NEMZETI KÖZSZOLGÁLATI EGYETEM
VÉDELMI-BIZTONSÁGI SZABÁLYOZÁSI ÉS KORMÁNYZÁSTANI KUTATÓMŰHELY

VÉDELMI-BIZTONSÁGI SZABÁLYOZÁSI ÉS KORMÁNYZÁSTANI MŰHELYTANULMÁNYOK

2023/5.

BODÓ ATTILA PÁL

A kiberbiztonsági stratégia módosításának kérdései: kihívások és lehetséges válaszok egy változó világban

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 2023/5.

Szerző:
Dr. Bodó Attila Pál

Szerkesztő:
Dr. Kádár Pál PhD dandártábornok

Kiadja
Nemzeti Közszolgálati Egyetem
Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely

Kiadó képviselője
Dr. Kádár Pál PhD dandártábornok

A kézirat lezárva: 2023. június

ISSN 2786-2283

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

Bodó Attila Pál

A KIBERBIZTONSÁGI STRATÉGIA MÓDOSÍTÁSÁNAK KÉRDÉSEI: KIHÍVÁSOK ÉS LEHETSÉGES VÁLASZOK EGY VÁLTOZÓ VILÁGBAN

"A stratégia egy megértendő folyamat,

mintsem egy tanítandó diszciplína."

(John L. Thompson)

1. Bevezetés

Magyarország *Nemzeti Kiberbiztonsági Stratégiájának*[1] (a továbbiakban: Kiberstratégia) kihirdetése óta eltelt több mint tíz év, így módosításának – szükségszerűen újraírásának és hatályon kívül helyezésének – kérdése időszerű. Ez az időszerűség nem csak az idő múlásából ered, indokoltságot ad a teljes körű felülvizsgálatnak az is, hogy az elmúlt évek világméretű eseményeinek hatására – gazdasági válság, COVID járvány, orosz-ukrán háború – a társadalmi, gazdasági, politikai folyamatok átalakultak. Ezeknek a változásoknak, valamint a technológiai, infokommunikációs fejlődésnek a hatására megnövekedett az egyének, a szervezetek, az államok és a társadalmak biztonság iránti igénye. Ezen igény megjelenése mellett a stratégiai szintű változtatást indukálja az is, hogy fokozatosan nő a kibertérből eredő fenyegetettségek száma és komplexitása, amely veszélyek – kül- és belbiztonsági tevékenységek, gazdasági-, társadalmi-, állami működés megzavarására, megszakítására, illetve megakadályozására irányuló, és egyéb károkozó tevékenységek – egyre nagyobb biztonsági kockázattal járnak az államok és a társadalom tagjai, a gazdasági szereplők számára. Mindez újabb és újabb válaszokat követel az egyéni biztonsági intézkedések megtételétől kezdve a rendszerszintű, szervezeti védelmi intézkedések megszervezésén át, egészen az állami szabályozásig kiterjedően. Mindemellett az elmúlt tíz évben bekövetkezett stratégiai irányváltások és a jogi környezet változása is arra mutat rá, hogy a felmerült kihívásokra a válaszokat magas szintű, hosszú távú tervezéssel kell megtalálni.

Fentiek tükrében alapvetésként kell rögzíteni, hogy a Kiberstratégia felülvizsgálatát, újragondolását és újraírását záros határidőn belül el kell végezni. Jelen tanulmány célja, hogy rendszertani és jogi aspektusból világítson rá azokra a kérdésekre, amelyeket a felülvizsgálat során át kell tekinteni, keresve ezekre a lehetséges válaszokat. Nem célja a tanulmánynak azonban az egyes cselekvési pontok kibontása és a végrehajtás eszközeinek meghatározása.

2. Stratégiai alapvetés

A hatékony és tervezhető állami szerepvállalás és feladatellátás egyik alapvető eszköze, hogy az egyes szakterületeket érintően megfogalmazott célok és azok elérésének lehetséges módjai – figyelemmel a fennálló és meglévő képességekre – meghatározásra kerüljenek, azaz a stratégiai tervdokumentumok kidolgozása megtörténjen. Egy ilyen magas szintű és a szakpolitika jövőjét meghatározó dokumentum esetében alapkövetelményként kell rögzíteni, hogy honnan, hová és

[1] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III.21.) Korm. határozat (a továbbiakban: Kiberstratégia) - https://njt.hu/ (2023.05.15.)

milyen eszközökkel akarunk eljutni, amellett a kitűzött célokat hogyan akarjuk elérni, s mindezt milyen társadalmi, gazdasági, jogi környezetben kell megtenni.

