciák kutatásában, és alapvetően formálta a kritikus infrastruktúrák védelmének elméleti kereteit. A szerzők abból indulnak ki, hogy a modern infrastruktúrák egyre kiterjedtebb kapcsolatrendszerben működnek, így a rendszerszintű kockázat nem érthető meg az ágazatok elkülönült vizsgálatával.

A cikk egyik legfontosabb hozzájárulása az interdependenciák négy típusának meghatározása a fizikai, az információs, a földrajzi és a logikai függőségek elkülönítése. Ezek a kategóriák máig a nemzetközi szakirodalom alapfogalmai, és számos későbbi modellezési és kockázatelemzési keretrendszer kiindulópontjául szolgálnak. A szerzők példákon keresztül szemléltetik, hogy a kritikus szervezetek közötti kapcsolatokat gyakran rejtett, nemlineáris hatásmechanizmusok alakítják, ami megnehezíti a zavarok következményeinek előrejelzését. [20]

A cikk jelentősége abban áll, hogy nemcsak leírja a függőségeket, hanem elemzi azok dinamikus természetét, vagyis azt, hogy az interdependenciák időben és körülmények között változhatnak. A szerzők rámutatnak, hogy ugyanaz a kapcsolat békeidőben rugalmas működést eredményezhet, míg válsághelyzetben kritikus sebezhetőséget jelenthet. Különösen értékes az a megállapítás, hogy az infrastrukturális hálózatok közötti kölcsönhatások gyakran többlépcsős hatásláncokat hoznak létre, amelyekben egy lokális zavar rövid idő alatt országos vagy akár nemzetközi zavarokat okozhat. Ez a felismerés később alapja lett annak a szemléletnek, amely a kockázatkezelésben a láncreakciószerű és fokozódó meghibásodású modellek vizsgálatát is kötelezővé tette.

A szerzők hangsúlyozzák, hogy a kritikus infrastruktúrák védelmében a kockázatelemzés csak akkor lehet hatékony, ha képes integrálni az interdependenciák vizsgálatát, és nem kizárólag egyetlen ágazat belső kockázataira koncentrál. Ezzel a tanulmány lényegében megalapozta az ágazati kockázatelemzés modern, integrált megközelítését, amelyben az egyes ágazatok szektorok elemzését összhangba kell hozni a kölcsönhatások elemzésével. A cikk máig hivatkozási alap a kritikus szervezetek rezilienciájának kutatásában, mivel világosan kimutatja, hogy a kritikus szervezetek működőképessége erőteljesen függ más infrastruktúrák állapotától, így a reziliencia nem értelmezhető elszigetelt rendszerként. Mindezek alapján a tanulmány nemcsak történeti jelentőségű, hanem a mai napig meghatározza a komplex kritikus infrastruktúra rendszerek kockázatelemzési és védelmi megközelítését. [20]

Irene Eusgeld, Cen Nan és Sven Dietz cikke a rendszerek rendszere szemléletet alkalmazza a kritikus infrastruktúrák kockázatelemzésében, hangsúlyozva, hogy a hagyományos, lineáris modellek nem képesek kezelni a valós működési komplexitást. A szerzők egy olyan integrált kockázatkezelési keretet javasolnak, amely képes a többágazatú működés kiesések és kölcsönhatások értékelésére. A módszer jól alkalmazható a kritikus szervezetek koncepciójában, ahol a szolgáltatásfolytonosság több rendszer együttes teljesítményétől függ. A tanulmány gyakorlati példákat is bemutat energetikai és digitális infrastruktúrák esetében. [128]

A Resilience Measurement Index tanulmánya reziliencia mérő index koncepcióját mutatja be, amely egy számszerűsített eszköz a kritikus infrastruktúrák reziliencia mérésére. A szerzők kvantitatív mutatókkal értékelik a megelőzési, reagálási és helyreállítási képességeket. A módszertan az infrastruktúrák működési ciklusát vizsgálja, külön figyelmet szentelve a redundancia és adaptivitás szerepének. A tanulmány nagy előnye, hogy a reziliencia fogalmát kézzelfogható mérőszámokra fordítja le. Alkalmas ágazati és szervezeti szintű összehasonlításokra is. [129]

Kröger kritikusan elemzi a hagyományos kritikus infrastruktúra megközelítést, és új fogalmi keretet javasol a kockázatok komplexitásának kezelésére. A szerző szerint a kritikus infrastruktúra rendszerek ma már túl összetettek ahhoz, hogy izolált ágazati szemlélettel védhetők legyenek. A cikk hangsúlyozza az adaptív, reziliencia központú megközelítés szükségességét, amelyben a kockázatelemzés folyamatos alkalmazkodását igényli. [130]

Hollnagel klasszikus reziliencia elméleti cikke négy alapelemre bontja a rezilienciát, a megérzésre, a monitorozásra, a reagálásra és a tanulásra. Bár nem kizárólag kritikus infrastruktúra rendszerekre fókuszál, a tanulmányt gyakran alkalmazzák a kritikus infrastruktúrák működésbiztonságának értékelésére. A szerző szerint a szervezetek rezilienciája erősebben meghatározza a zavarok túlélését, mint a puszta védelmi intézkedések. [131]

Johansson, Hassel és Cedergren 2011-es tanulmánya a kritikus infrastruktúrák sérülékenységének elemzésére fókuszál, különös tekintettel az ágazatok közötti interdependenciákra, amelyeket egy konkrét és rendkívül komplex esettanulmány a svéd vasúti rendszer segítségével mutat be. A cikk alapfeltevése, hogy a modern infrastruktúrák annyira összekapcsoltak és kölcsönösen egymásra utaltak, hogy egyetlen ágazat izolált vizsgálata nem képes reális képet adni a valós működési kockázatokról.

A svéd vasúti rendszer választása indokolt, a vasúti hálózat működését nagymértékben befolyásolják más kritikus infrastruktúrák, például az energiaellátás, az információs és irányítási rendszerek, a kommunikációs hálózatok, valamint a logisztikai és meteorológiai szolgáltatások. A kutatás célja annak megértése, hogyan idézhet elő egy látszólag kis, lokális zavar nagy területű, országos hatásokat az összekapcsolt rendszerek miatt.

A tanulmány egyik legfontosabb hozzájárulása, hogy részletes módszertani keretet mutat be az interdependenciák elemzésére. A szerzők egyrész strukturális elemzést végeznek, amely feltérképezi a különböző infrastruktúra elemek közötti kapcsolati hálót, másrészt funkcionális elemzést, amely a zavarok terjedésének mechanizmusait vizsgálja.

A kutatás során többféle függőség típust azonosítanak, például a fizikai úgy, mint áramellátás szükségessége a váltók és jelzők működtetéséhez, az információs úgy, mint forgalomirányító rendszerek, és az operatív függőségeket úgy, mint személyzeti rendelkezésre állás, logisztikai támogatás. A szerzők rámutatnak, hogy ezek a függőségek gyakran nemlineáris kockázati hatásokat okoznak, mivel egy kisebb meghibásodás is gyorsan láncreakciót válthat ki a hálózatban. A modell különösen fontos megállapítása, hogy a vasúti rendszer sérülékenysége nem feltétlenül azon elemeknél a legnagyobb, amelyek a legkritikusabb funkciót töltik be, hanem ott, ahol a legtöbb interdependencia fut össze.

A tanulmány szimulációkat is alkalmaz az infrastruktúrák közötti zavarátvitel megértésére, és a különböző meghibásodási forgatókönyvek alapján elemzi azok következményeit. Ezek a szimulációk kimutatják, hogy a vasút működését leginkább az energiaellátásban bekövetkező zavarok, valamint az informatikai és kommunikációs rendszerek hibái veszélyeztetik. A kutatás egyik fontos tanulsága, hogy a kockázatértékelés során a láncreakciók és az egyre növekvő meghibásodások vizsgálata kritikus fontosságú, mivel ezek képesek a normál működést percek alatt teljesen ellehetetleníteni. A szerzők továbbá kiemelik, hogy a szervezeti és irányítási folyamatok, mint például a válságkommunikáció, a hibadetektálás, és az üzemirányítás legalább annyira fontosak a rendszer rezilienciájának szempontjából, mint a technikai komponensek.

A tanulmány a gyakorlati alkalmazhatóság szempontjából is jelentős. A szerzők konkrét javaslatokat fogalmaznak meg a svéd vasúti rendszer rezilienciájának növelésére úgy, mint a redundáns energiaellátási pontok kiépítése, a rugalmasabb kommunikációs protokollok és több forrásból származó információk integrált monitorozása, illetve alternatív működési forgatókönyvek fejlesztése. Ezek az ajánlások túlmutatnak a vasútrendszeren, és általánosíthatók más kritikus szervezetekre is, amelyek több ágazatból származó inputokra támaszkodnak.

A cikk összegzése szerint a kritikus infrastruktúrák sérülékenységének értékelése csak akkor lehet valósághű és hasznos, ha az interdependenciák mélyreható vizsgálatára épül, és nem csupán az egyes komponensek meghibásodási valószínűségére koncentrál. Ez a szemlélet teljes mértékben összhangban áll a modern ágazati kockázatelemzés és a kritikus szervezetek rezilienciája megközelítésével, amely szerint a kockázat az ágazatok közötti kapcsolódási pontokon keletkezik, és ott terjed tovább. [132]

A kritikus infrastruktúra kockázatkezelésének döntéselemzéséről szóló 2013-as kézikönyv a döntéselemzés eszközeit alkalmazza a kritikus infrastruktúrák kockázatkezelésében. A szerzők többszempontú döntési modelleket mutatnak be, amelyek támogatják a védekezési intézkedések rangsorolását erőforrás korlátos környezetben. A cikk hangsúlyozza a bizonytalanság kezelését és a valószínűségi modellek alkalmazását. [133]

Arjen Boin és Michel van Eeten 2013-as cikkükben azt vizsgálják, miért vallanak gyakran kudarcot a hagyományos kritikus infrastruktúra védelmi megközelítések, és hogyan tehetők fenntarthatóbbá a kritikus szervezetek. A tanulmány szerint a szervezetek rugalmassága sokkal fontosabb, mint a merev védelmi protokollok. A cikk bemutatja a reziliens szervezet modelljét, amely a decentralizációt, tanulóképességet és adaptivitást helyezi előtérbe. Kiváló elméleti háttér a reziliencia, mint kulcskategória értelmezéséhez. [134]

A vizsgált tanulmányok átfogó képet adnak arról, hogyan fejlődött a kritikus infrastruktúrák és kritikus entitások kockázatelemzésének tudományos megközelítése az elmúlt két évtizedben. A klasszikus cikkek például Rinaldi, Peerenboom és Kelly, illetve Ouyang – megalapozták az interdependencia alapú gondolkodást, rámutatva, hogy a kritikus infrastruktúrák sérülékenységét nem elsősorban az egyedi komponensek gyengesége határozza meg, hanem az ágazatok közötti komplex kapcsolatrendszer. [29] Ezek a kutatások kimutatták, hogy a fizikai, információs, földrajzi és logikai függőségek olyan nemlineáris hatásmechanizmusokat hozhatnak létre, amelyek láncreakciós működés kieséshez vezetnek. A modern ágazati kockázatelemzés tehát nem értelmezhető interdependencia elemzés nélkül. [20]

A későbbi publikációk – például Johansson és munkatársai– tovább mélyítették ezt a szemléletet valós esettanulmányokon keresztül, amelyek rávilágítottak arra, hogy a kritikus infrastruktúrák működési zavarai gyakran ágazatközi eredetűek. A svéd vasúti rendszer elemzése jól szemlélteti, hogy a működésfolytonosság elsősorban nem a vasúti komponenseken, hanem a külső rendszerek – energiaellátás, kommunikáció, IT-irányítás – stabilitásán múlik. Ezek az eredmények megerősítik, hogy a kritikus entitások rezilienciája csak több szektor együtt vizsgálatával értékelhető érdemben. [132]

A szakirodalom másik markáns iránya a kiberreziliencia és a kiber és fizikai rendszerek kockázatelemzése. Ezek a tanulmányok kiemelik, hogy a digitalizáció miatt a kritikus infrastruktúrák sérülékenysége egyre inkább a kiberterületről ered, és a fizikai védelem önmagában már nem elegendő. A kockázatelemzést ezért integrált módon kell végezni, a fenyegetések, a sebezhetőségek és a kockázatok nem külön szakterületi szigetek, hanem összekapcsolódó tényezők, amelyek egymás hatását erősíthetik.

A reziliencia szemlélet fejlődését Ayeni & Oluwagbenga, és Lubis és még számos szerző képviseli, akik hangsúlyozzák, hogy a kritikus infrastruktúrák védelmének központi célja már nem a zavarok teljes megelőzése, hanem a rendszerek alkalmazkodó és helyreállító képessége. A reziliencia mérésére javasolt indexek és mutatók például a redundancia, a helyreállítási idő és az adaptivitás alkalmasak arra, hogy objektív alapot adjanak a kritikus szervezetek teljesítményének értékeléséhez. Ezzel párhuzamosan a szakirodalom, például Papamichael felhívja a figyelmet arra is, hogy a kockázatértékelés gyakorlati megvalósítása nagymértékben függ a szervezeti kultúrától, az információáramlástól és a döntéshozatal minőségétől.

Összességében a vizsgált kutatások egyértelmű trendet rajzolnak ki, a kritikus infrastruktúrák és kritikus szervezetek védelme ma már rendszerszintű, interdependenciákra épülő, multidiszciplináris megközelítést igényel. A kockázat ma már nem egyetlen ágazat belső tulajdonsága, hanem több hálózat, technológia és szervezet kölcsönhatásának eredője. Az ágazati kockázatelemzés ennek megfelelően csak akkor lehet hatékony, ha a fenyegetéseket és sebezhetőségeket nem izoláltan, hanem a teljes kritikus szervezetek és infrastruktúrák hálózatának részeként értelmezi.

Ez a szemlélet teljes mértékben összhangban áll a CER Irányelvvel és a magyar kritikus szervezetekre vonatkozó jogszabályokkal, amelyek a reziliencia és a kockázatkezelés integrált értelmezését teszik kötelezővé. További nemzetközi szakirodalmi és módszertani áttekintés a kritikus infrastruktúrák és kritikus szervezetek témájában a kockázatelemzésekkel összefüggésben a 7. mellékletben található.

2.4 Az ágazati kockázatelemzés módszertani keretének kidolgozása és fejlesztési irányai

Az ágazati kockázatelemzés bevezetése kiemelt jelentőségű a kritikus infrastruktúrák védelme és a nemzeti reziliencia erősítése szempontjából. A modern társadalmak működése egyre inkább összetett hálózatokra épül, ahol az energia-, víziközmű-, távközlési és közlekedési rendszerek egymással szoros kölcsönhatásban látják el feladataikat. Ebben a komplex környezetben elengedhetetlen egy olyan módszertani keretrendszer, amely rendszerszinten értékeli a fenyegetettségeket, a sérülékenységeket és a következményeket, és ezáltal átfogó képet ad a kritikus ágazatok állapotáról.

Az ágazati kockázatelemzés legfontosabb előnye, hogy képes egységes, összehasonlítható és átlátható kockázati képet kialakítani az összes releváns szereplőre vonatkozóan.

Míg a szervezeti szintű elemzések általában csak lokális szempontokat tárnak fel, az ágazati szintű megközelítés lehetőséget ad a kölcsönös függőségek, úgynevezett interdependenciák feltárására is.

Ez különösen fontos, mivel egyetlen meghibásodás vagy incidens, például egy gázellátási zavar, könnyen kihatással lehet a villamosenergia hálózatokra, a víziközmű szolgáltatásokra és akár az egész ellátási láncra. Az interdependenciák feltérképezése ezért kulcsfontosságú a dominóhatások megelőzése és a legkritikusabb pontok azonosítása szempontjából.

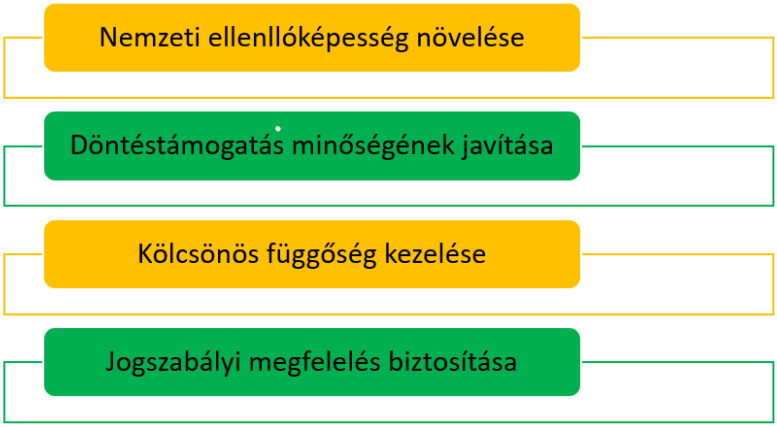
Az ágazati kockázatelemzés másik jelentős előnye, hogy hatékony döntéstámogatást nyújt a stratégiai és operatív szintű irányítás számára. Az súlyozott értékelés révén a döntéshozók pontos képet kapnak az egyes szervezetek kockázati profiljáról, ami lehetővé teszi az intézkedések rangsorolását. Ez különösen fontos az erőforrások optimális elosztásához, hiszen a véges pénzügyi és humán kapacitások oda irányíthatók, ahol a legnagyobb biztonsági hatás érhető el. Az ágazati elemzések eredményei egyúttal hozzájárulnak a nemzeti kockázatkezelési stratégiákhoz is, mivel összehangolják a különböző szervezetek, hatóságok és ágazatok intézkedéseit.

A módszertan illeszkedik az uniós és hazai szabályozási keretekhez, beleértve a NIS2, a CER és a DORA irányelveket, valamint a Kszetv.-t. Ez azt jelenti, hogy az ágazati kockázatelemzés alkalmazásával a szervezetek nemcsak belső biztonsági szintjüket erősítik, hanem biztosíthatják jogszabályi megfelelésüket is. Az egységesített metodikai alapok előnye, hogy az elkészített kockázati jelentések nemzetközi szinten is összehasonlíthatóvá válnak, ami megkönnyíti a határon átnyúló infrastruktúrák védelmét és a nemzetközi együttműködést.

Az ágazati szintű megközelítés további értéke, hogy lehetőséget biztosít korai figyelmeztetési és monitoring rendszerek kiépítésére. A módszertan alapján meghatározott indikátorok és kockázati küszöbértékek lehetővé teszik a valós idejű fenyegetésfigyelést, amely segíti a gyors reagálást kritikus helyzetekben. Ezzel összhangban az ágazati kockázatelemzés a fizikai és kiberbiztonsági dimenziókat is integrálja, így olyan kombinált kockázati térképet biztosít, amely figyelembe veszi az összes lényeges veszélyt. [6]

Mindezek mellett az ágazati kockázatelemzés elősegíti a válságkezelési képességek fejlesztését és a helyreállítási folyamatok hatékonyságát. A forgatókönyv alapú stressztesztek révén pontosan modellezhetők azok a helyzetek, amikor több kritikus infrastruktúra egyszerre sérül, és így a szervezetek felkészültebben tudják kezelni a válsághelyzeteket.

Az elemzés ösztönzi a kockázati kultúra fejlesztését is az ágazaton belül, a szereplők közötti adatmegosztás, az egységes terminológia és a közös metodikai alapok megerősítik az ágazaton belüli együttműködést.



9. ábra: Ágazati kockázatelemzés előnyei, Készítette: a Szerző, 2025.

Összességében az ágazati kockázatelemzés bevezetése egyértelműen hozzájárul a nemzeti reziliencia növeléséhez, a döntéstámogatás minőségének javításához, a kölcsönös függőségek kezeléséhez és a jogszabályi megfelelés biztosításához. A módszertan alkalmazásával átfogó, adatvezérelt és összehasonlítható kockázati profilok hozhatók létre, amelyek megalapozzák a hatékony stratégiai tervezést és lehetővé teszik a proaktív kockázatkezelést. Ez a megközelítés nemcsak a jelenlegi fenyegetések kezelésében nyújt előnyt, hanem kulcsszerepet játszik a jövőbeli kihívásokra való felkészülésben is.

Javaslatom alapján a kritikus szervezetek és infrastruktúrák ágazati kockázatelemzése olyan átfogó folyamat, amely azonosítja, értékeli és rangsorolja az adott ágazaton belüli infrastruktúrát érintő kockázatokat. Az elemzés elkészítése létfontosságú a lakosság, a gazdaság és a nemzetbiztonság számára fontos alapvető szolgáltatások ellenálló képességének és biztonságának biztosításához.

2.4.1 Az ágazati kockázatelemzés intézményi és szereplői modellje

Az ágazati kockázatelemzést a jelenleg hatályos rendszerben az ágazati szakhatóság végezné el, a kritikus szervezetek és szakmai szervek bevonásával. A felelős hatóság a nemzeti kockázatelemzést követően készül el az ágazati kockázatelemzés, ami évente kerül felülvizsgálatra minden év május 15-ig. Az ágazati kockázatelemzés segítségével:

- prioritást állíthatunk fel annak rangsorolására, hogy az ágazaton belül mely eszközök vagy rendszerek a legkritikusabbak és legsebezhetőbbek. Ez segít az erőforrások hatékony elosztásában a legfontosabb infrastrukturális elemek védelme érdekében.

- releváns információt kapunk a felkészültségi és reagálási stratégia kidolgozásához és a tervek kidolgozásához, a zavarok megelőzése, az azokra történő reagálás és helyreállítás érdekében.

Az ágazati kockázatelemzés hatékonyságának növelése érdekében javasolt lenne megalakítani az Ágazatközi Reziliencia Munkacsoportot (a továbbiakban: ÁRM). Ennek célja, hogy összehozza a kritikus szervezeteket különböző ágazatainak szakértőit, hogy megvitassák és értékeljék a közös kockázatokat és egymásrautaltságokat. Ez a munkacsoport elősegíti az átfogó kockázatkezelési stratégiák és ágazati kockázatelemzés kidolgozását, amelyek figyelembe veszik az ágazatok közötti kölcsönös függőségeket és a dominóhatásokat. A munkacsoport évente ülésezik, amit lebonyolít minden év április 15-ig. A munkacsoport ülésen elhangzottakat az ágazatok be tudják építeni az ágazati kockázatelemzésükbe. Az ÁRM tagjai a kijelölő hatóságok, javaslatevő hatságok vagy ágazati szakhatóságok és kijelölő hatóságok által delegált szakértők.

Javaslatom alapán a kritikus szervezetek ágazati kockázatelemzését az alábbiak szerint szükséges végrehajtani, lefolytatni:

1. A kritikus eszközök és funkciók azonosítása:

a) Kritikus eszközök: Az első lépés az ágazat működése szempontjából kulcsfontosságú fizikai és kibereszközök azonosítása. Ezek közé tartoznak azok a létesítmények, rendszerek, hálózatok és technológiák, amelyek megzavarása jelentős következményekkel járhat.

b) Kritikus funkciók: A fizikai eszközökön túl elengedhetetlen az ágazat által nyújtott kulcsfontosságú funkciók és szolgáltatások azonosítása, amelyek kritikusak a működés és a szolgáltatásnyújtás fenntartása szempontjából [87].

2. Fenyegetettségi értékelés:

a) Természeti fenyegetések: Értékelje a természeti veszélyek, például földrengések, árvizek, szélsőséges időjárás és világjárványok valószínűségét és lehetséges hatását, amelyek megzavarhatják az üzemfolytonosság fenntartását.

b) Ember által okozott veszélyek: Az emberi tevékenységek által okozott kockázatok értékelése, beleértve a terrorizmust, a szabotázst, a kibertámadásokat és a baleseteket. Ez magában foglalja a geopolitikai kockázatok és a lehetséges ellenséges fellépések értékelését is.

c) Technológiai fenyegetések: A rendszerhibákból, technológiai meghibásodásokból vagy elavulásból eredő kockázatok mérlegelése.

3. Sebezhetőségi értékelés:

a) Fizikai sebezhetőségek: A fizikai infrastruktúra gyenge pontjainak meghatározása, mint például az elöregedett infrastruktúra, a redundancia hiánya vagy a rossz karbantartás, amelyeket a fenyegetések kihasználhatnak.

b) Kiberbiztonsági sebezhetőségek: Értékelje az ágazat kiberbiztonsági helyzetét, beleértve a kibertámadások lehetséges belépési pontjait, a szoftver és a hardver gyengeségeit, valamint az adatvédelem sebezhetőségeit.

c) Szervezeti sebezhetőségek: Vizsgálja meg az ágazat felkészültségét és képességét a zavarokra való reagálásra, beleértve az irányítás, a politikák és az incidensekre való reagálási tervek hatékonyságát.

4. Hatáselemzés:

a) Gazdasági hatás: Elemezze a zavarok lehetséges gazdasági következményeit, beleértve a leállások, a javítás és a helyreállítás költségeit, valamint a gazdaságra gyakorolt szélesebb körű hatásokat.

b) Működési hatás: Annak értékelése, hogy a zavarok hogyan befolyásolhatják az ágazatnak a kritikus funkciók és szolgáltatások fenntartására vonatkozó képességét.

c) Társadalmi és politikai hatás: Vegye figyelembe a közbiztonságra, az egészségügyre és a kormányzati intézményekbe vetett bizalomra gyakorolt lehetséges hatásokat, valamint a nemzetbiztonságra gyakorolt tágabb hatásokat. [88]

5. Kölcsönös függőségek és dominóhatások:

a) Ágazatok közötti kölcsönös függőségek: Az ágazatok közötti kölcsönös függőségek azonosítása és értékelése. Például, hogy az energiaágazatban bekövetkező zavar hogyan hathat a távközlésre, a közlekedésre vagy az egészségügyre.

b) Dominóhatás: Mérlegelje, hogy az egyik ágazatban bekövetkező incidens hogyan válthat ki dominó szerű meghibásodásokat más ágazatokban, ami szélesebb körű zavarokhoz vezethet. [89]

2. Kockázatértékelés és rangsorolás:

a) Kockázati pontozás: Használjon kockázati mátrixot vagy hasonló eszközöket a kockázatok valószínűségük és potenciális hatásuk alapján történő pontozásához. Ez segít

annak rangsorolásában, hogy mely kockázatok igényelnek azonnali figyelmet és erőforrásokat.

b) Kritikus kockázatok azonosítása: Azonosítsa a legkritikusabb kockázatokat, amelyekkel foglalkozni kell az ágazat eszközeinek és funkcióinak védelme érdekében. [90]

6. Enyhítő intézkedések és stratégiák

a) Kockázatcsökkentési stratégiák: Az azonosított kockázatok mérséklésére irányuló stratégiák kidolgozása és végrehajtása, például a fizikai biztonság fokozása, a kiberbiztonsági intézkedések javítása és a redundancia beépítése a rendszerekbe.

b) Felkészültségi és reagálási tervek: Átfogó vészhelyzeti felkészültségi és reagálási tervek létrehozása és fenntartása az eseményekre való gyors és hatékony reagálás biztosítása érdekében.

c) Képzések és gyakorlatok: Rendszeres képzés és gyakorlatok végrehajtása a reagálási tervek hatékonyságának tesztelése és annak biztosítása érdekében, hogy minden érdekelt fél felkészült legyen az eseményekre való reagálásra. [91]

7. Folyamatos nyomon követés és felülvizsgálat:

a) Folyamatos nyomon követés: Rendszerek bevezetése a fenyegetések, a sebezhetőségek és az enyhítő intézkedések hatékonyságának folyamatos nyomon követésére.

b) Időszakos felülvizsgálat: A kockázatelemzés rendszeres felülvizsgálata és frissítése az új fenyegetések, az infrastruktúrában bekövetkezett változások vagy az üzemeltetési környezetben bekövetkezett változások figyelembevétele érdekében. [92]

8. Az érdekelt felek bevonása és együttműködés:

a) Szereplők közötti partnerségek: Az üzemeltetőkkel való együttműködés, mivel az elengedhetetlen az információk, erőforrások és legjobb gyakorlatok megosztásához.

b) Intézmények közötti együttműködés: Koordináció más kormányzati szervekkel, helyi hatóságokkal és nemzetközi partnerekkel a kritikus szervezetek védelmének egységes megközelítése érdekében. [93]

A kritikus szervezetek ágazati kockázatelemzésének elvégzése magában foglalja a lehetséges fenyegetések, sebezhetőségek és hatások részletes vizsgálatát, majd a kockázatok csökkentésére irányuló stratégiák kidolgozását. Ez a folyamat alapvető fontosságú a társadalom által igényelt kritikus szolgáltatások védelméhez és az infrastruktúra ellenálló képességének biztosításához a különböző kihívásokkal szemben. [94]

A kockázatelemzés elvégzését követően szükséges egy priorizált lista felállítása, ami megkönnyíti a védelem kialakítását. A lista elkészítésének fő szempontja az ágazatok közötti kölcsönös függőségek feltárása. Egyes ágazatok magasabb prioritást kaphatnak, ha azok kockázata dominóhatást válthat ki más ágazatokban, nincs ez másként egy adott ágazaton belüli rendszerelemekkel.

A rendszerelemeket a kockázati pontszámaik és az egymásra gyakorolt hatásuk alapján rangsorolják. A rendszerelem, amelyik a legnagyobb összetett kockázattal bír, az első helyre kerül, majd ezt követik a kevésbé kockázatos infrastruktúrák. [22]

15. táblázat: Súlyozási metodika a prioritás felállítására, Készítette: a Szerző, 2025.

Rendszerelem megnevezése	**XY**	**WY**	**ZY**
Kritikus szolgáltatásoktól és erőforrásokól történő függőség	1-5	1-5	1-5
Fizikai és infrastrukturális kapcsolódása (energia, víz)	1-5	1-5	1-5
Fizikai sérülékenysége egy esetleges támadás során	1-5	1-5	1-5
Ellátási láncban betöltött szerepe	1-5	1-5	1-5
Technológiai függőség	1-5	1-5	1-5
Dominóhatások	1-5	1-5	1-5
Helyreálló képessége támadás után, időbeni függőség	1-5	1-5	1-5
Rendszerszintű kockázatok	1-5	1-5	1-5
Összesen	**Max 20**	**Max 20**	**Max 20**

Az ágazatok közötti kölcsönös függőségi viszonyok meghatározásakor az alábbi szempontokat érdemes figyelembe venni:

1. Kritikus szolgáltatások és erőforrások: Azonosítani kell, hogy mely infrastruktúrák nyújtanak olyan alapvető szolgáltatásokat vagy erőforrásokat, amelyek más ágazatok működéséhez elengedhetetlenek pl. energiaellátás, vízellátás, telekommunikáció.
2. Fizikai és infrastrukturális kapcsolódások: Figyelembe kell venni, hogy az ágazatok fizikai infrastruktúrái hogyan kapcsolódnak egymáshoz, például közös infrastruktúraelemek, mint a közlekedési hálózatok, adatközpontok vagy elektromos hálózatok.
3. Fizikai sérülékenysége egy esetleges támadás során: A kritikus infrastruktúrák épülete vagy bázisa egy támadás során milyen mértékben sérülne, az mennyire lenne hatással annak működésére.
4. Ellátási láncban betöltött szerepe: Az ellátási láncok vizsgálata kulcsfontosságú az adott ágazatban, hogy megértsük, hogyan függnek egymástól a különböző iparágak alapanyagok, termékek, vagy szolgáltatások szállítása során.
5. Technológiai függőségek: Meg kell vizsgálni, hogy az ágazat milyen mértékben függnek bizonyos technológiáktól vagy informatikai rendszerektől, amelyek más ágazatokban működnek.
6. Dominóhatás: Fontos felmérni, hogy egy adott ágazatban bekövetkező zavarok milyen láncreakciókat indíthatnak el más ágazatokban. Például egy áramszünet milyen hatással lehet a telekommunikációra, a közlekedésre, vagy az egészségügyi szolgáltatásokra.
7. Helyreálló képessége támadás után, időbeni függőség: Az is lényeges, hogy az ágazat és infrastruktúrái közötti függőségek időben hogyan alakulnak. Egyes függőségek azonnali hatást váltanak ki, míg mások hosszabb idő alatt fejthetik ki hatásukat. Egy esetleges támadás során milyen gyorsan lehet helyreállítani annak működését.
8. Rendszerszintű kockázatok: Végül, a rendszerszintű kockázatok, például a természeti katasztrófák vagy kibertámadások, amelyek egyszerre több ágazatot is érinthetnek, különösen fontosak az összefüggések feltérképezésében. [95]

Ezek a szempontok hozzájárulnak a kölcsönös függőségek pontos azonosításához, ami alapot adhat az integrált kockázatkezelési stratégiák kidolgozásához. A rendszerelem tulajdonságaitól függően szakmai szempontból kell értékelni az adott rendszerelemet, szervezetet.

A súlyozás során 1-5-ig tudunk értéket párosítani az adott tényezőhöz, értelemszerűen az egy a legkisebb érték, ami jellemző rá és az 5 a maximális, ami nagyon jellemző. Maximálisan 20 értékpontot kaphatunk. [96]

2.4.2 Az ágazati kockázatelemzés implementációs modelljének elemzése

A fejezetrész célja a Magyarországon alkalmazható ágazati kockázatelemzés módszertanának kidolgozása, amely összehangolt a nemzetközi szabályokkal (ISO 31000, ISO/IEC 31010, ISO/IEC 27005), valamint megfelel az uniós jogi környezetnek (CER Irányelv, NIS2, DORA) és integrálja a magyar szabályozási környezetet és technikailag megalapozott, transzparens súlyozási szempontrendszert alkalmaz az értékeléshez. [97]

A javasolt ágazati kockázatelemzés alatt a kockázat a célok bizonytalanságából fakadó hatását, egy adott ágazat pl. energia, közlekedés, pénzügy, víz stb. keresztmetszeti, többszereplős, all-hazard szemléletű, interdependencia érzékeny kockázatelemzést értek. [98]

A szabályozási keret a nemzetközi szabványokra tekintettel, azaz az ISO 31000:2018 kockázatmenedzsment-elvárások, az ISO/IEC 31010:2019 kockázatértékelési technikák, az ISO/IEC 27005:2022 információbiztonsági kockázatmenedzsment figyelembevételével. Az európai uniós keret során a CER Irányelv, a NIS2 és a DORA rendeletetekkel is számolni kell, magyarországi kontextusban pedig a Kszektv-el, és az ahhoz kapcsolódó rendeletekkel, valamint a nemzeti kockázatelemzésről és stratégiáról szóló kormány határozatokkal egyaránt. [22]

Típusát illetően a minőségi, félkvantitatív vagy kvantitatív megközelítés kominációja ajánlott:

- Minőségi: Delphi, Bow-tie, HAZOP;
- Félkvantitatív: skálázott valószínűség×hatás mátrix, FMEA/FMECA;
- Kvantitatív: Monte Carlo szimuláció, bayesi hálók, hálózatelemzés (interdependenciák), input output és ágazati stressztesztek.

Ágazati szinten a hierarchikus hibrid megközelítés célszerű asset szintű módszerekből (FMEA/HAZOP) aggregált indikátorok, ezek ágazati kockázatelemzés szintű többkritériumos értékeléssel és hálózati rendszerszintű kockázatmodullal egészülnek ki. [89]

Azonban szükséges figyelembe venni, hogy az ágazati kockázatelemzés felhasználóbarát legyen, ne rójon többletmunkát sem a kritikus szervezetekre, sem a hatóságokra, így célom volt egy olyan könnyített kockázatelemzés létrehozása, ami gyorsan elvégezhető, átlátható és a kockázati profilokat összehasonlíthatóvá teszi az ágazat összes szereplője között. [99]

2.4.3 Az ágazati kockázatelemzés javasolt módszertani folyamatának modellalapú leírása

A disszertációban bemutatott egyszerűsített ágazati kockázatelemzés módszertana több, egymással összhangban álló nemzetközi szabványra és tudományos megközelítésre épül. Elméleti alapját az ISO 31000 kockázatmenedzsment-keretrendszere, az ISO/IEC 31010 kockázatértékelési technikákra vonatkozó iránymutatásai, valamint a NIST SP 800-30 ajánlásai adják, amelyek közös nevezője a kockázat valószínűségi és hatásoldali megközelítése. Ezeket egészíti ki a kritikus infrastruktúrák védelmével foglalkozó nemzetközi szakirodalom, különösen Rinaldi és munkatársai interdependencia elmélete, Utne ágazatközi sérülékenység elemzése, valamint a JRC által kidolgozott kritikus infrastruktúra kockázatelemzési keretek. A módszertan kialakításakor tudatos cél volt, hogy az elméleti megalapozottság mellett a gyakorlati alkalmazhatóság is biztosított legyen, különösen olyan környezetben, ahol az ágazati szereplők érettségi szintje, erőforrás ellátottsága és adat hozzáférése jelentős eltéréseket mutat. [146]

Az alkalmazott modell a kockázat klasszikus értelmezéséből indul ki, amely a fenyegetettség, a sérülékenység és a bekövetkezés következményeinek együttes vizsgálatán alapul. Ez a megközelítés széles körben elfogadott a kritikus infrastruktúrák kockázatelemzésében, ugyanakkor a disszertációban bemutatott eljárás ezt egy normalizált, egyszerűsített formában alkalmazza annak érdekében, hogy ágazati szinten is aggregálható, összehasonlítható eredmények szülessenek. Az indikátorkészlet tudatos redukálása jellemzően öt–nyolc alapmutatóra nem a módszertani mélység csökkentését célozza, hanem az értékelés skálázhatóságát és széles körű bevezethetőségét. Ez az elv összhangban áll az OECD és az ENISA által is hangsúlyozott minimumszintű, de egységes kockázatértékelési megközelítésekkel, amelyek szerint az ágazati lefedettség és az összehasonlíthatóság elsődleges fontosságú a nemzeti szintű döntéstámogatás szempontjából. [38]

A módszertan eljárási logikája az egységes skálázás és az átlátható számítási szabályok alkalmazására épül. Az indikátorok 1–5 közötti ordinális skálán történő értékelése az ISO/IEC 31010 által is elfogadott gyakorlat, amely lehetővé teszi a szakértői becslések strukturált bevonását anélkül, hogy túlzott adatigényt támasztana. A kockázati érték normalizálása – a maximálisan elérhető pontszámhoz viszonyítva – biztosítja, hogy az eredmények egységes 0 és 1 közötti tartományba essenek, ezáltal egyszerűen kategorizálhatók és vizuálisan is jól megjeleníthetők. Ez a megoldás kifejezetten alkalmas ágazati kockázati profilok kialakítására, valamint különböző szervezetek és alágazatok közötti összehasonlításra. [143]

A disszertációban bemutatott egyszerűsített kockázatelemzési modell nem önálló, zárt megoldásként értelmezendő, hanem egy többlépcsős ágazati kockázatelemzési rendszer alap rétegeként. Funkciója elsősorban az, hogy egységes adatgyűjtési és önértékelési keretet biztosítson minden kritikus szervezet számára, beleértve a kisebb, korlátozott erőforrásokkal rendelkező szolgáltatókat is. E felépítés lehetővé teszi, hogy az ágazati kockázatelemzés egyszerre legyen széles körben alkalmazható és tudományosan megalapozott, miközben megfelel a hazai és uniós szabályozási elvárásoknak is. Az egyszerűsített ágazati kockázatelemzés számítási modellje a kockázat klasszikus, nemzetközileg elfogadott értelmezésére épül, amely szerint a kockázat a fenyegetések bekövetkezési valószínűségének és a várható következményeknek a függvénye, kiegészítve a rendszer sérülékenységének vizsgálatával. A disszertációban alkalmazott modell ezen elméleti alapokat adaptálja egy olyan formában, amely ágazati szinten is összehasonlítható és aggregálható eredményeket biztosít.

