Nemzeti Közszolgálati Egyetem
Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely

Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok

2025/9.

Till Szabolcs Péter

A kritikus szervezetek ellenálló képességéről szóló törvény, valamint a Magyarország kiberbiztonságról szóló törvény kapcsolódásai a védelmi és biztonsági szabályrendszerhez

Rólunk

A műhelytanulmány (working paper) műfaja lehetőséget biztosít arra, hogy a még vállaltan nem teljesen kész munkák szélesebb körben elérhetővé váljanak. Ezzel egyrészt gyorsabban juthatnak el a kutatási részeredmények a szakértői közönséghez, másrészt a közzététel a végleges tanulmány ismertségét is növelheti, végül a megjelenés egyfajta védettséget is jelent, és bizonyítékot, hogy a később publikálandó szövegben szereplő gondolatokat a working paper közzétételekor a szerző már megfogalmazta.

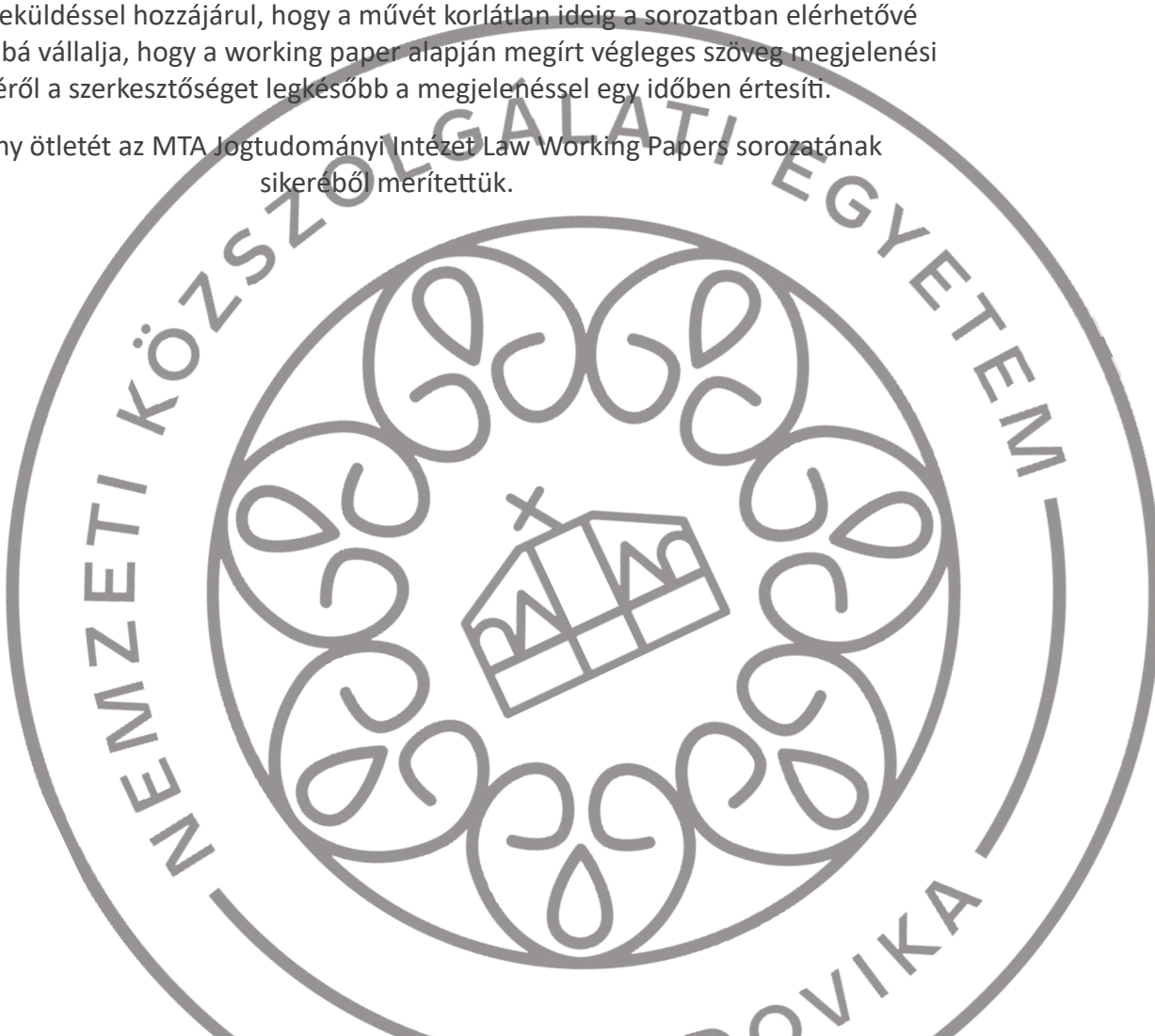
A Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok célja, hogy a Nemzeti Közszolgálati Egyetem Védelmi-biztonsági Szabályozási és Kormányzástani Kutatóműhely küldetéséhez kapcsolódó területek kutatási eredményeit a formális publikációt megelőzően biztosítsa, segítve a láthatóságot, a friss kutatási eredmények gyors közzétételét, megosztását és a tudományos vitát.

A beküldéssel a szerzők vállalják, hogy a mű megírásakor az akadémiai őszinteség szabályai és a tudományosság általánosan elfogadott mércéje szerint jártak el. A sorozatban való megjelenésnek nem feltétele a szakmai lektorálás.

A műfaji jellegből adódóan a leadott szövegekre vonatkozó terjedelmi korlát és egységes megjelenési forma nincs, a szerzőtől várjuk az absztraktot és a megjelentetni kívánt művet oldalszámozással, egységes hivatkozásokkal.

A szerző a beküldéssel hozzájárul, hogy a művét korlátlan ideig a sorozatban elérhetővé tegyük, továbbá vállalja, hogy a working paper alapján megírt végleges szöveg megjelenési helyéről a szerkesztőséget legkésőbb a megjelenéssel egy időben értesíti.

A kiadvány ötletét az MTA Jogtudományi Intézet Law Working Papers sorozatának sikeréből merítettük.



Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2025/5.

Szerző:

Dr. Till Szabolcs Péter ezredes, egyetemi magántanár

Szerkesztő:

Dr. Kádár Pál dandártábornok

Kiadja

Nemzeti Közszolgálati Egyetem
Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely

Kiadó képviselője

Dr. Kádár Pál dandártábornok

ISSN szám
2786-2283

A kézirat lezárva: 2025. november 28.

Elérhetőség:
Nemzeti Közszolgálati Egyetem
Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely
1441 Budapest, Pf.: 60
Cím: 1083 Bp., Ludovika tér 2.
Központi szám: 36 (1) 432-9000

Till Szabolcs Péter

A KRITIKUS SZERVEZETEK ELLENÁLLÓ KÉPESSÉGÉRŐL SZÓLÓ TÖRVÉNY, VALAMINT A MAGYARORSZÁG KIBERBIZTONSÁGRÓL SZÓLÓ TÖRVÉNY KAPCSOLÓDÁSAI A VÉDELMI ÉS BIZTONSÁGI SZABÁLYRENDSZERHEZ

1. Bevezetés

A védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény (a továbbiakban: Vbö.) bár 2022. november 1-i hatályba lépése óta sokszor módosult, azonban az ország védelme és biztonsága szempontjából jelentős szervezetek és infrastruktúrák szabályozására hivatott V/A. fejezet[1] beépülése volt az első alkalom, amely a törvény szerkezete vonatkozásában is következményekkel járt. A fejezet közvetlen kapcsolódását az azt beépítő, *a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvényhez* (a továbbiakban: Kszetv.), valamint *a Magyarország kiberbiztonságról szóló 2024. évi LXIX. törvényhez* (a továbbiakban: Kiberbiztv.[2]) önálló tanulmányban elemeztük a terminológiai kapcsolódások alapján, az 5W+H metodika alkalmazásával.

A jelen tanulmány – e kutatás folytatásaként –a kapcsolódó jogintézményi csomópontok feltárását bővíti, ennek során az érintett három törvényben megosztott módon szabályozott folyamatok feltérképezésére törekszik. A vizsgálat szempontjából azok a kérdések jelentősek, ahol a védelmi és biztonsági igazgatás központi szerve (vagy annak funkcionális eleme) a Kszetv. vagy a Kiberbiztv. szempontjából meghatározott tárgykörökbe beépülve feladatot kap, vagy éppen a védelmi és biztonsági szabályozás valamelyik eleme bukkan fel a másik két törvény által kiterjesztett tartalommal. A kapcsolódások egyre komplexebbé válásának jeleként értékelhető, hogy 2025. második félévében több parlamenti tárgyalási szakban lévő törvénycsomag is érinti a vizsgált három törvényt, sőt a Kiberbiztv. hivatalos rövidítése is csak most fog beépülni a jogrendszerbe.[3]

[1] V/A. fejezet Az ország védelme és biztonsága szempontjából jelentős szervezetek, az ország védelme és biztonsága szempontjából jelentős infrastruktúrák; 43/A. – 43/N. § alcímrendje: 14/A. Általános szabályok, 14/B. Az eljáró hatóságok, 14/C. Különös szabályok.

[2] TILL Szabolcs Péter: Az ország védelme és biztonsága szempontjából jelentős szervezetek és infrastruktúrák szabályozása (Hogyan változtatta meg a szatellit-fejezet *„jelentős" -sége* a Vbö.-t?) *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok* 2025/4.

[3] Az Európai Unió kiberrezilienciáról szóló rendeletének magyarországi végrehajtásáról és egyes kiberbiztonsági rendelkezések módosításáról szóló T/12793. számú törvényjavaslat 10. §-a értelmében a Kiberbiztv. új 52/A. alcímmel és 90/A. §-sal egészül ki a kihirdetését követő 8. napon: ezt követően hivatalos rövidítéssé a Kiberbiztonsági tv. válik. Mivel a kézirat lezárása e fordulónapot megelőzi, a korábban használt rövidítést tartjuk fenn a jelen tanulmányban.