A stratégiai tervezéshez kiindulási alapnak a még hatályos, a kormányzati stratégiai irányításról szóló 38/2012. (III. 12.) Korm. rendeletet (továbbiakban: R.) szükséges alapul venni, mely meghatározza azokat az egységes szempontokat és elveket, amelyek szerint sor kerül a kormányzati stratégiai dokumentumok kidolgozására, nyomon követésére, értékelésére és felülvizsgálatára. Az R. rendelkezései mellett figyelemmel kell lenni a védelmi és biztonsági tevékenységek összehangolásáról szóló törvény[2] (a továbbiakban: Vbö.) és a végrehajtási rendeleteként kiadott, a védelmi és biztonsági célú tervezés szabályairól szóló 400/2022. (X. 21.) Korm. rendelet (a továbbiakban: VböR.) előírásaira is. Ezen szabályzók kapcsolódó rendelkezéseit a 3. fejezetben tárgyaljuk.

A kiberbiztonság[3], mint szakterület jellegéből adódóan az R. szerinti tervdokumentációk közül a Kiberstratégiát a nemzeti középtávú stratégiákhoz[4] kell besorolni, ebből adódóan legalább négy, legfeljebb tíz éves időtávra kell, hogy vonatkozzon. A bevezetőben említettek szerint tehát a Kiberstartégia szavatossága 2023-ban lejár(t). Mint szakterületi dokumentumnak és részstratégiának a Kiberstratégiának igazodnia kellett az R. szerinti legmagasabb szintű biztonsági stratégiához, az akkor hatályos Magyarország Nemzeti Biztonsági Stratégiájához[5].

A Kiberstratégia a kihirdetése idején hatályos Nemzeti Biztonsági Stratégia[6] figyelembevételével került kidolgozásra, amely Magyarország oldaláról biztonsági kihívásként azonosította a kibertérben potenciális megjelenő vagy ténylegesen jelentkező fenyegetéseket. Elsődleges feladatnak a kockázatok rendszeres felmérését és priorizálását, a kormányzati koordináció erősítését, a társadalmi tudatosság fokozását, valamint a nemzetközi együttműködést hangsúlyozta.[7]

2020-ban megjelent Magyarország új Nemzeti Biztonsági Stratégiája *„Biztonságos Magyarország egy változékony világban”*[8] (a továbbiakban: NBS), amely dokumentum már elnevezésében is hordozza az új biztonsági kihívásokat és az arra történő felkészülés igényét.

Az NBS mind felépítésében, mind szellemiségében változott, a kiberbiztonságot, annak megteremtését, fenntartását és erősítését alapvető értékként nevesíti[9]. Ezen értékmeghatározás

[2] a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény (a továbbiakban. Vbö.) - https://njt.hu/ (2023.05.15.)

[3] Kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez – Kiberstratégia 5. pont

[4] A nemzeti középtávú stratégia olyan átfogó, horizontális megközelítésű társadalmi, gazdasági, környezeti célrendszert leíró, a célok elérését bemutató, középtávú stratégiai tervdokumentum, amely tartalmazza:
a) az átfogó társadalmi, gazdasági, környezeti helyzetelemzést;
b) a jövőképet és az érintett közpolitikai célkitűzések meghatározását;
c) a beavatkozási területek és eszközök beazonosítását;
d) a beavatkozások pénzügyi hátterének meghatározását és
e) a megvalósítás alapelveit. – a kormányzati stratégiai irányításról szóló 38/2012. (III. 12.) Korm. rendelet 27. § (1) bekezdés - https://njt.hu/ (2023.05.15.)

[5] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat 51. pont https://njt.hu/ (2023.05.15.)

[6] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat

[7] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat 31. pont a) és b) alpont

[8] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról - https://njt.hu/ (2023.05.15.)