A kockázat számszerűsítésére az alábbi összefüggés kerül alkalmazásra:

A módszertan három fő komponensre épül:

Fenyegetettség (F) x Sérülékenység (S) x Hatás/Következmény (H).

Az indikátorok száma jelentősen csökkenthető, például mindössze 5-8 tényezőre, amelyet a szolgáltatók és hatóságok 1-től 5-ig terjedő skálán értékelnek. Az indikátorok száma szándékosan alacsony, hogy kisebb szervezetekre is könnyen lehessen alkalmazni. Az összes indikátor maximum 4-5 tényező.

16. táblázat: Összefoglaló táblázat a kockázatelemzésről

Készítette: a Szerző, 2025.

Dimenzió	**Indikátor**	**Értékelési skála (1–5)**	**Példa**
Fenyegetettség (F)	Külső támadások, időjárási szélsőségek, technológiai hibák	1 = ritka, 5 = gyakori	Árvíz, kiberincidens
Sérülékenység (S)	Biztonsági érettség, tartalék kapacitások	1 = magas ellenállóképesség, 5 = alacsony	Redundáns vízbázis
Hatás (H)	Ellátáskimaradás következménye	1 = minimális, 5 = súlyos	Regionális áramszünet
Interdependencia (I)	Más ágazatoktól való függőség	1 = alacsony, 5 = kritikus	Vízszivattyú energiaellátása

Az összesített kockázati szintet egy egyszerű szorzatos képlet adja:

$$R = \frac{F\ x\ S\ x\ H}{125}$$

ahol R az adott szervezet vagy infrastruktúra normalizált kockázati értéke, F a fenyegetettség mértéke, SS a sérülékenység mértéke, míg H a bekövetkező esemény várható hatását fejezi ki. Mindhárom tényező 1–5 közötti ordinális skálán kerül értékelésre. A képlet számlálójában szereplő szorzat a kockázati tényezők együttes hatását fejezi ki, míg a nevezőben szereplő 125 a maximálisan elérhető pontszám (5×5×5), amely a kockázati érték normalizálását szolgálja. [100] A normalizálás célja kettős. Egyrészt biztosítja, hogy a kockázati értékek 0 és 1 közötti tartományban helyezkedjenek el, ami megkönnyíti a különböző szervezetek, alágazatok és ágazatok közötti összehasonlítást. [143] Másrészt lehetővé teszi az egységes küszöbértékek meghatározását, amelyek alapján a kockázatok kategóriákba sorolhatók. Ez a megközelítés különösen előnyös ágazati szinten, ahol nem egyedi, hanem rendszerszintű kockázati képre van szükség. [88]

A fenyegetettség (F) értéke az adott ágazatra jellemző külső és belső veszélyforrások gyakoriságát és intenzitását fejezi ki. Ide tartozhatnak természeti eredetű veszélyek, technológiai meghibásodások, kiberfenyegetések vagy ellátási lánc zavarai. A sérülékenység (S) azt mutatja meg, hogy az adott szervezet vagy infrastruktúra milyen mértékben képes ellenállni ezeknek a fenyegetéseknek, figyelembe véve a meglévő védelmi intézkedéseket, redundanciákat és szervezeti felkészültséget. [118] A hatás (H) a szolgáltatás kiesésének vagy romlásának társadalmi, gazdasági és biztonsági következményeit ragadja meg. A három tényező szorzása azt az alapfeltevést tükrözi, hogy a kockázat csak akkor válik jelentőssé, ha mindhárom komponens egyidejűleg magas értéket vesz fel. [6]

A képlet alkalmazhatósága elsősorban a gyors, felhasználóbarát kockázatértékelésekben mutatkozik meg. Előnye, hogy kis adatigénnyel működik, nem igényel komplex statisztikai vagy hálózatelemzési előkészítést, és lehetővé teszi a kisebb, alacsonyabb érettségű szervezetek bevonását is az ágazati kockázatelemzési folyamatba. Ugyanakkor a modell korlátja, hogy az ordinális skálák használata óhatatlanul bizonytalanságot hordoz, különösen a sérülékenységi és hatásértékek szakértői becslése esetén. [118]

A rendszerszintű kockázatok jobb megragadása érdekében a modell opcionálisan kiegészíthető egy interdependencia-korrekciós tényezővel, amely az ágazatok közötti kölcsönös függőségeket veszi figyelembe:

$$R^* = R \cdot (1 + \beta \cdot I)$$

ahol R∗ az interdependenciákkal korrigált kockázati érték, I az interdependencia mértéke 1–5 skálán, míg β egy ágazatspecifikus súlyparaméter. Ez a kiegészítés azon a felismerésen alapul, hogy a kritikus infrastruktúrák működése erősen hálózatos jellegű, és egyetlen rendszer meghibásodása más ágazatokban is jelentős következményekkel járhat. A korrekciós tényező koncepcionálisan illeszkedik a Rinaldi-féle interdependencia-modellhez és a JRC által javasolt dominóhatás-érzékeny kockázati megközelítésekhez. [148]

Az interdependencia-modul alkalmazása növeli a modell realitását, ugyanakkor újabb bizonytalansági tényezőt is bevezet. Az I értékének meghatározása gyakran szubjektív szakértői becslésen alapul, míg a β paraméter megválasztása ágazatonként eltérő lehet, és empirikus adatok hiányában nehezen kalibrálható. Emiatt a disszertáció hangsúlyozza, hogy az interdependencia-korrekció elsősorban döntéstámogató, nem pedig abszolút kockázati érték meghatározására szolgál. [149]

A normalizált kockázati értékek értelmezését és gyakorlati felhasználását a következő küszöbérték-alapú besorolás segíti:

$$Kockázati\ kategória = \begin{cases} Alacsony\ R \leq 0{,}30 \\ Közepes\ 0{,}30 < R \leq 0{,}60 \\ Magas\ R > 0{,}60 \end{cases}$$

E küszöbértékek nem abszolút biztonsági határértékek, hanem döntéstámogató orientációs pontok, amelyek lehetővé teszik a kockázatok gyors priorizálását. A kategorizálás célja, hogy az ágazati döntéshozók számára egyértelmű jelzést adjon arról, mely szervezetek vagy infrastruktúrák igényelnek azonnali beavatkozást, további részletes elemzést vagy fokozott monitoringot. [88]

Összességében a bemutatott képletek egy olyan számítási keretet alkotnak, amely egyensúlyt teremt a módszertani egyszerűség és a rendszerszintű gondolkodás között. Bár a modell nem képes a kritikus infrastruktúrák minden komplex összefüggését teljes mértékben leképezni, alkalmas arra, hogy egységes alapot biztosítson az ágazati kockázatelemzéshez.

Példa számítás:

- F = 4 (magas fenyegetettség)
- S = 3 (közepes sérülékenység)

- H = 5 (kritikus következmény)

$$R = \frac{4\ x\ 3\ x\ 5}{125} = 0{,}48 \rightarrow közepes\ kockázat.$$

A módszer célja, hogy a végfelhasználó egyszerű kockázati térképet kapjon:

- Zöld (R ≤ 0,3): alacsony kockázat
- Sárga (0,3 < R ≤ 0,6): közepes kockázat
- Piros (R > 0,6): magas kockázat

A jelentés mindössze egyoldalas, tartalmazva:

- a legkritikusabb indikátorokat,
- a szervezet R-pontszámát,
- az ágazati átlaghoz viszonyított helyzetet. [101]

További számítási példák az ágazati kockázatelemzés alkalmazására a 9. mellékletben található.

17. táblázat: *Az egyszerűsített módszertan és egy komplex módszertan összehasonlítása*
Készítette: a Szerző, 2025.

Szempont	**Komplex módszertan**	**Egyszerűsített módszertan**
Indikátorok száma	20–40	5–8
Adatigény	Nagy	Alacsony
Súlyozás	Hibrid (szakértői + adatvezérelt)	Egyszerű, fix súlyozás
Kimenet	Többlépcsős aggregált érték	Egyértelmű R-pontszám
Alkalmazhatóság	Szabályozói, kutatói környezetben ideális	Gyors ágazati felmérésekhez ideális
Felhasználói csoport	Döntéshozók, kutatók	Szolgáltatók, kisebb üzemeltetők

Az ágazati kockázatelemzés hagyományos, komplex módszertana pontos, reprodukálható és tudományosan megalapozott eredményeket nyújt, azonban jelentős adat-, idő- és erőforrásigénnyel jár.

Az ágazatokban működő kisebb szolgáltatók, például helyi víziközmű-társaságok vagy regionális energiaelosztók gyakran nem rendelkeznek azzal a kapacitással, amely szükséges a több száz indikátorra épülő részletes kockázatelemzések elvégzéséhez.

Az egyszerűsített ágazati kockázatelemzés egy olyan módszertani alternatíva, amely lehetővé teszi, hogy az ágazat összes szereplője függetlenül a mérettől és technikai felkészültségtől összehasonlítható módon mérje fel a saját kockázatait. A módszer célja tehát a gyors, felhasználóbarát, standardizált kockázatértékelés, ami egyszerű adatszolgáltatási alapot biztosít az országos szintű elemzésekhez és a kritikus szerveztek védelmének kialakításához.

Az egyszerűsített kockázatelemzés célja, hogy minimális számú indikátort használjon, ugyanakkor lefedje a legfontosabb ágazati kockázatokat. Az értékelés során 5–8 kulcstényezőt javasolt figyelembe venni.

18. táblázat: Javasolt indikátorrendszer,

Készítette: a Szerző, 2025.

Dimenzió	**Indikátor**	**Értékelési skála (1–5)**	**Példa energiaágazatban**	**Példa víziközmű-ágazatban**
Fenyegetettség (F)	Külső események (időjárás, kiber, ellátási lánc)	1 = ritka, 5 = gyakori	Villamoshálózati meghibásodás	Árvíz okozta vízbázis-szennyezés
Sérülékenység (S)	Biztonsági szint, redundancia, tartalékok	1 = magas ellenállóképesség, 5 = alacsony	Tartalékerőművek száma	Ivóvízbázisok diverzifikáltsága
Hatás (H)	Ellátáskimaradás vagy szolgáltatáskiesés következménye	1 = minimális, 5 = súlyos	Regionális áramszünet hatása	Települési vízhiány
Interdependencia (I) (opcionális)	Más ágazatoktól való függés	1 = alacsony, 5 = kritikus	Gázüzemű erőművek gázellátása	Víztisztítók energiafüggése

Az opcionális interdependencia indikátor akkor használható, ha az ágazati szereplőnél jelentős a más rendszerektől való függés. [102]

A kockázatelemzés kimeneteként az R-pontszám egyértelműen besorolja a szervezetet három kockázati kategóriába:

19. táblázat: Kockázati szintek

Készítette: a Szerző, 2025.

R-pontszám	Kockázati szint	Ajánlott intézkedések
0,00 – 0,30	**Alacsony**	Alapszintű monitoring, folyamatos adatszolgáltatás
0,31 – 0,60	**Közepes**	Kockázatcsökkentő módszerek priorizálása
0,61 – 1,00	**Magas**	Azonnali kockázatkezelési terv, erőforrás-átcsoportosítás

Ez a megközelítés nemcsak egyszerűsíti az értékelést, hanem összehasonlíthatóvá teszi az ágazat minden szereplőjének eredményeit. [103]

2.4.4 Az ágazati kockázatelemzéssel összefüggő jelentések struktúrája és vizualizációs eszközei

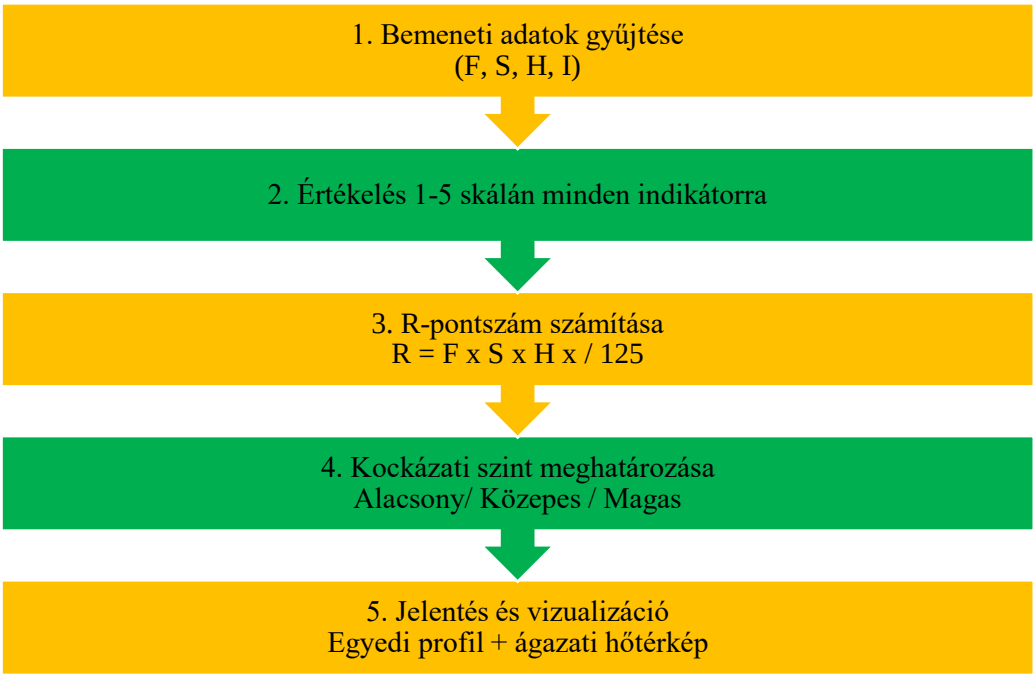
Az egyszerűsített kockázatelemzés alkalmazásával minden szolgáltató számára egységes kockázati jelentési sablon készíthető, amely tartalmazza:

- a szolgáltató R-pontszámát,
- a kockázati szintjét,
- a legkritikusabb tényezőket,
- a javítási prioritásokat.

Ehhez kapcsolódhat egy hőtérkép, amely az ágazat összes szereplőjét elhelyezi egy vizuális kockázati mátrixon, segítve a döntéshozókat a prioritások meghatározásában.

Előnye:

- Gyors végrehajtás, egyszerű kérdőíves felmérés, akár 1–2 órán belül elvégezhető.
- Felhasználóbarát, nem igényel mély statisztikai vagy hálózatelemzési tudást.
- Egységesíthető, összehasonlítható adatokat biztosít minden ágazati szereplőről.
- Szabályozói támogatás, könnyen beilleszthető a nemzeti kockázatértékelési folyamatba. [104]



10. ábra: Ágazati kockázatelemzés folyamata

Készítette: a Szerző, 2025.

Az egyszerűsített ágazati kockázatelemzés egy felhasználóbarát, költséghatékony és standardizált módszer, amely lehetővé teszi az ágazat teljes lefedését, beleértve a kisebb szolgáltatókat is. Eredményei egyszerűen értelmezhetők, és vizuálisan ábrázolhatók. Ez a megközelítés jelentősen javítja az országos kockázatértékelés minőségét, növeli az átláthatóságot, és támogatja a stratégiai döntéshozatalt. [141]

Az implementáció során javasolt egy 12 hónapos ütemterv, amely során az első 1-2 hónapban a metodika kialakítása történik, majd a 3-4. hónapban indikátor pilot a három kiválasztott alágazatban, majd 5–6. hónapban a súlyozás elvégzése, a 7–8. hónapban hálózati modell és stressztesztek lebonylítása, a 9–10. hónapban validáció, majd a 11–12. hónapban az ágazati kockázatelemzés és szabályozói egyeztetés. [20]

2.4.5 A kockázatkezelési intézkedések végrehajtásának és hatékonyságának értékelési kerete

A kockázatkezelési intézkedések hatékonyságának értékelése a kockázatmenedzsment kulcsfontosságú eleme, amely biztosítja, hogy a meghozott döntések és alkalmazott intézkedések ténylegesen hozzájáruljanak a célok eléréséhez, valamint a biztonság és üzemmenet folytonosság fenntartásához. Az értékelés célja, hogy visszajelzést adjon az intézkedések eredményességéről, feltárja a hiányosságokat, és támogassa a folyamatos fejlesztést. A hatékonyság mérésére a gyakorlatban több, egymást kiegészítő eszköz és módszer áll rendelkezésre.

A kockázati mátrix változásának vizsgálata a legegyszerűbb mérési módszer, elemezni szükséges, hogy a bevezetett intézkedések után csökkent-e a kockázatok valószínűsége agy hatása. Ha a kockázatok jelentős része alacsonyabb kategóriába kerül, akkor az ágazati elemzés és az arra épített intézkedések hatékonyak voltak. Ha nem változott vagy növekedett a kockázati szint, az az elemzés hiányosságát jelzi.

A gyakorlatok révén tesztelhető, hogy az elemzés reális feltevéseken alapul e. A gyakorlat során sikerült -e kezelni azokat a helyzeteket, amelyeket az ágazati elemzés kritikusnak minősített, vagy ütköznek-e olyan vakfoltba, amelyeket az elemzés nem vett figyelembe. Összességében a gyakorlatok eredményeinek értékelésével visszaellenőrizhető a kockázatelemzés hatékonysága.
Emellett az ágazatok szereplőinek, szakértőinek bevonásával véleményezhető a kockázatelemzés, hogy az releváns kockázati kategóriákat tartalmaznak, helyesen lettek e súlyozva a fenyegetések, továbbá az intézkedések valós problémákat kezelnek e.

Az elemzés hatékonyságának egyik mérőszáma, hogy az ágazat szereplői mennyire tudták megvalósítani az abból származó intézkedéseket. A mérőszám a végrehajtott intézkedések arányából, a végrehajtás átfutási idejéből és a szükséges kiegészítő intézkedések számából látható. Ha sok intézkedés megvalósult, általában jól strukturált volt az elemzés.

Ezek a monitoring és értékelési tevékenységek beépítése a kockázatkezelési rendszerbe biztosítják a folyamatos fejlesztést és adaptivitást, ami különösen fontos a kritikus szervezetek esetében, ahol a működésbiztonság, az adatvédelem és a üzemmenet folytonosság alapvető követelmény.

2.5 Az ágazati kockázatelemzés eredményeinek adatfeldolgozási és elemzési módszertana

Az ágazati kockázatelemzés hatósági szintű hasznosíthatóságának egyik alapfeltétele, hogy az egyedi kritikus szervezetek által készített kockázatelemzésekből összehasonlítható, aggregálható és döntéstámogatásra alkalmas információ nyerhető ki. Ennek biztosítására az Ágazati kockázati összesítő mátrix (ÁKÖM) alkalmazását javaslom, amely az egyedi kockázati eredményeket egységes, normalizált indikátorok mentén foglalja rendszerbe. Az ÁKÖM módszertani alapját a többkritériumos döntéstámogatás egyszerűsített, indikátor-alapú megközelítései, valamint a kritikus infrastruktúrák kockázatelemzésével foglalkozó európai és nemzetközi szakirodalom adják, amelyek egybehangzóan hangsúlyozzák, hogy az ágazati szintű értékelés nem az egyedi technikai elemzések újraértékelésén, hanem az összehasonlítható mutatók szintézisén kell, hogy alapuljon. [140]

Az ÁKÖM koncepciója abból az alapfeltevésből indul ki, hogy a hatósági döntéshozatal számára az információ értékét nem annak részletezettsége, hanem annak strukturáltsága és értelmezhetősége határozza meg. Ennek megfelelően a mátrix az egyedi kockázatelemzések során keletkező komplex információkat úgy, mint fenyegetettség, sérülékenység, következmény és interdependencia – egy korlátozott számú, előre definiált indikátorba sűríti, majd ezeket normalizált kockázati mutatókká alakítja. Ez az eljárás összhangban áll az ISO 31000 azon alapelvével, amely szerint a kockázati információknak a döntéshozók számára érthető és használható formában kell megjelenniük, valamint a kockázati portfóliók kezelésére vonatkozó nemzetközi gyakorlattal, amely a kockázatokat nem izoláltan, hanem egymással összefüggő halmazként értelmezi. [22]

Az ÁKÖM egyik lényeges módszertani sajátossága, hogy az alapkockázat (R) mellett explicit módon megjeleníti az interdependenciákkal korrigált kockázati értéket (R*), ezáltal lehetővé téve a közvetlen és a dominóhatások elkülönített, de egymással összekapcsolt értelmezését. Ez a megközelítés közvetlenül kapcsolódik a kritikus infrastruktúrák interdependencia elemzésével foglalkozó szakirodalomhoz, különösen Rinaldi és munkatársai tipológiájához, valamint az Európai Bizottság Közös Kutatóközpontja által kidolgozott módszertani keretekhez, amelyek szerint a rendszerszintű kockázatok jelentős része nem az egyedi sérülékenységekből, hanem az infrastruktúrák közötti függőségekből ered. [20]

Amennyiben a kritikus szervezetek egységes módszertan alapján elvégzik kockázatelemzésüket és azt felterjesztik az illetékes ágazati hatósághoz vagy szakhatósághoz, a hatóság számára a fő kihívást nem az adatok mennyisége, hanem azok strukturált feldolgozhatósága és értelmezhetősége jelenti. Ennek megoldása több egymásra épülő lépésben valósítható meg. [118]

1. Strukturált adatbefogadás és validáció

Az összesítés első feltétele, hogy a beérkező kockázatelemzések standardizált adatstruktúrában érkezzenek. Ez nem feltétlenül jelent teljes módszertani egységességet, de minimálisan biztosítania kell, hogy az alapindikátorok úgy, mint a fenyegetettség, a sérülékenység, a hatás, és az interdependencia egységes skálán és definíciók mentén kerüljenek rögzítésre.

A hatóság feladata ebben a fázisban nem a tartalmi újraértékelés, hanem az adatminőség ellenőrzése, például:

- hiányzó vagy inkonzisztens értékek kiszűrése,

- szélső értékek azonosítása,
- formai és módszertani megfelelőség ellenőrzése.

Ez a lépés biztosítja, hogy az aggregáció tudományosan védhető alapokon nyugodjon.

2. Ágazati aggregáció statisztikai eszközökkel

A validált adatok alapján a hatóság több szinten képes összesítést végezni. Az egyszerűsített kockázati pontszámok (R, illetve R*) lehetővé teszik az alapstatisztikai aggregációt, például:

- ágazati átlag, medián és szórás számítását,
- kockázati kategóriák szerinti megoszlás vizsgálatát,
- időbeli trendek kimutatását.

Ezek az összesítések gyors képet adnak arról, hogy az adott ágazat egészét tekintve mennyire koncentráltak a kockázatok, illetve hogy egyes alágazatok vagy szervezettípusok kiemelkednek-e a mezőnyből. [153]

3. Kockázati profilok és klaszterek azonosítása

A puszta átlagolás azonban nem elegendő a döntéstámogatáshoz. A hatóság számára különösen értékes információt jelent, ha az egyedi szervezetek kockázati mintázatok alapján csoportosíthatók. Ez megvalósítható például:

- kockázati klaszterek képzésével pl. magas hatás–alacsony sérülékenység, alacsony hatás–magas sérülékenység,
- kritikus szervezetek „profilozásával” az indikátorok kombinációi alapján.

Ez a megközelítés lehetővé teszi, hogy a hatóság ne egyedi szervezetekre, hanem kockázati típusokra reagáljon, ami hatékonyabb szabályozási és felügyeleti eszközöket tesz lehetővé. [20]

4. Interdependenciák és rendszerszintű kockázatok feltárása

Az interdependencia-indikátorok különösen fontos hozzáadott értéket jelentenek az összesítés során. Amennyiben a szervezetek az interdependencia mértékét is jelentik, a hatóság képes:

- azonosítani azokat a szereplőket, amelyek több más kritikus szervezet működésére hatással vannak,

- feltérképezni a potenciális dominóhatások irányát és erősségét,
- kijelölni az ágazat „rendszerszinten kritikus csomópontjait”.

Ez a tudás túlmutat az egyedi kockázatelemzéseken, és közvetlenül hozzájárul a nemzeti szintű reziliencia értékeléshez. [118]

5. Prioritások és beavatkozási pontok kijelölése

Az aggregált adatok alapján a hatóság képes prioritási sorrendet felállítani, például:

- mely szervezetek igényelnek részletesebb kockázatelemzést,
- hol indokolt célzott ellenőrzés vagy támogatás,
- mely alágazatokban szükséges szabályozói beavatkozás vagy iránymutatás frissítése.

Ez a lépés különösen fontos abból a szempontból, hogy segíti a hatóság munkáját, hogy hol, milyen beavatkozás szükséges. [20]

6. Döntéstámogató jelentések és visszacsatolás

Az összesítés végső célja nem az adatok tárolása, hanem a hasznosítható információ előállítása. Ennek érdekében a hatóság döntéstámogató jelentéseket készíthet, amelyek:

- bemutatják az ágazati kockázati profilt,
- kiemelik a kritikus trendeket és gyenge pontokat,
- javaslatokat fogalmaznak meg intézkedésekre.

Ezzel párhuzamosan fontos a visszacsatolás a kritikus szervezetek felé, az összesített eredmények alapján a hatóság iránymutatást adhat és elősegítheti a kockázatkezelési gyakorlatok fejlődését. [118]

2.5.1 A strukturált adatbefogadás és validáció módszertani kerete - ágazati kockázati összesítő mátrix

Fontos megvizsgálni, hogy mire is van szüksége a hatóságnak, mit tud kinyerni az adatokból. A hatóság nem egyedi kockázatelemzéseket olvas újra ezáltal, hanem arra keresi a választ, hogy hol koncentrálódik az ágazati kockázat, mely szervezetek kritikusak rendszerszinten, valamint hol indokolt a beavatkozás, az ellenőrzés, és a támogatás. Ez egy standardizált táblázat, amelybe minden kritikus szervezet megtalálható az ágazatban sorban megjelenítve, az összehasonlítható kockázati információk pedig oszloponként kerülnek megjelenítésre. [118]

20. táblázat: Ágazati kockázati összesítő táblázat, Készítette: a Szerző, 2026.

Szervezet ID	Alágazat	F	S	H	I	R	R*	Kategória	Rendszerszintű szerep	Hatósági jelzés
E-01	Energia – elosztás	3	4	5	3	0,48	0,70	Magas	Kulcscsomópont	Mélyelemzés
E-07	Energia – átvitel	4	3	5	4	0,48	0,77	Magas	Országos	Prioritás
K-03	Vasút	3	2	4	4	0,19	0,31	Közepes	Regionális	Monitor
IT-02	Adatközpont	5	3	4	5	0,48	0,96	Magas	Ágazaton átívelő	Azonnali

- Az R és R* értékek már normalizáltak, tehát összehasonlíthatók ágazaton belül és ágazatok között is.
- A hatósági jelzés automatikusan generálható szabályok alapján.

Az ÁKÖM-re épülő kockázati térkép alkalmazása a normalizált kockázati mutatók vizuális és elemző értelmezését teszi lehetővé hatósági szemlélettel. A kockázati térkép módszertani gyökerei a kockázati mátrixok és térképek széles körben alkalmazott gyakorlatában találhatók, amelyek az ISO/IEC 31010 szabványban is szereplő kockázatértékelési technikák közé tartoznak. A disszertációban alkalmazott megoldás ugyanakkor túlmutat a hagyományos valószínűség–hatás mátrixokon, mivel a térkép tengelyei nem közvetlen kockázati komponenseket, hanem két eltérő értelmezési szintet reprezentáló mutatót jelenítenek meg. Az egyik tengely az alapkockázatot fejezi ki, amely az adott szervezet belső működési és védelmi jellemzőit tükrözi, míg a másik tengely az interdependenciákkal korrigált kockázatot jeleníti meg, amely a szervezet ágazati és rendszerszintű beágyazottságát is figyelembe veszi. [153]

Ez a kétdimenziós megjelenítés lehetővé teszi a kockázatok relatív pozíciójának értelmezését, ami hatósági szempontból különösen fontos, mivel a döntéshozatal jellemzően nem abszolút határértékekre, hanem prioritásokra és összehasonlításokra épül. A kockázati térkép segítségével gyorsan azonosíthatók azok a kritikus szervezetek, amelyek kockázati szintje az interdependenciák figyelembevételével jelentősen megnövekszik, még akkor is, ha az alapkockázatuk önmagában mérsékelt. Ez a jelenség a szakirodalomban gyakran rejtett rendszerszintű kockázatként jelenik meg, és különösen jellemző a nagy hálózati beágyazottságú infrastruktúrákra. [135]

A hatóság az alapkockázat és az interdependenciával korrigált kockázat alapján kockázati térképet tud összeállítani két dimenzió mentén, az X tengely adja az alapkockázatot az Y pedig az interdependenciával korrigált kockázatot.

Ezáltal jól lehet szemléltetni és azonnal kitűnik, hogy mely szervezetek csúsznak fel úgymond a térképen rendszerszintű okból és hol van rejtett ágazati sérülékenység. Ezáltal kimutatható, hogy az interdependencia nem kiegészítő információ, hanem kockázaterősítő tényező.

Az egységes, normalizált kockázati mutatókra épülő ágazati összesítő táblázat lehetővé teszi, hogy az egyedi szervezeti kockázatelemzésekből a hatóság rendszerszintű, összehasonlítható és döntéstámogatásra alkalmas információt nyerjen ki. A módszer legnagyobb hozzáadott értéke, hogy az interdependenciák hatását explicit módon jeleníti meg, ezáltal feltárva azokat a rejtett ágazati kockázatokat, amelyek szervezeti szinten nem azonosíthatók. [135]

2.5.2 Esetlegesen felmerülő nehézségek vizsgálata

Az ágazati kockázatelemzés és az ahhoz kapcsolódó kockázat összehasonlító mátrix alkalmazása során több, módszertanilag releváns nehézség és bizonytalansági tényező is azonosítható, amelyek befolyásolhatják az eredmények értelmezhetőségét és döntéstámogató értékét.

Az egyik legfontosabb kihívás az, hogy az összehasonlító mátrixok jellemzően ordinális skálákra és szakértői becslésekre épülnek, ami szükségszerűen magában hordozza a szubjektivitás és az értelmezési eltérések kockázatát, különösen akkor, ha az értékelést eltérő szervezeti kultúrával, kockázati étvággyal vagy módszertani érettséggel rendelkező szereplők végzik. További bizonytalanságot jelenthet az ágazatokon belüli heterogenitás, mivel az azonos ágazatba sorolt szervezetek infrastruktúrája, technológiai színvonala és működési környezete jelentősen eltérhet, ami megnehezíti az egységes mátrix kategóriák következetes alkalmazását.

Az interdependenciák kezelése szintén kritikus pont, hiszen a mátrix alapú összehasonlítások gyakran statikus képet adnak, miközben az ágazatok közötti függőségek dinamikusan változnak, és egy adott esemény hatása időben és térben is eltérő módon terjedhet tovább. Emellett adatbizonytalanságot okozhat a korlátozott hozzáférés a megbízható incidens- és teljesítményadatokhoz, különösen biztonsági vagy üzleti okokból érzékeny területeken, ami az értékelések konzervatív vagy éppen torzított irányba való elmozdulását eredményezheti.

Mindezek alapján a kockázat összehasonlító mátrix és az ágazati kockázatelemzés elsősorban döntéstámogató, orientáló eszközként értelmezendő, amely megfelelő kalibráció, rendszeres felülvizsgálat és kiegészítő módszerek alkalmazása mellett képes megbízható alapot nyújtani az ágazati szintű kockázatok értékeléséhez. [135]

2.6 Összegzés

Az ágazati szintű kockázatelemzés olyan módszertani megközelítés, amely lehetővé teszi a kritikus infrastruktúrák és szolgáltatók fenyegetettségeinek, sérülékenységeinek és kölcsönös függőségeinek átfogó, rendszerszintű értékelését. Az egyes szervezetek szintjén végzett elemzések gyakran csak lokális képet adnak, azonban a modern ellátási láncok, hálózati rendszerek és interdependenciák bonyolultsága miatt ma már elengedhetetlen, hogy az energia, a víziközmű, és más ágazatok kockázatai integrált keretrendszerben kerüljenek elemzésre. Ennek legnagyobb előnye, hogy lehetővé válik a dominóhatások feltárása, vagyis annak megértése, hogyan vezethet egyetlen esemény, például egy földgázellátási zavar, széleskörű villamosenergia kimaradáshoz, majd ennek következtében vízellátási problémákhoz és további ellátási lánc fennakadásokhoz. Az ágazati szintű elemzés képes azonosítani azokat a kritikus csomópontokat is, ahol a beavatkozás a legnagyobb reziliencia növelő hatással járhat, ezáltal hatékonyabbá téve a stratégiai döntéshozatalt és a források elosztását.

Az ágazati kockázatelemzés módszertani megközelítése kiemelt szerepet játszik a döntéstámogatásban, mivel lehetővé teszi a kockázatok értékelését, ami alapján a döntéshozók objektív, adatvezérelt módon tudják meghatározni a legfontosabb beavatkozási területeket. A módszertan támogatja a nemzeti kockázatkezelési stratégiák és ágazati biztonsági intézkedések összehangolását, lehetőséget teremtve arra, hogy az intézkedések ne elszigetelten, hanem összehangoltan szolgálják a kritikus szervezetek védelmét. A keretrendszer jelentős előnye, hogy illeszkedik az uniós és hazai jogszabályi elvárásokhoz, beleértve a NIS2 és CER irányelvek, a DORA rendelet, valamint a Kszetv. követelményeit.

Összességében az ÁKÖM és az arra épülő kockázati térkép együttes alkalmazása olyan integrált módszertani keretet alkot, amely alkalmas az egyedi kritikus szervezetek által készített kockázatelemzésekből származó információk egységes szerkezetű, normalizált és összehasonlítható módon történő összesítésére és hatósági szintű értelmezésére. A megközelítés lehetővé teszi, hogy a heterogén módszertani mélységű és eltérő érettségű szervezeti kockázatelemzések ne izolált dokumentumokként jelenjenek meg, hanem egy ágazati szintű, rendszerszemléletű kockázati kép elemeiként legyenek értelmezhetők.

A kutatás önálló és innovatív tudományos hozzájárulása ebben a kontextusban abban ragadható meg, hogy a kritikus infrastruktúrák kockázatelemzésében eddig jellemzően kvalitatív, leíró vagy eseti jelleggel alkalmazott interdependencia elemzéseket egy normalizált, kvantifikált és összehasonlítható indikátorrendszerbe integrálja.

Az interdependenciák hatása nem pusztán kiegészítő magyarázó elemként jelenik meg, hanem a kockázati értékelés szerves részévé válik, amely explicit módon módosítja az alapkockázati szintet, és ezáltal mérhetővé teszi a rendszerszintű kockázaterősítő hatásokat.

További újdonságot jelent, hogy a normalizált kockázati mutatókra épülő kockázati térkép a hatósági döntéshozatal számára értelmezhető módon teszi láthatóvá a közvetlen és a dominóhatások közötti különbségeket, valamint azokat a rejtett rendszerszintű sérülékenységeket, amelyek szervezeti szinten nem, vagy csak korlátozottan azonosíthatók. Ez a vizuális és analitikus megközelítés hidat képez az elméleti interdependencia modellek és a gyakorlati szabályozói, felügyeleti alkalmazások között, amely a hazai és nemzetközi szakirodalomban jelenleg csak korlátozott mértékben jelenik meg.

A kidolgozott és bemutatott módszertani keret ezáltal nem csupán az ágazati kockázatelemzés hatékonyságát növeli, hanem tudományosan megalapozott módon járul hozzá a kockázatalapú szabályozás és felügyelet erősítéséhez, valamint a kritikus infrastruktúrák és szervezetek ágazati szintű rezilienciájának mérhető és összehasonlítható fejlesztéséhez.

Összességében az ágazati szintű kockázatelemzés olyan eszköz, amely stratégiai előnyt biztosít mind a döntéshozók, mind az érintett szervezetek számára. Lehetővé teszi a kritikus ágazatok kockázati profiljának átfogó, összehasonlítható és reprodukálható értékelését, támogatja az erőforrások célzott allokációját, és hosszú távon hozzájárul a nemzeti reziliencia erősítéséhez. Az integrált módszertan alkalmazásával nemcsak a jelenlegi fenyegetettségek kezelhetők hatékonyabban, hanem megalapozható egy proaktív, előretekintő kockázatkezelési kultúra is, amely képes alkalmazkodni a folyamatosan változó geopolitikai, gazdasági és technológiai környezethez. Ez a megközelítés közvetlenül felhasználható a nemzeti kockázatértékelési jelentésekben és az ágazati stratégiák kialakításában.

2.7 Részkövetkeztetések a 2. fejezethez

A kutatási eredményeimre alapozva megállapítható, hogy Magyarországon az ágazati szintű kockázatelemzés bevezetése a kritikus szervezetek rezilienciájának növelése szempontjából elengedhetetlen. A jelenlegi gyakorlatban a kockázatértékelés szervezeti és nemzeti szinten történik, és nem veszi figyelembe az ágazatok közötti kölcsönös függőségeket, interdependenciákat. Az irodalmi áttekintés, a hazai jogszabályi környezet és a nemzetközi jó gyakorlatok alapján megfogalmazható fő megállapítások és javaslatok az alábbiakban foglalom össze:

1. A magyar kritikus szervezetek kockázatelemzése jelenleg jellemzően szervezeti szinten zajlik, így hiányzik az ágazati szintű átfogó kockázati kép. Ez különösen problémás a dominóhatások és az ágazatközi függőségek feltérképezésekor, például az energia-, víziközmű-, és közlekedési rendszerek kölcsönhatásai esetében.
2. Jelenleg nincs egységes, szabványosított indikátorkészlet vagy súlyozási módszertan, amely lehetővé tenné az ágazatokon belüli és azok közötti kockázati szintek összehasonlítását. A szereplők heterogén módon végzik a kockázatelemzést, ami akadályozza az adatok aggregálhatóságát és a nemzeti szintű jelentéskészítést.