Míg a Vbö. kommentárjának kibővített második kiadásába is beépült korábbi értékelés kulcsszavaként a reziliencia, a nemzeti ellenálló képesség volt rögzíthető, [4] jelen vizsgálatunk szervezeti szempontú fókusza így a védelmi és biztonsági igazgatás központi szerve, vagy annak szervezeti egysége megjelenése, általános jelleggel pedig a „védelmi és biztonsági" szókapcsolat előfordulása. Ennek alapján csomópontokként emelhetők ki a stratégiai tervdokumentumok, illetve a védelmi és biztonsági esemény fogalmainak kiterjesztése, valamint a válságkezelés fokozatossági kapcsolódásainak megjelenése. E kapcsolódások közül egyébként a parlamenti tárgyalás elősegítésére hivatott képviselői tájékoztató anyagok felhívták a figyelmet a kritikus infrastruktúrák[5] és ellátási láncok kiberbiztonsági veszélyeztetettségére,[6] valamint a válságreagálási rendszer uniós szintjének erősítésére,[7] mint az új szabályozások szükségességét megalapozó tényezőkre. A szabályozási okok tehát részlegesen kiemelést nyertek, maguk a kezelésre hivatott szabályozási megoldások viszont nem.

2. Az illeszkedő tárgykörök

A szabályozási és folyamat-szintű kapcsolódások a törvények mellett a vizsgálat körébe vonják a kormányrendeleti szabályokat is, különösen *a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendeletet* (a továbbiakban: Kiberbiztr.), valamint *a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról szóló 474/2024. (XII. 31.) Korm. rendeletet* (a továbbiakban: Kritkr.). Ennek indoka, hogy már a Vbö. is – alapvetően a Kormány szervezet-alakítási szabadságát hangsúlyozva – a „védelmi és biztonsági igazgatás központi szerve" megjelölés alkalmazására törekedett törvényi szinten, amit kormányrendelet azonosított be Védelmi Igazgatási Hivatalként.[8] E feladatkör szempontjából meghatározott szabályozási megoldás elsődleges célja a Kormány szervezet-alakítási szabadságának biztosítása, amelynek részévé vált a kijelölő hatóságok kormányrendeleti nevesítése, valamint a kritikus infrastruktúrákkal és a kibervédelemmel kapcsolatos feladatok megosztása is az alapvető kategóriák törvényi szintű rögzítését kiegészítve.

2.1 A kapcsolódások szintjei és alanyai

A szabályozási rendszerben tipikusan a feladatok szervezetekre, ezáltal azok vezetőire címzettek elsődlegesen, kivételesen ugyanakkor előfordulhat az alárendelt szervezeti egységre nevesített

[4] Kádár Pál (szerk.): *A védelmi és biztonsági szabályozás magyarországi reformja*; Nemzeti Közszolgálati Egyetem Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely 2025. XIX. fejezet 333-348.

[5] A jelen tanulmány a kritikus infrastruktúrák megjelölését gyűjtőfogalmi értelemben használja, e kategória részeként kezelve a védelmi és biztonsági szempontból jelentős szervezeti és infrastrukturális kört is. Az elkülönítés értékelését lásd Till 2025. im.

[6] Baranyi-Müller Tamás (szerk.): Kiberbiztonság az Európai Unióban és Magyarországon; *Infojegyzet* 2024/28. Országgyűlés Hivatala 2024. október 31. 1-2.

[7] Tóth Melinda Dr. (szerk.): Létfontosságú rendszerek védelme; *Infojegyzet* 2024/25. Országgyűlés Hivatala 2024. október 31. 2-4. a horizontális kijelölési kritériumokkal összefüggésben, valamint Baranyi-Müller 2024. im. 3-4.

[8] Lásd a Védelmi Igazgatási Hivatalról szóló 377/2022. (IX. 7.) Korm. rendelet.

szabályozás is, amely esetben a lényeges feladatok koncentrálhatók, ha például a szervezet egészének szabályozási körbe vonását a részelem minőségi sajátossága alapozza meg. Voltaképpen a Kszetv. szabályozási filozófiája eleve erre a különbségtételre épül, amikor a kritikus szervezetek (és a kapcsolódó Vbö.-fejezet esetében a védelmi és biztonsági szempontból jelentős szervezetek) vonatkozásában a kritikus/jelentős szervezeti minőséget megalapozó rész védelmére[9] épül a szabályozás célja, a kijelölés megalapozásában nem érintett szervezetrészek pedig a fókuszon kívül maradhatnak. Hasonló módon a Kiberbiztv. 12. § (2) bekezdésében az elektronikus információs rendszer biztonságáért felelős személyek által irányított szervezeti egységek állományának kiemelése jelenik meg képzési és továbbképzési vonatkozásban, mint a működtetés folyamatossága szempontjából meghatározó jelentőségű fókuszterületnek a szabályozási cél szempontjából elkülönített szektora.

E kiemelési technika ugyanakkor a nemzeti eseménykezelő képesség szempontjából a Vbö-ben eredendően is kimutatható: a szabályozás kiinduló pontja az 52. § c) pontja,[10] amely nem szükségszerűen érvényesülő funkcióként rögzíti a nemzeti eseménykezelő központ működtetését, valamint némileg relativizálja viszonyát a védelmi és biztonsági igazgatás központi szervéhez, a Védelmi Igazgatási Hivatalhoz. Az eredetileg kihirdetett változatához képest módosult c) pont szerint ugyanis – ellentétben a korábban rögzített szabályozási céllal – a nemzeti eseménykezelő központ működtetése külön kormányzati döntéshez kötött, így aktiválható eseti és időszakos jelleggel, végleges bevezetésére irányuló döntés esetén pedig azt formálisan el kell rendelni. Minden változat esetében egyaránt érvényesülő opció ugyanakkor, hogy a nemzeti eseménykezelő képesség tevékenysége mind a válságkezelésre felkészülés érdekében, mind pedig a megvalósult védelmi és biztonsági esemény következtében a válságkezelés összkormányzati szemléletének erősítésére irányul,[11] igazodva a Védelmi Igazgatási Hivatal hozzáadott szemléleti értékéhez.

---

[9] Példaként lásd a Kszetv. 20. § (4) bekezdésének f) pontját és a 26. § (1) bekezdését, kivonatos közlés, kiemelés hozzáadásával: „**20. §** (4) A kritikus szervezet ellenálló képességéért felelős vezető
f) megszervezi a kritikus szervezet és **a kritikus infrastruktúra ellenálló képességét befolyásoló szervezeti egységek közötti koordinációt,** bevonja őket a részfeladatok kidolgozásába…"
„**26. §** (1) A rendkívüli eseményt az ellenálló képességi tervben **a kritikus szervezet rendkívüli esemény kezelésére meghatározott szervezeti egysége** az alábbiak szerint köteles bejelenteni…"

[10] Vbö. „**52. §** A védelmi és biztonsági igazgatás központi szerve (…)
c) **a Kormány erre irányuló döntése esetén,** az eseménykezelés érdekében **nemzeti eseménykezelő központot működtet**, amelynek fő feladata az összkormányzati válságkezelés, illetve a különleges jogrendi feladatellátás szakmai koordinációja és összehangolása felkészülési időszakban, valamint védelmi és biztonsági esemény idején, …" Kivonatos közlés, kiemelés hozzáadva. Az eredeti, külön kormányzati aktiválásra nem irányuló változat szerint a feladatok azonosak lettek volna, csak a megvalósítás módja lett volna automatikus: „c) nemzeti eseménykezelő központot működtet, amelynek fő feladata az összkormányzati válságkezelés, illetve a különleges jogrendi feladatellátás szakmai koordinációja és összehangolása felkészülési időszakban, valamint védelmi és biztonsági esemény idején, …"

[11] A korábbi ad hoc válságkezelési fókuszokkal összevetésben lásd Lakatos Tibor: Az integrált rendészeti törzsek szerepe a veszélyhelyzetek kezelésében; *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok* 2023/9. 11-12.

Kapcsolódó adatkezelési szabályként a Vbö. 66. § (4) és (5) bekezdése[12] az érzékeny adatok kezelése vonatkozásában adatkezelőként önállóan nevesíti egyaránt a védelmi és biztonsági igazgatás központi szervét, valamint annak munkaszervezetét, vélelmezhetően a nemzeti eseménykezelő központot, amelynek – berendelések esetén – feladatait ellátó állománya végső soron túl is terjedhet a Védelmi Igazgatási Hivatal állandó személyzetén. E kivételes szabályozási elemre tekintettel adott a szervezet / szervezeti egység szempontú differenciálás a Vbö. eredeti szabályozási rendszerében is,[13] amelyet a két kapcsolódó törvény hatályba lépése további hangsúlyokkal egészített ki.

A mindhárom törvényben kimutatható releváns szervezeti egység kiemelésére irányuló fókusz így lehetővé teszi a törvények közötti kapcsolódások kétszintű kialakítását, jelentőséget nyerhet a szervezet mellett a szervezeti egység közvetlen megkeresése és kapcsolódása is. Értelemszerűen a megkeresés indításának felelőse is lehet szervezeti egység, így összesen a 2-2 szereplői szintből 4-féle kapcsolódás modellezhető a szervezeti egységek és szervezetek között alapesetben, amely modell – további szereplő beépülése esetén – további kapcsolódási lehetőségeket biztosít.

E kapcsolódási lehetőségek közül több modell is kimutatható a törvényekben. Megítélésünk szerint vitatható ugyanakkor, hogy egyik adatközlési út során közölt adatok védettségére sem terjed ki a Vbö. 66/B. § (1) bekezdése szerinti honvédelmi vagy nemzetbiztonsági érdekű tájékoztatás-megtagadási lehetőség, mivel az információ tárgya a kiemelt esetekben nem azonosítható a Vbö. szerinti taxatív felsorolás elemeivel.[14] Maga az együttműködési kapcsolatokra épített szabályozási modell ugyanakkor rendszer-szinten a Vbö.-nek a védelmi és biztonsági igazgatás központi szerve feladatköreit rögzítő 52. §-a, mind pedig az összehangolt védelmi

[12] Vbö. „**66. §** (4) A védelmi és biztonsági igazgatás központi szerve a (3) bekezdés szerint megismert, az érintett azonosítását lehetővé tevő egészségügyi adatnak nem minősülő adatot - ha jogszabály vagy az EU kötelező jogi aktusa másként nem rendelkezik - **kizárólag a védelmi és biztonsági igazgatás központi szerve, annak munkaszervezete** tevékenységében az intézkedés megtétele érdekében közvetlenül részt vevő személy ismerheti meg, egyebekben az ilyen adatot más, az intézkedésben közvetlenül részt vevő személy számára csak az adat személyazonosításra alkalmatlanná tételét vagy álnevesítését követően lehet megismerhetővé tenni.
(5) A (2) bekezdés szerint megismert, az érintett azonosítását lehetővé tevő egészségügyi adatot - ha jogszabály vagy az EU kötelező jogi aktusa másként nem rendelkezik - **kizárólag a védelmi és biztonsági igazgatás központi szerve, annak munkaszervezete** tevékenységében az intézkedés megtétele érdekében közvetlenül részt vevő orvos ismerheti meg, egyebekben az ilyen adatot más, az intézkedésben közvetlenül részt vevő személy számára csak az adat személyazonosításra alkalmatlanná tételét vagy álnevesítését követően lehet megismerhetővé tenni.” (Kiemelés hozzáadva.)