[9] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról III/7. pont

mentén a biztonságtudatosság alacsony szintjét olyan adottságnak tekinti, amely folyamatos fejlesztését kormányzati szerepvállaláshoz kapcsolja, rögzítve ezzel a stratégiai célkitűzés teljesítéséhez kapcsolódó intézkedések címzetti körét.[10] Tényként kezeli az általános biztonsági környezet átrendeződését, amely okaként a digitalizáció fejlődésével megjelenő kockázatokat azonosítja, ezek között az elektronikus információs rendszerek sérülékenységét, a kiberbűnözői csoportok megjelenését és a kibertér kriminalizálódását, amellett, hogy a kiberteret olyan önálló műveleti térként – mint új szintér megjelenését – definiálja, amely a szervezet bűnözés mellett az állami hírszerzési tevékenységeknek is teret ad.[11]

Ebben az átrendeződött biztonsági környezetben Magyarország a kiberképességeket és azok műveleti alkalmazását a fizikai biztonságra is kiterjedő fegyveres agressziónak tekinti, melyre – összhangban a NATO Biztonsági Stratégiájával és az Észak-atlanti szerződés 5. cikkelyével – fizikai térben megvalósuló, akár fegyveres válaszadást is lehetségesnek tart. Ebből ered részben, hogy az NBS a kibertámadásoknak, mint kiemelt biztonsági kockázatnak a kármértékét jelentős károkozó hatásként azonosítja. [12]

Fenti alapvetések mentén az NBS célkitűzésként rögzíti a kiberbiztonsággal összefüggésben:

a) a hatékony nemzeti intézkedéseket és az együttműködést,

b) a megelőzést, a védelmi intézkedések fenntarthatóságát és rugalmasságát,

c) a fegyveres szervek részvétele mellett a civil szektor aktív szerepvállalását,

d) a biztonságtudatosság erősítését és védelmi képességek fejlesztését.[13]

A célkitűzések eléréséhez feladatként és intézkedési fókuszpontként:

a) a kibertérben ténylegesen jelentkező vagy potenciális kihívások, kockázatok és fenyegetések azonosítását, nyomon követését,

b) a jogi szabályozás fejlesztését,

c) az állami és a magánszektor szereplői, az oktatási és a tudományos intézmények és az egyéni felhasználók közötti partnerség kialakítását,

d) a felhasználók biztonságtudatos viselkedésének elősegítését,

e) a kiberbiztonsággal kapcsolatos nemzetközi együttműködés bővítését,

f) a kormányzati koordináció erősítését,

g) a kormányzati infokommunikációs rendszerek, a nemzeti létfontosságú információs infrastruktúra, a minősített információk és a nemzeti adatvagyon védelmének erősítését,

h) a Magyar Honvédség kibervédelmi és kiberműveleti erőinek fejlesztését,

i) a kibervédelmi kutatás-fejlesztés erősítését, a mesterséges intelligencia-alapú rendszerek fejlesztését és biztonságos üzemeltetését,

rögzíti.[14] Ezen feladatok ellátásához stratégiai dokumentáció szintjén ágazati szakpolitikák és részstratégiák szükségesek. Az NBS előírja, hogy a szak-, és részstratégiáknak és a szakági

[10] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról IV/32. pont és VI/106. pont
[11] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról V/69-71. pontok
[12] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról VI/101. pont és VII/124. pont d) alpont
[13] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról VIII/125-131. pontok
[14] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról IX./159-162. pontok

szabályzóknak összhangban kell állniuk az NBS-ben rögzítettekkel, azok megalkotása és felülvizsgálata során figyelemmel kell lenni a stratégiában leírtakra.[15]

Fentiek és az NBS szerinti irányváltás is a Kiberstartégia felülvizsgálatát indokolja, amely során figyelemmel kell lenni a már elért eredményekre, valamint arra a cél és eszközrendszerre, amely létjogosultságát az elmúlt évek gyakorlata igazolta. De miből is lehet és miből szükségszerű építkezni a stratégia felülvizsgálat folyamata során?

3. A meglévő örökség és a stratégiai behatások, kötelezettségek

Nyilvánvaló kérdésként merül fel, hogy a vannak-e a Kiberstratégiának ilyen hosszú távlatból vizsgálva olyan időtálló alkotóelemei, melyeket ésszerű és szükségszerű tovább használni. A válasz – nem vizsgálva az elhagyható vagy átírható részeket – egyértelmű igen, egyrészt azért, mert az az alapvető stratégiai cél, hogy *„a kibertér biztonsági környezetének elemzése alapján meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is,”*[16] melynek szabad, demokratikus jogállami és biztonságos működését Magyarország alapvető értéknek és érdeknek tekinti[17], olyan generális célmeghatározás, amely még ma is helytálló. Ez az érték és érdek alapú célmeghatározás már a későbbi NBS szellemiségét idézi, ahogy a biztonságpolitikai környezeti elemzés szükségességének rögzítése is.