A nemzetközi gyakorlatban alkalmazott ágazati kockázatelemzések alapján végzett összehasonlító elemzések eredményei alapján a következő megállapításokra és kapcsolódó javaslatokra jutottam:

1. Be kell építeni a kritikus szervezetek védelmébe az ágazati kockázatelemzést, amit évente felül kell vizsgálni. Az egyszerűsített ágazati kockázatelemzés célja, hogy a gyakorlatban mindenki számára felhasználóbarát, gyors és standardizált értékelési lehetőséget biztosítson.
2. A feltárt eredmények alapján megállapítható, hogy fejleszteni szükséges a hatóságok közötti kommunikációt az ágazati függőségek feltárása és kezelése érdekében, ezért szükséges létrehozni egy Ágazatközi Reziliencia Munkacsoportot.
3. A kutatás azt jelzi, hogy prioritást szükséges felállítani, hogy az ágazaton belül mely eszközök vagy rendszerek a legkritikusabbak és legsebezhetőbbek. Ez segít az erőforrások hatékony elosztásában a legfontosabb infrastrukturális elemek védelme érdekében.
4. A kutatási eredmények arra utalnak, hogy releváns információt kapunk a felkészültségi és reagálási stratégiák és tervek kidolgozásához, a zavarok megelőzése, az azokra történő reagálás és helyreállítás érdekében. Az ágazati kockázatértékelések kulcsfontosságúak, mivel lehetővé teszik a sebezhetőségek és fenyegetések célzott, ágazatspecifikus megértését. Az ilyen értékelések elvégzésével az ország rangsorolhatja az erőforrásokat, fokozhatja az érdekelt felek közötti koordinációt, és hatékonyabb védelmi intézkedéseket dolgozhat ki a kritikus szervezeteknek a veszélyek széles körével szembeni biztosítására.

A fenti kutatómunkára alapozva a kritikus szervezetek és infrastruktúrák jövőbeni védelmének fejlesztési lehetőségeivel összefüggésben az alábbi javaslatokat fogalmaztam meg:

1. Az ágazati kockázatelemzés a sebezhetőségek azonosításával és a kockázatcsökkentési stratégiák végrehajtásával fokozza a kritikus infrastruktúrák ellenálló képességét, így javaslom annak kialakítását és beépítését a kritikus szervezetek védelmébe.
2. A korlátozott erőforrások jobb elosztása érdekében javaslom egy priorizált lista felállítása, ami megkönnyíti a védelem kialakítását. A lista elkészítésének fő szempontja az ágazatok közötti kölcsönös függőségek feltárása.
3. Javaslom létrehozni, egy Ágazatközi Reziliencia Munkacsoportot, ami elősegíti a hatóságok közötti kommunikációt és az ágazati függőségek feltárását, kezelését.
4. Az ágazati kockázatelemzés összegző szerepével kapcsolatban, az ágazati kockázatelemzés alkalmazása alapvető feltétele annak, hogy a kritikus szervezetek egyedi kockázati értékelései rendszerszinten értelmezhetővé váljanak. A kutatás alapján megállapítható, hogy kizárólag szervezeti szintű megközelítéssel nem azonosíthatók azok a kockázati koncentrációk és kölcsönös függőségek, amelyek az ágazatok működését ténylegesen meghatározzák. Az ágazati szintű szintézis ezért nem az egyedi kockázatok mechanikus összegzése, hanem a kritikus infrastruktúrák hálózatos működéséből fakadó rendszerszintű kockázatok feltárásának eszköze.
5. A kockázati mátrix korlátozott, de strukturáló szerepével összefüggésben, a kockázati mátrix az ágazati kockázatelemzésben elsősorban előszűrő és strukturáló funkciót tölt be, mivel egyszerű és egységes keretet biztosít a kockázatok besorolásához. Ugyanakkor a kutatás alapján megállapítható, hogy a hagyományos mátrixalapú megközelítés önmagában nem alkalmas az interdependenciák és dominóhatások kezelésére, ezért ágazati szinten kizárólag kiegészítő eszközként értelmezhető, nem pedig önálló döntéstámogató megoldásként.
6. A kockázati térkép döntéstámogató többletértékével összefüggésben, a normalizált kockázati mutatókra épülő kockázati térkép olyan összegző döntéstámogató eszközt jelent, amely egyértelműen elkülöníti a közvetlen és a rendszerszintű kockázatokat. Az alapkockázat és az interdependenciával korrigált kockázat együttes megjelenítése lehetővé teszi a rejtett rendszerszintű sérülékenységek azonosítását, és közvetlenül támogatja a hatósági prioritásképzést.

   A kutatás eredményei alapján a kockázati térkép alkalmazása érdemi többletet nyújt a kockázatalapú szabályozás és felügyelet megalapozásában.

Összefoglalva, a kritikus infrastruktúrák és szervezetek ágazati kockázatelemzése létfontosságú a kulcsfontosságú ágazatokat fenyegető konkrét kockázatok azonosításához és kezeléséhez. Az elemzés nemcsak az ellenálló képességet és a biztonságot növeli, hanem támogatja a hatékony erőforrás felhasználást, és jobb döntéshozatalt és a felek közötti szorosabb együttműködést is.

Véleményem szerint a lehetséges fejlesztéseknek mind honvédelmi, mind katasztrófavédelmi és üzemeltetői felhasználási lehetőségeket is biztosítania kell.

3. A KRITIKUS SZERVEZETEK KOCKÁZATELEMZÉSI ÉS KOMMUNIKÁCIÓS FOLYAMATAINAK ÉRTÉKELÉSE ÉS FEJLESZTÉSI LEHETŐSÉGEI

A kritikus szervezetekhez kapcsolódó kockázatok elemzése mind a NATO, mind az EU keretein belül kiemelt fontosságú az alapvető infrastruktúrák működőképességének és szolgáltatás-folytonosságának biztosítása szempontjából. Az elmúlt évtizedekben jelentős erőfeszítések történtek a potenciális fenyegetések azonosítására, értékelésére és mérséklésére, mivel ezen infrastruktúrák sérülése rendszer- és szövetségi szintű következményekkel járhat. A kockázatelemzés ugyanakkor összetett és dinamikusan változó feladat, amelyet technológiai, szervezeti és hálózati tényezők együttesen befolyásolnak.

A NATO esetében az egyik legjelentősebb nehézség az egymással összekapcsolt védelmi, kommunikációs és logisztikai infrastruktúrák komplexitásából fakad. A tagállamok különböző technológiai szintje, intézményi felkészültsége és kockázatkezelési kultúrája miatt a kockázatelemzési módszerek összehangolása és az interoperabilitás biztosítása folyamatos kihívást jelent. A változatos fenyegetéskörnyezet – különösen a gyorsan alakuló kiberfenyegetések és a hibrid jellegű műveletek – tovább nehezíti az egységes és naprakész kockázati profilok fenntartását.

A NATO szakmai anyagai és gyakorlatértékelései rendre hangsúlyozzák, hogy a kockázatkezelés folyamatos frissítést, a rendszerszintű összefüggések vizsgálatát és a tagállami együttműködés erősítését igényli.

Az EU esetében a kritikus szervezetek kockázatelemzését többek között a szabályozási normák heterogenitása és a tagállamok eltérő műszaki fejlettségi szintje nehezíti. A CER Irányelv és a NIS2 éppen e különbségek csökkentésére törekszik, azonban a harmonizáció továbbra is jelentős feladat. Az európai uniós szakirodalom és szakpolitikai dokumentumok kiemelik, hogy az ágazatok közötti – különösen az energia-, közlekedési és információs infrastruktúrák közötti – határokon átnyúló függőségek rendszerszintű sebezhetőségeket hoznak létre, amelyek kezeléséhez átfogó, többágazatos megközelítés szükséges.

A természeti katasztrófák növekvő gyakorisága és az éghajlatváltozás okozta komplex terhelések tovább növelik az alkalmazkodó és előrejelző képességeket is igénylő kockázatelemzési gyakorlatok jelentőségét.

Mind NATO-, mind EU szinten jelentős előrelépés történt a kritikus szervezetek és infrastruktúrák kockázatelemzési keretrendszereinek kialakításában, azonban az interoperabilitással, a szabályozási harmonizációval és a gyorsan változó fenyegetettségi környezettel kapcsolatos kihívások továbbra is fennmaradnak. A jelen fejezet további részében ezért a kockázatelemzés gyakorlati tapasztalatait esettanulmányok segítségével vizsgálom meg, majd bemutatom és összehasonlítom a különböző módszertani megközelítéseket. Ezt követően elemzem, hogy milyen nehézségek merülnek fel a kritikus szervezetek vezetői és a hatóságok közötti kommunikációban, végül javaslatot teszek a reziliencia és a kockázatkezelési együttműködés fejlesztési lehetőségeire. [46]

3.1 A kockázatelemzéssel összefüggő tapasztalatok szisztematikus feldolgozása

A NATO kritikus szervezetre és azok infrastruktúráira vonatkozó kockázatelemzési stratégiája olyan átfogó megközelítés, amelynek célja a szövetség védelmi és operatív rendszereit fenyegető veszélyek értékelése és mérséklése. A NATO kockázatelemzés szisztematikus, többrétegű módszertanra alapozva mind a hagyományos, mind az újonnan megjelenő fenyegetések azonosítására helyezi a hangsúlyt, beleértve a fizikai, a kiber- és a hibrid kockázatokat is. A stratégia fejlett kockázatértékelési modelleket tartalmaz az összekapcsolt rendszerekben bekövetkező zavarok valószínűségének és hatásának értékelésére, különös tekintettel a tagállamok infrastruktúrái közötti kölcsönös függőségekre.

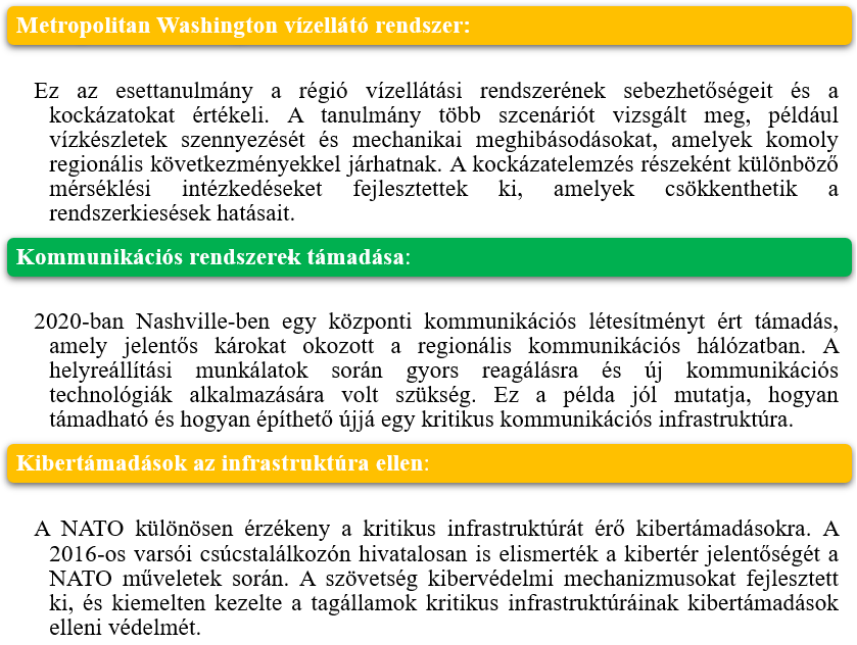
A NATO megközelítésének központi eleme a hírszerzési adatok, a valós idejű megfigyelés és a forgatókönyv alapú szimulációk integrálása a döntéshozatal megalapozása érdekében. A stratégia a tagállamok közötti együttműködést is elősegíti a kockázatkezelési gyakorlatok egységesítése és az ellenálló képesség fokozása érdekében. Az interoperábilis rendszerek összetettsége és a modern fenyegetések például a kiberhadviselés és az éghajlati veszélyek dinamikus jellege azonban jelentős kihívást jelent az egységes kockázatelemzési keretrendszer megvalósítása szempontjából.

A kockázatelemzés fejlesztési lehetőségeinek vizsgálata során fontos megvizsgálni a NATO „Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency" című kézikönyvet, amely a NATO stratégiáit elemzi. A dokumentum vizsgálja a fizikai fenyegetéseket, a terrorizmust, a természeti katasztrófákat, a kiber jellegű támadásokat és a hibrid hadviselés hatásait a kritikus infrastruktúrák védelme során. A tanulmány hangsúlyozza az állami és magánszféra közötti partnerségek, a kockázatértékelés és a nemzetközi együttműködés fontosságát a sebezhetőségek mérséklése érdekében. Emellett esettanulmányokon, például az ukrajnai energiaválságon keresztül vizsgálja az infrastruktúra védelmének összetettségét,

kiemelve a NATO szerepét e modern biztonsági kihívások kezelésében [105]. A dokumentumban található kockázatelemzéssel kapcsolatos megállapítások a következő fő szempontokra fókuszálnak:

- Rendszeralapú megközelítés: A kockázatelemzés során az infrastruktúrák kölcsönös függőségeit is figyelembe veszik, különösen, hogy hogyan befolyásolhatják egymást a különböző kockázati tényezők, például a természeti katasztrófák és terrorista támadások. A kockázatokat olyan portfóliókba rendezték, amelyek lehetővé teszik az azonos típusú kockázatok közvetlen összehasonlítását.
- Valószínűség és hatás kombinációja: A kockázatelemzés alapját a valószínűség és a kockázat bekövetkezésének hatása adja. A résztvevők különböző eshetőségeket értékeltek, mint például a vízellátás kiesésének kockázata, amely jelentős gazdasági és társadalmi hatásokkal járhat.
- Megerősítő stratégiák: Az elemzés kimenetelét felhasználva fejlesztették ki a lehetséges kockázatkezelési intézkedéseket, amelyek csökkenthetik a kockázati forgatókönyvek hatásait. Ezek az intézkedések az infrastruktúra megerősítésére, a redundanciák kialakítására és a vészhelyzeti tervek fejlesztésére összpontosítanak. [46]

A dokumentumban található esettanulmányokat elemezve és figyelembe véve a NATO szerepét a kritikus infrastruktúra védelmében és kockázatelemzésében a következő fontos következtetések állapíthatóak meg:



11. ábra: Infrastruktúrák elleni támadások, Készítette: a Szerző, 2025. [46]

A védekezés során a NATO felállított hibrid fenyegetések elleni védelmi eszközöket, beleértve az információk megosztását és a kiberbiztonsági szakértőket támogató gyakorlatokat, mint a Locked Shields gyakorlat. Ezek a gyakorlatok valós időben szimulálják az infrastruktúrát érő kibertámadásokat, így a résztvevők fejleszthetik képességeiket. Emellett a NATO nagy hangsúlyt fektet a tagállamok energiafüggetlenségének növelésére és az energiainfrastruktúra védelmére, különösen a hibrid fenyegetésekkel szemben, amelyek az energiaellátás megszakítására irányulnak. [46]

Összességében megállapítható, hogy a NATO nem csak katonai, hanem kibervédelmi és kritikus infrastruktúrára vonatkozó erőfeszítéseket is tesz a tagállamok és partnerek védelme érdekében. [105]

3.1.1 Esettanulmányokon alapuló elemzések

Az alábbi esettanulmányok célja, hogy bemutassák a kritikus infrastruktúrák és szervezetek kockázatelemzésében alkalmazott módszertanok gyakorlati használatát, különös tekintettel azokra az elemzési lépésekre, amelyek meghatározzák a rendszerek sérülékenységét és ellenállóképességét. A vizsgálat közös szempontjai a következők:

- a vizsgált infrastruktúra kritikus elemeinek azonosítása és műszaki jellemzése,
- a releváns fenyegetések feltárása, beleértve a fizikai, kiber- és természeti eredetű veszélyeket
- a sebezhetőségek elemzése eszköz-, rendszer- és hálózati szinten,
- a kockázatok értékelése a valószínűség és következmény kombinációja alapján,
- az ellenállóképesség növelését szolgáló intézkedések meghatározása, különös tekintettel a redundanciára, a gyors helyreállíthatóságra és a védelmi mechanizmusok fejlesztésére, valamint,
- a prioritások kijelölése és a védelmi források optimális elosztása.

E szempontok lehetővé teszik a módszerek összehasonlítását, és rámutatnak arra, hogyan támogatják különböző analitikai keretek – például a BIRR, CARVER, RAMCAP-Plus, Sandia, illetve a NIPP Risk Management Framework – a kritikus infrastruktúrák biztonsági és reziliencia céljainak megvalósítását. [46]

I. Better infrastructure risk and resilience (BIRR) módszertan (elektromos hálózat)

Az Egyesült Államokban egy nagy elektromos hálózat üzemeltetője alkalmazta a BIRR módszertant a hálózat sebezhetőségének és ellenállóképességének értékelésére. A cél az volt, hogy azonosítsák a kritikus csomópontokat és azok lehetséges gyengeségeit, különösen kiberfenyegetések és természeti katasztrófák esetén. Az esettanulmány középpontjában a közlekedési infrastruktúrák védelme állt.

Első lépésként meghatározták az eszközöket és eszközkarakterisztikát, azaz az elektromos hálózat különböző elemeit úgy, mint az átalakítók, transzformátorok, és alállomások azonosítását és jellemzését végezték el. Ezt követően azonosították a fenyegetéseket, beleértve a fizikai támadásokat, a kiber korszerűséget és természeti eseményeket. Emellett végrehajtották a sebezhetőségek elemzését minden eszközre és rendszerre tekintettel majd kiértékelték azokat a különböző fenyegetésekre nézve. Ezt követte a kockázatok meghatározása a fenyegetések valószínűségének és következményeinek kombinálása révén. Az ellenállóképesség fejlesztése elérhető az intézkedések kidolgozásával, a sebezhetőségek csökkentésére és a rendszer gyors helyreállításának biztosítására katasztrófa esetén. [106]

12. ábra: Elektromos hálózat védelme, Készítette: a Szerző, 2025. [46]

Az esettanulmány révén azonosították a hálózat legkritikusabb pontjait, amelyek leginkább ki vannak téve a fenyegetéseknek. Javaslatokat tettek a kiberbiztonsági intézkedések megerősítésére, valamint a fizikai védelmi rendszerek fejlesztésére, továbbá növelték a rendszer ellenállóképességét azáltal, hogy redundáns elemeket vezettek be és javították a gyors reagálási képességet.

II. CARVER (Criticality, accessibility, recuperability, vulnerability, effect, recognizability) módszer (közlekedés)

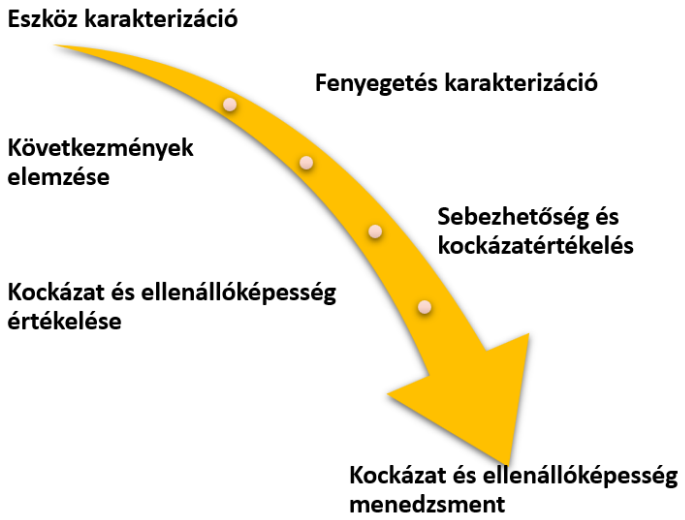
Egy nagyvárosi közlekedési infrastruktúra, rendszer üzemeltetője használta a CARVER módszert a rendszere sebezhetőségének elemzésére és a kritikus pontok prioritásának meghatározására. A folyamat során a CARVER kritériumok alapján rangsorolták a közlekedési rendszer elemeit, azaz a lehetséges célpontokat. Ezt követően meghatározták, mely pontok kritikusak a rendszer működésének szempontjából. A sebezhetőségi értékelés révén felmérték, hogy mely pontok a leginkább sebezhetők a támadásokkal vagy a természetes katasztrófákkal szemben, majd kijelölték a prioritásokat, a legkritikusabb és a legsebezhetőbb pontok prioritásának meghatározásával a védelmi intézkedések implementálása érdekében. [107]

Ennek eredményeként sikeresen azonosították a központi csomópontokat, például a fő vasútállomást és a központi buszparkolót, mint legkritikusabb elemeket. Javaslatokat tettek a fizikai és kiberbiztonsági intézkedések megerősítésére ezeknél a pontoknál és optimalizálták a védelmi források elosztását a legnagyobb kockázatot jelentő területekre, növelve ezzel a rendszer általános biztonságát.

III. RAMCAP-Plus módszertan (vízellátás)

Egy kanadai vízellátó vállalat alkalmazta a RAMCAP-Plus (Risk assessment and management for critical asset protection) módszertant a vízellátó rendszer kockázatainak és ellenállóképességének értékelésére. Elsőként azonosította a vízellátó rendszer összes kritikus komponensét úgy, mint víztisztító telepek, elosztó hálózatok, tartályok és jellemezte azokat. Ezt követően elemezték a lehetséges fenyegetéseket, például biológiai szennyeződéseket, fizikai támadásokat és természeti katasztrófákat. A következmények elemzése során kitértek a különböző fenyegetések értékelésére a vízellátás folyamatosságára és a közegészségügyre nézve. Ezentúl a sebezhetőségek és a kockázatértékelés során összevetette a fenyegetések valószínűségét és következményeit, majd azonosították a kritikus pontokat és javaslatokat tettek azok védelmére, valamint a rendszer gyors helyreállításának biztosítására katasztrófa esetén.

A kockázatok és ellenállóképesség menedzselése révén intézkedéseket dolgoztak ki és implementáltak a kockázatok csökkentésére és a rendszer ellenállóképességének növelésére.



13. ábra: A módszertan folyamata, Készítette: a Szerző, 2025. [157]

A fentiek eredményeként felmérték a vízellátó rendszer sebezhetőségét különböző fenyegetésekre nézve, majd bevezették a szennyezés elleni további védelmi rétegeket és megerősítették a fizikai biztonsági intézkedéseket. Növelték a rendszer gyors helyreállítási képességét azáltal, hogy kidolgozták a vészhelyzeti reagálási terveket és a redundáns rendszereket. [157]

IV. Sandia Risk Assessment Methodology (kommunikációs hálózat)

A Sandia Nemzeti Laboratóriumok által fejlesztett módszertant egy országos kommunikációs hálózat védelmére alkalmazták, különösen a kiberfenyegetések ellen. A létesítményben a kommunikációs hálózat összes kritikus elemeit úgy, mint adótornyok, adatközpontok, routerek azonosították, majd meghatározták a lehetséges kiberfenyegetések és a hálózatok kritikus pontjait.

A következmények meghatározásához értékelték a különböző kiberfenyegetések hatásait a hálózat működésére és az ország kommunikációjára tekintettel. Emellett a fenyegetések definiálása is kiemelten fontos mozzanat, így azonosításra került a kommunikációs hálózatot érintő konkrét kiberfenyegetések. Ezt követte a meglévő kiberbiztonsági intézkedések hatékonyságának felmérése, a kockázatok meghatározása a fenyegetések valószínűségének és következményeinek alapján, majd az intézkedések kidolgozása a hálózat védelmének megerősítésére és a kockázatok csökkentésére.

A fentiek eredményeként azonosították a kommunikációs hálózat legkritikusabb kiberbiztonsági pontjait, javasoltak további tűzfalakat, behatolásérzékelő rendszereket és rendszeres biztonsági auditokat, majd növelték a hálózat ellenállóképességét azáltal, hogy redundáns kommunikációs útvonalakat és gyors helyreállítási protokollokat vezettek be. [158]

V. National Infrastructure Protection Plan (NIPP) Risk Management Framework (tömegközlekedés)

Az Egyesült Államok Nemzeti Infrastruktúra Védelmi Terve (NIPP) keretében egy nagyvárosi tömegközlekedési rendszer alkalmazta a Risk Management Framework-öt a rendszer védelmének erősítésére. A cél a tömegközlekedési rendszer védelmének és működésének folyamatos biztosítása, majd a fizikai támadások, a kiberfenyegetések, a természeti katasztrófák és a technikai meghibásodások azonosítása. Fontos értékelni és priorizálni a különböző fenyegetések kockázatának meghatározását és rangsorolni a valószínűségük és következményeik alapján. Szükséges validálni a meglévő védelmi intézkedések hatékonyságának felmérését és szükség esetén további intézkedések kidolgozása szükséges. A kockázatok csökkentése érdekében intézkedéseket kell implementálni, például a rendszeres karbantartás, a biztonsági protokollok megerősítése és a dolgozók képzése, ezt követően szükséges a bevezetett intézkedések hatékonyságának folyamatos monitorozása és szükség esetén módosítása. A fentiek eredményeként felmérték a tömegközlekedési rendszer sebezhetőségét különböző fenyegetésekre, bevezették a fejlett kiberbiztonsági intézkedéseket és fizikai biztonsági rendszereket a forgalomcsomópontoknál, valamint javították a rendszer gyors helyreállítási képességét vészhelyzet esetén azáltal, hogy kidolgozták a vészhelyzeti reagálási terveket és a redundáns rendszereket. [94]

VI. VI. ISO 31000-alapú integrált kockázatmenedzsment (egészségügyi infrastruktúra)

Egy dél-európai ország országos egészségügyi szolgáltatója az ISO 31000 szabványt alkalmazta a kritikus egészségügyi infrastruktúrák – különösen a kórházi energiaellátó rendszerek, gyógyszerlogisztikai láncok és sürgősségi szolgáltatások – kockázatainak áttekintésére. [22] A folyamat első lépéseként azonosították az egészségügyi rendszer kritikus elemeit, mint a mentési kommunikációs csatornákat, műtői energetikai tartalékokat, hűtőlánc-rendszereket és informatikai platformokat. Ezt követően strukturált módon feltárták a fizikai, biológiai, kiber és ellátási láncokhoz kapcsolódó fenyegetéseket, különös figyelemmel a gyógyszer- és eszközellátási zavarokra.

A sebezhetőségi értékelés kiterjedt az épületgépészeti tartalékokra, a redundáns adatkapcsolatokra, valamint az emberi hibákból fakadó sérülékenységekre. A kockázatok rangsorolását a valószínűség–hatás mátrix alapján végezték el. [159]

Az esettanulmány eredményeként meghatározták azokat a létesítményeket és szolgáltatásokat, amelyek működéskiesése a legjelentősebb következményekkel járna, például a sürgősségi központok kommunikációs rendszerei vagy a kritikus gyógyszerkészleteket biztosító raktárak. A szervezet javaslatokat dolgozott ki a redundáns tartalék-energiaellátó rendszerek bővítésére, a gyógyszerlogisztikai útvonalak diverzifikálására és az informatikai védelmi protokollok frissítésére, növelve ezzel az egészségügyi infrastruktúra ellenállóképességét. [160]

VII. VII. Bow-Tie (BT) módszertan alkalmazása (ipari veszélyes üzem)

Egy nyugat-európai vegyipari üzem a Bow-Tie (BT) módszert alkalmazta egy potenciális veszélyes esemény – mérgező anyag kiszabadulása – ok-okozati és következményláncának feltárására. A folyamat a centrális veszélyes esemény meghatározásával kezdődött, majd elkészítették a kiváltó okok ábráját (Fault Tree) és a következmények modelljét (Event Tree). A módszer lehetővé tette a technikai, humán és szervezeti sebezhetőségek részletes elemzését, különös hangsúllyal a karbantartási hibákra, a valós idejű monitoring hiányosságaira és a védelmi berendezések megbízhatóságára.

A védekezést nehezítő tényezők értékelése során azonosították, mely kontrollok hatékonyak, és hol szükséges megerősítés – ilyenek voltak például a gázdetektorok redundanciája, az operátorok képzési protokolljai, valamint a karbantartási ciklusok felülvizsgálata. Az alkalmazott Bow-Tie diagram rávilágított a kritikus összefüggésekre, és segítette a vezetést a védelmi intézkedések prioritásának meghatározásában. Az üzem ennek eredményeként modernizálta a monitoring rendszereket és korszerűsítette a vészleállítási mechanizmusokat, jelentősen csökkentve a lehetséges következmények súlyosságát. [161]

VIII. VIII. STRIDE kockázatmodell alkalmazása (digitális infrastruktúra)

Egy közép-európai ország nemzeti adatközpontja a STRIDE módszert alkalmazta a kiberfenyegetések strukturált elemzésére. A STRIDE keretrendszer hat kategóriába sorolja a támadástípusokat: szabotázs, manipuláció, támadás, információk nyilvánosságra hozatala, szolgáltatás megtagadása, jogosultságok kiterjesztése. Az esettanulmány első lépésként feltérképezte az adatközpont szolgáltatásait, hálózati kapcsolatait és identitáskezelési folyamatait. Ezt követően minden komponensre pl. tűzfalak, szerverek, felhőösszeköttetések, adminisztrátori fiókok elvégezték a fenyegetés típusonkénti vizsgálatot. [162]

A sebezhetőségek feltárása során kimutatták, hogy bizonyos adminisztrátori hozzáférések túl széles jogosultsági körrel rendelkeztek, valamint több kapcsolat esetében hiányoztak a naplózási és monitorozási kontrollok. A kockázatok súlyosságának értékelése feltárta, hogy a szolgáltatásmegtagadási támadások (DoS) jelentős rendelkezésre állási kockázatot hordoznak, míg az információszivárgás potenciálisan adatvédelmi incidenseket eredményezhet. A szervezet ennek alapján bevezetett többfaktoros hitelesítést, finomhangolta a jogosultsági struktúrát, frissítette a naplózási rendszereket és növelte a hálózat redundanciáját, ezáltal jelentősen csökkentve a kritikus digitális infrastruktúra sérülékenységét. [163]

Az esettanulmányok elemzése alapján megállapítható, hogy a kritikus infrastruktúrák és szervezetek kockázatelemzési módszertanai jelentős eltéréseket mutatnak az alkalmazott technikai megközelítésekben, ugyanakkor közös struktúrával rendelkeznek. Mindegyik módszer a kritikus elemek azonosítására, a releváns fenyegetések feltárására, a sebezhetőségek értékelésére, valamint a valószínűség hatás alapú kockázati rangsorolásra épül. A különböző ágazati példák, az energia, a közlekedés, a vízellátás, a kommunikáció, az egészségügy, az ipari veszélyes üzemek és a digitális infrastruktúrák azt mutatják, hogy a hatékony kockázatelemzés elengedhetetlen feltétele a rendszerszintű függőségek feltárása és a reziliencia növelését szolgáló intézkedések prioritásainak kijelölése.

A bemutatott módszertanok hozzájárulnak ahhoz, hogy a szervezetek olyan védelmi és működésbiztonsági stratégiákat alakítsanak ki, amelyek a gyorsan változó fenyegetési környezetben is biztosítják a szolgáltatások folytonosságát. A tapasztalatok azt mutatják, hogy nincs univerzálisan alkalmazható módszer, a választás mindig az adott ágazat technológiai jellemzőitől, a fenyegetési környezettől, valamint a szervezet működési sajátosságaitól függ. Ugyanakkor a módszertanok összehasonlítása rávilágít arra, hogy a kockázatértékelés hatékonysága jelentősen növelhető az integrált megközelítések, a kiber és fizikai elemzés, a hálózati interdependenciák vizsgálata és a reziliencia orientált tervezés alkalmazásával.

Összességében az esettanulmányok egyértelműen bizonyítják, hogy a kockázatelemzés nem statikus feladat, hanem olyan folyamat, amely a technológiai, szervezeti és fenyegetettségi változásokhoz folyamatosan alkalmazkodik. [108]

Az esettanulmányok elkészítése során vizsgált módszertanokról szóló összehasonlító táblázat a 8. mellékletben található meg.

3.1.2 A kockázatelemzési módszertanok gyakorlati alkalmazásának értékelése

Enrico Zio "Challenges in the Vulnerability and Risk Analysis of Critical Infrastructures" című cikke a kritikus infrastruktúrák sebezhetőségének és kockázatainak elemzésével kapcsolatos kihívásokat tárgyalja. A kritikus infrastruktúrák, mint az energiaellátás, vízellátás, közlekedés és kommunikációs rendszerek, komplex és egymással szorosan összefüggő hálózatok, amelyek létfontosságúak a társadalom működése szempontjából. A cikk rámutat arra, hogy ezeknek a rendszereknek a sebezhetőségi elemzése különösen fontos a kockázatok azonosítása és minimalizálása érdekében, ám számos akadállyal kell szembenézni. [8]

Zio szerint a legnagyobb kihívás a rendszerek összetettsége és egymásra épülése, amely miatt egyetlen komponens meghibásodása vagy támadása az egész rendszer működésképtelenségéhez vezethet. A cikk kiemeli, hogy a kockázatelemzés során nem csak az egyes elemek, hanem az egész rendszer viselkedését kell figyelembe venni, különösen a dominóhatásokat és az interdependenciákat. Továbbá, a kockázat- és sebezhetőségi elemzést bonyolítja az is, hogy a rendszerek dinamikusan változnak, és a potenciális fenyegetések egyre bonyolultabbá válnak, például a kibertámadások terjedésével. Felhívja a figyelmet arra is, hogy a jelenlegi elemzési módszerek gyakran nem tudnak lépést tartani e komplexitással, ezért új, fejlettebb modellek és módszerek kidolgozására van szükség. A cikk záró részében javaslatot tesz a modern adatgyűjtési technikák, a nagy adatmennyiségek feldolgozása, valamint a mesterséges intelligencia alkalmazására a kritikus infrastruktúrák biztonsági elemzése során. [109]

A kritikus szervezetek kockázatelemzésének fejlesztése érdekében megvizsgáltam és összehasonlítottam a napjainkban alkalmazott kockázatelemzési módszereket különböző paraméterek alapján. Fontosnak tartottam megvizsgálni azokat tanulmányozni használhatósági kör, és felhasználói nehézség alapján, milyen adatok szükségesek az alkalmazhatóságához, továbbá mennyire használható a kölcsönös függőségek mérésére. Az összehasonlító táblázat az alábbiak szerint alakul:

21. táblázat: Kockázatelemzési módszerek összehasonlítása, Készítette: a Szerző, 2025 [106].