[13] A Vbö. 83. § (5) bekezdése alapján adott a szabályozási felhatalmazás a nemzeti eseménykezelő központ feladatainak és működési rendjének meghatározására, e felhatalmazás azonban még nem került eddig kitöltésre.

[14] „**66/B. §** (1) Ha - az állam külső és belső biztonságának hatékony és eredményes védelme biztosításával összefüggő - a védelmi és biztonsági igazgatás központi szerve által kezelt, **a beszerzésekre, a szerződésekre, a gazdálkodási adatokra, a személyi állományra**, valamint a védelmi és biztonsági igazgatás központi szerve által működtetett **nemzeti eseménykezelő központ felépítésére, működésére, technikai eszközeire és felszerelésére** vonatkozó valamely adat megismerése Magyarország honvédelmi vagy nemzetbiztonsági érdekeit veszélyezteti, annak megismerése iránti igény teljesítését az adat keletkezésétől számított tíz évig meg kell tagadni.” Kiemelés hozzáadva.

tevékenység Vbö. 75. § (1) bekezdés d) pontjában hangsúlyozott együttműködési kötelezettség szempontjából illeszthető.

2.1.1) Szervezeti egység – reagáló szervezetek – szervezeti egység

A Kszetv. 26. § (2) bekezdése[15] szerinti bejelentési rendben a kritikus szervezet rendkívüli esemény kezelésére kijelölt szervezeti egységétől indul az információ, amely értesítés végpontja – ágazatok szerint differenciált alternatív útvonalak közbeiktatásával – a Vbö. szerinti nemzeti eseménykezelő központ. Az alternatív útvonalak csomópontjainak száma az ágazati ügyeletszervezés módjától függően eltérhet, a katasztrófavédelem területileg illetékes szerve, valamint az általános kijelölő hatóság ugyanakkor feltétlenül aktiválandó szereplő, a nemzeti eseménykezelő központ felé így legalább kettős információ-áramlási felelősséget aktiválva. A rendkívüli esemény kezelésének lezárását követően a tapasztalatfeldolgozó jelentést az (5) bekezdés szerint[16] már a kritikus szervezet ellenálló képességéért felelős vezető aktiválja a kijelölésben érintett hatóságok és szakhatóságok útján a nemzeti eseménykezelő központ irányába. Hasonló az eljárásrend a (9) bekezdés szerint is,[17] csak éves összesítéssel a kontrollált rendkívüli események tapasztalatai vonatkozásában.

---

[15] Kszetv. „**26. §** (1) A rendkívüli eseményt az ellenálló képességi tervben a kritikus szervezet rendkívüli esemény kezelésére meghatározott szervezeti egysége az alábbiak szerint köteles bejelenteni:[15]
(2) A rendkívüli eseményt az általános kijelölő hatóság által közzétett formanyomtatványon
a) minden esetben
aa) a hivatásos katasztrófavédelmi szerv területi szervének ügyeleti szolgálata,
ab) az általános kijelölő hatóság,
b) az adott ágazatot érintően
ba) az ágazati minisztérium által meghatározott ügyeleti szolgálat,
bb) az ágazati szakhatóság által meghatározott kapcsolati hely,
c) az energetikai ágazati kijelölő hatóság által kijelölt kritikus szervezet, kritikus infrastruktúra esetén az energetikai ágazati kijelölő hatóság
részére kell bejelenteni, amely szervek értesítik a védelmi és biztonsági tevékenységek összehangolásáról szóló törvény szerinti nemzeti eseménykezelő központot."

[16] Kszetv. **26. §** „(5) A rendkívüli esemény lezárását követően a kialakulásáról, a megtett intézkedésekről, a hasonló események megelőzése érdekében tett intézkedésekről a kritikus szervezet ellenálló képességéért felelős vezető az általános kijelölő hatóság által meghatározott határidőre jelentést nyújt be
a) a kritikus szervezet vezetője,
b) valamennyi kritikus szervezet esetében az általános kijelölő hatóság és a kritikus szervezet kijelölésében hatáskörrel rendelkező ágazati szakhatóság, valamint
c) az energetikai ágazati kijelölő hatóság által kijelölt kritikus szervezet esetében az energetikai ágazati kijelölő hatóság részére, amely szervek a jelentést megküldik a védelmi és biztonsági tevékenységek összehangolásáról szóló törvény szerinti nemzeti eseménykezelő központ részére."

[17] Kszetv. **26. §** „(9) A kontrollált rendkívüli esemény kialakulásáról, a megtett intézkedésekről, a hasonló események megelőzése érdekében tett intézkedésekről a kritikus szervezet ellenálló képességéért felelős vezető éves jelentést nyújt be
a) a kritikus szervezet vezetője,

2.1.2) Szervezet – reagáló szervezet – szervezeti egység

Az ország védelme és biztonsága szempontjából jelentős honvédelmi kijelölésű szervezetek és infrastruktúrák esetében a Vbö. 43/L. § szerinti eljárásrend abból a szempontból a megelőző egyszerűsített variánsa, hogy itt a köztes szereplő kizárólagosan a honvédelemért felelős miniszter által kijelölt ügyeleti szolgálat mindhárom jelentési forma esetében, így a nemzeti eseménykezelő központ tájékoztatására ez az ügyelet kötelezett,[18] nem alakulnak ki többszörözött jelentési útvonalak.

2.1.3) Szervezet– szervezet

Voltaképpen a szervezet-szervezet közötti információáramlás lenne a szabályozás modellje szempontjából az alapvető szabályozási variáns, bár a főszabály mégsem gyakran alkalmazott megoldás a három törvény viszonyrendszerében. A Kszetv. 6. § (3) bekezdése[19] a javaslattétel lehetősége esetében tartalmazza a Védelmi Igazgatási Hivatal – kijelölő hatóság irányt, fordított irányú információ-áramlásként, a védelmi és biztonsági igazgatás központi szerve felé a Kszetv.

- 23. § (4) bekezdés 5. pontja[20] részben felkészülési, részben pedig eseménykezelési információ-áramlást biztosít;
- 25. § (4) és (5) bekezdése alapján a kiemelt éves gyakorlatok körébe bevont kritikus szervezetek adatközlési kötelezettsége a komplex ellenálló képességi gyakorlatról szóló

b) az általános kijelölő hatóság és a kritikus szervezet kijelölésében hatáskörrel rendelkező ágazati szakhatóság, valamint

c) az energetikai ágazati kijelölő hatóság által kijelölt kritikus szervezet esetében az energetikai ágazati kijelölő hatóság részére, amely szervek a jelentést megküldik a védelmi és biztonsági tevékenységek összehangolásáról szóló törvény szerinti nemzeti eseménykezelő központ részére."

[18] Vbö. „**43/L. §** (1) A rendkívüli eseményt az általános kijelölő hatóság által közzétett formanyomtatványon az ország védelme és biztonsága szempontjából jelentős honvédelmi kijelölésű szervezet és az ország védelme és biztonsága szempontjából jelentős honvédelmi kijelölésű infrastruktúra esetén a honvédelemért felelős miniszter által kijelölt ügyeleti szolgálat részére kell bejelenteni, amely szervek értesítik a nemzeti eseménykezelő központot.

(2) A rendkívüli esemény lezárását követően annak kialakulásáról, a megtett intézkedésekről, a hasonló események megelőzése érdekében tett intézkedésekről az ellenálló képességért felelős vezető az általános kijelölő hatóság által meghatározott határidőre jelentést nyújt be az ország védelme és biztonsága szempontjából jelentős honvédelmi kijelölésű szervezet esetében a honvédelmi ágazati kijelölő hatóság részére, amely szervek a jelentést megküldik a nemzeti eseménykezelő központ részére.

(3) A kontrollált rendkívüli esemény kialakulásáról, a megtett intézkedésekről, a hasonló események megelőzése érdekében tett intézkedésekről az ellenálló képességéért felelős vezető éves jelentést nyújt be az ország védelme és biztonsága szempontjából jelentős honvédelmi kijelölésű szervezet esetében a honvédelmi ágazati kijelölő hatóság részére, amely szervek a jelentést megküldik a nemzeti eseménykezelő központ részére."

[19] Kszetv. „**6. §** (3) A védelmi és biztonsági igazgatás központi szerve javaslatot tehet a kijelölő hatóság részére kritikus szervezet kijelölésére irányuló hatósági eljárás megindítására."

[20] Kszetv. „**23. §** (4) A nyilvántartó hatóság a nyilvántartásból adatot szolgáltat (...)

5. a védelmi és biztonsági igazgatás központi szerve részére a védelmi és biztonsági esemény bekövetkezésekor, illetve az erre, vagy különleges jogrendre való felkészülési folyamatban részt vevő, továbbá az eseménykezelésben és a helyreállításban részt vevő szervek tevékenységének támogatása céljából, ..." (Kivonatos közlés)

előzetes tájékoztatásra vonatkozik[21] az együttműködőkészség tesztelhetősége érdekében, közvetlenül a tervek végrehajthatóságát értékelve;

- látszólag egyoldalú adatszolgáltatási kötelezettségeket tartalmaz a 39. § (7) bekezdése[22] a nemzetközi kapcsolattartás köztes szereplőjeként, ahol azonban vélelmezhető a visszacsatolás, így a kétirányú szervezetközi kommunikációs folyamat.