A válasz másrészt azért is igen, mert olyan képességek elérést tűzte ki stratégiai célként – Magyarország hatékony megelőzési, észlelési, reagálási, válaszadási és helyreállítási képességekkel rendelkezzen, nemzeti adatvagyonát megfelelően védje, létfontosságú rendszereit üzembiztosan működtesse, az oktatásra és kutatásra kiemelt figyelmet fordítson [18] – amely képességek megléte továbbra is alapszükséglet a kiberbiztonság rendszerszintű megvalósításához, amellett, hogy a kiberbiztonsági szereplők és szervezetek közötti együttműködés nemzeti és nemzetközi szinten egyaránt a képességek megszerzéséhez és fenntartásához szükségszerű alapkövetelmény[19].

A Kiberstratégiában rögzített cselekvési területek között vannak olyan feladatok és végrehajtási eszközök, melyek továbbra is aktuálisak, fenntartásuk és továbbfejlesztésük indokolt. A kilenc azonosított cselekvési terület és az ehhez kapcsolt végrehajtási eszközrendszer közül ide sorolható a kormányzati koordináció fenntartása és a szabályozási környezet (ki)alakítása – figyelemmel az időközben kihirdetett törvényekből[20] eredő hatósági és koordinációs feladatokra és információbiztonsági szabályozásukkal való összhangra –, az együttműködés erősítése nemzeti és nemzetközi szinten egyaránt, az oktatás és a kutatás-fejlesztés szinten tartása és fejlesztése.[21]

Az elmúlt években a Kiberstratégia mellett a magas szintű tervdokumentációk között meghatározó szerepet töltött be Magyarország hálózati és információs rendszerek biztonságára

[15] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról X./176-178. pontok
[16] Kiberstratégia 1. pont
[17] Kiberstratégia 6. pont
[18] Kiberstratégia 9. pont
[19] Kiberstratégia 7. pont
[20] a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény és a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény - https://njt.hu/ (2023.05.15.)
[21] Kiberstratégia 10. pont

vonatkozó stratégiája[22] (a továbbiakban: HIRBS), amely stratégiaalkotási kötelezettséget a NIS irányelv[23] írta elő. Az irányelv rendelkezik arról, hogy valamennyi uniós tagállamnak kötelező elkészítenie és elfogadnia azt a nemzeti stratégiáját, amelyben az alapvető szolgáltatásként érintett ágazatokra *(energia, közlekedés, banki szolgáltatások, pénzügyi piaci infrastruktúrák, egészségügy, ivóvízellátás és -elosztás, digitális infrastruktúra)*, és a digitális szolgáltatókra *(online piactér, online keresőprogram, felhőalapú számítástechnikai szolgáltatás)* vonatkozóan meg kell határozni a stratégiai célokat, valamint a hálózati és információs rendszerek magas szintű biztonságának megteremtéséhez és fenntartásához szükséges szakpolitikai és szabályozási intézkedéseket[24].

A NIS irányelv minimum követelményként rögzíti a tagállamok részére a nemzeti stratégia kötelező tartalmi elemeit, ezek között:

a) a stratégiai célok és prioritások, valamint ezek teljesítését szolgáló irányítási keretrendszernek (ideértve a kormányzati szervek és egyéb érintett szereplők szerepkörét és felelősségét),

b) a felkészültségre, a reagálásra és a helyreállításra vonatkozó intézkedések azonosításának (ideértve a köz- és a magánszféra közötti együttműködést),

c) a kapcsolódó oktatási, tájékoztató és képzési programok, valamint a kutatási és fejlesztési tervek megjelölésének,

d) a kockázatok feltárására szolgáló kockázatértékelési terv rögzítésének,

e) a végrehajtásába bevont szereplők jegyzékének

a szerepeltetését[25].