Szempont	**FEMA (Failure Mode and Effect Analysis)**	**CARVER**	**Bow-Tie Analysis**	**HAZOP (Hazard and Operability Study)**	**RAMCAP (Risk Analysis and Management for Critical Asset Protection)**	**Monte Carlo Simulation**	**FTA (Hibafa elemzés)**	**Inoperability Input-Output Model (IIM)**
Cél	A lehetséges hibamódok és azok hatásainak azonosítása	A kritikus eszközök rangsorolása	Kockázatok és ellenőrzések azonosítása	A folyamat veszélyeinek és működési kockázatainak azonosítása	A kritikus eszközöket érintő kockázatok értékelése és kezelése	Kockázat számszerűsítése a bizonytalanságok szimulálásával	A rendszerhibák kiváltó okainak elemzése	Az infrastruktúra meghibásodásának gazdasági hatásának értékelése
Rövid leírás	Szisztematikus megközelítés annak azonosítására, hogy hol és hogyan hibásodhat meg egy rendszer, és a hatás értékelésére.	Célpontok rangsorolására szolgál a kritikusság, a hozzáférhetőség, a helyreállíthatóság, a sebezhetőség, a hatás és a felismerhetőség elemzésével.	Vizuális módszer a kockázati útvonalak és a megfelelő kontrollok elemzésére	Strukturált és szisztematikus technika a rendszerben lévő potenciális veszélyek azonosítására.	A kritikus infrastrukturális eszközöket érintő kockázatok értékelésére összpontosít.	Véletlenszerű mintavételt használ a bizonytalanságok rendszer teljesítményére gyakorolt hatásának modellezésére.	Felülről lefelé irányuló megközelítést alkalmaz a nem kívánt eseményhez vezető hibakombinációk azonosítására.	Elemzi, hogy egy infrastruktúra-ágazat meghibásodása hogyan hat más ágazatokra és a gazdaság egészére.
Alkalmazási kör	Mérnöki rendszerek, gyártás	Katonai, infrastrukturális	Biztonsági, környezeti rendszerek, infrastruktúra Esemény- és veszélyadatok	Folyamatipar, vegyi üzemek	Kritikus infrastruktúra-ágazatok	Bármilyen rendszer számszerűsíthető bizonytalanságokkal	Műszaki rendszerek, biztonságkritikus rendszerek	Gazdasági rendszerek, infrastrukturális hálózatok
Bemeneti adatok típusa	Rendszerteljesítmény adatok, korábbi meghibásodási adatok	Eszközinformációk, fenyegetési adatok	1. A veszélyek azonosítása, a lehetséges következmények elemzése 3. Megelőző és enyhítő ellenőrzések azonosítása	Folyamatáramlási diagramok, üzemeltetési adatok	Az eszközök sebezhetőségére vonatkozó adatok, fenyegetettségi adatok	Valószínűségi eloszlások, rendszerteljesítmény adatok	Hibaadatok, rendszertervezési információk	Gazdasági input-output adatok, kölcsönös függőségi adatok

Szempont	FEMA (Failure Mode and Effect Analysis)	CARVER	Bow-Tie Analysis	HAZOP (Hazard and Operability Study)	RAMCAP (Risk Analysis and Management for Critical Asset Protection)	Monte Carlo Simulation	FTA (Hibafa elemzés)	Inoperability Input-Output Model (IIM)
Főbb lépések	1. A lehetséges hibamódok azonosítása 2. A meghibásodás hatásainak értékelése 3. Prioritás megállapítása a súlyosság alapján	1. Az eszközök értékelése a CARVER kritériumok alapján. 2. Az eszközök rangsorolása. 3.A legveszélyeztettebb eszközök elemzése	Kockázati utak és kockázatcsökkentő intézkedések	1. A normál működéstől való eltérések azonosítása. 2. A kockázatok értékelése. 3. Intézkedések ajánlása.	1. A fenyegetések azonosítása. 2. A sebezhetőségek értékelése. 3. A kockázat számszerűsítése. 4. Veszélycsökkentési stratégiák kidolgozása.	1. Kockázati változók meghatározása 2. Valószínűségi eloszlások hozzárendelése 3. Szimulációk futtatása 4. Elemezze a kimenetet	1. A legfőbb esemény meghatározása 2. Hibafa felépítése 3. A meghibásodás útjainak elemzése	1. Az ágazati függőségek meghatározása 2.Hibaforgatókönyvek alkalmazása 3. A gazdasági hatás értékelése
Eredmények típusa	Kockázatok rangsorolt listája.	Az eszközök rangsorolása.	Egyértelmű, vizuális ábrázolás.	A lehetséges eltérések és a kapcsolódó kockázatok listája.	Kvantitatív kockázati pontszám, rangsorolt eszközlista	Valószínűségi kockázati tartományok	Logikai hibaútvonalak	Gazdasági veszteség és helyreállítási mérőszámok
Előnye	Könnyen alkalmazható, hatékony az alkatrészszintű hibák azonosításában	Egyszerű, gyorsan alkalmazható	Nagy rendszerek esetén összetetté válhat	Alapos, komplex kockázatok megragadására alkalmas	Kvantitatív, különböző ágazatokra adaptálható	Robusztus valószínűségi betekintést nyújt	Nagyon részletes, jó a kiváltó okok megértéséhez	Megragadja a rendszerszintű kölcsönös függőségeket
Hátránya	Összetett rendszerek esetében időigényes	Korlátozott hatókör, nem elég mély az összetett rendszerek esetében	Korlátozott képesség a dinamikus kockázatok megragadására	Munkaigényes és időigényes	Részletes adatbevitelt igényel	Számítási igényes	Nagy rendszerek esetében bonyolulttá válhat	Nagyméretű, pontos adatkészleteket igényel

Szempont	FEMA (Failure Mode and Effect Analysis)	CARVER	Bow-Tie Analysis	HAZOP (Hazard and Operability Study)	RAMCAP (Risk Analysis and Management for Critical Asset Protection)	Monte Carlo Simulation	FTA (Hibafa elemzés)	Inoperability Input-Output Model (IIM)
Korlátai	Az egyes összetevőkre összpontosít, figyelmen kívül hagyhatja a rendszerszintű kockázatokat	Elsősorban fizikai célpontokra összpontosít	Alapvető módon kezeli a kölcsönös függőségeket	Működési problémákra korlátozódik	Korlátozottan összpontosít az operatív kockázatokra	Pontos bemeneti adatokat igényel	Nagy rendszerek esetén időigényes	Magas adat- és számítási követelmények
Kölcsönös függőségek kezelése	Nem veszi kifejezetten figyelembe a kölcsönös függőségeket	Nem veszi figyelembe az egész rendszerre kiterjedő kölcsönös függőségeket.	Mérsékelt	Csak részben foglalkozik a kölcsönös függőségekkel	Nem kezeli mélyen a kölcsönös függőségeket	Nem összpontosít kifejezetten a kölcsönös függőségekre	Korlátozott a rendszerszintű kölcsönös függőségek kezelésében	Kifejezetten kezeli a kölcsönös függőségeket
Alkalmazás nehézségi foka	Mérsékelt	Könnyű	Mérsékelt	Magas	Mérsékelt	Magas	Magas	Magas
Felhasználói szakértelem szükségessége	Némi szakértelmet igényel	Minimális szakértelem szükséges	Némi szakértelmet igényel	Jelentős szakértelmet igényel	Speciális szakértelmet igényel	Jelentős szakértelmet igényel	Műszaki szakértelmet igényel	Magas szintű szakértelmet igényel
Költsége	Alacsony	Alacsony	Alacsony vagy közepes	Magas	Közepes	Magas	Közepes	Magas
Szoftveres támogatása	Jellemzően nem szoftveralapú	Jellemzően nem szoftveralapú	Speciális szoftverek állnak rendelkezésre	Elérhető szoftver (pl. PHA-Pro)	Speciális szoftver áll rendelkezésre	Széles körben elérhető szoftverek (pl. MATLAB, RISK)	Elérhető szoftver (pl. OpenFTA)	Elérhető szoftverek (pl. GTAP, GAMS)
Alkalmazásához szükséges idő	Közepes (napoktól hetekig)	Rövid (órák és napok között)	Közepes (napoktól hetekig)	Hosszú (hetektől hónapokig)	Közepes (hetek)	Hosszú (hetektől hónapokig)	Közepes (hetek)	Hosszú (hetektől hónapokig)

A kritikus infrastruktúrák kockázatelemzésére számos módszer létezik, amelyek különböző megközelítésekkel és alkalmazási területekkel rendelkeznek. A fentiekben megadott módszereket összehasonlítva az alábbi eredményeket kapjuk:

a. Az FMEA az alkatrészszintű kockázatok azonosítására alkalmas módszer, amely szisztematikusan elemzi az egyes komponensek lehetséges meghibásodási módjait, azok okait és következményeit. Hatékonysága abban rejlik, hogy részletesen feltárja az egyedi alkatrészek hibáinak hatásait, azonban nem alkalmas a rendszerszintű kölcsönös függőségek átfogó elemzésére, mivel főként az egyes komponensekre fókuszál, és nem veszi figyelembe a rendszerek közötti komplex interakciókat. [110]
b. A CARVER módszer egyszerű és gyors módot kínál a kritikus szervezetek és eszközök rangsorolására, különösen biztonsági és védelmi kontextusban. A módszer pontozási rendszere lehetővé teszi az eszközök fontosságának és sebezhetőségének gyors értékelését, azonban nem elég részletes vagy átfogó a komplex kockázatelemzésekhez, mivel hiányzik belőle a mélyebb analitikus mélység és a rendszerszintű összefüggések kezelése. [111]
c. A Bow-Tie módszer vizuálisan ábrázolja a kockázatokat, azok okait, következményeit és az alkalmazott ellenőrzési intézkedéseket. Ez a szemléletes megközelítés különösen hasznos a kockázatok kommunikálásában és megértésében. Nagyobb rendszerek esetén azonban az elemzés bonyolulttá és nehezen kezelhetővé válhat, mivel a diagramok mérete és összetettsége gyorsan nőhet, ami korlátozza a praktikus alkalmazhatóságot.
d. A HAZOP egy strukturált és részletes kockázatértékelési módszer, amelyet főként folyamatok és rendszerek hibáinak azonosítására használnak. Különösen hatékony a potenciális veszélyek és működési problémák feltárásában, de idő- és erőforrás igényes, mivel alapos szakértői elemzést és csoportmunkát igényel, ami korlátozhatja a gyors alkalmazását. [112]
e. A RAMCAP módszer kifejezetten a kritikus infrastruktúrák védelmére lett kifejlesztve, és az eszközök rangsorolására fókuszál a kockázatok és fenyegetések alapján. Hatékonysága abban rejlik, hogy integrált keretrendszert nyújt a kockázatok kezelésére, azonban alkalmazása speciális kontextusokra korlátozódik, és nem feltétlenül alkalmas minden típusú kockázatelemzésre. [157]
f. A Monte Carlo-szimuláció egy valószínűségi módszer, ami statisztikai modellezéssel nyújt betekintést a kockázatok bizonytalanságába és valószínűségébe.

Kiválóan alkalmas komplex rendszerek sztochasztikus elemzésére, de jelentős számítási erőforrásokat és adathalmazokat igényel, ami korlátozhatja a kisebb szervezetek számára való hozzáférhetőségét. [113]

g. Az FTA hatékony eszköz a rendszerhibák kiváltó okainak azonosítására, logikai diagramok segítségével modellezi a hibák ok-okozati összefüggéseit. Bár rendkívül pontos és részletes, a rendszer méretével arányosan nő a komplexitása, ami időigényes és szakértői tudást igénylő folyamattá teheti. [114]
h. Az IIM a kritikus infrastruktúrák gazdasági hatásainak elemzésére specializálódott, különösen a rendszerek közötti kölcsönös függőségek figyelembevételével. Ez a módszer egyedülálló a gazdasági következmények modellezésében, de alkalmazása fejlett szakértelmet és nagy adathalmazokat igényel, ami korlátozhatja a gyakorlati alkalmazását. [115]

Összességében ezek a módszerek különböző erősségekkel és korlátokkal rendelkeznek, és alkalmazásuk a konkrét kockázatelemzési feladatoktól és a rendelkezésre álló erőforrásoktól függ. A táblázat strukturált módot kínál a különböző módszerek összehasonlítására azok fő jellemzői és a különböző kritikus infrastruktúra kockázatelemzési feladatokra való alkalmassága alapján.

A kockázatelemzési módszerek vizsgálatának eredményeképpen megállapítható, hogy integrált megközelítés szükséges, mivel a kritikus szervezetek és infrastruktúrák védelme nem korlátozódhat az egyes rendszerekre, figyelembe kell venni a kölcsönös függőségeket és a több rendszerre és ágazatra kiterjedő meghibásodások lehetőségét. Emellett a rugalmasság fontossága elengedhetetlen, mivel a kockázatok puszta felmérésén túlmenően ki kell emelni az ellenálló infrastruktúra kiépítésének fontosságát, amely képes ellenállni a zavaroknak és gyorsan helyreállni azokból. A módszertanok célja, hogy eszközöket biztosítson a döntéshozók számára a kockázatok jobb értékeléséhez. Hangsúlyozni szükséges annak fontosságát, hogy csökkentsük a komplexitást, és olyan magas szintű modellek létrehozására összpontosítsunk, amelyek időben tájékoztatják a döntéseket.

A technológiai, gazdasági és ellenálló képességi modellek kombinálása elengedhetetlen, hogy jobban megértsük és csökkentsük a kritikus szervezetek és infrastruktúrák megszakadásával kapcsolatos kockázatokat, és ezáltal szilárd keretet biztosítsunk az infrastruktúra biztonságának és ellenálló képességének fokozásához Európa szerte. [79]

3.2 A kritikus szervezetek és a hatóságok közötti kommunikációs folyamatok elemzése

A kritikus szervezetek és infrastruktúrák ellenálló képességért felelős vezetői és a hatóságok közötti kommunikációs problémák akadályozhatják a hatékony együttműködést és a kockázatkezelést. Gyakori probléma közé tartozik az egyértelmű kommunikációs csatornák hiánya. A kritikus szervezetek ellenálló képességért felelős vezetői és a különböző hatóságok közötti következetlen vagy nem egyértelmű kommunikációs csatornák késedelmeket és zavart eredményezhetnek.

Ennek eredményeként az időben történő információcsere hiányához vezethet, különösen válsághelyzetek vagy sürgős helyzetek esetén, ami lelassítja a fenyegetésekre vagy zavarokra való reagálást. Másik gyakori probléma a nem megfelelő információmegosztás, mivel előfordulhat, hogy a vezetők nem kapnak elegendő vagy részletes információt a hatóságoktól a felmerülő fenyegetésekről, a szabályozási változásokról vagy a legjobb gyakorlatokról. Emiatt a szervezetek felkészületlenül maradhatnak, ami megnehezítheti a sebezhetőségek időben történő kezelését.

Problémaként jelenik meg, hogy a hatóságok egymásnak ellentmondó vagy folyamatosan változó iránymutatásokat adhatnak, különösen a különböző ágazatokban vagy régiókban, így a kritikus szervezetek ellenálló képességért felelős vezetői számára nehézséget jelent naprakésznek maradni és lépést tartani a változásokkal. Ennek következtében a vezetők nehezen tudják összehangolni biztonsági intézkedéseiket a változó követelményekkel, ami növeli a megfelelés hiányának vagy a biztonsági hiányosságok kockázatát.

Ezenfelül a kritikus szervezeteknek nem biztos, hogy elegendő lehetőségük van arra, hogy visszajelzést adjanak a hatóságoknak az előttük álló kihívásokról. Megfelelő visszajelzési körök nélkül a hatóságok nem lehetnek tisztában a helyszínen felmerülő problémákkal, ami olyan ajánlásokhoz vezethet, amelyek nem gyakorlatiasak vagy nem hatékonyak.

A vészhelyzetek vagy biztonsági események során a kritikus szervezetek és infrastruktúrák biztonságával foglalkozó vezetők és a hatóságok közötti koordináció késhet, amely lassú vagy széttagolt válaszlépéseket eredményezhet, ami növeli a kritikus rendszerek esetleges károsodását vagy leállását.

Ezen felül problémaként jelenhet meg, hogy a vezetők nem férnek hozzá a hatóságok birtokában lévő, a potenciális fenyegetésekről szóló minősített vagy érzékeny információkhoz, azonban az átfogó fenyegetési információkhoz való hozzáférés nélkül a kritikus szervezetek és infrastruktúrák védelmére irányuló erőfeszítések veszélybe kerülhetnek, mivel a biztonsági intézkedések nem feltétlenül a legfontosabb vagy legjelentősebb kockázatokra irányulnak. Itt nem azon van a hangsúly, hogy a kritikus szervezetek ellenálló képességért felelős vezetői minden minősített irathoz hozzáférjenek, hanem a számukra releváns kockázatokról értesüljenek.

Mindemellett a hatóságok esetleg nem kommunikálnak elég gyakran az kritikus szervezetekkel, ami hiányosságokat okoz az információáramlásban. Ez azt eredményezi, hogy a szervezetek nincsenek tisztában az aktuális kockázatokkal, a szabályozások frissítéseivel vagy a biztonsági környezetben bekövetkezett változásokkal. [116]

Figyelembe kell venni, hogy a hatóságoknak és a kritikus szervezeteknek eltérő prioritásaik lehetnek a biztonság szempontjából legfontosabb kérdéseket illetően, ami a célok és intézkedések összehangolatlanságához vezet. Ez súrlódásokat okozhat a biztonsági intézkedések végrehajtásában, és azt eredményezheti, hogy a kulcsfontosságú területeket figyelmen kívül hagyják. Emellett előfordulhat, hogy a kritikus szervezetek és a hatóságok nem kapnak megfelelő képzést arról, hogyan kommunikáljanak hatékonyan egymással rutinműveletek vagy válsághelyzetek során. Félreértés alakulhat ki, ami csökkenti a biztonsági erőfeszítések általános hatékonyságát és a reagálás gyorsaságát. [127]

Összegezve a fentieket, a kritikus szervezetek és infrastruktúrák biztonságáért felelős vezetők és a hatóságok közötti hatékony kommunikáció elengedhetetlen a fenyegetések időben történő észleléséhez és elhárításához, a jogszabályoknak való megfeleléshez és az infrastruktúra védelméhez. E kommunikációs problémák megoldásához világos protokollokra, rendszeres és átlátható információcserére, valamint jobb koordinációs mechanizmusokra van szükség mind a rutinműveletek, mind a válsághelyzetek során.

3.2.1 A kommunikáció fejlesztési lehetőségei a kritikus szervezetek és a hatóságok között

A kritikus szervezetek ellenálló képességért felelős vezetői és a hatóságok közötti kommunikáció javítása alapvető fontosságú az együttműködés fokozása és a kritikus szervezetek és infrastruktúrák hatékony védelmének biztosítása szempontjából. Az alábbiakban megvizsgálom a kommunikációs gyakorlatok, fórumok és tájékoztatók révén történő javításának módszereit.

A közös gyakorlatok révén, amelyek során a kritikus szervezetek ellenálló képességért felelős vezetői és a hatóságok együtt vesznek részt a kritikus szervezetek és infrastruktúrát fenyegető forgatókönyvek végrehajtásában. Ezeknek a gyakorlatoknak valós élethelyzeteket kell szimulálniuk, például kibertámadásokat, természeti katasztrófákat vagy terrorista fenyegetéseket. A gyakorlatok segítenek azonosítani a kommunikációs hiányosságokat, egyértelmű kommunikációs protokollokat kialakítani, és javítja a valós idejű döntéshozatalt nyomás alatt. Javasolt lenne több olyan gyakorlat szervezése, amelyeken a különböző kritikus szervezetek ágazatai (pl. energia, közlekedés, kommunikáció) együtt dolgoznak a hatóságokkal. Ez javítja a kölcsönös függőségek megértését és elősegíti az ágazatok közötti összehangolt kommunikációs stratégiák kialakítását. [127]

Az ágazatközi gyakorlatok ösztönzik az ágazatközi együttműködést, biztosítja, hogy vészhelyzetben valamennyi ágazat hatékonyan meg tudja osztani egymással a kritikus információkat. Az interoperabilitási gyakorlatok arra összpontosítanak, hogy a különböző ágazatok infrastruktúrái hogyan hatnak egymásra válsághelyzetekben. Javasolt minden gyakorlatot követően strukturált eligazítást kell tartani mind a kapcsolattartókkal, mind a hatóságokkal, hogy megvitassák, mi működött jól, és hol van szükség a kommunikáció javítására. A gyakorlatok lehetővé teszik az azonnali visszajelzést, és fejleszti a kommunikációs stratégiák hatékonyságát.
A kritikus szervezetek ellenálló képességért felelős vezetőinek rendszeres fórumon történő részvétele, ahol a vezetők és a hatóságok találkoznak elősegítenék a folyamatos kapcsolatot, biztosítva, hogy mindkét fél tájékozott maradjon és helyszínt biztosít a biztonsági kérdésekről folytatott nyílt párbeszédhez. A rendszeres fórumokon meg tudják vitatni a folyamatban lévő kérdéseket, megosztják a friss tudásokat és visszajelzést adhatnak a jelenlegi kommunikációs gyakorlatokról. [171]

Ezentúl javítaná a kommunikációt az ágazatspecifikus munkacsoportok létrehozása, amely célzott megbeszéléseket és megoldásokat biztosít, amelyek az egyes ágazatok egyedi igényeihez igazodnak. A munkacsoportok konkrét ágazatokra pl. pénzügyek, egészségügy, közlekedés összpontosítanak, ahol a kapcsolattartók és a hatóságok rendszeresen találkozhatnak, hogy az ágazatspecifikus kihívásokkal s kommunikációs igényekkel foglalkozzanak. Ilyen az előző fejezetben is javasolt ágazati munkacsoport. A hatékony kommunikációt nagyban javítaná a folyamatos tájékoztatás, a kritikus szervezetek ellenálló képességért felelős vezetői és a hatóságok rendszeresen tudnak tájékozódni az újonnan felmerülő fenyegetésekről, szabályozási változásokról és a legjobb biztonsági gyakorlatok frissítéséről.

Ezek a tájékoztatások történhetnek személyesen, virtuálisan vagy írásbeli jelentéseken keresztül. Ez lehetővé tenné, hogy a kapcsolattartókat folyamatosan tájékoztassa a legújabb fejleményekről, és biztosítsa, hogy biztonsági döntéseikhez a legfrissebb információkkal rendelkezzenek. Ezek havi vagy negyedéves fenyegetésinformációs tájékoztatók vagy hírlevelek, amelyek összefoglalják a legújabb fenyegetéseket, riasztásokat. Emellett gyors és biztonságos információcserét tenne lehetővé rutinműveletek és veszélyhelyzet során egy technológiai platform használata. Az lehetővé tenné az információk valós idejű megosztását az ellenálló képességért felelős vezetői és a hatóságok között, például titkosított üzenetküldő alkalmazások vagy a kritikus infrastruktúrákban érdekeltek számára létrehozott kommunikációs portálok. Ezentúl a rendszeres képzés biztosítja mind a felelős vezetői, mind a hatóságok számára a válsághelyzetekben történő hatékony kommunikációt A képzés kiterjedhet a minősített információk kezelésére, a több ügynökséget érintő válaszlépések koordinálására és a potenciális sebezhetőségek jelentésére. A képzések biztosítják, hogy mindkét fél jól felkészült legyen a hatékony kommunikációra. [117]

Az ellenálló képességért felelős vezetők és a hatóságok közötti kommunikáció javítása többoldalú megközelítést igényel, beleértve a közös gyakorlatokat, strukturált fórumokat és rendszeres tájékoztatókat. Ezek a tevékenységek bizalmat építenek, javítják a kölcsönös szerepek megértését, és javítják a kritikus információk áramlását a válságok előtt, alatt és után. Ezen intézkedések végrehajtásával mind a kapcsolattartók, mind a hatóságok jobb felkészültséget, gyorsabb reagálási időt és a kritikus szervezetek és infrastruktúrák hatékonyabb védelmét biztosíthatják. A kritikus szervezetek hatóságai és vezetői közötti kommunikáció fejlesztése nagyban hozzájárulna a kockázatelemzés elkészítéséhez, mivel a kritikus szervezetek ellenálló képességért felelős vezetői kellő tájékoztatást kapnának a Magyarországot érintő fenyegetésekről és naprakészen tudják tartani a kockázatelemzést, ezzel felkészülve a hibrid fenyegetésekre és azok hatásaira. [127]

3.3 A kockázati jelentés fejlesztésének koncepcionális kerete

Az aktuális fenyegetésekről való folyamatos és célzott tájékoztatás a kritikus szervezetek és infrastruktúrát ellenálló képességért felelős vezetői számára kiemelt jelentőséggel bír a modern kockázatmenedzsment szempontjából. A gyorsan változó kiberfenyegetések, természeti katasztrófák és geopolitikai kockázatok olyan komplex és dinamikus környezetet teremtenek, amelyben a stratégiai döntések megalapozottsága közvetlenül összefügg az aktuális információk rendelkezésre állásával és feldolgozásával.

A vezetők naprakész informálása elősegíti, hogy a kockázatelemzési folyamatok során ne csupán a régebbi adatokra, hanem a jelenlegi és jövőbeli veszélyforrásokra is építhessenek. Ennek köszönhetően a kockázatelemzés nem statikus dokumentummá válik, hanem élő, folyamatosan frissülő elemzési és döntéstámogató eszközzé. Ez jelentősen növeli a szervezet rezilienciáját, hiszen így gyorsabban képes reagálni az újonnan felmerülő fenyegetésekre, és a megelőző intézkedések is célzottabbá válnak. [118]

Továbbá a naprakész tájékoztatás erősíti a vezetők kockázattudatosságát, ami hozzájárul a felelős döntéshozatali kultúra kialakulásához. Így a szervezet nem csupán a jogszabályi kötelezettségek teljesítésére összpontosít, hanem proaktív módon képes kezelni a komplex kockázati környezetből fakadó kihívásokat. Összességében tehát az aktuális fenyegetésekről szóló rendszeres tájékoztatás a kockázatelemzés hatékonyságának és pontosságának alapvető feltétele, amely végső soron a kritikus szervezet biztonságát és működésének folyamatosságát szolgálja.

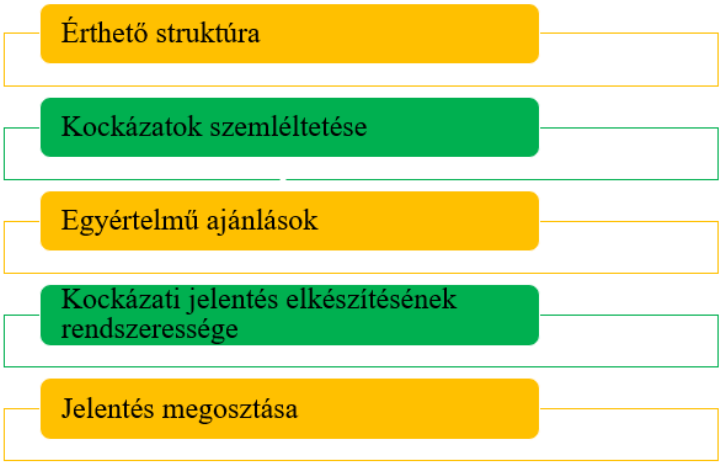
Amennyiben a kritikus szervezetek és infrastruktúrák ellenálló képességért felelős vezetői nem kapnak elegendő, pontos és időszerű információt a hatóságoktól az aktuális fenyegetésekről, az több szempontból is komoly problémákat okoz. Egyrészt jelentősen csökken a kockázatelemzés és a kockázatkezelési intézkedések megbízhatósága. Az információhiány miatt a vezetők kénytelenek részleges vagy elavult adatokra támaszkodni, ami félrevezető kockázatértékeléshez és nem megfelelő döntésekhez vezethet. Ez különösen kritikus lehet a gyorsan változó kiberfenyegetések, természeti katasztrófák vagy geopolitikai események esetén, ahol a késlekedés vagy a téves reakció súlyos következményekkel járhat. Másrészt az információhiány aláássa a szervezet reagálóképességét, ellenállóképességét, és rezilienciáját. [119] A megfelelő célzott intézkedések hiányában nő az esélye annak, hogy egy váratlan esemény jelentős fennakadást, szolgáltatás kiesést vagy akár katasztrófát okoz, ami nemcsak gazdasági, hanem társadalmi és nemzetbiztonsági szempontból is súlyos következményekkel járhat. Végül a hatóságok és a kritikus szervezetek közötti bizalom is sérül, ha a vezetők nem jutnak hozzá a döntéseikhez szükséges információkhoz. Ez hosszú távon akadályozhatja az együttműködést, és gyengítheti a nemzeti szintű kockázatkezelési és válságkezelési rendszerek hatékonyságát. Összességében tehát az információhiány közvetlen és közvetett módon is növeli a társadalom egészét érintő kockázatokat.

A kockázati jelentés szerepe és szükségessége a kritikus szervezetek védelmében

A kommunikációs problémák kiküszöbölése és a kockázatelemzés naprakészen tartása érdekében javaslom egy kockázati jelentés bevezetését.

Ennek eredményeképpen az üzemeltetők világos képet kapnak a szervezeten belülről eredő potenciális kockázatokról, például a rendszer sebezhetőségéről, emberi vagy eljárási hibákról. A külső fenyegetések, például természeti eredetű fenyegetések, kiberfenyegetések, valamint geopolitikai és társadalmi fenyegetések kockázatainak áttekintésével az üzemeltetők jobban előre láthatják a zavarokat és felkészülhetnek azokra. Az átfogó kockázati jelentés segíti a kritikus szervezetek ellenálló képességért felelős vezetőit abban, hogy megalapozott döntéseket hozzanak arról, hogy hova osszák el az erőforrásokat, rangsorolják a kockázatcsökkentési stratégiákat és hajtsák végre a biztonsági intézkedéseket. [120]

A rendszeres negyedéves vagy féléves jelentések segítenek a felmerülő kockázatok folyamatos azonosításában és a korábban azonosított kockázatok nyomon követésében, biztosítva, hogy a kockázatkezelési folyamat dinamikus és reagáló maradjon. A kockázati jelentések áttekintésével az üzemeltetők a reaktívról a proaktív megközelítésre térhetnek át, és az események megelőzésével nem csak reagálhatnak azokra. A kockázati jelentés biztosítja, hogy a kritikus kockázati információk egyértelműen dokumentálva legyenek, és azokat minden érintett féllel közöljék beleértve a vezetőséget, a biztonsági csapatokat és a külső partnereket. A kockázati jelentések áttekintése lehetővé teszi az üzemeltetők számára, hogy értékeljék a meglévő ellenőrzések és kockázatcsökkentő intézkedések hatékonyságát, lehetőséget teremtve a folyamatos javításra. A kritikus szervezetek és infrastruktúrákban az ágazatok pl. energia, közlekedés közötti kölcsönös függőségek megértése alapvető fontosságú. A kockázati jelentés rávilágíthat arra, hogy az egyik területen jelentkező kockázatok hogyan hathatnak más területekre. A rendszeres jelentések bizonyítják, hogy a szervezet aktívan kezeli a kockázatokat. A fentiek alapján a kockázati jelentés készítésekor az alábbi fő pontokat javaslom kidolgozni:

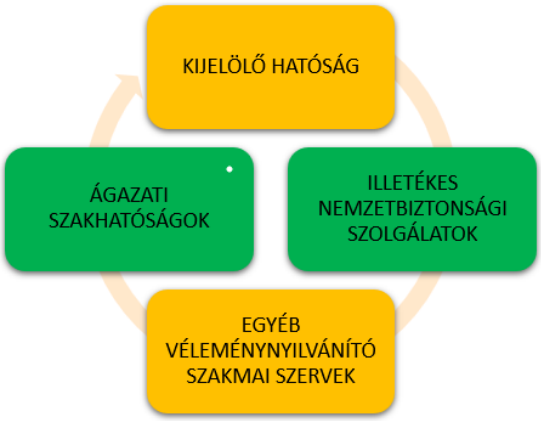


14. ábra: kockázati jelentés elkészítésekor figyelembe veendő szempontok

Készítette: a Szerző, 2025. [174]

1. A jelentésnek világos és érthető struktúrával kell rendelkeznie a könnyű feldolgozás érdekében. Pl.: kockázati kategóriák (pl. belső, külső, kiber, működési) szerint legyen rendezve átláthatóan.
2. Kockázati rangsorolás során szemléltetni szükséges a kockázati mátrixal vagy pontozási rendszerrel a fenyegetéseket valószínűség és hatás alapján.
3. A jelentésnek tartalmaznia kell egyértelmű ajánlásokat a kockázatcsökkentési stratégiákra, a végrehajtás ütemezésére és a felelős csapatokra vonatkozóan.
4. Biztosítani szükséges, hogy a kockázati jelentések rendszeresen (pl. negyedévente, félévente) készüljenek, hogy tükrözzék a fenyegetések alakulását.
5. A jelentés szükséges megosztani az összes érdekelt féllel, hogy megértsék az azonosított kockázatok kezelésében betöltött szerepüket.

A fentiekre tekintettel a kockázati jelentést a szakmailag illetékes szervek állítanák össze, ezzel biztosítva, hogy az illetékes ágazat a megfelelő kockázatokról tájékoztatja az illetékes kritikus szervezet és infrastruktúra ellenálló képességért felelős vezetőjét. Javaslom, hogy az ágazati kijelölő hatóságok, az ágazati szakhatóságok és a védelemben illetékes szervek bevonásával készítsék el a kockázati jelentést, így megalapozott és teljes körű dokumentumot tudnak szolgáltatni a szervezetek számára. [121]



15. ábra: Kockázati jelentés elkészítésében részt vevő szervek, Készítette: a Szerző, 2025. [174]

A kockázati jelentés elkészítése nemcsak jó gyakorlat, hanem a kritikus szervezetek és rendszerek hatékony kockázatkezeléséhez elengedhetetlen. Fokozza a tudatosságot, megkönnyíti a proaktív kockázatcsökkentést, biztosítja a megfelelőséget és támogatja a folyamatos fejlesztést. A belső és külső veszélyek figyelembevételével az üzemeltetők átfogó képet kapnak a rájuk leselkedő kockázatokról, és jobban felkészülnek rendszereik és infrastruktúrájuk védelmére. [122]

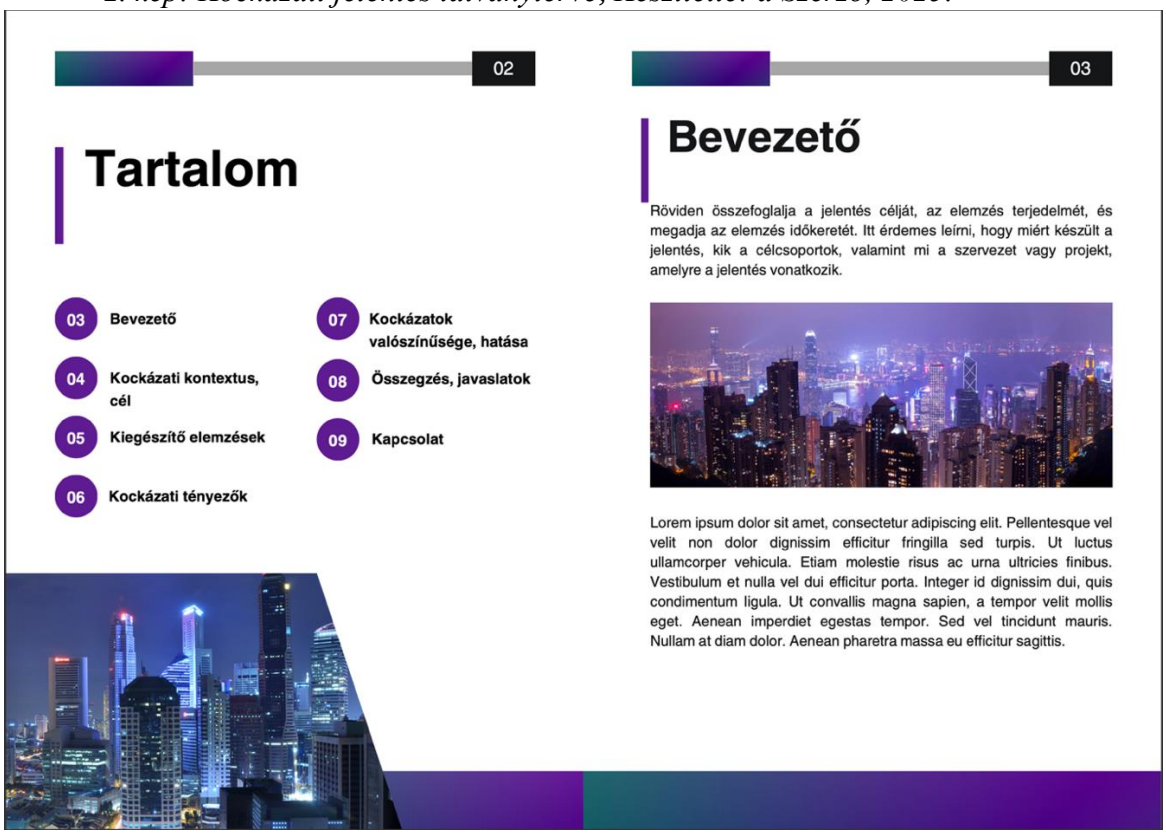
3.3.1 A kockázati jelentés felépítésének és tartalmi elemeinek elemzése

A kockázati jelentés felépítése szisztematikus és részletes, ügyelve arra, hogy minden fontos szempontot lefedjen, és hatékony eszköz legyen a döntéshozók számára a kockázatok kezelésére. Az alábbiakban bemutatom a kockázati jelentés főbb tartalmi elemeit és felépítését:

I. Cím és bevezetés

- A jelentés rövid, tömör megnevezése, ami tükrözi a kockázatelemzés célját.
- A bevezetés röviden összefoglalja a jelentés célját, az elemzés terjedelmét, és megadja az elemzés időkeretét. Itt érdemes leírni, hogy miért készült a jelentés, kik a célcsoportok, valamint mi a szervezet vagy projekt, amelyre a jelentés vonatkozik.

1. kép: Kockázati jelentés látványterve, Készítette: a Szerző, 2025.



2. kép: Kockázati jelentés első oldalai, Készítette: a Szerző, 2025.

II. Kockázati kontextus és cél

- A kockázati kontextus ismerteti a szervezet működési környezetét, a kockázati tényezők hátterét, és leírja azokat a körülményeket, amelyek befolyásolhatják a kockázatokat. Ezen a ponton azonosítani kell a szervezet fő tevékenységi területeit, és az ezekhez kapcsolódó fenyegetéseket.
- A cél rögzíti, hogy mi a jelentés fő célja pl. kockázatcsökkentés, új kockázatok azonosítása, valamint a kockázatelemzés hatókörét pl. mely rendszerekre, vagy tevékenységekre vonatkozik.

3. kép: Kockázati jelentés, kontextus és elemzés, Készítette: a Szerző, 2025.

III. Kockázatok azonosítása

- Részletezi a belső és külső kockázati tényezőket, amelyeket az elemzés során azonosítottak. Ezek lehetnek működési, pénzügyi, technológiai, szabályozási vagy külső kockázatok pl. természeti katasztrófák, kibertámadások, hibrid fenyegetések.
- Egy vizuális eszköz a kockázatok súlyosságának és valószínűségének rangsorolására. A mátrixban jellemzően a valószínűség és a hatás tengelyek mentén helyezkednek el a

kockázatok.

4. kép: Kockázati jelentés tartalma, Készítette: a Szerző, 2025.

IV. Kockázatok értékelése

- Minden azonosított kockázatot értékelnek a bekövetkezés valószínűsége és a potenciális hatása alapján. Ez alapján rangsorolnak, például magas, közepes, vagy alacsony kockázati szinteket határoznak meg.
- Elemzi, hogy az egyes kockázatok hogyan befolyásolhatják egymást vagy más rendszereket. Ezzel a szervezet interdependens rendszereinek biztonságát is szem előtt tartják.

- Kockázatcsökkentési javaslatok
- Részletezi a kockázatok mérséklésére vonatkozó javaslatokat, mint például új szabályozások, technológiai megoldások, képzések vagy vészhelyzeti tervek bevezetése.
- A legfontosabb kockázatokhoz társított prioritási sorrendet, amely figyelembe veszi a kockázat súlyosságát és a szervezet kockázatvállalási hajlandóságát.
- Minden javasolt intézkedéshez tartozik egy idővonal a végrehajtásra és a felelős személy

vagy csapat kijelölése.

V. Eredmények és következtetések

- Összefoglalja az elemzés legfontosabb megállapításait, például mely kockázatok a legnagyobb hatásúak, és milyen kockázatcsökkentő intézkedések szükségesek.
- Bemutatja, hogyan lehet a szervezet vagy rendszer működését biztonságosabbá és hatékonyabbá tenni a kockázatok kezelésével.

VI. Mellékletek és dokumentáció

- A jelentés tartalmazhat minden olyan háttérinformációt és adatot, amelyet a jelentés készítése során felhasználtak.
- Esetleg további részletek vagy statisztikák, amelyek alátámasztják a kockázatelemzést.

5. kép: Kockázati jelentés befejezése, Készítette: a Szerző, 2025.