2.1.4) Nem önálló szervezeti munkaforma (Operatív Törzs) – szervezeti egység (nemzeti eseménykezelő központ)

A Kiberbiztv. 74. § (1) bekezdése alapján lehetséges eljárásrend a jelentős vagy nagyszabású kiberbiztonsági incidens esetén a Nemzeti Kiberbiztonsági Munkacsoport Operatív Törzsének javaslata alapján a kiberbiztonsági válsághelyzetté minősítés. Ennek során a védelmi és biztonsági esemény kezelésével összegfüggésben bekért adatok megosztását írja elő a Kiberbiztv. 74. § (6) és (7) bekezdése[23] a nemzeti eseménykezelő központtal a nemzetbiztonsági adatok két lépcsős mérlegelése kivételével. Voltaképpen e szabályozási megoldás a 2.1.1) alpont egyszerűsített, áttétel nélküli variánsa, ahol azonban a reagálás a Védelmi Igazgatási Hivatal szervezeti szintű aktiválását váltja ki. A Kiberbiztv. 74. § (11) és (12) bekezdése[24] így a kiberbiztonsági

---

[21] Kszetv. „**25. §** (4) Az általános kijelölő hatóság által az éves ellenőrzési tervben, továbbá a védelmi és biztonsági tevékenységek összehangolásáról szóló törvényben foglaltakra is figyelemmel kijelölt kritikus szervezet az általános kijelölő hatóság együttműködésével komplex ellenálló képességi gyakorlatot tart, melyről megkezdését megelőzően legalább 30 nappal értesíti a védelmi és biztonsági igazgatás központi szervét.
(5) A komplex ellenálló képességi gyakorlat célja a kritikus szervezet ellenálló képességi tervében megjelölt szervezeti és eszközrendszer alkalmasságának, továbbá a kritikus szervezet és a rendkívüli esemény kezelésében érintett szervezetek együttműködésének vizsgálata."

[22] Kszetv. „**39. §** (7) Az Európai Bizottság felé ezen § szerinti jelentést és az (5) bekezdés szerinti adatszolgáltatást megelőzően az egyedüli kapcsolattartó pont az érintett adatokat megküldi a védelmi és biztonsági igazgatás központi szerve részére."

[23] Kiberbiztv. „**74. §** (6) A kiberbiztonsági válsághelyzet ideje alatt a kiberbiztonsági válsághelyzet megelőzése, megismerése, felderítése és továbbterjedésének megakadályozása, valamint az állami szervek összehangolt feladatellátásának megszervezése céljából az Operatív Törzs- a kiberbiztonsági válsághelyzettel összefüggően-
a) adatszolgáltatást kérhet bármely szerytől, jogi személytől vagy jogi személyiséggel nem rendelkező szervezettől, amely ezen adatszolgáltatásnak köteles haladéktalanul, térítésmentesen eleget tenni,
b) kezeli a kiberbiztonsági incidens kezelése során megismert személyes adatokat.
(7) Az Operatív Törzs a (6) bekezdés alapján kezelt adatokat a nemzetbiztonsági tevékenységre vonatkozó információk kivételével köteles átadni a nemzeti eseménykezelő központnak.
"

[24] Kiberbiztv. „**74. §** (11) A kiberbiztonsági válsághelyzettel érintett szervezet- a (12) bekezdésben foglalt kivétellel- a nemzeti kiberbiztonsági incidenskezelő központ, valamint a védelmi és biztonsági igazgatás központi szervének kérésére köteles a (10) bekezdésben meghatározott tervvel, valamint a kiberbiztonsági válsághelyzet kezelése érdekében bevezetett intézkedésekkel kapcsolatos adatokat, információkat összegyűjteni, és elektronikus formában átadni vagy egyéb módon hozzáférhetővé tenni.
(12) A honvédelmi célú elektronikus információs rendszerek tekintetében a (11) bekezdésben meghatározott adatokat a honvédelmi kiberbiztonsági incidenskezelő központ, valamint a védelmi és biztonsági igazgatás központi szerve számára kell- kérésük esetén- hozzáférhetővé tenni."

válsághelyzettel érintett szervezet vonatkozásában – a feladatkörrel érintett általános, vagy honvédelmi kiberbiztonsági incidenskezelő központ mellett – a védelmi és biztonsági igazgatás központi szervét nevesíti terv, adat- és információ-továbbítási be kérésre jogosult szervként.

A kiberbiztonsági válsághelyzetek kezelése során *a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet* 67. § (1) bekezdésének e) pontja szerint a folyamatos információcsere alanyaivá a 2. § 15. pontja alapján beazonosított nemzeti kiberbiztonsági incidenskezelő központ válik a nemzeti eseménykezelő központ partnerévé[25] arra is figyelemmel, hogy a nemzetközi kapcsolattartás megosztott szakértői és vezetői szintje a Védelmi Igazgatási Hivatal feladatellátását is aktiválja. A Kiberbiztr. 106. §-a alapján[26] a kiberbiztonsági válsághelyzetek kezelésének rendszerében a védelmi és biztonsági igazgatás központi szervének több feladata és a kapcsolattartás eltérő szintje is megjelenik:

- a (3) bekezdés alapján a nemzeti eseménykezelő központ igazgatási és koordinációs feladatellátása során az az érintett kiberbiztonsági incidenskezelő központtal működik együtt,
- a (4) bekezdés alapján az ágazati válságkezelési tájékoztatások a Védelmi Igazgatási Hivatal szintjén kerülnek becsatornázásra,

[25] Kiberbiztr. „67. § (1) A Központ ellátja a következő feladatokat: (…)
3. kiberbiztonsági válsághelyzetek kezelését érintő feladatkörében: (…)
e) a kiberbiztonsági válsághelyzet hatékony kezelése érdekében folyamatos kapcsolatot tart a nemzeti eseménykezelő központtal; …” (Kivonatos közlés.)

[26] Kiberbiztr. „106. § (1) A kiberbiztonsági válsághelyzet kezelésével kapcsolatos feladatokat az érintett személyek, szervek és szervezetek a Kiberbiztonsági tv.-ben és az e rendeletben meghatározottak figyelembevételével, a rájuk vonatkozó jogszabályi rendelkezések és közjogi szervezetszabályozó eszközben előírtak alapján hajtják végre.
(2) A kiberbiztonsági válsághelyzet feltételeinek a fennállását az Operatív Törzs folyamatosan figyelemmel kíséri, és ha a kiberbiztonsági válsághelyzet elrendelésének a feltételei már nem állnak fenn, kezdeményezi az informatikáért felelős miniszternél, hogy tegyen javaslatot a Kormánynak a kiberbiztonsági válsághelyzetet elrendelő kormányrendelet hatályon kívül helyezésére.
(3) A kiberbiztonsági válsághelyzet kezelésével kapcsolatos igazgatási és koordinációs feladatokat a Vbö. 52. § c) pontjában meghatározott nemzeti eseménykezelő központ (a továbbiakban: nemzeti eseménykezelő központ) biztosítja, az érintett kiberbiztonsági incidenskezelő központ aktív támogatásával.
(4) A kiberbiztonsági válsághelyzet kezelésével kapcsolatban megtett ágazati intézkedésekről a védelmi és biztonsági igazgatás központi szervét, valamint az informatikáért felelős miniszter előterjesztése útján a Védelmi Tanácsot haladéktalanul tájékoztatni kell.
(5) A kiberbiztonsági válsághelyzet kezelésével kapcsolatos nemzetközi együttműködéssel összefüggő feladatokat, az IPCR felületen történő tagállami információcsere koordinációját a védelmi és biztonsági igazgatás központi szerve végzi.
(6) A kiberbiztonsági válsághelyzet kezelésével kapcsolatos szakmai feladatokat Magyarország képviseletében az EU-CyCLONE-ban
a) vezető tisztviselői, ügyvezetői szinten a védelmi és biztonsági igazgatás központi szerve,
b) szakértői szinten
ba) a Nemzetbiztonsági Szakszolgálat,
bb) az informatikáért felelős miniszter által vezetett minisztérium és felkérés alapján a honvédelemért felelős miniszter által vezetett minisztérium
látja el.”

- az (5) bekezdés szerint az EU politikai szintű integrált válságelhárítási mechanizmus (a továbbiakban: *IPCR)* tagállami információs koordinátora a védelmi és biztonsági igazgatás központi szerve, amely a (6) bekezdés alapján az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatának (a továbbiakban: EU-CyCLONE) szervezetében vezető tisztviselői, ügyvezetői szinten jár el, amelyhez a 111. § alapján nagyszabású kiberbiztonsági incidensekről tájékoztatási kötelezettség is társul – a tagállamokra is kiterjedő módon – a képviselő felelősségeként.

A Kiberbiztr. 107. §-a alapján[27] a kiberbiztonsági tervezés kiinduló stratégiai szintű dokumentuma a Magyarország nemzeti kiberválságkezelési terve, amelynek előkészítésében a Védelmi Igazgatási Hivatal csak a Nemzeti Kiberbiztonsági Munkacsoport-részvétel[28] útján, áttételesen bedolgozóként jelenik meg, bár az Ország Összehangolt Védelmi Tervéhez igazítás követelményét, és a kifejezett felelősségi körként rögzített EU-kapcsolattartási feladatokat a kormányrendelet hangsúlyozza.