A HIRBS elfogadásával a NIS irányelvnek – mint az első mérföldkőnek az információbiztonság közösségi szintű szabályozásának területén – a hazai implementációjához járult hozzá Magyarország. A HIRBS – az irányelvvel összhangban és a minimum tartalmi elemek rögzítése mellett – a köz- és a magánszféra közötti együttműködés jegyében alapvetésként rögzíti, hogy a kiberbiztonság megvalósítása a kiberbiztonsággal foglalkozó szakemberek, állami és piaci szereplők, illetve az állampolgárok közös érdeke, közös feladata. Ez az együttműködési igény rendszeresen visszatérő stratégiai célkitűzés nemzetközi és nemzeti szinten egyaránt.

Mint szakpolitikai stratégia a HIRBS a Kiberstratégia értékrendszerét megtartva célként határozza meg – többek között – a szabad, biztonságos és innovatív kibertér megteremtését, az innovációk, az új technológiai megoldások biztonságos módon történő bevezetését és adaptálását a digitalizálódott kormányzati és gazdasági területeken, továbbá a biztonságtudatosság növelését és a felkészültség emelését a társadalom minden területén[26]. Ezen alapelvek és célok továbbra is szükségszerűen adaptálhatók az új stratégiai irányokhoz.

A hálózati és információs rendszerek, mint kritikus információs infrastruktúrák elleni kibertámadások növekedését és komplexitását a HIRBS olyan fenyegetésként kezeli, amelyek a társadalom működésének fenntartásához szükséges alapfunkciók működését veszélyeztetik, ezért

[22] Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat - https://njt.hu/ (2023.05.15.)

[23] a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016. július 6-i 2016/1148 (EU) európai parlamenti és tanácsi irányelv (a továbbiakban: NIS irányelv) - https://eur-lex.europa.eu (2023.05.15.)

[24] NIS irányelv 7. cikk (1) bekezdés

[25] NIS irányelv 7. cikk (1) bekezdés

[26] Hálózati és információs rendszerek biztonságára vonatkozó Stratégia (a továbbiakban: HIRBS) - https://nki.gov.hu/wp-content/uploads/2020/11/Strat%C3%A9gia-a-h%C3%A1l%C3%B3zati-%C3%A9s-inform%C3%A1ci%C3%B3s-rendszerek-biztons%C3%A1g%C3%A1ra.pdf (2023.05.15.)

e körben az ágazati együttműködést és védelem komplexitását helyezi előtérbe a válaszintézkedések között.[27] A kiberbiztonsággal kapcsolatos jelenlegi és jövőbeni kihívások hatékony kezeléséhez a HIRBS a nemzeti kiberirányítási rendszer szükségességét hangsúlyozza, amellett, hogy elismeri a Kiberstratégia és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) által létrehozott intézményrendszert és eredményeit, a Nemzeti Kiberbiztonsági Koordinációs Tanács szerepét.[28] Ezen nemzeti intézményrendszer fejlesztése – a megváltozott jogi és társadalmi, gazdasági környezetben – szükségszerű és stratégiai célkitűzésként ismételten megfogalmazható.

A HIRBS célkitűzései között 3 fő prioritás szerepel, a digitális környezet iránti bizalom erősítése, a digitális infrastruktúra-védelem és a gazdasági szereplők támogatása, amely három fő prioritás 12 témakörben kerül kibontásra, 56 darab intézkedés nevesítésével együtt. Ezen prioritások, témakörök és intézkedések közül továbbra is célkitűzésként, fejlesztendő területként és szükséges intézkedésként célszerű azonosítani az alábbiakat:

a) a szakmai együttműködés keretén belül[29] felül kell vizsgálni és erősíteni kell a kormányzati, piaci, oktatási és civil szereplők együttműködését, kiberbiztonsági gyakorlatokat kell tartani és azokon nemzeti és nemzetközi szinten fokozott szerepvállalással részt kell venni, valamint támogatni és ösztönözni kell a köz- és magánszféra közös felelősségvállalását;

b) az infrastruktúra védelem keretén belül[30] az informatikai fejlesztések egységes biztonsági követelményrendszerének kötelező előírását erősíteni kell, amellett, hogy nemzeti szinten a meglévő kibervédekezési, elhárítási és reagálási képességeket rendszerezni, rendelkezésre állásukat fejleszteni és irányításukat, koordinációjukat egységesíteni szükséges;

c) a gazdasági szereplők támogatásával összefüggésben[31] a felsőoktatási és tudományos kutatóműhelyekkel kialakított stratégiai együttműködést kell szorgalmazni, valamint a K+F feladatok nyomonkövetését és erősítését, amellett, hogy az információbiztonságban dolgozó személyi állomány képzettségi követelményrendszerének felülvizsgálatát is el kell végezni.