Egy jól felépített kockázati jelentés részletesen bemutatja a kockázatok azonosításának, elemzésének és kezelésének folyamatát. A jelentés célja, hogy átfogó képet nyújtson a potenciális kockázatokról, és konkrét javaslatokat tegyen a kockázatok mérséklésére és a szervezet működésének biztonságosabbá tételére. [174]

A kritikus szervezetek és infrastruktúrák interdependenciája napjaink összetett, hálózatos rendszereiben számos kockázatot hordoz, egyetlen ágazatban bekövetkező zavar dominóhatásként tovagyűrűzve súlyos következményeket okozhat más területeken is. E kölcsönös függőségek feltárása és kezelése különösen indokolt a létfontosságú szolgáltatásokat nyújtó szervezetek esetében, ahol az ellátás folyamatossága társadalmi és gazdasági szempontból is kritikus. [123]

Egy kockázatelemzési jelentés ebben a folyamatban kulcsszerepet játszhat, rendszerszintű áttekintést nyújt azokról a kapcsolódási pontokról, amelyek mentén az ágazatok egymásra hatnak. Az elemzés során célszerű nemcsak a direkt, hanem az indirekt, másodlagos és harmadlagos hatásokat is azonosítani, beleértve az ellátási láncban, kommunikációs és informatikai rendszerekben, energiabiztonságban vagy humánerőforrásban megnyilvánuló összefüggéseket. A jelentés eredményeire építve több gyakorlati megoldás is javasolható az interdependencia mérséklésére. Az egyik legfontosabb az ágazatok közötti információmegosztás és kommunikáció intézményesítése, például közös kockázati fórumok, egyeztetések vagy tematikus munkacsoportok létrehozásával. Ez lehetőséget teremt a potenciális kockázati láncolatok feltérképezésére és a tapasztalatok megosztására. Ezen túl a közös gyakorlati szimulációk és forgatókönyv alapú gyakorlatok is elősegíthetik, hogy a különböző ágazatok jobban megértsék egymás kitettségét, és összehangolják vészhelyzeti terveiket. Ezek során felszínre kerülhetnek olyan függőségek, amelyek a papíralapú tervezés során rejtve maradnának. [124]

Összességében tehát egy jól kidolgozott, több ágazatot átfogó kockázatelemzési jelentés nemcsak a kockázatok pontosabb feltérképezését segíti, hanem alapot teremt olyan célzott intézkedésekhez is, amelyek mérsékelhetik az ágazatok közötti kölcsönös függőségek hatásait, és ezáltal növelik a teljes rendszer rezilienciáját.

3.4 A kockázatelemzéssel kapcsolatos problémák feltárása a kritikus szervezetek szemszögéből

A kritikus szervezetek és infrastruktúrák ellenálló képességért felelős vezetőinek kérdőíves megkérdezése a kockázatelemzés és a stratégiai tervezés szempontjából kiemelten fontos eszköz. Ennek egyik legfőbb előnye, hogy közvetlen és strukturált módon teszi lehetővé a döntéshozók tapasztalatainak, észleléseinek és véleményének feltárását, amelyek gyakran nem tükröződnek a formális jelentésekben vagy statisztikai adatokban.

A kérdőíves megkérdezés révén naprakész képet kaphatunk arról, hogy azok mely fenyegetéseket tartják a legsúlyosabbnak, milyen működési gyengeségeket érzékelnek, és hol látják a legnagyobb hiányosságokat a védekezés terén. Ez a módszer hozzájárul a kockázatelemzési folyamatok pontosításához, valamint támogatja az egységes kockázati szemlélet kialakulását is.

Továbbá a kérdőívek kitöltése ösztönzi a vezetőket arra, hogy tudatosabban végig gondoljak saját szervezetük kitettségét, sérülékenységeit és felkészültségét, ami közvetve erősíti a kockázattudatos vezetői kultúrát is. Összességében tehát a kérdőíves megkérdezés nemcsak információt gyűjt, hanem aktívan hozzájárul a megelőző stratégia fejlesztéséhez, a fenyegetések jobb megértéséhez és végső soron a szervezet biztonságának növeléséhez is. Kutatásom során fontosnak tartottam, hogy ne csak a hatóságok szemszögéből közelítsem meg a kritikus szervezetek védelmét, hanem a kritikus szervezetek ellenálló képességéért felelős vezetők problémáit, véleményét is tanulmányozzam. Ennek érdekében kérdőív formájában meginterjúvoltam a honvédelmi ágazat ellenálló képességért felelős vezetőit, hogy a kutatásom valódi problémákra, kérdésekre reflektáljon, és pontosabban fogalmazzam meg javaslataimat.

A kérdőív felépítése és tartalmi fókusza alapján megállapítható, hogy jól illeszkedik a kritikus infrastruktúrákkal kapcsolatos kockázatelemzési gyakorlatok feltárását célzó kutatáshoz. A kérdések négy nagy területet fednek le, a biztonsági összekötők felkészültsége és képzési tapasztalatai, a hatóságokkal való kommunikáció minősége, a kockázatelemzési tevékenységek gyakorlata és módszertani szintje, a szervezeti interdependenciák és dominóhatások vizsgálata. Ez a struktúra lehetővé teszi, hogy a kitöltők visszajelzései mentén azonosíthatók legyenek a jelenlegi kockázatkezelési rendszer erősségei és hiányosságai, különösen a kockázatelemzés, a kommunikáció és a döntéstámogatás hármas metszéspontjában.

A kérdőív külön erőssége, hogy nem csupán a formális megfelelésre kérdez rá, hanem a tényleges működésre, például a kockázatelemzési eredmények visszacsatolására, az interdependenciák kezelésére, a hatóságokkal való kommunikáció gördülékenységére és a rendelkezésre álló erőforrásokra. A kvalitatív válaszok például a „fenyegetési adatokat várunk”, „nincs elegendő információ”, „több audit, több módszertani útmutató kell” erősítik azt a tudományos felismerést, hogy a kritikus infrastruktúravédelemben a kockázati információáramlás minősége sokszor nagyobb hatással van a rezilienciára, mint a formális szabályozási követelmények.

A kérdőív zárt és nyitott kérdéseket tartalmaz, mindösszesen 18 zárt és 9 nyitott kérdésre válaszoltak a kritikus szervezetek. A kérdőívet 2024. augusztus 20 - 2024. december 10. között tudták kitölteni, online formában a Google Forms-on keresztül.

A 29 szervezetből összesen 20-an töltötték ki a kérdőívet, ami 68,97%-os jó válaszadási aránynak számít, így megbízható és érdemben elemezhető mintát tudtam értékelni.

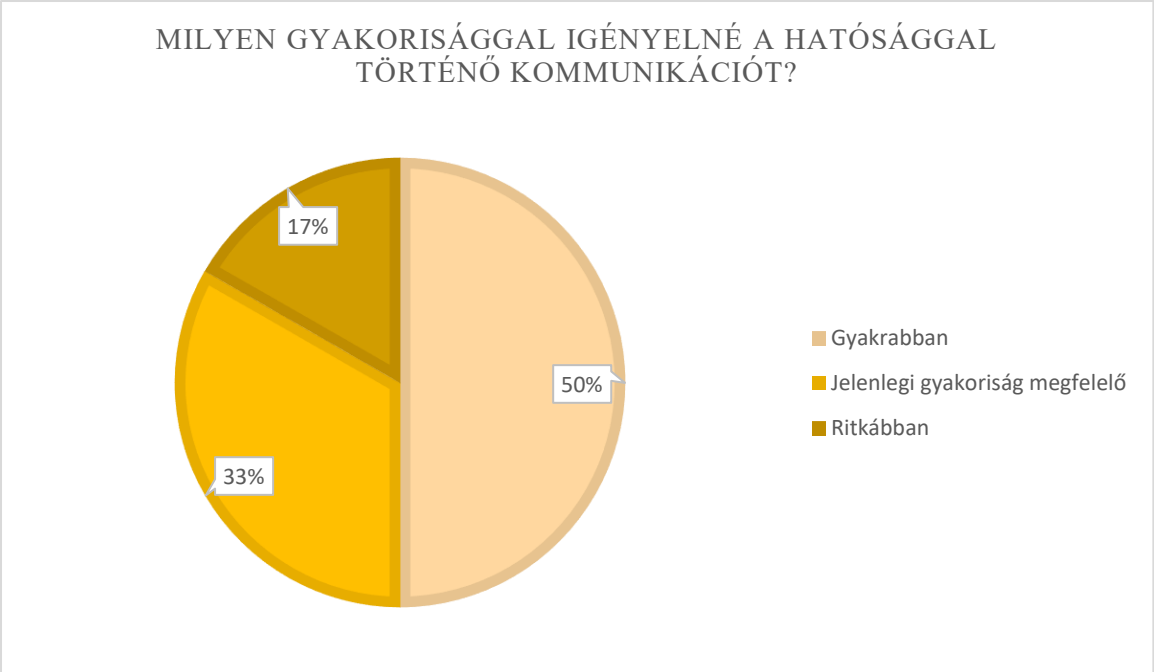
A kérdőív kettős kijelölésű kritikus szervezetek ellenálló képességért felelős vezetőinek is ki lett küldve, így annak kitöltése az alábbiak szerint alakult:

- 10 honvédelem
- 3 egészségügy
- 3 közlekedés
- 1 víz
- 3 infokommunikációs-technológiák.

Ebből 11 vezető több mint 5 éve látja el a feladatát, 3 vezető 5 éve és 6 vezető 3 éve. Arra a kérdésre, hogy milyen mértékben kap megfelelő képzést és támogatás a munkájához kapcsolódó feladatok ellátásában a válaszadók 33,3%-a mondta, hogy teljes mértékben, szintén 33,3% válaszolt erre úgy, hogy nagy mértékben, 16,7% válaszolt úgy, hogy korlátozottan vagy egyáltalán nem. Emellett 66,6% vallotta, hogy a munka ellátásához gyakran rendelkezésre állnak a szükséges erőforrások, és 16,7% szerint ritkán vagy soha nem állnak rendelkezésre. A kérdőív alapján a kritikus szervezet ellenálló képességért felelős vezetőjének munkáját segítenék a rendszeres képzések, és a gyakorlati példák bemutatása, valamint egy helyettes kinevezése.

Az elégedettség és kommunikáció szakaszban a hatóságok és a kritikus szervezetek közötti kommunikáció minőségének felmérése volt a cél. A válaszadók 33,3%-a mondta azt, hogy teljes mértékben elégedett a kommunikációval, 16,7%-a elégedett, 33,3%-a fejleszteni szükséges és 16,7 % válaszolta azt, hogy egyáltalán nem elégedett.

A kommunikáció fejlesztése érdekében a vezetőnek javasolt lenne a különféle jogszabályi, törvényi és személyi változásokról gyors tájékoztatást adni a hatóságok részéről. Szabályozott időközönként 3-6 hónap gyakorisággal kötelező lehetne az oda vissza történő kapcsolattartás. A válaszadók 50%-a javasolta azt, hogy a jelenleginél gyakrabban lenne szükséges a kommunikáció. A munkavégzésben akadályozó tényezőként szerepelt a jogszabályi változások nyomon követése. A legnagyobb kihívást a munkában az információhiány jelenti, ezt követi az erőforráshiány, képzési hiányosságok, valamint a túl sok adminisztráció.



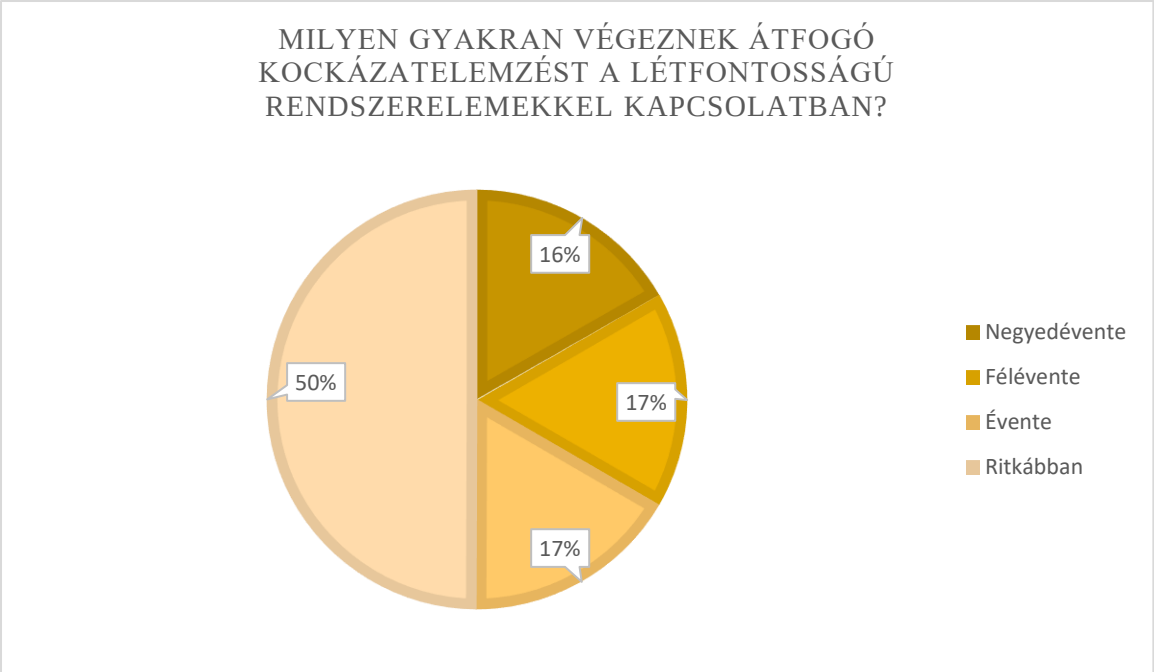
16. ábra: Hatósággal történő kommunikáció gyakorisága

Készítette: a Szerző, 2025.

A kritikus szervezet ellenálló képességért felelős vezetője és a hatóságok kommunikációjának javítása érdekében javaslom a rendszeres képzések és tapasztalatcsere bevezetését, külső kommunikáció, aktualizált módszertani segédleteket készítését és a vezetők részére történő rendelkezése bocsátását, valamint rendszeres szinten tartó, ismeretbővítő auditok lebonyolítását. Arra a kérdésre, hogy a szervezet milyen mértékben van felkészülve egy kritikus eseményre vagy támadásra, a megkérdezettek 50%-a válaszolt úgy, hogy nagy mértékben felkészült, 16,7% mondja, hogy teljes mértékben felkészült, részben felkészült és nem eléggé felkészült.

A kockázatelemzés szakaszban célom az volt, hogy felmérjem a kritikus szervezetek és infrastruktúrák szemszögéből a kockázatelemzés folyamatát, valamint az esetlegesen felmerülő problémákat.

A kritikus szervezet ellenálló képességért felelős vezetőinek válaszai alapján 16,7% végez átfogó kockázatelemzést negyedévente, 16,7% évente és félévente és 50% ennél ritkábban.



17. ábra: Átfogó kockázatelemzés gyakorisága

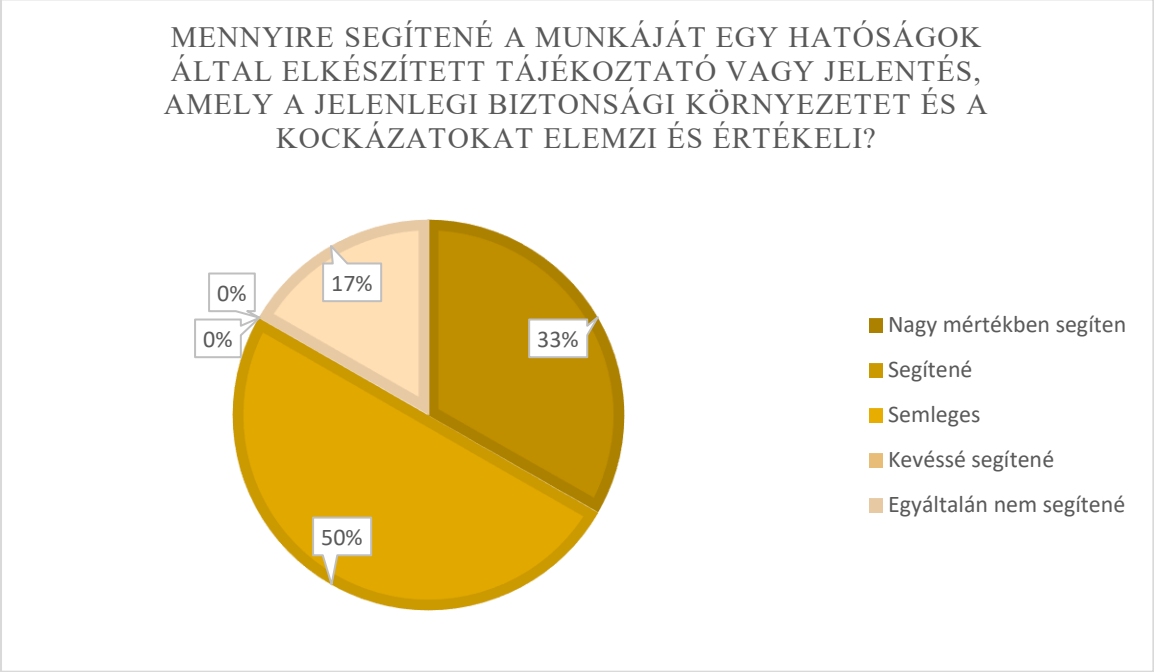
Készítette: a Szerző, 2025.

A vezetők belső szakemberek által készített informatikai, minőségirányítási dokumentumokat használnak forrásként a kockázatelemzés elvégzéséhez, valamint államilag elkészített stratégiákat, terveket, belső és külső adatokat, elöljárói intézkedéseket, biztonságpolitikai elemzéseket.

18. ábra: Kockázatelemzéshez használt források, Készítette: a Szerző, 2025.

A válaszadók 66,7%-a szerint nagy mértékben megfelelőek a kockázatelemzési módszerek és 16,7%-uk szerint nem megfelelőek vagy kevéssé megfelelőek. Ugyanennyi arányban érkezett válasz arra a kérdésre, hogy kap-e elegendő és megfelelő adatot a kockázatelemzés elvégzéséhez, felülvizsgálatához, 66,7% azt a választ adta, hogy többnyire igen, 16,7% pedig azt válaszolta, hogy igen, minden esetben vagy egyáltalán nem.

A megkérdezettek 33,3%-a mondta azt, hogy nagy mértékben segítené a munkáját a hatóságok által elkészített tájékoztató a jelenlegi biztonsági környezet és kockázatok értékeléséről, elemzéséről, 50% szerint segítené és 16,7% szerint egyáltalán nem segítené. Emellett 50%-uk mondja azt, hogy rendszeresen frissíti a kockázatelemzést az aktuális biztonságpolitikai helyzetnek megfelelően, 33,3% szerint alkalomszerűen frissíti és 16,7% nem frissíti.

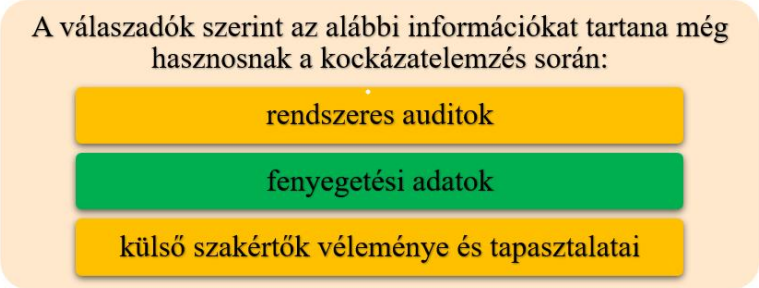


19. ábra: Tájékoztató szükségessége

Készítette: a Szerző, 2025.

A vezetők 66,7%-a érzi úgy, hogy a kockázatelemzésből származó eredmények alapján megfelelő intézkedések születnek a kockázatok csökkentésére, 16,7%-uk úgy gondolja, hogy semleges vagy egyáltalán nem elégedett. Eközben 50% mondja azt, hogy nagy mértékben alkalmazzák a kockázatelemzésben javasolt intézkedéseket, 16,5% pedig vagy teljes mértékben, korlátozottan vagy egyáltalán nem. 83,3% mondja azt, hogy közepesen nehéz beépíteni a kockázatelemzési ajánlásokat, és 16,7 % mondja, hogy nagyon nehéz.

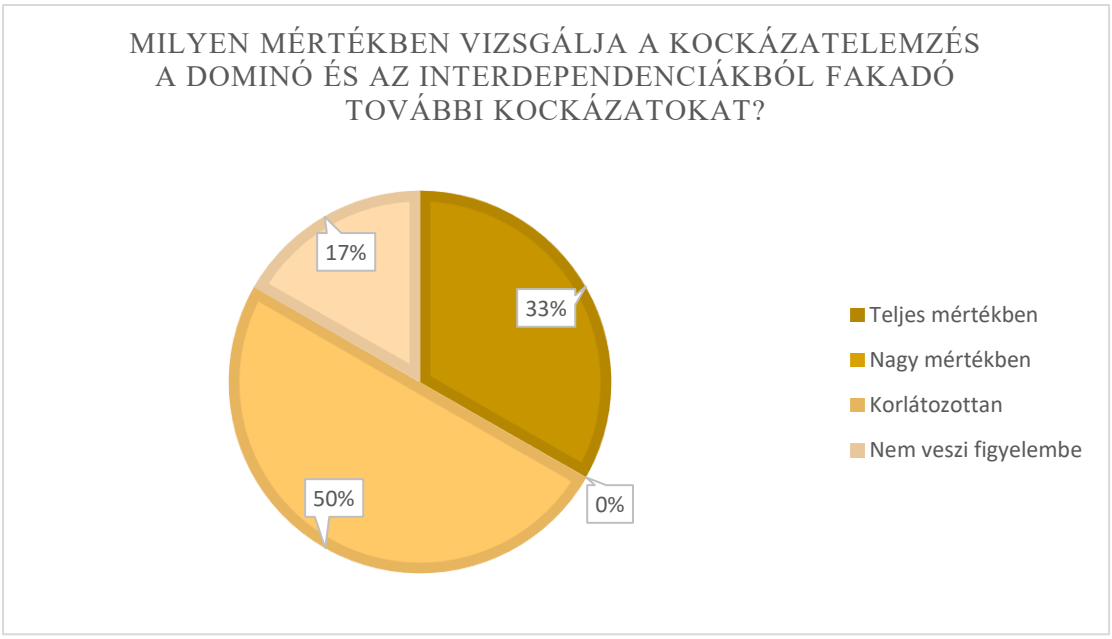
A válaszadók szerint az alábbi információkat tartana még hasznosnak a kockázatelemzés során:



20. ábra: Hasznos információk, Készítette: a Szerző, 2025.

A vezetők fele úgy értékeli, hogy a kockázatelemzés az interdependenciákból fakadó további kockázatokat korlátozottan vizsgálja, 16,7% úgy gondolja, hogy nem veszi figyelembe és 33,3%-uk mondja, hogy teljes mértékben vizsgálja. A kockázatelemzési fejlesztési javaslatok a kritikus szervezetek és infrastruktúrák védelme érdekében a kritikus szervezetek ellenálló képességért felelős vezetőinek tollából:

- automatizált eszközök, központi kockázati adatbázis,
- a környezetvédelem területén,
- informatika területén,
- dominó- és az interdependencia hatás területén.



21. ábra: Interdependencia vizsgálata

Készítette: a Szerző, 2025.

A kockázatelemzés hatékonyabb elvégzéséhez javasolt lenne az automatizált eszközök megléte, külső szakértői, tanácsadói támogatás, és szervezetek közötti intenzívebb áramlást biztosító rendszerek, programok bevezetése. A kockázatelemzési eredmények kommunikációját és megvalósítását hatékonyabbá tenné a belső képzés, a folyamatos belső kommunikáció és a magasabb vezetői támogatás, továbbá a fennálló kockázatok vezetői felismerése, elfogadása és azokra történő intézkedések meghozatala.

A kritikus infrastruktúrát működtető szervezetek ellenálló képességért felelős vezetőinek kérdőíves megkérdezése a kutatás egyik kulcseleme volt, amely több szempontból is indokolt és szakmailag megalapozott módszertani döntésnek bizonyult. A kérdőíves adatgyűjtés lehetőséget teremtett arra, hogy a vezetők közvetlen tapasztalataira és kockázatértékelésére építve pontosabb képet kapjak azokról a fenyegetésekről és sebezhetőségekről, amelyekkel a szervezetek szembenéznek a mindennapi működés során.

Az így nyert adatok rávilágítanak azokra a problématerületekre is, amelyeket a formális riportok és szabványos kockázatelemzési eljárások gyakran nem fednek fel. Az előnye továbbá abban rejlik, hogy elősegíti a kockázattudatos gondolkodás elmélyítését a szervezeti vezetés szintjén, ösztönözve őket saját rendszereik és folyamataik kritikus felülvizsgálatára. A teljes kérdőív a 10. mellékletben tekinthető meg.

Összességében tehát a kérdőíves megkérdezés nemcsak az adatok gyűjtését szolgálta, hanem hozzájárult a kutatás gyakorlati relevanciájához és a kockázatmenedzsment valósághűbb, több szempontot integráló megértéséhez is. Ezáltal a kutatás eredményei jobban illeszkednek a vezetői döntéshozatal igényeihez, és alkalmasabbak arra, hogy támogassák a szervezetek hosszú távú biztonsági stratégiáinak kialakítását és fejlesztését. A kérdőív eredményei jól illeszkednek a kutatási kérdésekhez, és megerősítik azt a feltételezést, hogy a kritikus szervezetek ellenálló képességért felelős vezetői a jelenleginél részletesebb és rendszeresebb tájékoztatásra tartanak igényt. Az adatok azt mutatják, hogy a vezetők nemcsak strukturált kockázati jelentések formájában várják az információkat, hanem igényt tartanak interaktív fórumokra és szakmai egyeztetésekre is, amelyek lehetőséget biztosítanak a tapasztalatok megosztására és a közvetlen visszacsatolásra. Ez alátámasztja, hogy a fenyegetésekről szóló tájékoztatás többcsatornás és rendszeres formája jelentős mértékben hozzájárulhat a kockázatértékelési folyamatok hatékonyságához és a szervezeti reziliencia erősítéséhez.

A kérdőív eredményei alapján jól látható, hogy a hazai kritikus szervezetek jelentős erőfeszítéseket tesznek a kockázatelemzési kötelezettségek teljesítésére, ugyanakkor a rendszer jelenleg módszertani és kommunikációs szempontból töredezett.

A kockázatelemzések formálisan léteznek, de sok esetben hiányosak a fenyegetési információk, eltérő a módszertani mélység, és nem áll rendelkezésre egységes reziliencia értékelési keretrendszer. A szervezetek közötti és a hatósággal folytatott kommunikáció nem elég konzisztens, ami tovább gyengíti a kockázatelemzési eredmények döntéstámogató funkcióját. A legkritikusabb hiányosság az interdependencia elemzés alacsony szintje, valamint a monitoring folyamat hiánya. Mindezek alapján elmondható, hogy a kockázatkezelési rendszer fejlesztése elsősorban standardizált módszertani útmutatást, ágazati szintű fenyegetés információs rendszert és formális visszacsatolási mechanizmusokat igényel.

3.5 Az adatbiztonság és adatvédelem szerepe a kockázati kommunikációs folyamatokban

A Kszetv. és a Kszetv. Vhr. egyértelműen előírja, hogy a kritikus szervezeteknek olyan információbiztonsági rendszert kell működtetniük, amely biztosítja az adatok bizalmasságát, sértetlenségét, és rendelkezésre állását.

E három alapelv nem pusztán kiberbiztonsági követelmény, hanem működési feltétel is. Az adatáramlás sérülése egy válsághelyzetben közvetlenül befolyásolhatja az ágazati koordinációt és a helyreállítási képességet. Ennek érdekében a Kszetv., a NIS2 Irányelvvel összhangban kiterjeszti az adatintegritás fenntartásának és a titoktartási kötelezettségnek az ellenőrzési és auditálási körét is. [13]

A kritikus szervezetek és a hatóságok közötti adatmegosztás nem kizárólag technikai, hanem bizalmi és etikai kérdés is. A gyakorlatban három alapelv érvényesítése kulcsfontosságú:

- minimális adatelv, csak a cél eléréséhez feltétlenül szükséges információk kerülnek megosztásra,
- transzparencia elve, a felek számára világos, hogy ki, mikor és milyen célból férhet hozzá az adatokhoz,
- visszacsatolás és korrekció elve, az adatmegosztás nem egyszeri aktus, hanem folyamatos folyamat, amelynek során a visszajelzések alapján az adatkezelés és -védelem is fejleszthető. [3]

A bizalmi alapú együttműködéshez szükséges az adatgazdák és adatkezelők közötti felelősségi határok egyértelmű rögzítése, valamint az adat hozzáférési protokollok dokumentálása pl. ki jogosult operatív adatok fogadására, ki jogosult a szervezeti oldaláról a kockázati jelentések kezelésére.

A nemzetközi tapasztalatok pl. Németország, Kanada egyértelműen alátámasztják, hogy a kritikus szervezetek közötti horizontális bizalmi háló legalább annyira fontos, mint a vertikális hatósági kommunikációs lánc. Az információmegosztás nem csupán adatáramlás, hanem intézményi tanulás és adaptáció is, a szervezetek egymás incidenseiből és reakcióiból képesek fejleszteni saját ellenálló képességüket. A bizalmi kapcsolatok erősítése tehát a reziliencia egyik puha, de kulcsfontosságú tényezője az adatsérthetetlenség technikai biztosítása önmagában nem elegendő a tényleges együttműködéshez. [46]

Az információmegosztás biztonságának és etikai dimenzióinak megerősítése elengedhetetlen a kritikus szervezetek működési rezilienciájához. A bizalmasság, az adatintegritás és a titoktartás követelményei nemcsak kiberbiztonsági, hanem szervezeti kockázatkezelési kérdések is. Ezen alfejezet hozzájárul annak bemutatásához, hogy a stratégiai együttműködés akkor válik valóban működőképessé, ha a technológiai biztonságot bizalmi, etikai és szervezeti kultúra is kíséri.

3.6 Összegzés

A kutatás eredményei rámutatnak arra, hogy a kritikus szervezetek biztonságának növeléséhez elengedhetetlen egy több ágazatot lefedő, rendszeres és strukturált kockázatelemzési jelentés bevezetése. Egy ilyen elemzés nemcsak a fenyegetések pontosabb azonosítását teszi lehetővé, hanem megalapozza azokat a célzott intézkedéseket is, amelyek képesek mérsékelni az ágazatok közötti kölcsönös függőségekből adódó hatásokat. Ennek eredményeként növelhető a teljes nemzeti rendszer rezilienciája, valamint javítható a krízishelyzetekből való gyors helyreállítás képessége.

A kérdőíves vizsgálat gyakorlati relevanciája abban mutatkozott meg, hogy nem csupán adatgyűjtésként szolgált, hanem feltárta a vezetői elvárásokat is a kockázatmenedzsment információk minőségével és elérhetőségével kapcsolatban. Az eredmények egyértelműen igazolják, hogy a kritikus szervezetek vezetői a jelenleginél részletesebb, rendszeres és könnyen értelmezhető kockázati jelentéseket igényelnek. Emellett hangsúlyosan jelenik meg az igény a szakmai egyeztetésekre és interaktív fórumokra, amelyek támogatnák a tapasztalatcserét és a közvetlen visszacsatolást.

Mindezek alapján javasolt a fenyegetésekről szóló tájékoztatás többcsatornás, rendszeres és szakmailag egyeztetett formájának kialakítása. Ez nemcsak a vezetői döntéshozatal pontosságát növeli, hanem hozzájárul a kockázatértékelési folyamatok hatékonyságához és a szervezeti reziliencia hosszú távú erősítéséhez.

3.7 Részkövetkeztetések a 3. fejezethez

Jelen fejezetben első célkitűzésem volt a kockázatelemzéssel összefüggő tapasztalatok feldolgozása, és a kockázatelemzési módszertan kutatása és fejlesztése, amelynek során az alábbi főbb következtetésekre jutottam:

1. A vizsgált esettanulmányok világosan bemutatják, hogy a különféle kockázatértékelési módszertanok miként járulnak hozzá a kritikus infrastruktúrák védelméhez. Bár mindegyik megközelítés eltérő hangsúlyokat alkalmaz és más szemszögből közelít, közös céljuk a rendszerek sebezhetőségének mérséklése és az ellenállóképesség növelése. A módszerek eredményes gyakorlati használatához elengedhetetlen, hogy az adott infrastruktúra sajátosságainak és a konkrét fenyegetési környezetnek megfelelően válasszuk ki a leginkább megfelelő értékelési eljárást. Egyetlen kockázatelemzési módszertan sem ad teljes körű megoldást, szükség van az eltérő megközelítések ötvözésére.
2. A kutatás rámutatott arra is, hogy a kizárólag egyes rendszerekre összpontosító kockázatelemzés önmagában nem elegendő. A kritikus szervezetek és infrastruktúrák védelmében elengedhetetlen az integrált megközelítés, amely figyelembe veszi az ágazatok közötti kölcsönös függőségeket, valamint a több rendszert érintő, láncreakciós meghibásodások kockázatát. Az ágazatok közötti függőségek és a rendszerek közötti kapcsolatok figyelmen kívül hagyása jelentős kockázatot hordoz.
3. Fontos kiemelni a rugalmasság szerepét is, nemcsak a kockázatok azonosítására és elemzésére kell összpontosítani, hanem olyan infrastruktúrák kialakítására, amelyek képesek ellenállni a váratlan zavaroknak, és gyorsan visszaállni a működőképességbe. A különböző módszertanok fő feladata, hogy hatékonyan támogassák a döntéshozatalt a kockázatok pontosabb értékelésével.

Második célkitűzésem volt a kritikus szervezetek ellenálló képességért felelős vezetői és a hatósággal kapcsolatos kommunikáció nehézségeinek vizsgálata és fejlesztési lehetőségeinek kutatása, amelynek során az alábbi főbb következtetésekre jutottam:

1. A kritikus szervezetek és infrastruktúrák biztonságáért felelős vezetők és a hatóságok közötti hatékony kommunikáció elengedhetetlen a fenyegetések időben történő észleléséhez és elhárításához, a jogszabályoknak való megfeleléshez és az infrastruktúra védelméhez.

E kommunikációs problémák megoldásához a gyakorlatban világos protokollokra, rendszeres és átlátható információcserére, valamint jobb koordinációs mechanizmusokra van szükség mind a rutinműveletek, mind a válsághelyzetek során. A munkájuk során a kritikus szervezetek hatóságai és vezetői közötti kommunikáció fejlesztése nagyban hozzájárulna a kockázatelemzés elkészítéséhez, mivel a kritikus szervezetek ellenálló képességért felelős vezetői kellő tájékoztatást kapnának a Magyarországot érintő fenyegetésekről és naprakészen tudják tartani a kockázatelemzést, ezzel felkészülve a hibrid fenyegetésekre és azok hatásaira, amit be tudnak építeni a kockázatelemzésbe. Ennek érdekében javaslom a kutatásom során elkészített kockázati jelentés beépítését a kritikus szervezetek és hatóságok közötti kommunikációba.

2. Az eredményeim és a válaszok azt mutatják, hogy egy jól kidolgozott, több ágazatot átfogó kockázatelemzési jelentés nemcsak a kockázatok pontosabb feltérképezését segíti, hanem alapot teremt olyan célzott intézkedésekhez is, amelyek mérsékelhetik az ágazatok közötti kölcsönös függőségek hatásait, és ezáltal növelik a teljes rendszer rezilienciáját. A kutatás azt jelzi, hogy fontos lenne megvizsgálni egy kétirányú információcsere bevezetésének szükségességét.

Harmadik célkitűzésem volt a kockázatelemzéssel kapcsolatos problémák vizsgálata a kritikus szervezetek szemszögéből, amelynek során az alábbi főbb következtetésekre jutottam:

1. A kérdőív válaszaiból kirajzolódik, hogy a kritikus szervezetek ellenálló képességért felelős vezetői egyértelműen nagyobb hangsúlyt helyeznek a részletes, rendszeres és személyre szabott tájékoztatásra. Ennek alapján javasolt bővíteni a gyakorlatban az információátadás formáit, a formális jelentések mellett szükség van interaktív platformokra, workshopokra és konzultációs lehetőségekre.
2. A kérdőív eredményei megerősítik azt a feltételezést, hogy az információszolgáltatásnak nem szabad kizárólag strukturált jelentésekre korlátozódnia. A vezetők egyre inkább igénylik az interaktív fórumokat, szakmai egyeztetéseket és a kétirányú kommunikáció lehetőségét, ahol a tapasztalatmegosztás és közvetlen visszacsatolás is megvalósulhat. A vizsgálat tehát rávilágított, hogy érdemes kialakítani egy olyan többcsatornás tájékoztatási rendszert, amely lehetővé teszi a fenyegetésekkel kapcsolatos gyors, célzott és személyre szabott kommunikációt.

3. A kutatás alapján megállapítható, hogy a fenyegetésekről szóló tájékoztatás többcsatornás, rendszeres és élő kapcsolatot biztosító formája jelentősen növelheti a kockázatértékelés gyakorlati hasznát, és hozzájárul a szervezeti reziliencia megerősítéséhez. Ezért az adatok alapján érdemes lenne egy rendszeresen frissített, releváns és célzott kockázati jelentés bevezetése, amely a döntéshozók igényeire szabott módon készül el.

ÖSSZEGZETT KÖVETKEZTETÉSEK

I. A kritikus szervezetek és infrastruktúrák védelmi rendszerének elméleti és szabályozási megalapozása, kutatása és fejlesztése területén

Az első fejezetben fő kutatási célkitűzésem volt **a kritikus szervezetek védelmének intézményi és szabályozási keretrendszerének elemzése, azok fenyegetettségének, kritikus függőségi pontjainak feltárása,** amelynek alapján a következő összegzett következtetésekre jutottam:

1. A műszaki szakirodalom alapján egyértelműen megállapítható, hogy a kritikus infrastruktúrák kockázatelemzése területén a legtöbb modell, legyen az hálózatelméleti, megbízhatósági vagy rendszerdinamikai alapú közös nevezőként a komponensek sérülékenységének és a rendszerszintű összekapcsoltság hatásainak együttes értékelését tekinti meghatározónak. A vizsgált források ugyanakkor rámutatnak, a klasszikus műszaki megközelítések önmagukban nem képesek kezelni az ágazatközi interdependenciákból fakadó komplex hatásláncokat, ezért szükségessé vált az ilyen rendszerekre optimalizált hibrid modellek alkalmazása.
2. A szakirodalmi vizsgálat másik fontos tanulsága, hogy a műszaki alapú kockázatelemzési módszerek akkor biztosítanak valós döntéstámogató értéket, ha a numerikus mutatókat normalizált, összehasonlítható formában kezelik, és transzparens súlyozási eljárásokkal kapcsolják össze. A publikációk hangsúlyozzák, hogy a súlyozási struktúrák átláthatósága és reprodukálhatósága kulcsfontosságú a megbízható ágazati rangsorok és kockázati profilok kialakításához, különösen olyan heterogén infrastruktúrarendszerek esetében, ahol a műszaki paraméterek és a működési környezet ágazatonként jelentősen eltér.
3. A nemzetközi szakirodalom arra mutat rá, hogy a modern kockázati környezetben a kritikus infrastruktúrákat már nem lehet elszigetelten vizsgálni, a digitális hálózatok meghibásodása befolyásolja az energiairányítást és a közlekedési folyamatokat, a rendszerek sérülékenysége kihat a navigációra és hálózati időszinkronra, míg az energiaellátás kiesése a többi ágazat működésének alapfeltételeit veszélyezteti. Mindezek alapján szükséges a hálózatalapú megközelítések, a dominóhatások és az interdependenciák módszeres feltérképezése.