A gyakorlatok előkészítése során ugyanakkor a Kiberbiztr. 109. §-a alapján[29] főszabályként az Operatív Törzs – Védelmi Igazgatási Hivatal kapcsolattartás lép be az ágazati szakmai szervezetek

[27] Kiberbiztr. „107. § (1) Magyarország nemzeti kiberválságkezelési tervét (a továbbiakban: nemzeti kiberválságkezelési terv) a kiberbiztonságért felelős biztos koordinációjával a Központ – a Nemzeti Kiberbiztonsági Munkacsoport javaslatai alapján – készíti el.
(2) A nemzeti kiberválságkezelési tervet az Ország Összehangolt Védelmi Tervében foglaltakra figyelemmel, azzal összhangban kell elkészíteni.
(3) A nemzeti kiberválságkezelési terv legalább az alábbiakat határozza meg:
a) a nemzeti felkészültségi intézkedések és tevékenységek célkitűzései,
b) a kiberbiztonsági válsághelyzetek kezelésével foglalkozó hatóságok feladatai és felelősségei,
c) a kiberbiztonsági válsághelyzetek kezelésére szolgáló eljárások, beleértve azok integrálását az általános nemzeti válságkezelési keretbe és az információcserére szolgáló csatornákba,
d) nemzeti felkészültségi intézkedések, beleértve a gyakorlatokat és a képzési tevékenységeket,
e) az érintett állami és magán érdekelt felek, valamint az érintett infrastruktúra azonosítása,
f) nemzeti eljárások és megállapodások az érintett nemzeti hatóságok és szervek között.
(4) A nemzeti kiberválságkezelési terv elfogadását követő három hónapon belül be kell nyújtani az Európai Bizottság és az EU-CyCLONE részére a (3) bekezdésben foglalt releváns információkat, amelyben nem szerepeltethetők a nemzetbiztonsági szempontból érzékeny információk, valamint amelyek közlése ellentétes lenne Magyarország nemzetbiztonsági, honvédelmi, közbiztonsági vagy alapvető érdekeivel vagy azokat sértené.
(5) A (4) bekezdés szerinti információkat a védelmi és biztonsági igazgatás központi szerve küldi meg az Európai Bizottság és az EU-CyCLONE részére a Védelmi Tanács véleményének kikérését követően."

[28] A Kiberbiztr. 92. § (2) bekezdés e) pontja a Nemzeti Kiberbiztonsági Munkacsoport tagjaként nevesíti a védelmi és biztonsági igazgatás központi szervének vezetője által delegált vezető beosztású személyt. A Kritkr. 36. § (6) bekezdés b) pontja – ezzel szemben – meghívott tagi státust biztosít az Ellenálló Képesség Fejlesztési Munkacsoportban a Védelmi Igazgatási Hivatal főigazgatójának vagy kijelölt képviselőjének.

[29] Kiberbiztr. „109. § (1) Az Operatív Törzs a kiberbiztonsági válsághelyzetekre történő felkészülés érdekében
a) ágazati vagy központi kiberbiztonsági válságkezelési gyakorlat, (…)
b) (…)
megszervezését kezdeményezheti.
(2) Az (1) bekezdés a) pontja szerinti gyakorlatot az Operatív Törzs

szükséges körű bevonása mellett, központi gyakorlattá minősítés esetében ugyanakkor a Hivatal átveszi az irányítói szerepet, a 110. § esetében[30] ugyanakkor felkészülési és válságkezelési szempontból egyaránt a nemzeti eseménykezelő központ szintjén nevesített az együttműködés a különböző típusú szolgáltatókkal.

Összességében a szervezet egésze / vezető / képviselő / szervezeti egység felelősségi és együttműködési körei vonatkozásában a Kiberbiztr. az áttekinthetőség szempontjából kihívásokat hordozó módon komplex szabályokat tartalmaz.

2.2 A védelmi és biztonsági esemény fogalmi kiterjesztése és a válságkezelési eljárásrend további kapcsolódási pontjai

A védelmi és biztonsági esemény fogalma – a súlyos vagy elhúzódó minősége esetén – a Vbö. 74. § (1) bekezdése alapján a béke idejű válságkezelés eszköztárát aktiváló kormányzati döntés, az összehangolt védelmi tevékenység kormányrendeleti kihirdetéséhez kapcsolódik, annak oka lehet. A Vbö. fogalommeghatározásokat tartalmazó 5. §-ának 15. pontja eredendően is egy viszonylag hosszú felsorolást tartalmazott a védelmi és biztonsági események vonatkozásában,[31] amely a Kszetv-vel összefüggésben nem is tett szükségessé kiegészítést, azonban a Kiberbiztv. következtében új i) ponttal bővült:

> „15. *védelmi és biztonsági esemény:*
> *a)* törvényben meghatározott ágazati üzemzavar, válsághelyzet vagy különleges jogrendnek nem minősülő veszélyhelyzet, illetve a lakosság ellátását, annak biztonságát vagy folytonosságát érintő súlyos esemény,
> *b)* katasztrófa vagy annak veszélye,
> *c)* az államhatár rendjét és annak megóvását érintő súlyos esemény,
> *d)* a törvényes rendet, a közrendet és közbiztonságot súlyosan fenyegető esemény,
> *e)* az államműködés folytonosságát sértő vagy veszélyeztető súlyos esemény,
> *f)* Magyarországot jelentősen érintő katonai fenyegetés,
> *g)* szövetségesi kötelezettség teljesítésére okot adó esemény, vagy

a) a nemzeti kiberbiztonsági hatósággal, a védelmi és biztonsági igazgatás központi szervével és a hivatásos katasztrófavédelmi szerv központi szervével, valamint az érintett ágazatot képviselő szervezettel együttműködve, indokolt esetben a Katonai Nemzetbiztonsági Szolgálat, valamint a Magyar Honvédség bevonásával szervezi,
b) a kritikus infrastruktúrákat üzemeltető, valamint az ország védelme és biztonsága szempontjából jelentős szervezetek szükség szerinti bevonásával bonyolítja le, valamint
c) központi gyakorlattá történő minősítés esetén a védelmi és biztonsági igazgatás központi szervének irányításával bonyolítja le." (Kivonatos közlés.)

[30] Kiberbiztr. „110. § A kiberbiztonsági válsághelyzetekre történő felkészülés, valamint a kiberbiztonsági válsághelyzetek kezelése érdekében – a jogszabályban meghatározott kiberbiztonsági feladatokra figyelemmel – az elektronikus hírközlési szolgáltató, a közvetítő szolgáltató, a központi rendszer felett rendelkezési jogot gyakorló szervezet, valamint a központi szolgáltató együttműködik a nemzeti eseménykezelő központtal, a Központtal és az Operatív Törzzsel."

[31] „Ez az értelmezés felöleli az árvíztől a háborús helyzetig az összes olyan rendkívüli helyzetet, amely széleskörű összefogást igényel a válság megelőzése, vagy annak bekövetkezése annak kezelése érdekében." Lakatos 2023. im. 11.

h) terrortámadás bekövetkezése, illetve annak jelentős veszélye,
i)[32] a kiberbiztonsági válsághelyzet;"

A beépített új elemmel a felsorolás eredeti elemeit összevetve megállapítható, hogy a kibertérből eredő kihívás – a külön törvény következtében determinált elemeitől eltekintve – a cél, érvényesülési terület és módszer szerinti differenciált elemekből álló felsorolás eltérő megközelítésű pontjaiban eredendően is értékelést nyerhet, például terrorkihívás, vagy megvalósult súlyos államműködési folytonosságot érintő esemény mozzanataként.

A Kiberbiztv. 73. § (4) bekezdése az ágazati válságkezelés sajátos szabályaként a kiberbiztonságért felelős biztos által irányított Operatív Törzs – Védelmi Igazgatási Hivatal együttműködéséhez kötött – minősítési jogkörébe utalja a jelentős vagy nagyszabású kiberbiztonsági incidens miatt bekövetkezett védelmi és biztonsági esemény kezelésére vonatkozó kezdeményezés kialakítását, ennek során az ágazati válságkezelési és veszélyhelyzet-kezelési intézkedések megtételét. E megoldás párhuzamba állítható a Vbö. 75. §-a szerinti összehangolt védelmi tevékenységgel összefüggő döntés-előkészítési koordinációs szereppel azzal az eltéréssel, hogy a védelmi és biztonsági igazgatás központi szervének szerepe az összehangolt védelmi tevékenység elrendelésére irányuló, 74. § szerinti kormánydöntés esetében nem kiemelt, bár az 52. § d) pontjában a felkészítésre irányuló szerep nevesítésre kerül. A döntés-előkészítői szerep mindamellett a Kiberbiztv. esetében egyértelműbben hangsúlyozott, de a fő felelősségi szintet el nem érő.

A Kiberbiztv. 74. §-a egészíti ki a Vbö. összehangolt védelmi tevékenységre vonatkozó szabályait a 76. § (1) bekezdés i) pontja szerinti kiutaláshoz kapcsolódva a kiberbiztonsági válsághelyzet-kezeléséhez kapcsolódó sajátos eljárásrenddel és a kiberbiztonsági válságkezelés specifikus intézkedési lehetőségeivel. A Kiberbiztv. 74. § (1) bekezdése szerint jelentős vagy nagyszabású kiberbiztonsági incidens esetén sem automatikus a kiberbiztonsági válsághelyzetté történő minősítés, és a (2) bekezdés alapján a kiberbiztonsági válsághelyzet – védelmi és biztonsági esemény minősége ellenére – sem feltétlenül eredményez összehangolt védelmi tevékenységet, az a Kormány további döntésének függvénye. A (3) bekezdés ugyanakkor – a *19/2023. (VIII. 7.) AB határozat* követelményeivel összevetve vitatható módon – a végrehajtási kormányrendeleti szabályoktól is függővé teszi a kapcsolódó Vbö. szabályok alkalmazhatóságát.[33] Már az első, kiberbiztonsági válsághelyzetté minősítő döntés esetén (értelemszerűen a specifikus

[32] Beiktatta: 2024. évi LXIX. törvény 124. §. Hatályos: 2025. I. 1-től.

[33] Kiberbiztv. „**74. §** (1) Jelentős vagy nagyszabású kiberbiztonsági incidens esetén a nemzeti kiberbiztonsági incidenskezelő központ kezdeményezése alapján a Nemzeti Kiberbiztonsági Munkacsoport Operatív Törzse javaslatot tehet a kiberbiztonsági incidens kiberbiztonsági válsághelyzetté történő minősítésére.
(2) A kiberbiztonsági válsághelyzet olyan védelmi és biztonsági esemény, amely esetén a Kormány az informatikáért felelős miniszter előterjesztése alapján összehangolt védelmi tevékenységet rendelhet el.
(3) Kiberbiztonsági válsághelyzet esetén - ha e törvény vagy a végrehajtására kiadott kormányrendelet eltérően nem rendelkezik - a Vbö. rendelkezéseit kell alkalmazni."