4. A szakpolitikai javaslatok ennek megfelelően a többágazatos, összehangolt kockázatelemzési gyakorlatok megerősítésére irányulnak. Indokolt az olyan elemzési módszerek szélesebb körű alkalmazása, amelyek a hálózati összefüggéseket és a szolgáltatás-folytonosságot is értékelik. A nemzetközi jó gyakorlatok alapján javasolt a digitális és világűrinfrastruktúrák időszinkronizációs függéseinek vizsgálata, a közlekedési alágazatok kritikus csomópontjainak részletes feltérképezése, valamint az energiaágazat vezérlőrendszereinek megerősítése.
5. A digitális, világűr-, közlekedési és energiaágazatok összehasonlító elemzése egyértelművé teszi, hogy ezek a rendszerek egymástól erősen függő, kiber és fizikai hálózatokként működnek, amelyek sérülése vagy kapacitáscsökkenése egyszerre több ágazatot érintő zavarokat idézhet elő.

A fenti következtetésekre alapozva ***igazoltnak látom az 1. hipotézisemben leírtak teljesülését, amellyel megalapoztam az 1. tudományos kutatási eredményemet***.

II. Az ágazati kockázatelemzés szükségességének elméleti és gyakorlati megalapozása területén

A második fejezetben kutatási célkitűzésem volt **egy ágazati kockázatelemzés kutatása és fejlesztése,** amelynek eredményei alapján az alábbi összegzett következtetésekre jutottam:

6. A magyar kritikus szervezetek kockázatelemzése jelenleg jellemzően szervezeti és nemzeti szinten zajlik, így hiányzik az ágazati szintű átfogó kockázati kép. Ez különösen problémás a dominóhatások és az ágazatközi függőségek feltérképezésekor, például az energia-, víziközmű-, és közlekedési rendszerek kölcsönhatásai esetében.
7. Jelenleg nincs egységes, szabványosított indikátorkészlet vagy súlyozási módszertan, amely lehetővé tenné az ágazatokon belüli és azok közötti kockázati szintek összehasonlítását. A szereplők heterogén módon végzik a kockázatelemzést, ami akadályozza az adatok aggregálhatóságát és a nemzeti szintű jelentéskészítést.
8. Az ágazati kockázatelemzés a sebezhetőségek azonosításával és a kockázatcsökkentési stratégiák végrehajtásával fokozza a kritikus infrastruktúrák ellenálló képességét, így javaslom annak kialakítását és beépítését a kritikus szervezetek védelmébe.
9. Az ágazati szintű kockázatelemzés és annak eredményei ezért nem az egyedi kockázatok mechanikus összegzése, hanem a kritikus infrastruktúrák hálózatos működéséből fakadó rendszerszintű kockázatok feltárásának eszköze.

A fenti következtetéseim alapján ***igazoltnak látom a 2. hipotézisem teljesülését, amely a 2. tudományos kutatási eredményemet alapozza meg.***

III. A kritikus szervezetek kockázatelemzési és kommunikációs folyamatainak értékelése és fejlesztése területén

A harmadik fejezetben fő kutatási célkitűzésem volt a **kritikus szervezetek és hatóságok közötti kommunikáció hatékonyságának kutatása és fejlesztése**, amelynek alapján a következő következtetésekre jutottam:

10. A kritikus szervezetek és infrastruktúrák biztonságáért felelős vezetők és a hatóságok közötti hatékony kommunikáció elengedhetetlen a fenyegetések időben történő észleléséhez és elhárításához, a jogszabályoknak való megfeleléshez és az infrastruktúra védelméhez. E kommunikációs problémák megoldásához a gyakorlatban világos protokollokra, rendszeres és átlátható információcserére, valamint jobb koordinációs mechanizmusokra van szükség mind a rutinműveletek, mind a válsághelyzetek során.
11. A kérdőív válaszaiból kirajzolódik, hogy a kritikus szervezetek ellenálló képességért felelős vezetői egyértelműen nagyobb hangsúlyt helyeznek a részletes, rendszeres és személyre szabott tájékoztatásra. Ennek alapján javasolt bővíteni a gyakorlatban az információátadás formáit, a formális jelentések mellett szükség van interaktív platformokra, workshopokra és konzultációs lehetőségekre.
12. A vizsgált esettanulmányok világosan bemutatják, hogy a különféle kockázatértékelési módszertanok miként járulnak hozzá a kritikus infrastruktúrák védelméhez. Bár mindegyik megközelítés eltérő hangsúlyokat alkalmaz és más szemszögből közelít, közös céljuk a rendszerek sebezhetőségének mérséklése és az ellenállóképesség növelése. A módszerek eredményes gyakorlati használatához elengedhetetlen, hogy az adott infrastruktúra sajátosságainak és a konkrét fenyegetési környezetnek megfelelően válasszuk ki a leginkább megfelelő értékelési eljárást.

A fenti következtetéseim alapján ***igazoltnak látom a 3. hipotézisem teljesülését, valamint véleményem szerint megalapoztam a 3. tudományos kutatási eredményemet is.***

ÚJ TUDOMÁNYOS EREDMÉNYEK

Kutatómunkám alapján az alábbi **<u>új tudományos eredmények elfogadására teszek javaslatot</u>**:

1. A kritikus szervezetek védelmének jogi szabályozási, fogalmi, eljárásrendi és műszaki szakirodalmára vonatkozó vizsgálatokra építve ***<u>megállapítottam</u>***, hogy a klasszikus műszaki kockázatelemzési megközelítések önmagukban nem képesek kezelni az ágazatközi interdependenciákból fakadó komplex hatásláncokat, ezért szükségessé vált az ilyen rendszerekre optimalizált hibrid modellek alkalmazása. Ennek függvényében ***<u>meghatároztam</u>*** a hálózati összefüggéseket és a szolgáltatás-folytonosságot is figyelembevevő kockázatelemzési módszereket, amelyek alkalmazása képes a vizsgált négy ágazat rendszerszintű kockázatainak mérséklésére és az ellenálló képességük növelésére.

2. A kritikus szervezetek védelmével összefüggő ágazati kockázatelemzés módszertanának megalapozása érdekében összehasonlítottam átfogó, többdimenziós elemzés keretében a különböző országok kockázatelemzési megközelítéseit, módszertani felépítéseit és interdependencia kezeléseit, melynek alapján ***<u>kidolgoztam</u>*** az ágazati kockázatelemzés módszertani kereteit és az ágazati szintű adatfeldolgozás elemzési alapjait, így biztosítva az ágazatokon belüli és azok közötti kockázati szintek összehasonlíthatóságát.

3. A kritikus szervezetek vezetői és a hatóságok közötti kommunikációs gyakorlat hatékonyságának értékelése és vizsgálata során ***<u>azonosítottam</u>*** a kommunikációs és koordinációs hiányosságokat, amelyek rendszerszintű kockázatokat generálnak. Ennek alapján ***<u>kidolgoztam</u>*** egy strukturált folyamatokra, és egységesített adatszolgáltatásra épülő módszertani eljárást, amely a hatóságok és akritikus szervezetek közötti egységesített adatszolgáltatásra épül, ezáltal támogatja a kockázatelemzések minőségének növelését és a döntéshozatal gyorsabb, megalapozottabb működését.

Az értekezés hipotéziseinek, kutatási célkitűzéseinek és tudományos eredményeinek egymásra épülését az ***5. mellékletben*** lévő táblázat szemlélteti**.**

AZ ÉRTEKEZÉS AJÁNLÁSAI

Az értekezésemben foglalt kutatási eredményekkel kapcsolatban az alábbi ajánlásokat teszem:

1. A kritikus szervezetek és infrastruktúrák védelmével, és kockázatelemzés fejlesztését érintő tanulmányt javaslom felhasználni a kritikus szervezetek védelmi célú kockázatelemzésének fejlesztési lehetőségeinek kimunkálásához.
2. Az ágazati kockázatelemzéssel összefüggő eredményeim kiválóan alkalmazhatók a kritikus szervezetek és infrastruktúrák hatósági feladatait ellátó szervek és kritikus szervezetek tevékenységében a műszaki követelmények és módszertanok kidolgozásához.
3. Az ellenálló képességért felelős vezetők és a hatóságok közötti kommunikáció érintő elemző és értékelő munkám során szerzett tapasztalatok és javaslatok széleskörűen alkalmazhatók a kockázatelemzés felülvizsgálatában és elkészítésében, illetve a kritikus szervezet védelmi tevékenységében.

A KUTATÁSI EREDMÉNYEK GYAKORLATI FELHASZNÁLHATÓSÁGA

A kutatómunka kutatási eredményeit az alábbiak szerint javaslom felhasználni:

1. Az értekezésemhez elkészített jogi szabályozással, a kritikus szervezetek védelmével foglalkozó elemzések és értékelések felhasználhatók az állami, az önkormányzati szervezetek, a kritikus szervezetek és hatóságok szakfeladatainak végrehajtásának fejlesztésére, illetve további szakmai és műszaki kutatások tudományos megalapozására.
2. A kockázatelemzés műszaki, technikai eszközrendszerével kapcsolatos vizsgálataim eredményei felhasználhatók a kockázati leírások, megvalósítási és rendszeresítési tervek elkészítéséhez, valamint az alkalmazási lehetőségek fejlesztéséhez.
3. Az értekezésem oktatási segédletként felhasználható a felsőoktatási intézmények kritikus infrastruktúrával összefüggő műszaki képzéseiben, valamint a rendvédelmi, honvédelmi és katasztrófavédelmi képzési intézmények által folytatott szakképzésben, továbbá a gazdálkodó szervezetek képzéseiben is.
4. A kutatás során kidolgozott ágazati kockázatelemzési módszertan és az ahhoz kapcsolódó kockázati modell közvetlenül alkalmazható a kritikus szervezetek és infrastruktúrák kockázatkezelési gyakorlatában, mivel egységes, összehasonlítható és skálázható értékelési keretet biztosít a különböző ágazatok között.
5. A javasolt eljárások alkalmasak a hatósági kockázati jelentések egységesítésére, a nemzeti szintű döntéstámogatás megalapozására, valamint az ágazatközi interdependenciákból fakadó rendszerszintű kockázatok feltárására.

A kifejlesztett egyszerűsített kockázati modell előnye, hogy alacsonyadat- és erőforrásigénnyel is megbízható, strukturált bemenetet biztosít az összetettabb, súlyozott ágazati elemzésekhez. Ezáltal a módszertan gyakorlati haszna abban áll, hogy támogatja a kritikus szervezetek kockázatértékelési érettségének növelését, javítja a hatóságok felé történő kommunikáció minőségét, és elősegíti a kockázatkezelési intézkedések priorizálását, különösen a szűkös erőforrásokkal rendelkező ágazatok esetében. A kutatás eredményei így kézzelfogható módon járulnak hozzá a nemzeti ellenállóképesség erősítéséhez és a döntéshozatal bizonytalanságának csökkentéséhez.

Budapest, 2026. február 15.

Ronyecz Lilla

HIVATKOZOTT IRODALOM

[1] Ronyecz L., „A new approach to the protection of critical infrastructures: the new directive on the resilience of critical entities," *AMERICAN JOURNAL OF RESEARCH EDUCATION AND DEVELOPMENT,* 1. kötet 1, pp. 65-79, 2024. https://red.devlart.hu/issues/2024_1.pdf (2025. 10. 02.)

[2] Ronyecz L., Bognár B., „Implement regulation on the resilience of critical entities in Hungary," *Védelem Tudomány 2024. különszám,* 1. kötet 9. pp. 119-123, 2024. https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/17977/14866 (2025. 02. 10)

[3] *Az Európai Palamentés Tanács 2022/2555 Irányelve (2022. december 14.) 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) 2016/1.*

[4] *Az ország védelme és biztonsága szempontjából jelentős szervezetek ellenálló képességéről szóló 475/2024. (XII. 31.) Korm. rendelet.*

[5] *Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti stratégiájáról szóló 1192/2025. (VI. 5.) Korm. határozatot.*

[6] M. Theoharidou, „Risk assessment methodology for interdependent critical infrastructures," *International Journal of Risk Assessment and Management, 2*. kötet , 15. szám, pp. 160-175, 2011. https://www.inderscienceonline.com/doi/abs/10.1504/IJRAM.2011.042113 (2025. 12. 22)

[7] National Strategy for Critical Infrastructure, Her Majesty Queen in Right of Canada, 2009. https://publications.gc.ca/collections/collection_2010/sp-ps/PS4-65-2009-eng.pdf (2025. 01. 05.)

[8] E. Zio, „Challenges in the vulnerability and risk analysis of critical infrastructures," *Reliability Engineering & System Safety,* 152. szám, pp. 137-150, 2016. https://www.researchgate.net/publication/303157279_Challenges_in_the_vulnerability_and_risk_analysis_of_critical_infrastructures (2025. 03. 12.)

[9] Cimmer Zs., Kátai-Urbán L. és Vass Gy., „Veszélyes üzemekkel kapcsolatos üzemazonosítási szabályozás értékelése-hazai szabályozás," *Hadmérnök, X.* kötet, 3. szám, pp. 67-77, 2015. http://hadmernok.hu/153_06_cimerzs_kul_vgy.pdf (2025. 04. 12.)

[10] . Mógor J és Angyal I., „A létfontosságú rendszerek védelmére vonatkozó szabályozás fejlesztése," *Scientia et Securitas, 3*. kötet, 2. szám, pp. 118-125, 2022. https://www.researchgate.net/publication/365398702_A_letfontossagu_rendszerek_vedelmere_vonatkozo_szabalyozas_fejlesztese (2025. 11. 12.)

[11] Mógor J. és Angyal I. , „A kritikus infrastruktúrák ellenálló képesség fejlesztését célzó szabályozás mérföldkövei 2022-2025,” *Védelem Tudomány,* 10. kötet, 2. szám, pp. 11-21, 2025. https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/19455 (2025. 10. 11.)

[12] Sáfár B. és Kállai K., „A rezíliencia elméletek, mint az egyén és a közösségek alapvető képességének vizsgálata a krízishelyzetek és természeti katasztrófák kapcsán,” *Védelem Tudomány, 9.* kötet, 3. szám, pp. 45-51, 2024. https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/16952 (2025. 09. 01.)

[13] *A kritikus szervezetek ellenálló képességéről szóló* 2024. évi LXXXIV. törvény

[14] *A védelmi és biztonsági tevékenység összehangolásáról szóló 2021. évi XCIII. törvény*

[15] S. Keith, F. Joseph és S. karen, „NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security,” *National Institute of Standards and Technology,* 1. kötet, pp. 20-54, 2011. https://www.researchgate.net/publication/308175656_NIST_Special_Publication_800-82_Guide_to_Industrial_Control_Systems_ICS_Security (2025. 10. 12.)

[16] D. Shaun , J. Helge, N. Andrew , P. Tanuja és . W. Stuart, „SCADA security in the light of Cyber-Warfare,” *Computers & Security, 31*. kötet, 4. szám, pp. 418-436, 2012. https://www.sciencedirect.com/science/article/abs/pii/S0167404812000429 (2025. 01. 28.)

[17] D. Danae, G. Mavrotas és P. Lefteris, „Determining objective weights in multiple criteria problems: The CRITIC method,” *Computers & Operations Research, 22*. kötet, 7. szám pp. 736-770, 1995. https://www.sciencedirect.com/science/article/abs/pii/030505489400059H (2025. 01. 23.)

[18] *Joint Task Force Transformation Initiative, “Guide for Conducting Risk Assessments,” NIST SP 800-30 Rev. 1,,* 2012. https://csrc.nist.gov/pubs/sp/800/30/r1/final (2024. 03. 12.)

[19] Hunorfi P., Farkas T., „Cybersecurity of Operational Technology in Critical Infrastructures.,” Melügyi Szemle, *73*. kötet, 1. szám, pp. 183-197, 2025. https://belugyiszemlejournal.org/index.php/belugyiszemle/article/view/2145 (2025. 12. 13.)

[20] S. Rinaldi, J. Peerenboom és T. Kelly, „Identifying, understanding, and analyzing critical infrastructure interdependencies,” *IEEE Control Systems Magazine,* pp. 11-25, 2001. https://ieeexplore.ieee.org/document/969131 (2025. 03. 12)

[21] R. G. Little, „Controlling Cascading Failure: Understanding The Vulnerabilities of Interconnected Infrastructures,” *Journal of Urban Technology, 9*. kötet, 1. szám, pp. 109-123, 2002.

https://www.researchgate.net/publication/233202111_Controlling_Cascading_Failure_Understanding_The_Vulnerabilities_of_Interconnected_Infrastructures (2025. 11. 02.)

[22] *ISO 31000. Risk management,* 2018.

[23] *Hazard and operability studies (HAZOP) — Application guide (IEC 61882:2016). International Electrotechnical Commission.,* 2016.

[24] *Failure modes and effects analysis (FMEA and FMECA) (IEC 60812:2018). International Electrotechnical Commission.,* 2018.

[25] *European Union Agency for Cybersecurity- ENISA- Threat Landscape 2025,* 2025.

[26] R. Snee, „Failure Modes and Effects Analysis," *Encycelopedia of Statistics in Quality and Reliability.* , 2007. https://www.researchgate.net/publication/228011847_Failure_Modes_and_Effects_Analysis (2024. 12. 02.)

[27] A. E. Clifton , „Hazard Analysis Techniques for System Safety," *John Wiley and Sons. https://content.e-bookshelf.de/media/reading/L-3642282-189329dace.pdf (2023. 11. 12.)*

[28] D. Vose, „Risk Analysis – A Quantitative Guide," *John Wiley and Sons, 3*. kötet, 2008. https://www.researchgate.net/publication/259715934_Risk_Analysis_-_A_Quantitative_Guide (2024. 03. 23.)

[29] M. Ouyang, „Review on modeling and simulation of interdependent critical infrastructure systems," *Reliability Engineering & System Safety,* 121. kötet, pp. 43-60, 2014. https://www.deltaexpertise.nl/images/a/a4/Ouyang_2014.pdf (2024. 03. 23.)

[30] *Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről.*

[31] *A Tanács 2008/114/EK Irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről.*

[32] *A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény.*

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

[34] *A TANÁCS AJÁNLÁSA (2022. december 8.) a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről.*

[35] *Magyarország Alaptörvénye,* 2011.

[36] *A kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról szóló 474/2024. (XII.31.) Korm. rendelet.*

[37] *Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti kockázatértékeléséről szóló 1191/2025. (VI. 5.) Korm. határozatot.*

[38] ENISA. (2024). Threat Landscape 2024: Trends and Threats. European Union Agency for Cybersecurity.

[39] Angyal I, „Kritikus szervezetek ellenálló képességi szabályozási környezetének változása," *Védelem Tudomány, 9*. kötet, 9. szám, pp. 1-4, 2024. https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/17896 (2025. 04. 04.)

[40] Sáfár B., Kállai K. , „Szervezeti reziliencia a kritikus infrastruktúrák működésében – új kockázatok, új válaszok," *Védelem Tudomány, 8*. kötet8, 2. szám, pp. 115-132, 2023. https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/16952 (2025. 11. 12.)

[41] Ronyecz L., „Létfontosságú rendszerek és létesítmények védelmével kapcsolatos nemzetközi és európai uniós szabályozás értékelése," *Bolyai Szemle, 3*. szám, pp. 104-112, 2016. http://archiv.uni-nke.hu/uploads/media_items/bolyai-szemle-2016-03.original.pdf (2023. 11. 12.)

[42] Ronyecz L., „Létfontosságú rendszerek és létesítmények védelmével kapcsolatos nemzetközi tapasztalatok vizsgálata, azok integrálásának lehetőségei hazai rendszerbe," *Műszaki Katonai Közlöny, 26*. kötet, 2. szám, pp. 197-209, 2016. https://folyoirat.ludovika.hu/index.php/mkk/article/view/2177/1446 (2023. 03. 03.)

[43] *A Bizottság közlemenye - A létfontosságú infrastruktúrák védelmére vonatkozó európai programról.*

[44] Bónyai T., *A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében,* Budapest: Nemzeti Közszolgálati Egyetem, 2014. https://www.uni-nke.hu/document/uni-nke-hu/Bonnyai-Tunde_Doktori-ertekezes_2018.pdf (2022. 12. 12.)

[45] Ronyecz L., „Létfontosságú rendszerek és létesítmények árvízi veszélyeztetettsége, tapasztalatok vizsgálata esettanulmányon keresztül," Bolyai Szemle, *26*. kötet, 2. szám, pp. 89-108, 2017. https://www.uni-nke.hu/document/uni-nke-hu/Bolyai_Szemle_2017_02_kesz.pdf#page=89 (2022. 03. 02.)

[46] EU-NATO, „EU-NATO TASK FORCE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE-FINAL ASSESSMENT REPORT," 2023 . https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf (2024. 03. 03.)

[47] N. Cen, S. Giovanni és K. Wolfgang, „Building an Integrated Metric for Quantifying the Resilience of Interdependent Infrastructure Systems,” *Lecture Notes in Computer Science,* pp. 159-171, 2016. https://www.research-collection.ethz.ch/entities/publication/26645e7c-c156-432d-b6b6-dd4565f29fd2 (2022. 03. 03.)

[48] C. Scholz, S. Schauer és M. Latzenhofer, „The emergence of new critical infrastructures. Is the COVID-19 pandemic shifting our perspective on what critical infrastructures are?,” *International journal of disaster risk reduction,* p. 83, 4 november 2022. https://www.sciencedirect.com/science/article/pii/S2212420922006380 (2024. 04. 04.)

[49] F. Ferrer, „Considerations about The Cascading Effects of COVID-19 on Critical Infrastructure Sectors,” *National Disaster Resilience Councile,* pp. 1-10, 18 március 2020. https://www.csfa.net/csfa/images/csfa/PDFs/The-Cascading-Effects-of-COVID-19-on-Critical-Infrastructure-Sectors-20-March-2020.pdf (2024. 03. 03.)

[50] J. Pearce, „Netflix and YouTube to Reduce Stream Quality in Europe Due to Coronavirus,” *IBC,* 20 június 2020. https://www.mdpi.com/2079-9292/12/21/4542 (2024. 03. 03.)

[51] P. J. J. Welfens, „Russia's Attack on Ukraine: Economic Challenges, Embargo Issues & a New World Order,” *EIIW Discussion paper,* 2022. https://ideas.repec.org/p/bwu/eiiwdp/disbei312.html (2024. 02. 02.)

[52] N. RUZHIN és M. Mitrevska, „PROTECTION OF CRITICAL INFRASTRUCTURE – A STRATEGIC STAKE OF THE 21ST CENTURY,” *CONTEMPORARY MACEDONIAN DEFENCE,* pp. 33-45, 2024. https://www.ceeol.com/search/article-detail?id=1269523 (2024. 12. 04.)

[53] Stratégiai Védelmi Kutatóintézet Elemzések, „Az orosz–ukrán háború első évének tanulságai,” 3. szám, 2023. https://svkk.uni-nke.hu/document/svkk-uni-nke-hu-1506332684763/SVKI_Elemzesek_2023_3.pdf (2024. 03. 03.)

[54] F. Umbach, „New challenges in protecting critical EU infrastructure,” 26 február 2023. https://www.gisreportsonline.com/r/europe-critical-infrastructure/ (2024. 03. 03.)

[55] U. D. o. Defense, „Russian war in Ukraine - Timeline,” 25 augusztus 2024. [Online]. Available: https://www.defense.gov/Spotlights/Support-for-Ukraine/Timeline/.

[56] „CTI Jelentés - US Colonial Pipeline elleni támadás köetkezményei,” Nemzeti Kibervédelmi Intézet, Nemzetbiztonsági Szakszolgálat.

[57] Euronews/DB, „Szabotázs történhetett a német vasút kommunikációs rendszere ellen,” 2022. https://hu.euronews.com/2022/10/08/szabotazs-tortenhetett-a-nemet-vasut-kommunikacios-rendszere-ellen (2025. 02. 23.)

[58] Kárász B., „Globális kihívások a kibertérben: humán kockázatok kezelése a kritikus információs infrastruktúrák védelmében," *Biztonságtudományi Szemle, 7*. kötet, 1. szám, pp. 145-155, 2025. https://www.researchgate.net/publication/390134930_Globalis_kihivasok_a_kiberterben_human_kockazatok_kezelese_a_kritikus_informacios_infrastrukturak_vedelmeben (2024. 03. 03.)

[59] B. D. Trump, S. A. Mitoulis, S. Argyroudis és I. Linkov, „Resilience analytics in critical infrastructure: Adapting to complex system interdependencies," *Safety Science,* 170. kötet1, pp. 22-32, 2025. *https://carnegieindia.org/posts/2025/07/safeguarding-critical-infrastructure-key-challenges-in-global-cybersecurity?utm_source=chatgpt.com&lang=en (2025. 07. 10.)*

[60] O. Bures, T. Blažek, J. Němec és J. Schvach, „Factors impacting resilience of Internet of Things systems in critical infrastructure," *Journal of Strategic Security, 15*. kötet, 3. szám, pp. 25-44, 2022. *https://www.researchgate.net/publication/360936261_Factors_Impacting_Resilience_of_Internet_of_Things_Systems_in_Critical_Infrastructure (2025. 07. 10.)*

[61] D. Trifunovic, „Intelligence and Protection of Key (Critical) Infrastructure Objects," in *Critical Infrastructure Protection in the Light of the Armed Conflicts,* 2024. *https://link.springer.com/book/10.1007/978-3-031-47990-8 (2025. 07. 10.)*

[62] Ronyecz L. , Bognár B. és Kátai-Urbán L., „International experiences in risk analysis of critical infrastructures," in *International Disaster Management Scientific Conference - Focus on Changes in the Fire Safety Situation,* Budapest, 2024. https://www.tszvsz.hu/hu/hirek/konferencia-kiadvany *(2025. 07. 10.)*

[63] M. K. Shaymaa, B. Hayretdin és K. Tarmo, „Threat modeling of industrial control systems: A systematic literature review," *Computers & Security,* 136. kötet, 2024. https://www.researchgate.net/publication/374878417_Threat_modeling_of_industrial_control_systems_A_systematic_literature_review *(2025. 07. 10.)*

[64] S. Roberto és T. Marianthi, „Modelling Dependencies Between Critical Infrastructures," *Managing the Complexity of Critical Infrastructures,* pp. 19-41, 2016. https://www.researchgate.net/publication/313584638_Modelling_Dependencies_Between_Critical_Infrastructures *(2025. 07. 10.)*

[65] M. Theocharidou és G. Giannopoulos, Risk assessment methodologies for critical infrastructure protection. Part II: A new approach, Luxembourg: Publications Office of the European Union, 2015. https://publications.jrc.ec.europa.eu/repository/handle/JRC96623 *(2025. 07. 10.)*

[66] Gosztola A. és Horváth B., „A közlekedési hálózati érzékenység kutatásának alakulása és a kritikus elemek sérülékenységének vizsgálata – szakirodalmi áttekintés,"

Közlekedéstudományi Szemle, LXXV. kötet, 6. szám, pp. 44-55, 2025. https://ojs.mtak.hu/index.php/ktsz/article/view/20100 *(2025. 07. 10.)*

[67] E. Rodríguez-Núnez és C. J. Garcia-Palomares, „Measuring the vulnerability of public transport networks," *Journal of Transport Geography, 35*. kötet, pp. 50-63, 2014. https://www.sciencedirect.com/science/article/abs/pii/S0966692314000180 *(2025. 07. 10.)*

[68] A. Strzelczy és S. Guze, „An Approach to the Analysis of Critical Elements of Transport and Logistics Networks Using Graph Theory," *International Journal on Marine Navigation and Safety of Sea Transportation,* 18. kötet, 3. szám, pp. 535-544, 2024. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.transnav.eu/files/An_Approach_to_the_Analysis_of_Critical_Elements_of_Transport_and_Logistics_Networks_Using_Graph_Theory,1427.pdf&ved=2ahUKEwiE7PqDyo2SAxU-_7sIHfanKGkQFnoECCQQAQ&usg=AOvVaw0fFSgDtcyDNl4TUGakzA3X *(2025. 07. 10.)*

[69] Iman Seyedi, Antonio Candelieri, Enza Messina és Francesco Archetti, „Structural Vulnerability Assessment in Urban Transport Networks: A Network-Wide Geometric Approach Using Gromov-Wasserstein," *Cornell University,* pp. 1-19, 2025. https://arxiv.org/abs/2510.24306 *(2025. 07. 10.)*

[70] Albert R., J. Hawoong és Barabasi L. A., „Error and attack tolerance of complex networks," *Nature,* pp. 1-22, 2000. https://arxiv.org/abs/cond-mat/0008064 *(2025. 07. 10.)*

[71] S. Sicari, A. Rizzardi, L. A. Grieco és A. Coen-Porisini, „Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks, 76*. kötet, 15. szám, pp. 146-164, 2015. https://www.sciencedirect.com/science/article/abs/pii/S1389128614003971 *(2025. 07. 10.)*

[72] A. Mohiuddin, M. Abdun és H. Jiankun, „A Survey of Network Anomaly Detection Techniques," *Journal of Network and Computer Applications, 60*. kötet, 1. szám, pp. 19-31, 2015. https://www.researchgate.net/publication/286848340_A_Survey_of_Network_Anomaly_Detection_Techniques *(2025. 07. 10.)*

[73] *Sean Monaghan, Otto Svendsen, Michael Darrah, Ed Arnold, „NATO's Role in Protecting Critical Undersea Infrastructure," CSIS Briefs, pp. 1-17, 2023 december. https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure (2025. 07. 10.)*

[74] F. Casaril és L. Galletta, „Developing security metrics for space systems: A study considering the NIST Cybersecurity Framework 2.0 and the NIS2 Author links open overlay panel," *International Journal of Critical Infrastructure Protection,* 51. kötet, 1.

szám, pp. 1-32, 2025. https://www.sciencedirect.com/science/article/pii/S1874548225000666 *(2025. 07. 10.)*

[75] M. Dawson és H. A. Khan, „Cyber Defense of Space Systems: Taxonomy of Vulnerabilities and Framework for Resilient Infrastructure," *Land Forces Academy Review, 30.* kötet, 3. szám, pp. 454-465, 2025. https://reference-global.com/article/10.2478/raft-2025-0044 *(2025. 10. 10.)*

[76] N. Anjum és T. Farheen, „Securing the Final Frontier for Cybersecurity in Space-Based Infrastructure," *Division of Computer Science and Engineering, Louisiana State University,* 2025. https://www.researchgate.net/publication/393965512_SoK_Securing_the_Final_Frontier_for_Cybersecurity_in_Space-Based_Infrastructure *(2025. 10. 10.)*

[77] M. Ballard, G. Song és T. Zhu, „Satellite Cybersecurity Across Orbital Altitudes: Analyzing Ground-Based Threats to LEO, MEO, and GEO," *Cornell University,* 2025. https://www.arxiv.org/abs/2512.21367 *(2025. 10. 10.)*

[78] J. P. Peerenboom, W. K. Fooell, „A Decision Analysis Approach to Energy System Expansion Planning, vol. 6(3), pages 21-36, July. 1985. https://ideas.repec.org/a/sae/enejou/v6y1985i3p21-36.html (2025. 10. 10.)

[79] M. Yigit, M. A. Ferrag és I. H. Sarker, „Critical Infrastructure Protection: Generative AI, Challenges, and Opportunities," *Computers & Security,* %1. kötet137, pp. 45-60, 2024. *https://arxiv.org/abs/2405.04874 (2025. 07. 10.)*

[80] J. Järveläinen, „Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: A dynamic capabilities approach.," *Taylor & Francis Online,* %1. kötet34, %1. szám1, pp. 1-21, 2025. *https://osuva.uwasa.fi/bitstream/handle/10024/19146/Osuva_Järveläinen_Dang_Mekkanen_Vartiainen_2025.pdf?sequence=2&utm_source=chatgpt.com (2025. 07. 10.)*

[81] S. M. Rinaldi, J. P. Peerenboom, T. K. Kelly, „Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine ,* %1. kötet21, %1. szám6, pp. 11-25, 2001. https://www.researchgate.net/publication/3206740_Identifying_understanding_and_analyzing_critical_infrastructure_interdependencies *(2025. 07. 10.)*

[82] *IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.*

[83] *ERA/OPI/2020-2 Opinion of the European Union Agency for Railways to the European Commission regarding error corrections of current ERTMS baselines,* 2020.

[84] I. A. Yusta, P. M. Martinez-Ruiz és I. A. Jimenez-Zarco, „The Role of the Convenience and the Subjective Norm in the Intention of Purchase Across Internet (B2C): an application in the hospitality industry," *Revista Brasileira de Gestao de Negocios*, %1. kötet13, %1. szám39, pp. 137-158, 2011. https://www.researchgate.net/publication/272876593_The_Role_of_the_Convenience_and_the_Subjective_Norm_in_the_Intention_of_Purchase_Across_Internet_B2C_an_application_in_the_hospitality_industry (2024. 11. 03.)

[85] E. Hollnagel és D. D. Woods, „Resilience Engineering : Concepts and Precepts," *Resilience Engineering: Concepts and Precepts.* , 2006. https://www.researchgate.net/publication/50232053_Resilience_Engineering_Concepts_and_Precepts (2024. 04. 10.)

[86] I. Linkov, A. D. Eisenberg, K. Plourde, P. T. Seager, J. Allen és A. Kott, „Resilience metrics for cyber systems," *Environment Systems and Decisions, 33*. kötet, pp. 471-476, 2013. https://ideas.repec.org/a/spr/envsyd/v33y2013i4d10.1007_s10669-013-9485-y.html (2024. 11. 12.)

[87] M. Bruneau és A. Reinhorn, „Overview of the Resilience Concept," in *Proceedings of the 8th U.S. National Conference on Earthquake Engineering*, San Francisco, 2006. https://www.eng.buffalo.edu/~bruneau/8NCEE-Bruneau%20Reinhorn%20Resilience.pdf (2024. 10. 12.)

[88] *OECD Economic Outlook, Volume 2021 Issue 1,* 2021.

[89] M. Panteli és P. Mancarella, „Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies," *Electric Power Systems Research,* 127. kötet, pp. 259-270, 2015. https://files01.core.ac.uk/download/pdf/74062785.pdf (2024. 10. 12.)

[90] E. J. Boehm, H. Evans, A. Jillavenkatesa, M. Nadal, A. M. Przybocki, P. Witherell és A. R. Zangmeister, „2018 National Institute of Standards and Technology Environmental Scan," *NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD,* 2019. https://www.nist.gov/publications/2018-national-institute-standards-and-technology-environmental-scan (2024. 10. 12.)

[91] Risk Management Guide for Critical Infrastructure Sectors, Public Safety Canada. *https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rsk-mngmnt-gd/index-en.aspx* (2024. 10. 12.)

[92] Government of Canada, National Risk Profile - A national emergency preparedness and awareness tool, 2023. *https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2023-nrp-pnr/2023-npr-pnr-en.pdf (2025. 07. 10.)*

[93] P. S. Canada, „National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure," Her Majesty the Queen in Right of Canada, as represented by the Minister of Public Safety and Emergency Preparedness, 2021. *https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf (2025. 07. 10.)*

[94] *H. S. USA, „NIPP 2013 - Partnering for Critical Infrastructure Security and Resilience," 2013. https://www.cisa.gov/resources-tools/resources/nipp-2013-partnering-critical-infrastructure-security-and-resilience (2025. 07. 10.)*

[95] *Homeland Security Presidential Directive 7, 2023 december. https://www.cisa.gov/news-events/directives/homeland-security-presidential-directive-7. (2025. 07. 10.)*

[96] *America's Cyber Defence Agency, Infrastructure Resilience Planning Framework (IRPF), 2024 february. https://www.cisa.gov/resources-tools/resources/infrastructure-resilience-planning-framework-irpf (2025. 07. 10.)*

[97] *America's Cyber Defence Agency, Infrastructure Security is National Security: Drive Down Risk, BUILD RESILIENCE., 2022. https://www.cisa.gov (2025. 07. 10.)*

[98] *„UK National Risk Register," HM Government, 2023. https://www.gov.uk/government/publications/national-risk-register-2023 (2025. 07. 10.)*

[99] *C. Office, Public Summary of Sector Security and Resilience Plans, London, 2019. https://assets.publishing.service.gov.uk/media/5c8a7845ed915d5c1456006a/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf (2025. 07. 10.)*

[100] *U. D. a. S. Exports, Securing Critical National Infrastructure: An introduction to UK capability, 2023. https://www.gov.uk/government/publications/critical-national-infrastructure-an-introduction-to-uk-capability (2025. 07. 10.)*

[101] *G. o. Poland, „Rządowe Centrum Bezpieczeństwa - Critical infrastructure," [Online]. https://archiwum.rcb.gov.pl/en/critical-infrastructure/.(2025. 08. 25.)*

[102] *E. C. P. „National disaster management system," European Civil Protection and Humanitarian Aid Operations, https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/national-di (2025. 08. 25.)*

[103] *CZDEFENCE, „New cybersecurity law to include 6,000 entities in critical infrastructure," 16 január 2024.*

https://www.czdefence.com/article/new-cybersecurity-law-to-include-6000-entities-in-critical-infrastructure. (2025. 08. 20.)

[104] *Peyton LegalNew Critical Infrastructure Act. https://www.peytonlegal.cz/en/new-critical-infrastructure-act/. (2025. 07. 12)*

[105] *IPedia, „Critical Infrastructure Sector. Fraunhofer Institute. https://websites.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure_Sector. (2025. 04. 22)*

[106] A. F. Chancellery, „Austrian Programme for Critical Infrastructure Protection," *Cybersecurity activities and initiatives,* pp. 1-23, augusztus 2025.

[107] *Kritis Framework Law, Critical infrastructure and Kritis In Germany https://www.openkritis.de/it-Sicherheitsgesetz/German_Cip_Infrastructure_Kritis.html (2025. 08. 10.)*

[108] *European Commission, „Germany: National disaster management system.," European Civil Protection and Humanitarian Aid Operations, pp. 1-12,.*

[109] SilverBulletRisk, „How to reduce critical infrastructure risks by enhancing the security culture among employees?," pp. 1-23, 22 augusztus 2019.

[110] I. Šarūnienė, „ Risk assessment of critical infrastructures: A methodology suitable for cross-sector systems," *Reliability Engineering & System Safety, 250*. szám, pp. 1-15, 2024. https://www.sciencedirect.com/science/article/abs/pii/S0951832023007111 *(2025. 04. 22)*

[111] M. Papamichael, „Performing risk assessment for critical infrastructure: Influence of transnational challenges and decision-making biases,"," *International Journal of Disaster Risk Reduction, 79*. szám, pp. 1-12, 2024. https://www.sciencedirect.com/science/article/abs/pii/S1874548224000234 *(2025. 04. 22)*

[112] *Az ország védelme és biztonsága szempontjából jelentős szervezetek, infrastruktúrák azonosításáról, ellenőrzéséről, valamint az ezzel összefüggő adatok nyilvántartásáról szóló* 16/2025. (VI. 6.) HM utasítás.

[113] Szánási I., „Kritikus rendszerelemek jellemzői, azok kijelölése, valamint azok védelme," *Nemzetbiztonsági Szemle, 2*. kötet, 12. szám, pp. 18-37, 2024. https://folyoirat.ludovika.hu/index.php/nbsz/article/view/7432 *(2025. 04. 22)*

[114] Organisation for Economic Co-operation and Development. Publishing., „Ensuring the resilience of critical infrastructure," OECD Publishing.

https://www.oecd.org/en/publications/government-at-a-glance-2025_0efd0bcd-en/full-report/ensuring-the-resilience-of-critical-infrastructure_896f59cf.html *(2025. 04. 22)*

[115] National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF), 2025. [Online]. Available: https://www.ncsc.gov.uk. https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf *(2025. 04. 22)*

[116] *National Institute of Standards and Technology (NIST). (2022). Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1). U.S. Department of Commerce. https://csrc.nist.gov*

[117] *Department of Homeland Security (DHS). (2013). National Infrastructure Protection Plan (NIPP 2013): Partnering for Critical Infrastructure Security and Resilience. https://www.cisa.gov*

[118] U. B. Utne, „A method for assessing interdependencies in cross-sector risk and vulnerability analysis of critical infrastructures," *Safety Science,, 49*. szám, p. 498–505, 2011. https://www.researchgate.net/publication/251621610_A_method_for_risk_modeling_of_interdependencies_in_critical_infrastructures_Reliability_Engineering_System_Safety_96_671-678 *(2025. 04. 22)*

[119] A. Fošner, „Risk analysis of critical infrastructure with the MOSAR method," *Process Safety and Environmental Protection,* 102. szám, pp. 12-23, 2024. https://www.sciencedirect.com/science/article/pii/S2405844024024708 *(2025. 04. 22)*

[120] I. Šarūnienė, L. Martišauskas, R. Krikštolaitis, J. Augutis és R. Setola, „Risk assessment of critical infrastructures: A methodology based on criticality of infrastructure elements," *Reliability Engineering & System Safety, 243*. kötet, 2024. https://www.sciencedirect.com/science/article/abs/pii/S0951832023007111 *(2025. 04. 22)*

[121] A. A. Ardebili, M. Lezzi. és M. Pourmadadkar, „Risk assessment for cyber resilience of critical infrastructures: Methods, governance, and standards," *Applied Sciences,* 14. kötet, 24. szám, 2024. https://www.mdpi.com/2076-3417/14/24/11807 *(2025. 04. 22)*

[122] M. Lubis, F. M. Safitra, H. Fakhrurroja és N. A. Muttagin, „Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience," 25. kötet, 15. szám, 2025. https://www.researchgate.net/publication/331872485_Predictive_Formal_Analysis_of_Resilience_in_Cyber-Physical_Systems *(2025. 04. 22)*

[123] A. Z. Baig és S. Zeadally, „Cyber-security risk assessment framework for critical infrastructures," *Intelligent Automation & Soft Computing, 25*. kötet, 4. szám, 2018.

https://www.researchgate.net/publication/327047943_Cyber-security_risk_assessment_framework_for_critical_infrastructures *(2025. 04. 22)*

[124] S. S. Bagott és R. J. Santos, „A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Electric Power Grid," *Risk Analysis,* pp. 1-18, 2020. https://par.nsf.gov/servlets/purl/10207600 *(2025. 04. 22)*

[125] O. A. Ayeni, „Evaluating and enhancing resilience in critical infrastructure sectors: A comprehensive risk assessment methodology," *International Journal for Information Security Research,* %1. szám14, pp. 100-115, 2024. https://www.researchgate.net/publication/387133510_Evaluating_and_Enhancing_Resilience_in_Critical_Infrastructure_Strategies_for_Risk_Management *(2025. 04. 22)*

[126] M. Roshanaei, „Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies," *Journal of Computer and Communications* , %1. kötet9, %1. szám8, pp. 80-102, 2021. https://www.researchgate.net/publication/354121679_Resilience_at_the_Core_Critical_Infrastructure_Protection_Challenges_Priorities_and_Cybersecurity_Assessment_Strategies *(2025. 04. 22)*

[127] K. Hemme, „Critical Infrastructure Protection: Maintenance is National Security," *Journal of Strategic Security, 8*. kötet, 3. szám, pp. 25-39, 2015. https://www.researchgate.net/publication/283280777_Critical_Infrastructure_Protection_Maintenance_is_National_Security *(2025. 04. 22)*

[128] I. Eusgeld, C. Nan és S. Dietz, „System-of-systems" approach for interdependent critical infrastructures," *Reliability Engineering & System Safety, 96*. kötet, 6. szám, pp. 679-686, 2011. https://www.sciencedirect.com/science/article/abs/pii/S0951832010002668 *(2025. 04. 22)*

[129] D. F. Petit, W. G. Bassett, R. Black, A. W. Buehring, J. M. Collins, C. D. Dickinson, E. R. Fisher, A. R. Haffenden, A. R. Huttenga, S. M. Klett, A. J. Phillips, M. Thomas, N. S. Veselka, E. K. Wallace, G. R. Whietfield és P. J. Peerenboom, Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience, Argonne: Decision and Information Science Division, 2013. https://publications.anl.gov/anlpubs/2013/07/76797.pdf *(2025. 05. 22)*

[130] W. Kröger, „Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools," *Reliability Engineering & System Safety, 93*. kötet, 12. szám, pp. 1781-1787, 2008. https://www.researchgate.net/publication/222407344_Kroger_W_Critical_infrastructures_at_risk_A_need_for_a_new_conceptual_approach_and_extended_analytical_tools_Reliability_Engineering_and_System_Safety_9312_1781-1787 (2025. 02. 12.)

[131] E. Hollnagel, „The four cornerstones of resilience engineering," *Resilience Engineering Perspectives,* %1. kötet2, pp. 1-22, 2009. https://www.researchgate.net/publication/49948682_The_four_cornerstones_of_resilience_engineering (2024. 03. 11.)

[132] P. J. Jonas , H. Hassel és A. Cedergren, „Vulnerability analysis of interdependent critical infrastructures: Case study of the Swedish railway system," *International Journal of Critical Infrastructures,* %1. kötet7, %1. szám4, pp. 289-316, 2011. https://www.researchgate.net/publication/264822039_Vulnerability_analysis_of_interdependent_critical_infrastructures_Case_study_of_the_Swedish_railway_system (2024. 02. 22.)

[133] S. G. Parnell, A. T. Bresnick, N. S. Tani és E. Johnson R, Handbook of Decision Analysis, Wiley & Sons, Incorporated, John, 2013. https://www.wiley.com/en-us/Handbook+of+Decision+Analysis-p-9781118515853 *(2025. 05. 22)*

[134] A. Boin és M. van Eeten , „The Resilient Organization," *Public Management Review, 15*. kötet, 3. szám, pp. 1-32, 2013. https://www.tandfonline.com/doi/abs/10.1080/14719037.2013.769856 *(2025. 05. 22)*

[135] L. Galbusera, M. Cardarilli, M. Gómez Lara, G. Giannopoulos, Game-based training in critical infrastructure protection and resilience PInternational Journal of Disaster Risk Reduction 78. kötet, 3. szám, pp. 1-18, 2022. https://www.researchgate.net/publication/361323689_Game-based_training_in_critical_infrastructure_protection_and_resilience *(2025. 05. 22)*

[136] *IEC 60812. Failure Modes and Effects Analysis (FMEA and FMECA). IEC.,* 2018.

[137] *IEC 61882. Hazard and Operability Studies (HAZOP) — Application Guide. IEC.,* 2016.

[138] Finan and W. D. Macnamara, „An illustrative Canadian strategic risk assessment," *Canadian Military Journal,* 2001. https://publications.gc.ca/collections/collection_2016/rddc-drdc/D68-5-014-2012-eng.pdf *(2025. 05. 22)*

[139] Homeland Security, „National Infrastructure Protection Plan Risk Management Framework" 2006. https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf *(2025. 05. 22)*

[140] R. Filippini, M. Schimmer, G. Giannopoulos, Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art., Luxembourg (Luxembourg): Publications Office of the European Union;, 2012. https://publications.jrc.ec.europa.eu/repository/handle/JRC70046 *(2025. 05. 22)*

[141] M. Papamichael, C. Dimopoulos, G. Boustars, „Performing risk assessment for critical infrastructure protection: an investigation of transnational challenges and human decision-making considerations.," *Sustainable and Resilient Infrastructure,* pp. 1-19, 2024. https://www.researchgate.net/publication/379890045_Performing_risk_assessment_for_critical_infrastructure_protection_an_investigation_of_transnational_challenges_and_human_decision-making_considerations *(2025. 05. 22)*

[142] G. Kjølle, „Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies„" *Energy Policy, 45*. szám, pp. 406-414, 2012. https://www.researchgate.net/publication/257392030_Risk_analysis_of_critical_infrastructures_emphasizing_electricity_supply_and_interdependencies *(2025. 05. 22)*

[143] *ISO/IEC 31010. Risk management — Risk assessment techniques.,* 2019.

[144] *ISO/IEC 27005. Information security, cybersecurity and privacy protection — Guidance on information security risk management. ISO/IEC.,* 2022.

[145] K. L. Atoyev, „Mathematical model of risk assessment for critical infrastructure using a six-sector Lorenz model," *Annals of Operations Research, 312*. kötet, 2. szám, pp. 1-18, 2025. https://www.researchgate.net/publication/390243118_MATHEMATICAL_MODEL_FOR_RISK_ASSESSMENT_OF_CRITICAL_INFRASTRUCTURE *(2025. 05. 22)*

[146] *ISO 31000: Risk management – Guidelines. International Organization for Standardization.,* 2018.

[147] D. C. Petit, „Critical infrastructure interdependency analysis framework for regional resilience strategies," *International Journal of Critical Infrastructure Protection, 22*. szám, pp. 45-56, 2017. https://www.unisdr.org/files/66506_f415finallewisandpetitcriticalinfra.pdf *(2022. 05. 22)*

[148] R. Saaty, „The analytic hierarchy process—what it is and how it is used," *Mathematical Modelling, 9*. kötet, 3. szám, pp. 161-176, 1987. https://www.sciencedirect.com/science/article/pii/0270025587904738 *(2022. 05. 22)*

[149] V. Belton és T. J. Stewart, Multiple Criteria Decision Analysis: An Integrated Approach, Berlin: Springer-Science + Business Media, 2002. https://www.researchgate.net/publication/220693841_Multiple_Criteria_Decision_Analysis_An_Integrated_Approach *(2022. 05. 22)*

[150] C. G. Rieger, „Multi-agent systems for power engineering applications—Part I: Concepts, approaches, and technical challenges," *IEEE Trans. Power Systems, 22*. kötet, 2. szám, pp. 1743-1759, 2007. https://scispace.com/pdf/multi-agent-systems-for-power-engineering-applications-part-485uxyyn3d.pdf *(2022. 05. 22)*

[151] C. Nan, G. Sansavini és W. Kröger, „Building an integrated metric for quantifying resilience of interdependent infrastructure systems,” *Critical Information Infrastructures Security*, pp. 103-114, 2016. https://www.researchgate.net/publication/301932854_Building_an_Integrated_Metric_for_Quantifying_the_Resilience_of_Interdependent_Infrastructure_Systems *(2024. 10. 22)*

[152] J. F. Meyer, „Defining and evaluating resilience: A performability perspective,” *Workshop on Performability Modeling of Computer and Communication Systems*, pp. 103-114, 2009. http://webspn.hit.bme.hu/~pmccs2009/cr/01Meyer-PMCCS9-Final.pdf *(2024. 05. 23)*

[153] G. Giannopoulos, R. Filippini és M. Schimmer, Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art, Luxembourg: Publications Office of the European Union, 2012. https://publications.jrc.ec.europa.eu/repository/handle/JRC70046 *(2024. 05. 23)*

[154] C. V. Evans, C. Anderson, M. Baker, R. Bearse, S. Bicakci, S. Bieber, S. Cho, A. Dwyer, G. French, D. Harell, A. Lazari, R. Mey, T. Sabonis-Helf és D. Verner, Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency, Carlisle, PA: Centre of Excellence-Defense Against Terrorism, SSI & USAWC Press, 2022. https://www.coedat.nato.int/publication/researches/12-Enabling%20NATO_s%20Collective%20Defense_%20Critical%20Infrastructure%20Secur.pdf *(2024. 05. 23)*

[155] L. A. Cox, Risk Analysis Foundation, Models, and Methods, New York: Cox Associates and University of Colorado, 2022, pp. 43-129. https://www.researchgate.net/publication/268671607_Risk_Analysis_Foundations_Models_and_Methods *(2024. 05. 23)*

[156] T. Carter, R. Jones, X. Lu, S. Bhadwal, C. Conde, L. Mearns, B. O'Neill, M. Rounsevell és M. Zurek, „New Assessment Methods and the Characterisation of Future Conditions,” in *Climate Change 2007: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change*, Cambridge, Cambridge University Press, 2007, pp. 133-171. https://www.researchgate.net/publication/200471807_New_assessment_methods_and_the_characterisation_of_future_conditions *(2024. 05. 23)*

[157] American Water Works Association, „RAMCAP- Standard for Water and Wastewater Systems,,” AWWA GOVERNMENT AFFAIRS OFFICE, Denver, 2010. https://webstore.ansi.org/preview-pages/AWWA/preview_J100-2010+R2013.pdf?srsltid=AfmBOoqjGaS9iCkFUbzK_wVyTHKbdw4GH28xPGQl8cxx1WRa8wzvQYEh *(2024. 05. 23)*

[158] American Society of Military Engineers, Risk Analysis and Management for Critical Asset Protection (RAMCAP) 2006. https://files.asme.org/ASMEITI/RAMCAP/12604.pdf (2024. 05. 23)

[159] *World Health Organisation, Health Emergency and Disaster Risk Management Framework,* 2021. https://iris.who.int/server/api/core/bitstreams/219a1a08-9ec5-4f2d-9aff-54c713fcfa7c/content *(2024. 05. 23)*

[160] *European Centre for Disease Prevention and Control (ECDC): Critical healthcare dependencies in crisis situations. https://www.ecdc.europa.eu/sites/default/files/media/en/publications/Publications/Health_inequalities_financial_crisis.pdf (2024. 05. 23)*

[161] *CCPS- Center for Chemical Process Safety: Bow-Tie Risk Management Guidance,* 2020. https://onlinelibrary.wiley.com/doi/book/10.1002/9781119490357 *(2024. 05. 23)*

[162] *Microsoft Security Engineering Center: STRIDE Threat Model,* 2018. https://www.researchgate.net/figure/Microsofts-STRIDE-Threat-classification-system_tbl1_329726569 *(2024. 05. 23)*

[163] *NIST SP 800-154: Guide to Data-Centric System Threat Modeling,* 2017. https://csrc.nist.gov/files/pubs/sp/800/154/ipd/docs/sp800_154_draft.pdf *(2024. 05. 23)*

[164] Varga P. és Illés Z., „Kritikus infrastruktúrák hatás alapú modellezése," *Hadmérnök, IV*. kötet., 4. szám, pp. 390-399, 2009. http://hadmernok.hu/2009_4_vargap_illesi.pdf *(2024. 05. 23)*

[165] T. Bedford és R. Cooke, Probabilistic Risk Analysis: Foundations and Methods, Cambridge: Cambridge University Press, 2001. https://assets.cambridge.org/97805217/73201/frontmatter/9780521773201_frontmatter.pdf *(2024. 05. 23)*

[166] T. N. Mathieu és A. S. Rao, „Identifying drinking water and water treatment systems vulnerabilities using the CARVER matrix method," *International Journal of Critical Infrastructures, 7*. kötet, 1. szám, pp. 37-49, 21 October 2014. https://scispace.com/pdf/identifying-drinking-water-and-water-treatment-systems-2wtcq78tfv.pdf *(2024. 05. 23)*

[167] M. Al-Mhdawi, A. O'connor, A. Qazi, F. Rahimian és N. Dacre, „Review of studies on risk factors in critical infrastructure projects from 2011 to 2023," *Smart and Sustainable Built Environment,* %1. kötet14, %1. szám2, pp. 342-376, 2025. https://www.researchgate.net/publication/378262077_Review_of_studies_on_risk_factors_in_critical_infrastructure_projects_from_2011_to_2023 *(2025. 11. 23)*

[168] C. Gómez és M. Sánchez-Silva, „17 - Risk assessment and management of civil infrastructure networks: a systems approach,” in *Handbook of Seismic Risk Analysis and Management of Civil Infrastructure Systems*, Woodhead Publishing, 2013, pp. 437-464. https://www.sciencedirect.com/science/chapter/edited-volume/abs/pii/B9780857092687500177 *(2025. 11. 23)*

[169] Z. Román, „Teljes valószínűségi módszerek alkalmazása a kritikus infrastruktúra védelmében,” *Műszaki Katonai Közlöny, XXV*. kötet., 2. szám., pp. 131-142, 2015. https://folyoirat.ludovika.hu/index.php/mkk/issue/view/185 *(2025. 11. 23)*

[170] G. Ampratwum, V. W. Tam és R. Osei-Kyei, „Critical analysis of risks factors in using public-private partnership in building critical infrastructure resilience: a systematic review,” *Construction Innovation, 23*. kötet, 2. szám, pp. 360-382, 2023. https://www.researchgate.net/publication/357648847_Critical_Analysis_of_Risks_Factors_in_using_Public-Private_Partnership_in_building_Critical_Infrastructure_Resilience_A_Systematic_Review *(2025. 11. 23)*

[171] J. Huang, J.-X. You, H.-C. Liu és M.-S. Song, „Failure mode and effect analysis improvement: A systematic literature review and future research agenda,” *Reliability Engineering & System Safety, 199*. kötet, pp. 45-60, 2020. https://ideas.repec.org/a/eee/reensy/v199y2020ics095183201930105x.html *(2025. 11. 23)*

[172] A. V. Bochkov, „Hazard and Risk Assessment and Mitigation for Objects of Critical Infrastructure,” in *Diagnostic Techniques in Industrial Engineering*, Springer, Cham, 2018, pp. 57-135. https://www.researchgate.net/publication/320549450_Hazard_and_Risk_Assessment_and_Mitigation_for_Objects_of_Critical_Infrastructure *(2025. 11. 23)*

[173] P.-C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner és A. S. Reninger, „Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control,” in *2007 IEEE Symposium on Security and Privacy (SP '07)*, Berkeley, 2007. https://www.researchgate.net/publication/4251885_Fuzzy_Multi-Level_Security_An_Experiment_on_Quantified_Risk-Adaptive_Access_Control *(2025. 11. 23)*

[174] P. Auerswald, L. M. Branscomb, T. M. La Porte, E. Michel-Kerjan és E. Michel-Kerjan, „The Challenge of Protecting Critical Infrastructure,” *Issues in Science and Technology, 22*. kötet, 1. szám, pp. 77-83, 2005. https://issues.org/auerswald/ *(2025. 11. 23)*

[175] Megyeri L. és Farkas T., „Kockázatkezelés, tudomány vagy kuruzslás?,” *Hadmérnök, XII*. kötet., 3. szám, pp. 198-209, 2017.

[176] Z. Turskis, N. Goranin, A. Nurusheva és S. Boranbayev, „Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach," *Informatica: An International Journal of Computing and Informatics, 30*. kötet, 1. szám, pp. 187-211, 2019. https://www.researchgate.net/publication/332027147_Information_Security_Risk_Assessment_in_Critical_Infrastructure_A_Hybrid_MCDM_Approach *(2025. 11. 23)*

[177] D. Rehak, A. Splichalova, H. Janeckova, O. Ryska, A. Oulehlova, L. Michalcova, M. Hromada, M. Kontogeorgos és J. Ristvej, „Critical entities resilience strengthening tools to small-scale disasters," *International Journal of Critical Infrastructure Protection, 49*. kötet, pp. 34-56, 2025. https://www.researchgate.net/publication/391086973_Critical_Entities_Resilience_Strengthening_Tools_to_Small-scale_Disasters *(2025. 11. 23)*

[178] I. Aryriou és T. Tsoutsos, „Assessing Critical Entities: Risk Management for IoT Devices in Ports," *Journal of Marine Science and Engineering, 12*. kötet, 9. szám, pp. 10-21, 2024. https://www.mdpi.com/2077-1312/12/9/1593 *(2025. 11. 23)*

[179] Az EU Tanácsa, „Ukrajna ellen irányuló orosz kiberműveletek: a főképviselőnek az Európai Unió nevében tett nyilatkozata," 2022. https://www.consilium.europa.eu/hu/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/pdf/ *(2025. 11. 23)*

[180] *Javaslat AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE a kritikus fontosságú szervezetek rezilienciájáról,* 2020. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52020AE5749 *(2025. 11. 23)*

[181] Angyal I., „A kritikus szervezetek új típusú szabályozási modellje Magyarországon – a 2024. évi LXXXIV. törvény elemzése," *Magyar Közigazgatás, 74*. kötet, 1. szám, pp. 45-62, 2024. https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/17896 *(2025. 11. 23)*

[182] Angyal I. és Mógor J. , „A létfontosságú rendszerek védelmére vonatkozó szabályozás fejlesztése és összehangolása az uniós keretekkel," *Honvédelmi Szemle,* 149. kötet, 5. szám, pp. 72-86, 2021. https://www.researchgate.net/publication/365398702_A_letfontossagu_rendszerek_vedelmere_vonatkozo_szabalyozas_fejlesztese *(2025. 11. 23)*

A TÉMAKÖRBÓL KÉSZÜLT PUBLIKÁCIÓIM

LEKTORÁLT SZAKMAI FOLYÓIRATCIKKEK (ONLINE IS)

1. Ronyecz Lilla: A kritikus szervezetekkel kapcsolatos kockázat- és következményelemző módszerek kutatása – Együttműködési platform alkalmazása Szemelvények a katonai műszaki tudományok eredményeiből VI. Budapest, Ludovika Egyetemi Kiadó 2025.pp. 183-202. , 20 p.
2. Ronyecz Lilla: A létfontosságú infrastruktúra védelmének hazai kialakításával, a honvédelmi létfontosságú infrastruktúra védelmével kapcsolatos eredmények, A megújult védelmi igazgatás 10 éve 2021., ISBN 978 963 327 810 9 pp. 153-161.

Külföldi idegen nyelvű folyóiratban

Magyar nyelvű mértékadó folyóiratban idegen nyelven

3. Ronyecz Lilla: A new approach to the protection of critical infrastructures: the new directive on the resilience of critical entities, American Journal of Research, Education and Development, ISSN 2471-9986 2024/1 pp.65-79
4. Ronyecz Lilla: Critical infrastructure and resilience MŰSZAKI KATONAI KÖZLÖNY XXVIII. évf. 3. szám pp. 104-111. (2018)
5. Ronyecz Lilla, Bognár Balázs: Implement regulation ont he resilience of critical entities in Hungary Védelem Tudomány, Különszám 9. pp. 119-123. 2024

Magyar nyelvű mértékadó folyóiratban magyar nyelven

6. Ronyecz Lilla; Bognár Balázs; Révai Róbert: A létfontosságú rendszerelemek közötti interdependencia kockázatainak elemzése, különös tekintettel az egészségügyi ágazat rendszerelemeire és létesítményeire Hadmérnök (XIII. Évfolyam 1. szám – 2018. március) pp. 133-142.
7. Ronyecz Lilla: A létfontosságú rendszerelemek kijelölési eljárásának tapasztalatai MŰSZAKI KATONAI KÖZLÖNY XXVIII.: (2.) pp. 81-91. (2018)
8. Ronyecz Lilla: Létfontosságú rendszerek és létesítmények védelmével kapcsolatos kockázatelemzési módszertan szakirodalmának kutatása Védelem Tudomány III. Évfolyam 3. szám pp. 111-132. (2018)
9. Ronyecz Lilla; Pócsik Attila: Létfontosságú rendszerek és létesítmények közlekedést érintő tűzoltói beavatkozási tapasztalatainak értékelése Műszaki Katonai Közlöny XXVII.:(2.) pp. 99-112. (2017)

10. Ronyecz Lilla: Létfontosságú rendszerek és létesítmények védelmével kapcsolatos tagállami szabályozás értékelése Bolyai Szemle XXVI:(1) pp. 96-107. (2017)
11. Ronyecz Lilla; Muhoray Árpád: Létfontosságú rendszerek és létesítmények árvízi veszélyeztetettsége, tapasztalatok vizsgálata esettanulmányon keresztül Bolyai Szemle XXVI:(2) pp. 89-108. (2017)
12. Ronyecz Lilla: Létfontosságú rendszerek és létesítmények védelmével kapcsolatos nemzetközi tapasztalatok vizsgálata, azok integrálásának lehetőségei hazai rendszerbe Műszaki Katonai Közlöny XXVI.:(2.) pp. 197-209. (2016)
13. Ronyecz Lilla: Létfontosságú rendszerek és létesítmények védelmével kapcsolatos nemzetközi és európai uniós szabályozás értékelése Bolyai Szemle 25:(3) pp. 104-112. (2016)
14. Ronyecz Lilla; Vass Gyula; Kátai-Urbán Lajos: Veszélyes üzemi kockázat és következményelemző eszközök alkalmazhatósága Bolyai Szemle XXIV:(1) pp. 111-123. (2015)
15. Ronyecz Lilla; Grósz Zoltán: Az iparbiztonsági hatóság által ellenőrzött veszélyes tevékenységek Magyarországon Bolyai Szemle 2014 (1.): pp. 132-145. (2014)

NEMZETKÖZI SZAKMAI KONFERENCIA KIADVÁNYÁBAN MEGJELENT ELŐADÁS (ONLINE IS, HAZAI ÉS KÜLFÖLDI EGYARÁNT)

Lektorált idegen nyelvű előadás

HAZAI SZAKMAI KONFERENCIA KIADVÁNYBAN MEGJELENT (ON-LINE IS)

16. Ronyecz Lilla: Veszélyes üzemekkel kapcsolatos kockázat és következményelemző eszközök alkalmazása Magyarországon pp. 1-58. Magyarország XXXII. OTDK Had és Rendészettudományi Szekció, Iparbiztonsági tagozat I. helyezés, valamint különdíj (2015)
17. Ronyecz Lilla: Borsod-Abaúj-Zemplén megye iparbiztonsági szempontú veszélyeztetettségének elemzése, lehetséges súlyos balesetek hatásainak vizsgálata pp. 1-55. Magyarország XXXII. OTDK Had és Rendészettudományi Szekció (2015)
18. Ronyecz Lilla, Bognár Balázs, Kátai-Urbán Lajos: International experiences in risk analysis of critical infrastrcture International Disaster Management Scientific Conference - Focus on Changes in the Fire Safety Situation, Budapest, Magyar Tűzvédelmi Szövetség 2024. 154 p. pp. 112-118.

MELLÉKLETEK

1. Rövidítések jegyzéke

2. Fogalomjegyzék

3. Jogi szabályozás jegyzéke

4. Ábrák és táblázatok jegyzéke

5. Kohéziós táblázat

6. Ágazati és alágazati kockázatelemzési sajátosságok áttekintő táblázata

7. Nemzetközi szakirodalmi és módszertani áttekintés a kritikus infrastruktúrák és kritikus szervezetek kockázatelemzéséhez -2. fejezeti kiegészítés-

8. Összehasonlító táblázat a vizsgált módszertanokról az esettanulmány elkészítése során – kiegészítés a 3. fejezethez-

9. Számítási példák az ágazati kockázatelemzés alkalmazására

10. Ellenálló képességért felelős vezetőkkel készített kérdőív

1. Rövidítések jegyzéke

BM OKF - BM Országos Katasztrófavédelmi Főigazgatóság

ENSZ EGB - ENSZ Európai Gazdasági Bizottsága

EU - Európai Unió

MAVIR Zrt. - MAVIR Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zártkörűen Működő Részvénytársaság

MVM Zrt – Magyar Villamos Művek Zártkörűen Működő Részvénytársaság

ISO - International Organization for Standardization, Nemzetközi Szabványügyi Szervezet,

NATO - Észak Atlanti Szerződés Szervezete, North Atlantic Treaty Organisation

HAZOS – Hazard and Operability Study

FTA – Fault Tree Analysis

ETA – Event Tree Analysis

ICS – Industrial Control System

SCADA – Supervisory Control and Data Acquisition

FMEA Failure Mode and Effects Analysis

FMECA Failure Mode and Effects Analysis Criticality Analysis

MH - Magyar Honvédség

QRA - Quantitative Risk Assessment

ENSZ – Egyesült Nemzetek Szervezete

JRC - Joint Research Centre

ENISA -Európai Unió Kiberbiztonsági Ügynöksége

OECD – Gazdasági Együttműködési és Fejlesztési

JRC – Join Research Center

CIWIN - Critical Infrastructure Warning Information Network

EPCIP - European Programme for Critical Infrastructure Protection

MEKH -Magyar Energetikai és Közműszabályozási Hivatal

NMHH – Nemzeti Média- és Hírközlési Hatóság

EU IPCR – Integrated Political Crisis Response, Integrált Politikai Válságreagálás

UN OCHA – United Nations Office for the Coordination of Humanitrian Affairs

UNICEF – United Nations Children’s Fund

ITU – Nemzetközi Távközlési Egyesület

IAEA – International Atomic Energy Agency

LNG – Cseppfolyósított földgáz

VJT – választható jelzéstartalmú közúti jelzőlámpák

BGP – Border Gateway Protocol

GNSS – Global Navigation Satellite System

EU SST – Space Surveillance and Tracking

DSH – Amerikai Egyesült Államok Belbiztonsági Minisztérium

CISA – Amerikai Egyesült Államok Kiberbiztonsági és Infrastruktúrabiztonsági Ügynökségen

SRMA - Amerikai Egyesült Államok Ágazatspecifikus ügynökségek és ágazati kockázatkezelési ügynökségek

NRMC - Amerikai Egyesült Államok Nemzeti Kockázatkezelési Központ

NIPP - Amerikai Egyesült Államok Nemzeti infrastruktúra-védelmi terv

ISAC - Amerikai Egyesült Államok Információmegosztó és elemző központok

CPNI – Egyesült Királyság Nemzeti Infrastruktúra Védelmi Központ

NRR - Egyesült Királyság Nemzeti Kockázati Nyilvántartás

NCSC - Egyesült Királyság Nemzeti Kiberbiztonsági Központ

RCB – Lengyelországi Belbiztonsági Kormányzati Központ

APCIP – Ausztriai Kritikus Infrastruktúrák Védelmének Osztrák Programja

BBK – Németországi Szövetségi Polgári Védelmi és Katasztrófavédelmi Hivatal

ISMS – Német korszerű információbiztonsági irányítási rendszert

BCMS – Német üzletmenet-folytonossági rendszert

ZKI – Szlovéniai Kritikus Infrastruktúra Törvény

CPG - CISA Cross-Sector Cybersecurity Performance Goals

ÁRM - Ágazatközi Reziliencia Munkacsoportot

MCDA – Multi Criteria Decision Analysis

ÁKÖM - Ágazati kockázati összesítő mátrix

BIRR - Better infrastructure risk and resilience

CARVER – Criticality, accessibility, recuperability, vulnerability, effect, recognizability

RAMCAP-Plus - Risk assessment and management for critical asset protection

IIM – Inoperability Input-Output Model

2. Fogalomjegyzék

1. **Alapvető szolgáltatás**:(Kszek tv.) a kritikus szervezet által nyújtott, az 1. mellékletben foglalt táblázat „C” oszlopában meghatározott szolgáltatás, amely elengedhetetlen Magyarország társadalmi, gazdasági stabilitásához, és a biztonság, a környezet, a közegészségügy, a védelmi képességek és a nemzeti ellenálló képességi rendszer fenntartásához.
2. **Ágazati kritérium:** *(Kszek tv.)* olyan az 1. melléklet szerinti ágazattól függő, kormányrendeletben meghatározott szempont, amely alapján egy szervezet, eszköz, létesítmény elengedhetetlenként azonosítható Magyarország társadalmi, gazdasági stabilitásához és a biztonság, a környezet, a közegészségügy, a védelmi képességek és a nemzeti ellenálló képességi rendszer fenntartásához, és amely alapján az kritikus szervezetté, kritikus infrastruktúrává jelölhető ki.

3. **Ágazati szakhatóság:** *(Kszek tv.)* az általános kijelölő hatóság kivételével, az egyes közérdeken alapuló kényszerítő indok alapján eljáró szakhatóságok kijelöléséről szóló kormányrendeletben kijelölt szerv, amely az ott meghatározott szakkérdésben szakhatósági állásfoglalást ad ki a kritikus szervezet, kritikus infrastruktúra kijelölésére, a kijelölés fenntartására vagy a kijelölés visszavonására irányuló eljárásában, továbbá ellátja az e törvényben számára meghatározott egyéb feladatokat.

4. **Általános kijelölő hatóság***: (Kszek tv.)* a földgáz, hidrogén és villamos energia alágazatok kivételével kritikus szervezet, kritikus infrastruktúra kijelölésére, a kijelölés fenntartására vagy a kijelölés visszavonására irányuló közigazgatási hatósági eljárás lefolytatására kormányrendeletben kijelölt hatóság, amely az energetikai ágazati kijelölő hatóság kijelölési eljárása során az egyes közérdeken alapuló kényszerítő indok alapján eljáró szakhatóságok kijelöléséről szóló kormányrendeletben meghatározott esetekben szakhatóságként is közreműködik.

5. **Ellenálló képességi terv***:(Kszek tv.)* a kritikus szervezet és kritikus infrastruktúra ellenálló képességével összefüggésben a rendkívüli események bekövetkezésének megelőzése, következményeire való reagálás, a kockázatkezelési eljárások, riasztási folyamatok végrehajtása, a kritikus infrastruktúrák fizikai védelmének biztosítása, az alternatív megoldások azonosítása, az alapvető szolgáltatás nyújtásának újraindítása

érdekében, valamint a kritikus munkakörben foglalkoztatottak feladatrendszerének, oktatásának, gyakorlatok megszervezése érdekében megtett technikai, biztonsági és szervezeti intézkedéseket leíró dokumentum.

6. **Infrastruktúra:** (*Kszek tv.)* olyan eszköz, létesítmény, építmény, berendezés, hálózat, rendszer, vagy ezek része, amely szükséges egy szervezet működéséhez vagy egy szolgáltatás nyújtásához, azonban nem az alapvető szolgáltatás nyújtásához szükséges.

7. **Kockázatelemzés***: (Kszek tv.)* az a folyamat, amely célja a kockázat jellegének és jellemzőinek megértése, a kockázati szint megállapítása, a bizonytalanságok, a kockázati források, a következmények, a valószínűség, az események, a forgatókönyvek, az intézkedések, valamint azok eredményességének részletes vizsgálata.

8. **Kockázatértékelés:** *(Kszek tv.)* az azonosított kockázatok átfogó elemzésének olyan folyamata, amelyben a kockázatelemzés eredményeinek az előzetesen meghatározott kritériumokkal való összehasonlítása során megállapítható, hogy hol szükséges további intézkedés.

9. **Kölcsönös függőség:** *(Kszek tv.)* két entitás között fennálló kétirányú függőség.

10. **Kritikus infrastruktúra***: (Kszek tv.)* olyan eszköz, létesítmény, építmény, berendezés hálózat, rendszer, vagy ezek része, amely az alapvető szolgáltatás nyújtásához szükséges

11. **Az ország védelme és biztonsága szempontjából jelentős infrastruktúra:** *(Vbö.)* az általános kijelölő hatóság vagy a honvédelmi ágazati kijelölő hatóság által kijelölt olyan eszköz, létesítmény, építmény, berendezés, hálózat, rendszer, vagy ezek része, amely az alapvető szolgáltatás nyújtásához szükséges.

12. **Az ország védelme és biztonsága szempontjából jelentős szervezet***: (Vbö.)* az általános kijelölő hatóság vagy a honvédelmi ágazati kijelölő hatóság által kijelölt olyan alapvető szolgáltatást nyújtó szervezet, amely elengedhetetlen Magyarország társadalmi, gazdasági stabilitásához és a biztonság, a környezet, a védelmi képességek és a nemzeti ellenálló képességi rendszer fenntartásához.