összehangolt védelmi tevékenységre is kiterjedő módon) ugyanakkor megnyílik az alkalmazható kormányzati intézkedések katalógusa:

„(4) Kiberbiztonsági válsághelyzet és az az alapján elrendelt összehangolt védelmi tevékenység esetén a Kormány intézkedésként bevezetheti

1. a kiberbiztonsági válsághelyzet-kezelésben érintett szerv vagy szervezet készenlétének fokozását, prevenciós tevékenységét;

2. az 1. pont szerinti szervek vagy szervezetek műveleti vagy élőerős védelmét, valamint annak fokozását;

3. a honvédelmi szervezetek, a rendvédelmi szervek és a nemzetbiztonsági szolgálatok felderítő, elhárító, valamint kibertér műveleti erői tevékenységének fokozását a fenyegetettség Magyarországra történő átterjedésének, illetve a támadás elhárításának, valamint következményeinek megakadályozása érdekében;

4. a 3. pont szerinti szervek vagy szervezetek összehangolt védelmi tevékenység keretében végzett összehangolt vagy együttes fellépését;

5. a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához nélkülözhetetlen szolgáltatás, valamint az azt egyedül biztosító alapvető vagy fontos szervezetként még be nem azonosított szolgáltató haladéktalan azonosításának elrendelését;

6. elektronikus hírközlési szolgáltatások szüneteltetését, korlátozását és ellenőrzését, azokhoz való hozzáférés lehetetlenné tételét, továbbá az elektronikus informatikai hálózatok és eszközök, valamint az elektronikus hírközlő berendezések térítésmentes igénybevételét, használatra való átengedését, használatának mellőzését, valamint hozzáférhetetlenné tételét;

7. a kiberbiztonsági válsághelyzet-kezeléséhez szükséges szolgáltató működési helyiségeinek, technikai eszközparkjának, elektronikus információs rendszerének és létesítményeinek térítésmentes igénybevételét, használatra való átengedését;

8. az állami, valamint a kiberbiztonsági válsághelyzet-kezelésben érintett szerv vagy szervezet információs és kommunikációs rendszerei folyamatos üzemeltetésének biztosítása érdekében a javítókapacitások és alkatrészkészletek térítésmentes igénybevételét, vagy használatuk korlátozását, valamint a javítókapacitásokkal rendelkező társaságok tulajdonosait és munkavállalóit terhelő javítási, üzemeltetési szolgáltatások teljesítését;

9. a kiberbiztonság szavatolása szempontjából fontos termékek, eszközök készletezését, tartalékolását;

10. az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (a továbbiakban: EU-CyCLONE), valamint az Európai Bizottság és az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) kötelező tájékoztatását és dönt annak tartalmáról,

11. a kötelező hivatalos kormányzati tájékoztatás nyújtását az érintettek részére, valamint

12. az Európai Unió tagállamainak, valamint az Észak-atlanti Szerződés Szervezetén belüli szövetséges országok tájékoztatását a kiberbiztonsági válsághelyzet kapcsán a Kormány által megtett intézkedésekről a diplomáciai csatornák igénybevételével."[34]

Míg a Kiberbiztv. 74. § (4) bekezdésének felsorolása szerkezetében és intézményvédelmi elemeiben jelentős mértékben emlékeztet a honvédelmi válsághelyzet Hvt. 107. § (4) bekezdése szerinti, összehangolt védelmi tevékenységet kiterjesztő felsorolására,[35] a 4. pont kiutalása az összehangolt védelmi tevékenységre csak a második kihirdetési opció esetében megalapozott, az 5. pont szerinti intézkedés viszont – a soron kívüli kritikus, vagy jelentős szervezeti kijelölés vonatkozásában – a Vbö. és a Kszetv. elsődleges szabályozási feladatának átvétele mellett is támogatható. A külső kommunikációra irányuló 10-12. pontok esetében az adatvédelem és a minősített adatok védelmének uniós és nemzeti kötelezettsége egyaránt megerősített az (5) bekezdés szerinti kiemelésben, a (6) bekezdés szerint kiterjesztett adatszolgáltatási körre is kiterjedő módon, amely viszont – a nemzetbiztonsági információk (8) bekezdés szerint külön döntésre utalt, elkülönített kezelése kivételével – a nemzeti eseménykezelő központ részére is átadásra kerülnek a (7) bekezdés szerint.

Összességében a Kiberbiztv. 74. §-ra fókuszált kiberbiztonsági eseménykezelés során a hatékony válságkezelés és a titokvédelem érdekei közötti mérlegelést megjelenítő dilemmák szabályozhatóságának eltérő hangsúlyai jelennek meg hazai és uniós szegmensben egyaránt. Ennek során a nemzetbiztonsági érdek érvényesítése a Vbö. eljárásrendjéhez képest is hangsúlyosabb.

2.3 A stratégiai tervdokumentumokhoz való illeszkedés

A stratégiai tervdokumentumok kapcsolódásait meghatározó szabályozás súlypontja a Vbö., a két 2024-ben elfogadott törvény végső soron e törvény rendszerét egészítette ki további kapcsolódó

[34] Kiberbiztv. **74. §** (4) bekezdés.

[35] Hvt. „**107. §** (4) Honvédelmi válsághelyzetben a Vbö.-ben meghatározottak szerint – a Vbö.-ben meghatározott intézkedéseken túl – a Kormány intézkedésként bevezetheti
a) a honvédelmi szervezet készenlétének fokozását,
b) a KNBSZ és a Honvédség felderítő, elhárító, valamint kibertér műveleti erői tevékenységének fokozását a fenyegetettség Magyarországra történő átterjedésének, illetve magyarországi felerősödésének megakadályozása érdekében,
c) hivatalos állásfoglalások kötelező kiadását a közszolgálati műsorszórók részére,
d) a honvédelem szempontjából fontos termékek, energiahordozók, fogyasztási cikkek készletezését,
e) a közigazgatás, a honvédelmi igazgatás, a Honvédség, a honvédelemben közreműködő szervek működése szempontjából fontos beosztások, munkakörök – egyszerűsített eljárásban történő – feltöltését, túlmunka végzését,
f) a rádióspektrum használatra vonatkozó korlátozó szabályok bevezetését, speciális üzemmódok előkészítését,
g) a magyar légtérben és a repülőtereken a katonai légiforgalmi irányítás szükséges mértékű bevezetését,
h) az állampolgárokat is érintő riasztási fokozatok alkalmazását,
i) a súlyos, erőszakos cselekmények megelőzése vagy elhárítása érdekében a Honvédség és a rendőrség felkészített erőinek összehangolt fellépését egyes közintézmények és közforgalmú helyek megközelíthetőségének korlátozásával vagy kizárásával."

elemekkel. Míg a védelmi és biztonsági tervezés dokumentum-rend eredeti változatától függetlenül került nevesítésre *a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény* (a továbbiakban: Hvt.) 8. § (3) bekezdésében honvédelmi miniszteri előkészítési felelősségbe utalt két stratégiai dokumentum, [36] a Nemzeti Katonai Stratégia (NKS), valamint az ország fegyveres védelmi terve (OFVT), az utóbbi esetben a 10. § (2) bekezdése szerint a miniszterelnöki jóváhagyási jogkör kiemelésével, a kiegészítő szabályozások illeszkedési felülete kidolgozottabb.

A Vbö. 4. §-a szerinti alapelvek d) pontja a védelem és biztonság fenntartására és fejlesztésére irányuló feladatrendszer kiinduló pontjaként rögzíti a tervezést, „a kihívások és fenyegetések legszélesebb körére kiterjedő, átfogó tudományos ismereteket figyelembe vevő megközelítés", valamint az ágazati tapasztalatok összehangolásából kiindulva. A tervezési mozzanat a védelmi és biztonsági igazgatás, a szövetségi kötelezettségek, valamint a gazdaságfelkészítés fogalmi meghatározásainak egyaránt lényegi eleme,[37] illetve a Kormány által irányított védelmi és biztonsági célú tervezési rendszer általános leírását a Vbö. 20-22. § tartalmazza, meghatározva egyaránt az előkészítési és végrehajtási felelősségi köröket, valamint az ágazati tervezési kötelezettségeket általános szinten az összkormányzati feladatok rendszeréhez illesztve.[38]

A Vbö. 22. § (1) bekezdése szerinti kiemelt felsorolás tételes elvárásként tartalmazza Országgyűlési jogkörben a Biztonság- és Védelempolitika Alapelveit, valamint a Kormány publikus és minősített dokumentumaként a Nemzeti Biztonsági Stratégiát (NBS) és az Integrált Védelmi és Biztonsági Iránymutatást (IVBI), illetve a d) pontban kiutal törvényi vagy kormányrendeleti szabályozási lehetőségre további stratégiai dokumentumok előírása érdekében. Míg a d) pont végső soron a Hvt.-alapú stratégiai dokumentumokat is a Vbö. rendszeréhez kapcsolja, *a védelmi és biztonsági célú tervezés szabályairól szóló 400/2022. (X. 21.) Korm. rendelet* hivatott elsődlegesen a dokumentum-rendszer részletesebb kifejtésére, ennek körében az Ország Összehangolt Védelmi Terve (OÖVT) is itt jelenik meg. Kapcsolódó, de önálló alrendszerkét elkülönülő tervezési dokumentum-család a nemzetgazdaság védelmi és biztonsági célú felkészítésének és mozgósításának sajátos tervezési feladatrendszere, amely a Védelemgazdasági Alaptervre fókuszáltan a Vbö. 25. §-a alapján *a nemzetgazdaság védelmi és biztonsági felkészítésének, mozgósításának, valamint a tartalékolás végrehajtásának szabályozásáról* szóló *79/2023. (III. 13.) Korm. rendelet* szabályoz részletesen. A Kormány védelmi és biztonsági tervezéssel összefüggő feladatköreit a Vbö. 46. §-a foglalja össze, [39] amelyhez a 47. § kapcsolja az

[36] Hvt. „**8. §** (3) A honvédelemért felelős miniszter a honvédelmi irányítási jogkörében felelős különösen (…)
b) a Nemzeti Katonai Stratégia előkészítéséért,
c) az ország fegyveres védelmi tervének jóváhagyásra felterjesztéséért, …". (Kivonatos közlés)
[37] Lásd Vbö. 5. § 2. 10. és 16. pont.
[38] Lásd Vbö. „20. § (3) A védelmi és biztonsági tervezési rendszerben központilag meghatározott szempontrendszer szerint, ágazatilag elkülönülten, de kormányzati szinten összehangolt módon, a költségvetési források tervezésére is kiterjedő stratégiai és végrehajtási szintű tervdokumentumok kerülnek kialakításra."
[39] Vbö. „**46. §** (1) A Kormány a védelmi és biztonsági feladatok összehangolt irányítása és ezzel összefüggésben a Kormány irányítása alá nem tartozó szervekkel való együttműködés biztosítása érdekében

ágazati tervezési és végrehajtási feladatokat,[40] a védelmi és biztonsági igazgatás központi szervének a Vbö. 52. § b) pontja szerinti tervezési koordinációs feladatköréhez illeszkedve.

A Kszetv. szerinti kritikus szervezetekkel és áttételesen a Vbö. szerinti jelentős szervezetek vonatkozásában már korábban utaltunk arra, hogy két stratégiai dokumentum, *a Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti kockázatértékeléséről szóló 1191/2025. (VI. 5.) Korm. határozat, valamint a Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti stratégiájáról szóló 1192/2025. (VI. 5.) Korm. határozat*[41] *a Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV.21.) Korm. határozat, valamint a Magyarország Nemzeti Katonai Stratégiájáról szóló 1393/2021. (VI. 24.) Korm. határozat* újraalkotását megelőzően hatályba lépett, hasonlóan a *Magyarország Kiberbiztonsági Stratégiájáról szóló 1089/2025. (III. 31.) Korm. határozathoz.* Az illeszkedő ágazati stratégiák így frissebbek, mint az NBS és az NKS, amelyek a COVID-válságkezelés tapasztalatait tartalmazó, de az orosz-ukrán háborút megelőző időállapot szerint rögzültek, így a Kszetv. 4. § (1) bekezdés szerinti NBS-hez igazodás követelménye a frissebb dokumentum esetében eleve csak korlátozottan, a teljességre törekvés nélkül érvényesülhetett.

A Kszetv. szempontjából egyébként meghatározó jelentőségű a kockázat-alapú gondolkodás és kockázatkezelés az ellenálló képességi terv köré épített veszély-elhárítási tervezés során,[42] végső

---

a) az Országgyűlés elé terjeszti a Biztonság- és Védelempolitika Alapelveiről szóló határozati javaslatot és irányítja a védelmi és biztonsági célú tervezés további dokumentumainak kidolgozását, (…)
k) tervezi és meghatározza a védelmi és biztonsági célú felkészítés és feladatellátás kormányzati összehangolásának költségeit, ezen belül elkülönítve a kormányzás folytonosságát biztosító infrastrukturális és infokommunikációs beruházások költségeit,
(2) A Kormány a védelmi és biztonsági célú felkészítés és feladatellátás összehangolásának
a) tervezési és igazgatási feladatait a védelmi és biztonsági igazgatás központi szerve,
b) kormányzati döntéshozatali és szervezetvezetői egyeztetési feladatait az e célra kialakított döntés-előkészítési és döntéshozatali rendszer
útján látja el." (Kivonatos közlés.)

[40] Vbö. „**47. §** (1) A miniszter az általa irányított ágazat vonatkozásában jogszabály rendelkezésének megfelelően és a Kormány által a védelmi és biztonsági célú felkészülés és feladatellátás összehangolása keretében meghatározottak szerint irányítja az irányítása vagy felügyelete alá tartozó szervek és a feladatkörébe tartozó szakágazatok védelmi és biztonsági célú felkészítéssel és feladatellátással kapcsolatos tevékenységét.
(2) A miniszter az (1) bekezdésben foglaltak érdekében *(…)*
c) gondoskodik a védelmi és biztonsági célú tervezés magasabb szintű dokumentumai által meghatározott keretek között az ágazati dokumentumok kidolgozásáról, illetve a több ágazatot érintő tervezési feladatok tekintetében a szakágazati együttműködésről,
d) biztosítja a védelmi és biztonsági célú tervezéshez szükséges szakágazati információkat a védelmi és biztonsági igazgatás központi szerve számára, *(…)*
f) a hatáskörébe tartozó költségvetés keretében elkülönítetten tervezi a védelmi és biztonsági feladatok végrehajtásának költségeit." (Kivonatos közlés.)

[41] Vö. Till 2025. im. 19-20.

[42] Kszetv „**3. §** E törvény alkalmazásában (…)
11. *ellenálló képességi terv:* 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

soron a rendkívüli események megelőzése érdekében. Utóbbi fogalom tartalmi szempontból egyező, de megfogalmazási szempontból helyesebb változatát *a belügyi feladatellátás hatékonyságát támogató és a kapcsolati erőszak elleni küzdelmet erősítő törvények módosításáról szóló 2025. évi XXXV. törvény* 87. §-a állapította meg 2025. július 1-i hatályba lépéssel,[43] tehát már a Kszetv.-n alapuló nemzeti kockázatértékelés és stratégia megjelenését követően. A nemzeti kockázatértékelésre vonatkozó 5. § szerinti elvárások nevesítik egyrészt az Európai Uniós szabályzásból átszűrődő elemekhez, valamint a Vbö.-n alapuló tervezés rendszeréhez igazodás együttes követelményét, a szervezeti szintű[44] kockázat-kezelési tervek kialakításának kereteit meghatározva.[45]

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, (…)

21. *kockázat alapú gondolkodás:* a kockázatmenedzsment működtetése során egyfajta szemlélet alkalmazása, amelyben a kockázatok azonosításának, a kockázatelemzésnek, a kockázatértékelésnek és a kockázatkezelésnek olyan általános folyamata valósul meg, amely célja, hogy megalapozott döntést hozzanak arról, hogyan kezeljék a lehető legmagasabb szinten a felmerülő kockázatokat, mindezt hitelesen dokumentált információ, azaz az ellenálló képességi terv és ellenálló képességi mátrix formájában, (…)

25. *kockázatkezelés:* kockázatmenedzsment által alkalmazott, jóváhagyott döntésen alapuló tervezett folyamat, módszer vagy eszköz, amely egy várható negatív esemény bekövetkezésének valószínűségét, a felmerülő kockázatok hatásait és a kitettséget olyan módon befolyásolja, hogy általa csökkenjen a kockázatpotenciál, valamint a lehetséges kár hatásait enyhítse, ellensúlyozza," (Kivonatos közlés.)

[43] Kszetv. „**3. §** E törvény alkalmazásában (,,,)

32. *rendkívüli esemény:* olyan esemény, amely eléri a rendkívüli esemény kezelésében érintett szervek irányába történő bejelentés kormányrendeletben vagy annak hiányában a kritikus szervezet ellenálló képességi tervében meghatározott küszöbértékét, és

a) a kritikus infrastruktúra vagy az alapvető szolgáltatás olyan mértékű károsodását, sérülését, minőségének romlását vagy mennyiségének fennakadását okozza, amely a kritikus infrastruktúra vagy az alapvető szolgáltatás megszűnését, kiesését eredményezi, vagy

b) a kritikus infrastruktúra vagy az alapvető szolgáltatás megszűnését, kiesését nem eredményezi, de a kritikus infrastruktúra vagy az alapvető szolgáltatás megszűnésének, kiesésének elhárításához szükségessé vált a rendkívüli esemény kezelésében érintett más szervek közreműködése."

[44] A Magyar Nemzeti Bank vonatkozásában 2026. január 1-i hatályba lépéssel eltérő szabályokat iktatott a Kszetv.-be és jelentős részben deregulált *a rendészeti feladatellátás hatékonyságát támogató törvények módosításáról szóló 2025. évi LXXI. törvény.*

[45] Kszetv. „**5. §** (1) A kritikus szervezetek ellenálló képességére vonatkozó nemzeti kockázatértékelés (a továbbiakban: nemzeti kockázatértékelés) a Kormány által határozattal elfogadott tervezési dokumentum, amelyet a kritikus szervezetek és kritikus infrastruktúrák ellenálló képességének támogatása érdekében

a) az 1. melléklet szerinti ágazatokra,

b) Magyarország nemzeti katasztrófakockázat-értékelésére,

c) az általános és ágazatspecifikus kockázatokra, és az azokra kidolgozott ágazati védekezési tervekre,

***d)* az uniós jogi normák alapján készített, így különösen a terrorizmus elleni küzdelemről, a földgázellátás biztonságának megőrzését szolgáló intézkedésekről, a villamosenergia-ágazati kockázatokra való felkészülésről, az árvízkockázatok értékeléséről és a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről szóló szabályozások alapján készített ágazati kockázatelemzésekre vagy-értékelésekre,**

***e)* a védelmi és biztonsági tevékenységek összehangolásáról szóló törvény szerinti védelmi és biztonsági célú tervezéshez kapcsolódó feladatokra, és**

A Kiberbiztv. esetében a két tervezés szempontjából meghatározó jelentőségű fogalom *a digitális államhoz kapcsolódó egyes törvények módosításáról szóló 2025. évi XXXII. törvény* által pontosított uniós kapcsolódást biztosító nemzeti válságkezelési terv[46] és a sérülékenységek megszüntetésére hivatott sérülékenységkezelési terv. A korábban hivatkozott, az Európai Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló irányelvhez csatlakozó nemzeti kiberbiztonsági stratégia, valamint a nemzeti válságkezelési terv összeállítása és koordinációja a Kiberbiztv. 72. § (2) bekezdés szerint az informatikáért felelős miniszter által kijelölt kiberbiztonságért felelős biztos feladatköre a Nemzeti Kiberbiztonsági Munkacsoportot vezetése mellett.