3. Jogi szabályozás és szabványok jegyzéke

A. Nemzetközi jogi szabályozás

1. Az Európai Parlament és aTanács (EU) 2022/2555 irányelve (2022. december 14.) 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 hatályon kívül helyezéséről
2. Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről
3. A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről
4. A Tanács ajánlása (2022. december 8.) a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről

B. Magyarországi jogi szabályozás

1. Magyarország Alaptörvénye.
2. 2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről
3. 2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról
4. *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*
5. *474/2024. (XII. 31.) Korm. rendelet a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról*
6. *475/2024. (XII. 31.) Korm. rendelet az ország védelme és biztonsága szempontjából jelentős szervezetek ellenálló képességéről*
7. *65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról*
8. *1191/2025. (VI. 5.) Korm. határozat* a *Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti kockázatértékeléséről*
9. *1192/2025. (VI. 5.) Korm. határozat Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti stratégiájáról*
10. *16/2025. (VI.6.) HM utasítás az ország védelme és biztonsága szempontjából jelentős szervezetek, infrastruktúrák azonosításáról, ellenőrzéséről, valamint az ezzel összefüggő adatok nyilvántartásáról*

C. Szabványok, ajánlások, rendeletek jegyzéke

Száma	**Megnevezés**
ISO/IEC 31010	*Risk management*
ISO/IEC 27005.	*Information security, cybersecurity and privacy protection*
ISO 22301	The international standard for Business Continuity Management Systems

4. Ábrák, táblázatok és képek jegyzéke

Ábrák:

Táblázatok:

Fényképek:

5. Kohéziós táblázat

TUDOMÁNYOS PROBLÉMA	HIPOTÉZIS	CÉLKITŰZÉS	KUTATÁSI MÓDSZER	KÖVETKEZTETÉS	HIPOTÉZIS IGAZOLÁSA/ ELVETÉSE	ÚJ TUDOMÁNYOS EREDMÉNY
1. A kritikus szervezetek fenyegetettsége napjainkban jelentősen átalakult, így a védelmi rendszerek naprakészen tartása és fejlesztése a nemzetközi előírások és gyakorlati tapasztalatok figyelembevételév el indokolttá vált.	Feltételezésem szerint jelentős összefüggés van a kritikus szervezetek és infrastruktúrák rezilienciája és egy mindenre kiterjedő, a kritikus infrastruktúra sajátosságait részletesen figyelembe vevő kockázatelemzés között. Ennek alapján időszerűvé vált a kritikus infrastruktúrák védelmét meghatározó kockázatelemzés és a jelenleg is zajló konfliktusok, kritikus infrastruktúrákat ért támadások hatásainak elemzése, értékelése.	A kutatás során elemzem és értékelem a kritikus szervezetek védelmének intézményi és szabályozási keretrendszerét, különös tekintettel a jelenkori biztonságpolitikai környezetre és annak hatásaira. Feldolgozom és rendszerezem a kritikus infrastruktúrák fenyegetettségére, sebezhetőségére és interdependenciáira vonatkozó szakirodalmat, majd elemezni kívánom a kritikus szervezetek közötti kölcsönös függőségek kritikus pontjait és lehetséges töréspontjait. Célom, hogy a kutatás eredményeképpen feltárjam a kritikus szervezetek védelmének fejlesztési irányait, valamint azokat a mechanizmusokat, amelyek a reziliencia növelését és a rendszerszintű kockázatok mérséklését szolgálhatják.	Kellő körültekintéssel és a teljesség igényére törekedve a kutatómunkám megalapozása érdekében a kutatási problémákat szem előtt tartva megfelelő mértékben dolgoztam fel a nemzetközi, az európai uniós, valamint a hazai jogi szabályozást. Különös tekintettel a releváns külföldi és magyar szakirodalom értékelő-elemző vizsgálatára.	A műszaki szakirodalom alapján egyértelműen megállapítható, hogy a kritikus infrastruktúrák kockázatelemzése területén a legtöbb modell, közös nevezőként a komponensek sérülékenységének és a rendszerszintű összekapcsoltság hatásainak együttes értékelését tekinti meghatározónak. A vizsgált források ugyanakkor rámutatnak, hogy a klasszikus műszaki megközelítések önmagukban nem képesek kezelni az ágazatközi interdependenciákból fakadó komplex hatásláncokat.A szakirodalmi vizsgálat másik fontos tanulsága, hogy a műszaki alapú kockázatelemzési módszerek akkor biztosítanak valós döntéstámogató értéket, ha a numerikus mutatókat normalizált, összehasonlítható formában kezelik, és transzparens súlyozási eljárásokkal kapcsolják össze. A nemzetközi szakirodalom arra mutat rá, hogy a modern kockázati környezetben a kritikus infrastruktúrákat már nem lehet elszigetelten vizsgálni, mivel a digitális hálózatok meghibásodása befolyásolja az energiairányítást és a közlekedési folyamatokat.	A következtetésekr e alapozva igazoltnak látom az 1. hipotézisemben leírtak teljesülését, amellyel megalapoztam az 1. tudományos kutatási eredményemet.	A kritikus szervezetek védelmének jogi szabályozási, fogalmi, eljárásrendi és műszaki szakirodalmára vonatkozó vizsgálatokra építve megállapítottam, hogy a klasszikus műszaki kockázatelemzési megközelítések önmagukban nem képesek kezelni az ágazatközi interdependenciákból fakadó komplex hatásláncokat, ezért szükségessé vált az ilyen rendszerekre optimalizált hibrid modellek alkalmazása. Ennek függvényében meghatároztam a hálózati összefüggéseket és a szolgáltatás-folytonosságot is figyelembevevő kockázatelemzési módszereket, amelyek alkalmazása képes a vizsgált négy ágazat rendszerszintű kockázatainak mérséklésére és az ellenálló képességük növelésére.

TUDOMÁNYOS PROBLÉMA	HIPOTÉZIS	CÉLKITŰZÉS	KUTATÁSI MÓDSZER	KÖVETKEZTETÉS	HIPOTÉZIS IGAZOLÁSA/ ELVETÉSE	ÚJ TUDOMÁNYOS EREDMÉNY
2. A magyarországi kritikus szervezetek kockázatelemzése jelenleg jellemzően szervezeti szinten zajlik, így hiányzik az ágazati szintű kockázati kép. Ez különösen problémás a dominóhatások és az ágazatközi függőségek feltérképezésekor, például az energia-, víziközmű-, és közlekedési rendszerek kölcsönhatásai esetében, így annak kialakítása külön módszertan kialakítását igényli.	Feltételezésem szerint a kritikus szervezeteket és infrastruktúrákat veszélyeztető tényezők felméréséhez és az ellenálló képesség növeléséhez szükséges egy ágazati kockázatelemzés elvégzése, ami kiemeltem vizsgálja a rendszerelemek közötti interdependenciát.	A kutatásom célja egy olyan ágazati kockázatelemzési keretrendszer kialakítása, amely egységes, összehasonlítható és módszertanilag megalapozott módon támogatja a kritikus szervezetek kockázatkezelését. Ennek érdekében összehasonlító elemzést végzek több ország kockázatelemzési gyakorlatáról, különös tekintettel az alkalmazott módszerekre. A dolgozatban kidolgozom az ágazati kockázatelemzés módszertani keretét, amely tartalmazza az értékelési folyamat lépéseit, és a kockázati kritériumok rendszerét. Ezzel párhuzamosan felépítem az adatfeldolgozási és elemzési módszertant, amely biztosítja a különböző ágazatokból származó adatok integrálhatóságát és a rendszerszintű kockázatok vizsgálatát. A kutatás célja tehát egy olyan tudományosan megalapozott és gyakorlati alkalmazásra is alkalmas modell létrehozása, amely hozzájárul a nemzeti ellenállóképesség növeléséhez.	Külföldi műszaki megoldások és jó gyakorlatok tanulmányozása, a hazai műszaki technikai megoldásokkal történő összehasonlító elemzése.	A magyar kritikus szervezetek kockázatelemzése jelenleg jellemzően szervezeti és nemzeti szinten zajlik, így hiányzik az ágazati szintű átfogó kockázati kép. Ez különösen problémás a dominóhatások és az ágazatközi függőségek feltérképezésekor, például az energia-, víziközmű-, és közlekedési rendszerek kölcsönhatásai esetében. Jelenleg nincs egységes, szabványosított indikátorkészlet vagy súlyozási módszertan, amely lehetővé tenné az ágazatokon belüli és azok közötti kockázati szintek összehasonlítását. Az ágazati szintű kockázatelemzés és annak eredményei ezért nem az egyedi kockázatok mechanikus összegzése, hanem a kritikus infrastruktúrák hálózatos működéséből fakadó rendszerszintű kockázatok feltárásának eszköze.	A következtetéseim alapján igazoltnak látom a 2. hipotézisem teljesülését, amely a 2. tudományos kutatási eredményemet alapozza meg.	A kritikus szervezetek védelmével összefüggő ágazati kockázatelemzés módszertanának megalapozása érdekében összehasonlítottam átfogó, többdimenziós elemzés keretében a különböző országok kockázatelemzési megközelítéseit, módszertani felépítéseit és interdependencia kezeléseit, melynek alapján kidolgoztam az ágazati kockázatelemzés módszertani kereteit és az ágazati szintű adatfeldolgozás elemzési alapjait, így biztosítva az ágazatokon belüli és azok közötti kockázati szintek összehasonlíthatóságát.

TUDOMÁNYOS PROBLÉMA	HIPOTÉZIS	CÉLKITŰZÉS	KUTATÁSI MÓDSZER	KÖVETKEZTETÉS	HIPOTÉZIS IGAZOLÁSA/ ELVETÉSE	ÚJ TUDOMÁNYOS EREDMÉNY
3. A kritikus szervezetek feladatainak ellátásában részt vevő hatóságok és a kritikus szervezetek vezetői közötti kommunikáció gyakorisága igen szerteágazó, annak nincs jogszabályban foglalt útja, módja.	Feltételezésem szerint jelenleg az ellenállóképességért felelős vezetők nem rendelkeznek kellő információval a kockázatelemzés teljes körű felülvizsgálatához és elkészítéséhez. Míg a rendszerelem környezetében fellelhető veszélyeket tudják azonosítani, azonban a külső támadás, hibrid fenyegetés okozta fenyegetettség mértékét nem tudják önállóan megállapítani, mivel ilyen információval nem rendelkeznek.	A kutatásom célja a kritikus szervezetek és a hatóságok közötti kommunikáció hatékonyságának értékelése, valamint a kockázatelemzések elkészítéséhez szükséges információáramlás javítására alkalmas módszertani keret kidolgozása. Ennek érdekében összehasonlító elemzést végzek a különböző kockázatelemzési gyakorlatok között, több szempont – adatstruktúra, módszertani mélység, interdependencia-kezelés – alapján. A vizsgálatot esettanulmányok on alapuló elemzésekkel egészítem ki, amelyek feltárják a kommunikációs hibák, adathiányok és visszacsatolási problémák működési következményeit. A cél végül egy olyan, tudományosan megalapozott információáramlási és jelentési modell kialakítása, amely mind a kritikus szervezetek, mind a hatóságok kockázatkezelési tevékenységét hatékonyabban támogatja.	Elemző módszerekalkal mazása, amelynek szerves részét képezik a kritikus infrastruktúrákk al összefüggő módszertan értékelésében, illetve az ebből eredő következtetések levonása alapján javaslatok megfogalmazás a.	A kritikus szervezetek és infrastruktúrák biztonságáért felelős vezetők és a hatóságok közötti hatékony kommunikáció elengedhetetlen a rendkivüli események időben történő észleléséhez és elhárításához, a jogszabályoknak való megfeleléshez és az infrastruktúra védelméhez. E kommunikációs problémák megoldásához a gyakorlatban világos protokollokra, rendszeres és átlátható információcserére, valamint jobb koordinációs mechanizmusokra van szükség mind a rutinműveletek, mind a válsághelyzetek során. A kérdőív válaszaiból kirajzolódik, hogy a kritikus szervezetek ellenálló képességért felelős vezetői egyértelműen nagyobb hangsúlyt helyeznek a részletes, rendszeres és személyre szabott tájékoztatásra. Ennek alapján javasolt bővíteni a gyakorlatban az információátadás formáit, a formális jelentések mellett szükség van interaktív platformokra, workshopokra és konzultációs lehetőségekre.	A következtetéseim alapján igazoltnak látom a 3. hipotézisem teljesülését, valamint véleményem szerint megalapoztam a 3. tudományos kutatási eredményemet is.	A kritikus szervezetek vezetői és a hatóságok közötti kommunikációs gyakorlat hatékonyságának értékelése és vizsgálata során azonosítottam a kommunikációs és koordinációs hiányosságokat, amelyek rendszerszintű kockázatokat generálnak. Ennek alapján kidolgoztam egy strukturált folyamatokra, és egységesített adatszolgáltatásra épülő módszertani eljárást, amely a hatóságok és akritikus szervezetek közötti egységesített adatszolgáltatásra épül, ezáltal támogatja a kockázatelemzések minőségének növelését és a döntéshozatal gyorsabb, megalapozottabb működését.

6. Ágazati és alágazati kockázatelemzési sajátosságok áttekintő táblázata

Ágazat	Alágazat	Kockázatelemzési sajátosságok (műszaki, kiber-fizikai, üzemviteli)
Energia	Villamosenergia	N-1 hálózati kritérium; transzformátor- és alállomási redundancia, SCADA/ICS sebezhetőség; kaszkád- és dominóhatások, meghibásodási ráták jól becsülhetők (MTBF), extrém időjárás hatása.
	Földgáz	Nyomás- és kompresszorállomások kritikus pontjai, ellátási útvonal-függés, importkitettség, ICS sebezhetőség, robusztus, de lassan reagáló infrastruktúra.
	Kőolaj	Csővezeték-sérülékenység; szivattyúállomások energiafüggése; környezeti kockázatok, lassú helyreállítási képesség.
	Távhő	Magas energia- és gázfüggés, hőtermelő és elosztó pontok sérülékenysége, időjárás okozta terhelési ingadozás.
Közlekedés	Vasút	RAMS-rendszer, biztosítóberendezések és váltók kritikus szerepe, időjárásérzékenység; humán hiba jelentősége, ETCS és kommunikációs rendszer függősége (GSM-R).
	Közút	Kapacitás- és forgalmi kockázatok; ITS rendszerek sérülékenysége, extrém időjárás (hó, hőhullám) hatása, gyors terjedésű lokális zavarok.
	Légi	Navigációs és kommunikációs rendszerek (ILS/VOR/DME) sérülékenysége, erős kiberfüggés, ATC redundancia, globális interdependencia.
	Vízi	Vízszintfüggés, hajózsilip- és kikötői infrastruktúra kockázatai, GNSS navigációs függés, logisztikai dominóhatások.
Digitális	Elektronikus hírközlés (vezetékes)	Optikai gerinchálózat sérülékenysége, kábelvágás, BGP/DNS támadások, adatközponti függés, multipath routing.
	Mobilhálózat	Bázisállomások energiafüggése, túlterhelési kockázatok, DDoS és jelzavarás, nagy területi lefedettség miatt láncreakciós hatások.
	Adatközpontok	Hűtési rendszer meghibásodás, UPS/redundzancia szerepe, fizikai behatolás, ransomware és felhőszolgáltató-függés.

Ágazat	Alágazat	Kockázatelemzési sajátosságok (műszaki, kiber-fizikai, üzemviteli)
	Felhőszolgáltatások	Nemzetközi függőségi láncok, szolgáltatói koncentráció, adatlokáció és helyreállítási idő, API sebezhetősége.
Világűr	GNSS	Jamming és spoofing; napviharok (CME) hatása, városi kanyonok okozta jelromlás, kritikus szerep időszinkronban és navigációban.
	Műholdas kommunikáció	LEO/GEO műholdak pálya- és sugárzási kockázatai, antennarendszerek időjárásfüggése, kiberkockázatok földi szegmensben.
	Földmegfigyelés	Adatfeldolgozó rendszerek sérülékenysége, késleltetett adatátvitel, meteorológiai és katasztrófavédelmi kritikus szerep.
	Műholdkonstellációk	Ütközési kockázat (űrszemét), pályaszabályozási hibák, tömeges meghibásodások lehetősége, rendszerfüggés a földi hálózatokban.
Víziközmű	Ivóvízellátás	SCADA kitettség; hálózati nyomásingadozás, vízminőségi kockázatok, energiafüggő szivattyúzás.
	Szennyvíz	Gépészeti meghibásodások, áramkimaradás miatti túlfolyás, érzékenység extrém csapadékra, kiber-fizikai sebezhetőség.

7. Nemzetközi szakirodalmi és módszertani áttekintés a kritikus infrastruktúrák és kritikus szervezetek kockázatelemzéséhez - 2. fejezeti kiegészítés-

A nemzetközi szakirodalom és a szabályozási keretek az elmúlt két évtizedben jelentősen hozzájárultak ahhoz, hogy a kritikus infrastruktúrák és kritikus szervezetek védelme egyre inkább a kockázatalapú, indikátororientált és reziliencia-fókuszú megközelítésekre épüljön. Az Európai Unió, az OECD, az Egyesült Királyság és az Egyesült Államok szakpolitikai dokumentumai és módszertani keretrendszerei mind olyan hivatkozási pontokat jelentenek, amelyek a hazai szabályozási és elemzési gyakorlatok számára is hasznos mintákat kínálnak. A jelen melléklet célja, hogy áttekintést adjon a legfontosabb nemzetközi keretekről és azok alkalmazhatóságáról a kritikus szervezetek rezilienciájának és kockázati profiljának vizsgálatában.

I. Az Európai Unió módszertani keretei

JRC – a fenyegetettség–sérülékenység–következmény hármasára épülő indikátor-alapú modellek

Az Európai Bizottság Közös Kutatóközpontja (Joint Research Centre – JRC) kulcsszereplő a kritikus infrastruktúra-védelem módszertanának fejlesztésében. A JRC számos technikai jelentése (pl. *Resilience Assessment Frameworks, CIP Report Series, Interdependencies Analysis Reports*) olyan keretrendszert javasol, amely a kockázatelemzést három fő komponensre bontja:

- Threat (fenyegetettség): a lehetséges események jellege, gyakorisága.
- Vulnerability (sérülékenység): a rendszer struktúrájából, működéséből eredő érzékenység.
- Consequence (következmény): a működéskiesés társadalmi, gazdasági, környezeti hatása.

A JRC modelljeinek egyik előnye az indikátor-alapú struktúra, amely ágazati szinten is alkalmazható (energia, közlekedés, víz, digitális infrastruktúrák, egészségügy, űrinfrastruktúra). A JRC kiemeli a hálózati interdependenciák elemzésének szükségességét, valamint a dinamikus, időben változó reziliencia értékelést, ami különösen fontos a gyorsan átalakuló fenyegetési környezetben.
A módszertani megközelítések széles körben alkalmazhatók a hazai ágazati kockázatelemzésekben, például a kritikus pontok, kaskádhatások és működéskiesési forgatókönyvek azonosítására.

ENISA – az EU kiberfenyegetettségi dimenziójának meghatározó kerete

Az ENISA (European Union Agency for Cybersecurity) évente közzétett Threat Landscape jelentései az uniós kockázatelemzés egyik legfontosabb referenciaanyagát adják. Az ENISA rendszeresen elemzi:

- a kiberfenyegetések fő típusait,
- ezek előfordulási tendenciáit és technikai jellemzőit,

- a kritikus ágazatokra gyakorolt hatásaikat (pl. energia, digitális infrastruktúrák, egészségügy, közlekedés).

Az ENISA hangsúlyozza, hogy a kritikus entitások rezilienciájának értékeléséhez integrált kiber–fizikai megközelítés szükséges, különösen a SCADA/ICS rendszerek, a felhőalapú szolgáltatások és a hálózati időszinkron függései miatt. Az ENISA keretek közvetlenül hozzájárulnak a CER Irányelv és a NIS2 gyakorlati megvalósításához.

OECD – reziliens infrastruktúrakormányzás és klímareziliencia

Az OECD a kritikus infrastruktúrák rezilienciáját a kormányzási kapacitások, a szervezeti felkészültség és a klímaadaptáció oldaláról vizsgálja. A 2021–2025 között publikált anyagok kiemelik:

- a többágazatos kockázatkezelési rendszerek jelentőségét,
- az indikátorok szerepét a reziliencia mérésében,
- az időjárási extrémumok és klímaváltozás okozta infrastrukturális sérülékenységeket,
- a kormányzási mechanizmusok (policy cycle) minőségét, különösen energiában, közlekedésben, víz- és telekommunikációs ágazatokban.

Az OECD modellek különösen hasznosak a nemzeti reziliencia értékelések és a stratégiai beruházások tervezésénél.

Egyesült Királyság – NCSC Cyber Assessment Framework (CAF)

A brit National Cyber Security Centre (NCSC) által fejlesztett Cyber Assessment Framework (CAF) Európa egyik legkiforrottabb reziliencia értékelési keretrendszere. A CAF-et a létfontosságú szolgáltatók számára hozták létre, és négy kapacitásterület köré szerveződik:

1. Irányítás és kockázatkezelés.
2. Védelem a támadások ellen.
3. Kiberbiztonsági események észlelése.
4. Az incidensek hatásának minimalizálása.

A CAF különleges előnye, hogy önértékelésre és hatósági felügyeletre egyaránt alkalmas, és a kritikus entitások számára egyértelmű követelménycsomagot ad. A módszer jól illeszkedik a CER- és NIS2-követelmények gyakorlati alkalmazásához.

Egyesült Államok – NIST SP 800-30 és a kormányzati infrastruktúravédelem

Az Egyesült Államok módszertani alapját a NIST SP 800-30 jelenti, amely a kockázatelemzés „közös nyelveként” szolgál. A keret három fő elemre épül:

- valószínűség-hatás becslés,
- formális kockázati modell,
- az elemzési eredmények beépítése a teljes kockázatkezelési ciklusba.

A NIST megközelítése erősen folyamat-alapú, és kiemelten kezeli a dokumentált, átlátható kockázatértékelést. A tágabb kormányzati keretet a National Infrastructure Protection Plan és a CISA Cross-Sector Cybersecurity Performance Goals adják, amelyek ágazatközi szinten is meghatározzák a kritikus infrastruktúrák minimális biztonsági elvárásait, valamint a kritikus funkciók fenntartására szolgáló teljesítménycélokat.

Összegző értékelés

A nemzetközi szakirodalom és módszertani keretek összevetése alapján megállapítható, hogy a kritikus infrastruktúrák reziliencia értékelése világszerte hasonló alapelvekre épül:

- indikátor-alapú, többdimenziós kockázati modellek,
- interdependenciák és hálózati töréspontok vizsgálata,
- kiber–fizikai megközelítés,
- kormányzási kapacitások hangsúlyos szerepe,
- szolgáltatás-folytonosság és helyreállíthatóság előtérbe kerülése.

A JRC és ENISA technikai keretei, az OECD kormányzási modelljei, az NCSC CAF kimenetorientált rendszere, valamint a NIST és NIPP amerikai módszertanai mind olyan építőelemeket kínálnak, amelyek a magyar kritikus szervezetek kockázatelemzésében és rezilienciájának fejlesztésében közvetlenül alkalmazhatók.

8. Összehasonlító táblázat a vizsgált módszertanokról az esettannulmány elkészítése során – kiegészítés a 3. fejezethez-

Esettanulmány / Módszertan	Ágazat	Fő elemzési lépések	Fő eredmények	Erősségek
I. BIRR (Better Infrastructure Risk & Resilience)	Energia (elektromos hálózat)	Eszközök azonosítása; fenyegetések feltárása (kiber–fizikai–természeti), sérülékenység elemzés, kockázati rangsor, reziliencia-intézkedések	Kritikus hálózati csomópontok azonosítása, kiber- és fizikai védelmi fejlesztések, redundancia növelése	Hálózati szemlélet, reziliencia fókusz, mély műszaki részletezés
II. CARVER	Közlekedés	Kritikus célpontok rangsorolása CARVER kritériumok szerint	Legkritikusabb csomópontok (állomások, csomópontok) kijelölése, védelmi erőforrások optimalizálása	Gyors, priorizáló módszer, fizikai és kiber dimenziók integrálása
III. RAMCAP-Plus	Víziközmű / vízellátás	Kritikus komponensek feltérképezése; fenyegetések (biológiai, fizikai, természeti), kockázati mátrix, helyreállítási intézkedések	Vízkészlet-védelem erősítése, fizikai biztonság és szennyezés elleni védelem fejlesztése	Szektorsemlegeses, rendszer- és eszközszintű értékelés
IV. Sandia Methodology	Digitális + kommunikációs infrastruktúra	Kritikus elemek felmérése, kiberfenyegetések azonosítása, kontrollok elemzése, kockázati rangsor	Kritikus kiberpontok feltárása, behatolásérzékelés és redundancia bővítése	Kiber-fizikai integráció, mély technikai értékelés
V. NIPP Risk Management Framework	Tömegközleked és	Fenyegetések kategorizálása, kockázati elemzés,	Fizikai és kiberbiztonsági intézkedések javítása,	Ágazatközi szövetségi

Esettanulmány / Módszertan	Ágazat	Fő elemzési lépések	Fő eredmények	Erősségek
		intézkedések validálása, monitoring	reagálási tervek korszerűsítése	keret, ciklikus kockázatkezelés
VI. ISO 31000-alapú modell	Egészségügyi infrastruktúra	Kritikus szolgáltatások feltérképezése, fenyegetések (biológiai, logisztikai, kiber), sebezhetőség, kockázati mátrix	Készletlogisztika védelme, redundáns energia- és kommunikációs rendszerek fejlesztése	Nemzetközi szabvány, széles körben adaptálható
VII. Bow-Tie (BT)	Ipari veszélyes üzem	Kiváltó okok és következmények elemzése		

9. Számítási példák az ágazati kockázatelemzés alkalmazására

A következő számítási példák célja annak szemléltetése, hogy a disszertációban bemutatott egyszerűsített ágazati kockázatelemzési képletek hogyan alkalmazhatók különböző ágazatokban, eltérő működési és rendszerszintű sajátosságok mellett. A példák nem konkrét szervezetek auditjára szolgálnak, hanem tipikus ágazati helyzeteket modelleznek, amelyek alkalmasak a módszertan működésének és érzékenységének bemutatására.

A számítások minden esetben az alábbi összefüggésekre épülnek:

$$R = \frac{F\ x\ S\ x\ H}{125}$$

$$R^* = R \cdot (1 + \beta \cdot I)$$

ahol F a fenyegetettség, S a sérülékenység, H a hatás mértéke, I az interdependencia szintje, míg β az interdependencia kockázaterősítő paramétere.

1. Energia ágazat: villamosenergia-átviteli infrastruktúra

Az első példa egy országos jelentőségű villamosenergia-átviteli infrastruktúra tipikus kockázati profilját szemlélteti. Az ilyen rendszerek esetében a legfontosabb sajátosság a szolgáltatáskritikusság, egy esetleges meghibásodás nemcsak egy szűk fogyasztói körre, hanem a teljes gazdaság működésére hatással lehet. Emiatt a hatásérték magas, ugyanakkor az átviteli hálózatokra jellemző a magas műszaki és szervezeti érettség, ami a sérülékenységet mérsékli.

A fenyegetettség értéke a komplex technológiai környezetből, az időjárási szélsőségekből és a kibertér felől érkező fenyegetésekből adódik. A sérülékenység értéke a redundáns rendszerek és a szabályozott üzemirányítás miatt közepesnek tekinthető, míg a hatás a szolgáltatás országos jellege miatt maximális.

$$R = \frac{4\ x\ 3\ x\ 5}{125} = \frac{60}{125} = 0{,}48$$

A számítás eredménye közepes kockázati szintet jelez. Ez az érték jól tükrözi azt a helyzetet, hogy bár az infrastruktúra rendkívül kritikus, a magas szintű védelem és üzemeltetési fegyelem csökkenti a kockázat realizálódásának valószínűségét. A példa rámutat arra, hogy az egyszerűsített modell képes elkülöníteni a magas hatású, de jól védett rendszereket a valóban sérülékeny infrastruktúráktól.

A bizonytalanság ebben az esetben elsősorban a fenyegetettség jövőbeni alakulásából fakad, különösen a klímaváltozás és a kibertér dinamikusan változó kockázatai miatt.

2. Energia ágazat: regionális villamosenergia-elosztó hálózat

A második példa egy regionális elosztóhálózatot vizsgál, amelynek sajátossága, hogy bár területileg korlátozottabb, működése szoros függésben áll más infrastruktúrákkal, például az infokommunikációs rendszerekkel és a beszállítói láncokkal. Az ilyen rendszereknél a sérülékenység jellemzően magasabb, mivel kevesebb redundáns elem áll rendelkezésre, és a karbantartási erőforrások is korlátozottabbak.

A bemeneti értékek alapján az alapkockázat azonos a korábbi példával:

$$R = \frac{3\ x\ 4\ x\ 5}{125} = 0{,}48$$

Önmagában ez még közepes kockázati szintet jelentene, ugyanakkor az elosztóhálózat erős ágazatközi függőségei indokolttá teszik az interdependencia-korrekció alkalmazását:

$$R^* = 0{,}48 \cdot (1 + 0{,}15 \cdot 3) = 0{,}696$$

A korrigált kockázati érték már a magas kockázati tartományba esik. Ez az eredmény jól szemlélteti a módszertan egyik fontos hozzáadott értékét, az interdependenciák figyelembevétele képes lényegesen módosítani a kockázati képet, és rávilágítani olyan rendszerszintű sebezhetőségekre, amelyek az alapkockázati értékből nem lennének egyértelműen levezethetők.

A bizonytalanság itt elsősorban az interdependencia mértékének becsléséből fakad, amely jellemzően kvalitatív szakértői értékelésen alapul.

3. Közlekedési ágazat: vasúti irányító körzet

A harmadik példa egy vasúti irányító körzet kockázati helyzetét mutatja be. A vasúti rendszerek esetében a fenyegetettség és a hatás jellemzően közepes, mivel az események gyakran lokálisan kezelhetők, és a biztonsági előírások szigorúak. Ugyanakkor ezek a rendszerek erősen függnek az energiaellátástól és a távközlési infrastruktúrától.

Az alapkockázat számítása a következő:

$$R = \frac{3\ x\ 2\ x\ 4}{125} = 0{,}192$$

Ez az érték alacsony kockázati szintet jelez, ami összhangban van a vasúti rendszerek hagyományosan magas üzembiztonságával. Az interdependencia figyelembevételével azonban a kockázati kép módosul:

$$R^* = 0{,}192 \cdot (1 + 0{,}15 \cdot 4) = 0{,}307$$

A korrigált érték már a közepes kockázati kategóriába esik. Ez az eredmény jól mutatja, hogy az ágazati kockázatelemzés nem kizárólag az adott ágazat belső jellemzőire fókuszál, hanem képes feltárni azokat a külső függőségeket is, amelyek egyébként alulértékelt kockázatokat hordozhatnak.

4. Információs technológia ágazat: adatközpont vagy gerinchálózati szolgáltató

A negyedik példa az információs technológiai ágazatra fókuszál, amely tipikusan keresztágazati jellegű. Az IT infrastruktúrák magas fenyegetettségnek vannak kitéve, különösen a kiberfenyegetések miatt, miközben szolgáltatáskiesésük számos más ágazatra is közvetlen hatást gyakorolhat.

Az alapkockázat számítása:

$$R = \frac{5\ x\ 3\ x\ 4}{125} = 0{,}48$$

Ez önmagában közepes kockázati szintet jelent. Az interdependenciák figyelembevételével azonban a kockázat jelentősen felerősödik:

$$R^* = 0{,}48 \cdot (1 + 0{,}20 \cdot 4) = 0{,}96$$

A kapott eredmény egyértelműen magas kockázati szintet jelez. Ez a példa jól demonstrálja, hogy az IT ágazat esetében az interdependencia nem kiegészítő tényező, hanem a kockázat egyik meghatározó komponense. A bizonytalanság ebben az esetben elsősorban a fenyegetettség gyors változásából és a külső szolgáltatóktól való függésből adódik.

Összegző megjegyzés a melléklethez

A bemutatott számítási példák igazolják, hogy az egyszerűsített ágazati kockázatelemzési módszertan alkalmas különböző ágazatok kockázati sajátosságainak egységes, összehasonlítható értékelésére. A számítások egyben rávilágítanak arra is, hogy az interdependenciák figyelembevétele nélkül az ágazati kockázati kép torzulhat, különösen a magas fokon összekapcsolt infrastruktúrák esetében.

10. Ellenálló képességért felelős vezetőkkel készített kérdőív

Létfontosságú rendszerelemekkel, kritikus entitásokkal kapcsolatos tapasztalatok a biztonsági összekötő/üzemeltető szemszögéből

Üdvözlöm, Ronyecz Lilla vagyok, doktorandusz hallgató, jelenleg a doktori disszertációmat írom, melynek témája a létfontosságú rendszerelemekkel kapcsolatos kockázat- és következményelemző módszerek kutatása és fejlesztése. A doktori kutatásom során többek között célom a biztonsági összekötők kockázatelemzéssel kapcsolatos munkának segítése valamint a hatóságokkal történő kommunikáció javítása. Ennek felmérése céljából készítettem a alábbi kérdőívet, ami segítséget nyújt számomra a jelenlegi problémák feltárására. Előre is köszönöm a kérdőív kitöltését!

* Kötelező kérdés

Munkafolyamat és feladatok

1. Mely ágazatnál dolgozik biztonsági összekötőként? *

Soronként csak egy oválist jelöljön be.

- ◯ Energia
- ◯ Közlekedés
- ◯ Agrárgazdaság
- ◯ Egészségügy
- ◯ Pénzügy
- ◯ Infokommunikációs technológiák
- ◯ Víz
- ◯ Honvédelem
- ◯ Közbiztonság-védelem
- ◯ Egyéb: _____

2. Mióta látja el a biztonsági összekötői feladatokat?

Soronként csak egy oválist jelöljön be.

- ◯ Fél éve
- ◯ Egy éve
- ◯ Három éve
- ◯ Öt éve
- ◯ Több mint öt éve

3. Milyen mértékben kap megfelelő képzést és támogatást a munkájához kapcsolódó feladat ellátásához?

Soronként csak egy oválist jelöljön be.

- ◯ Teljes mértékben
- ◯ Nagy mértékben
- ◯ Korlátozottan
- ◯ Egyáltalán nem

4. Mennyire érzi úgy, hogy rendelkezésére állnak azok az erőforrások, amelyek szükségesek a munkája megfelelő ellátásához?

Soronként csak egy oválist jelöljön be.

- ◯ Mindig
- ◯ Gyakran
- ◯ Ritkán
- ◯ Soha

5. Milyen új eszközök vagy erőforrások segítenék a munkáját a biztonsági összekötői feladatc elvégzésében?

_____

Ugrás a(z) 6. kérdésre

Elégedettség és kommunikáció

6. Mennyire elégedett a hatóságokkal történő kommunikációval (javaslattevő, kijelölő, nyilvántartó hatóság, ellenőrzést koordináló szerv)?

Soronként csak egy oválist jelöljön be.

	1	2	3	4	5	
Egyá	◯	◯	◯	◯	◯	Nagyon elégedett

7. Mi az, amin javítana a hatóságokkal való kommunikáció során?

8. Milyen gyakorisággal igényelné a hatósággal történő kommunikációt? *

Soronként csak egy oválist jelöljön be.

- ◯ Gyakrabban
- ◯ Jelenlegi gyakoriság megfelelő
- ◯ Ritkábban

9. Van-e olyan tényező, amely akadályozza a munkája elvégzésében, mert nem kap hozzá elegendő információt?

10. Mely területeken látja a legnagyobb kihívásokat a munkájában? *

Soronként csak egy oválist jelöljön be.

- ◯ Információhiány
- ◯ Erőforráshiány
- ◯ Képzési hiányosságok
- ◯ Túl sok adminisztráció
- ◯ Egyéb: _____

11. Mit tartana hasznosnak a munkája megkönnyítése érdekében a biztonsági összekötői szerep betöltésekor?

_____

12. Milyen mértékben érzi úgy, hogy a szervezet megfelelően fel van készülve egy kritikus esemény vagy támadás esetére?

Soronként csak egy oválist jelöljön be.

- ◯ Teljes mértékben felkészült
- ◯ Nagy mértékben felkészült
- ◯ Részben felkészült
- ◯ Nem eléggé felkészült

Kockázatelemzés

13. Milyen gyakran végeznek átfogó kockázatelemzést a létfontosságú rendszerelemekkel kapcsolatban?

Soronként csak egy oválist jelöljön be.

- ◯ Negyedévente
- ◯ Félévente
- ◯ Évente
- ◯ Ritkábban

14. Milyen forrásokat használ a kockázatelemzés során (például belső adatok, külső tanácsadók, szabályozó testületek adatai)?

_____

15. Mennyire érzi úgy, hogy a jelenlegi kockázatelemzési módszerek megfelelőek a létfontosságú rendszerelemek védelméhez?

Soronként csak egy oválist jelöljön be.

- ◯ Teljes mértékben megfelelőek
- ◯ Nagy mértékben megfelelőek
- ◯ Közepesen megfelelőek
- ◯ Kevéssé megfelelőek
- ◯ Nem megfelelőek

16. Kap-e elegendő és megfelelő minőségű adatot a kockázatelemzés elvégzéséhez, felülvizsgálatához?

Soronként csak egy oválist jelöljön be.

- ◯ Igen, minden esetben
- ◯ Többnyire igen
- ◯ Ritkán
- ◯ Nem

17. Mennyire segítené a munkáját egy hatóságok által elkészített tájékoztató vagy jelentés, amely a jelenlegi biztonsági környezetet és a kockázatokat elemzi és értékeli?

Soronként csak egy oválist jelöljön be.

- ◯ Nagy mértékben segítene
- ◯ Segítene
- ◯ Semleges
- ◯ Kevéssé segítene
- ◯ Egyáltalán nem segítene
- ◯ Egyéb: _____

18. Milyen gyakran frissítik a kockázatelemzési eredményeket a rendszerelemek aktuális helyzetének megfelelően?

Soronként csak egy oválist jelöljön be.

- ◯ Rendszeresen
- ◯ Alkalomszerűen
- ◯ Ritkán
- ◯ Nem frissítik

19. Mennyire érzi úgy, hogy a kockázatelemzésből származó eredmények alapján megfelelő intézkedések születnek a kockázatok csökkentésére?

Soronként csak egy oválist jelöljön be.

- ◯ Nagyon elégedett
- ◯ Elégedett
- ◯ Semleges
- ◯ Kevéssé elégedett
- ◯ Egyáltalán nem elégedett

20. Mennyire érzi úgy, hogy a kockázatelemzési eredmények alapján javasolt intézkedéseket ténylegesen alkalmazzák a szervezetben?

Soronként csak egy oválist jelöljön be.

- ◯ Teljes mértékben
- ◯ Nagy mértékben
- ◯ KOrlátozottan
- ◯ Egyáltalán nem

21. Mennyire egyszerű vagy nehéz beépíteni a kockázatelemzési ajánlásokat a napi munkafolyamatokba?

Soronként csak egy oválist jelöljön be.

- ◯ Nagyon egyszerű
- ◯ Egyszerű
- ◯ Közepesen nehéz
- ◯ Nehéz
- ◯ Nagy nehéz

22. Milyen típusú információkat tartana még hasznosnak a kockázatelemzés során (például ú fenyegetési adatok, rendszeres auditok, külső szakértői vélemények)?

_____

23. Hogyan értékeli a különböző létfontosságú rendszerelemek közötti interdependenciákat a kockázatelemzés során?

Soronként csak egy oválist jelöljön be.

- ◯ Nagyon fontos
- ◯ Fontos
- ◯ Kevésbé fontos
- ◯ Nem fontos

24. Milyen mértékben vizsgálja a kockázatelemzés a dominó és az interdependenciákból fakadó további kockázatokat?

Soronként csak egy oválist jelöljön be.

- ◯ Teljes mértékben
- ◯ Nagy mértékben
- ◯ Korlátozottan
- ◯ Nem veszi figyelembe

25. Milyen területeken fejlesztené a kockázatelemzési folyamatokat a létfontosságú rendszerelemek védelme érdekében?

_____

_____

_____

_____

_____

26. Milyen további eszközökre vagy támogatásra lenne szüksége a kockázatelemzés hatékonyabb elvégzéséhez?

27. Hogyan lehetne hatékonyabbá tenni a kockázatelemzési eredmények kommunikációját és megvalósítását a szervezeten belül?