A Kiberbiztr. 107. § (2) további kapcsolódást eredményez a nemzeti kiberválságkezelési terv és az OÖVT, az Ország Összehangolt Védelmi Terve szempontjából, mivel az törvényi szinten nem nevesített tárgykör, mivel az csak a stratégia-alkotás megengedett kormányzati szegmenseként kormányrendeleti szinten, *a védelmi és biztonsági célú tervezés szabályairól szóló 400/2022. (X. 21.) Korm. rendelet* 1. § 7. pontjában „a Magyarországot fenyegető védelmi és biztonsági kihívással összefüggésben szükséges koordinált védelmi tevékenységet, eljárást és együttműködési feladatot meghatározó minősített tervdokumentum" -ként, a 16. §-ban rögzített feltételekkel és tartalommal került bevezetésre. Míg a Kiberbiztr. 108. § (1) bekezdése egyértelműen beazonosítja az intézményi szintű kiberbiztonsági terveket a Kiberbiztv. 74. § (10) bekezdése szerinti tartalmi követelményekkel, a Kiberbiztv. 72. § (2) bekezdés szerinti nemzeti válságkezelési terv és a Kiberbiztr. 107. § szerinti nemzeti kiberválságkezelési terv azonossága vagy kapcsolata a normaszövegek összevetése alapján nem dönthető el. Tartalmi követelmény minden esetre csak az utóbbihoz adott a Kiberbiztr. 107. § (3) bekezdése alapján. E kérdéskör ugyanakkor a Kiberbiztr. 107. § (5) bekezdése alapján a Védelmi Igazgatási Hivatal feladatkörét közvetlenül érinti uniós együttműködési vonatozásban.[47]

---

f) a rendkívüli események jelentésére és kezelésére vonatkozó információkra figyelemmel kell elkészíteni.
(2) A nemzeti kockázatértékelés figyelembevételével alakítja ki a kritikus szervezet
a) a kockázatértékelését, az ellenálló képességi mátrixot és
b) az ellenálló képességi intézkedéseit.
(3) Az egyedüli kapcsolattartó pont a 4 évente felülvizsgált nemzeti kockázatértékelés releváns információit az elfogadását követő három hónapon belül az Európai Bizottság rendelkezésére bocsátja." (Kiemelés hozzáadva.)

[46] Kiberbiztv. „**4. §** E törvény alkalmazásában (…)
80. *nemzeti válságkezelési terv:* az (EU) 2022/2555 európai parlamenti és tanácsi irányelv alapján a nagyszabású kiberbiztonsági incidensek és válságok elhárítására szolgáló nemzeti terv, amely meghatározza a nagyszabású kiberbiztonsági incidensek és válságok kezelésének célkitűzéseit és szabályait;" (Kivonatos közlés.)

[47] Kiberbiztr. „**107. §** (1) Magyarország nemzeti kiberválságkezelési tervét (a továbbiakban: nemzeti kiberválságkezelési terv) a kiberbiztonságért felelős biztos koordinációjával a Központ – a Nemzeti Kiberbiztonsági Munkacsoport javaslatai alapján – készíti el.
(2) **A nemzeti kiberválságkezelési tervet az Ország Összehangolt Védelmi Tervében foglaltakra figyelemmel, azzal összhangban kell elkészíteni.**
(3) A nemzeti kiberválságkezelési terv legalább az alábbiakat határozza meg:
a) a nemzeti felkészültségi intézkedések és tevékenységek célkitűzései,
b) a kiberbiztonsági válsághelyzetek kezelésével foglalkozó hatóságok feladatai és felelősségei,

3. Összegzés

A jelen tanulmány arra vállalkozott, hogy a Vbö. és a 2025. január 1-jén hatályba lépett, kritikus szervezetek ellenálló képességét, valamint a kiberbiztonságot érintő törvényi és kormányrendeleti szabályozások alapján beazonosítsa, hogy a két, védelmi és biztonsági szabályozási kontextusba tartozó tárgykörrel összefüggésben a Védelmi Igazgatási Hivatal feladatköreit értékelje.

Bár a vizsgált törvények és kormányrendeletek tartalma – tipikusan salátatörvények, ágazati módosító csomagok elemeiként – folyamatosan változik, a szabályozási rendszer koherenciájának erősítésére hivatott felülvizsgálat a hatályosulás első évében nem valósult meg. Elsődlegesen a jogharmonizációs kötelezettség időbeliségi kényszerére, és a felülvizsgálat hiányára is visszavezethető okokból kimutathatóak a hatályos szabályozásban a törvények között és egy-egy szabályozási tárgykör törvényi és kormányrendeleti elemei között is illeszkedési hiátusok, amelyek finomhangolása javasolt. Ennek során rendszerszintű átgondolást a szervezetek közötti kapcsolódási utak egységesítése, valamint az adatkezelési feltételrendszer pontosítása igényelne, amelyek tipikusan a nemzeti eseménykezelő képesség kialakításához kapcsolódnak. Utóbbi tárgykör felülvizsgálata ugyanakkor a Vbö. szabályozási rendszerén belül is újratervezést tenne szükségessé.

c) a kiberbiztonsági válsághelyzetek kezelésére szolgáló eljárások, beleértve azok integrálását az általános nemzeti válságkezelési keretbe és az információcserére szolgáló csatornákba,
d) nemzeti felkészültségi intézkedések, beleértve a gyakorlatokat és a képzési tevékenységeket,
e) az érintett állami és magán érdekelt felek, valamint az érintett infrastruktúra azonosítása,
f) nemzeti eljárások és megállapodások az érintett nemzeti hatóságok és szervek között.
(4) A nemzeti kiberválságkezelési terv elfogadását követő három hónapon belül be kell nyújtani az Európai Bizottság és az EU-CyCLONE részére a (3) bekezdésben foglalt releváns információkat, amelyben nem szerepeltethetők a nemzetbiztonsági szempontból érzékeny információk, valamint amelyek közlése ellentétes lenne Magyarország nemzetbiztonsági, honvédelmi, közbiztonsági vagy alapvető érdekeivel vagy azokat sértené.
(5) **A (4) bekezdés szerinti információkat a védelmi és biztonsági igazgatás központi szerve küldi meg az Európai Bizottság és az EU-CyCLONE részére a Védelmi Tanács véleményének kikérését követően**." (Kiemelés hozzáadva.)

Felhasznált irodalom:

- Baranyi-Müller Tamás (szerk.): Kiberbiztonság az Európai Unióban és Magyarországon; *Infojegyzet* 2024/28. Országgyűlés Hivatala 2024. október 31. https://www.parlament.hu/documents/d/guest/infojegyzet_2024_28_kiberbiztonsag
- Kádár Pál (szerk.): *A védelmi és biztonsági szabályozás magyarországi reformja*; Nemzeti Közszolgálati Egyetem Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely 2025. https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/A%20V%C3%89DELMI%20%C3%89S%20BIZTONS%C3%81GI%20SZAB%C3%81LYOZ%C3%81S%20MAGYARORSZ%C3%81GI%20REFORMJA%202025.pdf
- Lakatos Tibor: Az integrált rendészeti törzsek szerepe a veszélyhelyzetek kezelésében; *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok* 2023/9. https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK%20MT_2023_9_LAKATOS%20Tibor_Az%20integr%C3%A1lt%20rend%C3%A9szeti%20t%C3%B6rzsek%20szerepe%20a%20vesz%C3%A9lyhelyzetek%20kezel%C3%A9s%C3%A9ben.pdf
- Till Szabolcs Péter: Az ország védelme és biztonsága szempontjából jelentős szervezetek és infrastruktúrák szabályozása (Hogyan változtatta meg a szatellit-fejezet *„jelentős" -sége* a Vbö. -t?) *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok* 2025/4. https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK_MT_2025_4_Till%20Szabolcs%20P%C3%A9ter_Az%20orsz%C3%A1g%20v%C3%A9delme%20%C3%A9s%20biztons%C3%A1ga%20szempontj%C3%A1b%C3%B3l%20jelent%C5%91s%20szervezetek%20%C3%A9s%20infrastrukt%C3%BAr%C3%A1k%20szab%C3%A1lyoz%C3%A1sa.pdf
- Tóth Melinda Dr. (szerk.): Létfontosságú rendszerek védelme; *Infojegyzet* 2024/25. Országgyűlés Hivatala 2024. október 31. https://www.parlament.hu/documents/d/guest/infojegyzet_2024_25_letfontossagu_rendszerek_vedelme

- *2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról* (Vbö.)
- *2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről* (Hvt.)
- *2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről* (Kszetv.)
- *2024. évi LXIX. törvény Magyarország kiberbiztonságról* (Kiberbiztv.)
- *2025. évi XXXII. törvény a digitális államhoz kapcsolódó egyes törvények módosításáról*
- *2025. évi XXXV. törvény a belügyi feladatellátás hatékonyságát támogató és a kapcsolati erőszak elleni küzdelmet erősítő törvények módosításáról*
- *2025. évi LXXI. törvény a rendészeti feladatellátás hatékonyságát támogató törvények módosításáról*

- *T/12793. számú törvényjavaslat az Európai Unió kiberrezilienciáról szóló rendeletének magyarországi végrehajtásáról és egyes kiberbiztonsági rendelkezések módosításáról;* https://www.parlament.hu/irom42/12793/12933.pdf

- *377/2022. (IX. 7.) Korm. rendelet a Védelmi Igazgatási Hivatalról*
- *400/2022. (X. 21.) Korm. rendelet a védelmi és biztonsági célú tervezés szabályairól*

- *79/2023. (III. 13.) Korm. rendelet a nemzetgazdaság védelmi és biztonsági felkészítésének, mozgósításának, valamint a tartalékolás végrehajtásának szabályozásáról*
- *418/2024. (XII. 23.) Korm. rendelet a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról* (Kiberbiztr.)
- *474/2024. (XII. 31.) Korm. rendeletet a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról* (Kritkr.)
- *475/2024. (XII. 31.) Korm. rendelet az ország védelme és biztonsága szempontjából jelentős szervezetek ellenálló képességéről*

- *1163/2020. (IV.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról* (NBS)
- *1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról* (NKS)
- *1089/2025. (III. 31.) Korm. határozatMagyarország Kiberbiztonsági Stratégiájáról*
- *1191/2025. (VI. 5.) Korm. határozat Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti kockázatértékeléséről*
- *1192/2025. (VI. 5.) Korm. határozat Magyarország kritikus szervezetek ellenálló képességére vonatkozó nemzeti stratégiájáról*

- *az Országgyűlés 2023. július 4-i ülésnapján elfogadott, az állami építési beruházások rendjéről szóló törvény 4. § (3) bekezdése, 16. § (1) bekezdésének „vagy a 4. § (3) bekezdése szerinti miniszteri rendelet" szövegrésze, valamint az 59. § (2) bekezdés a) pontja alaptörvény-ellenességének megállapításáról szóló 19/2023. (VIII. 7.) AB határozat* (a T/3677. számú törvényjavaslat tárgyában előterjesztett előzetes normakontroll / jogforrási hierarchia)