A NIS irányelv – mint a HIRBS készítését előíró dokumentum – alapvetése[32], hogy a hálózati és információs rendszerek és szolgáltatások megbízhatósága és biztonsága kiemelt jelentőségű a gazdaság és a társadalom működése szempontjából, mivel a piac működését tekintve létfontosságúnak minősülnek, alapvető szerepet játszanak az áruk, a szolgáltatások és a személyek határokon átnyúló mozgásának biztosításában. Ezért a működési zavarok, a részleges vagy teljes szolgáltatás kiesések hatása rendszerszintű, kihatással lehet minden tagállamra, akár az egész Unióra. Ezen kockázatokhoz igazodva az irányelv célja, hogy harmonizált szabályozás bevezetésével megteremtse a hálózati és információs rendszerek biztonságának általános szintjét az Unióban, továbbá a tagállamok kibervédelmi felkészültségének egyenszilárdságát támogassa, amellett, hogy valamennyi tagállam számára kötelezettségeket[33] állapít meg. Ehhez igazította célkitűzéseit a HIRBS is.

A NIS irányelv alapvetése és célkitűzése ma is érvényes, attól függetlenül, hogy a tagállamok az előírt kötelezettségeket teljesítették, az irányelv átültetésével kialakított nemzeti jogszabályokat

[27] HIRBS 4. oldal - A hálózati és információs rendszerek biztonságára vonatkozó stratégia megalkotásának indokoltságával kapcsolatos megállapítások fejezet
[28] HIRBS 9-10. oldalak - A Stratégia Irányítási Keretrendszere fejezet
[29] HIRBS 11. oldal - 1. A digitális környezet iránti bizalom erősítése
[30] HIRBS 14-15. oldalak – 2. Digitális infrastruktúra védelem
[31] HIRBS 18-20. oldalak – 3. A gazdasági szereplők támogatása
[32] NIS irányelv bevezető (1)-(3) bekezdések
[33] NIS irányelv 1. cikk (2) bekezdés

alkalmazzák. Erre az irányelv felülvizsgálata is rámutatott, amely következtetést a NIS 2 irányelv[34] (a továbbiakban. NIS 2) bevezetője is tartalmazza[35], amellett, hogy a jelenlegi és jövőbeni kiberbiztonsági kihívások kezelésére további intézkedéseket tart szükségesnek.

A NIS 2 2023. január 3-án lépett hatályba[36] azzal, hogy rendelkezéseit a tagállamoknak 2024. október 18-tól kell kötelezően alkalmazni[37], és ezen időponttal a NIS irányelv hatályon kívül helyezésére is sor kerül[38]. A NIS 2 átültetésére a tagállamoknak 21 hónap áll rendelkezésére[39], amely kötelezettség teljesítése során nemzeti kiberbiztonsági stratégiát[40] (a továbbiakban: Kiberbiztonsági Stratégia) kell a tagállamoknak elfogadniuk (adaptálva a NIS irányelv korábbi rendelkezését).

A Kiberbiztonsági Stratégiával szemben továbbra is alapvető követelmény, hogy előírja a stratégiai célokat, a célok eléréséhez szükséges erőforrásokat, valamint a megfelelő szakpolitikai és szabályozási intézkedéseket. A NIS 2 – a NIS irányelvhez hasonlóan –előírja a Kiberbiztonsági Stratégia kötelező tartalmi elemeit[41] az alábbiak szerint:

a) stratégiai célok és prioritások rögzítése, különösen az alábbi ágazatok tekintetében:

   aa) kiemelten kritikus ágazatok: energia, szállítás, banki szolgáltatások, pénzügyi piaci infrastruktúrák, egészségügy, ivóvíz, szennyvíz, digitális infrastruktúra, információs és kommunikációs technológiai (a továbbiakban: IKT) szolgáltatások irányítása, közigazgatás, világűr;

   ab) egyéb kritikus ágazatok: postai- és futárszolgáltatások, hulladékgazdálkodás, vegyszerek gyártása, előállítása és forgalmazása, élelmiszer- termelés, feldolgozás és forgalmazás, gyártás, digitális szolgáltatók, kutatás;

   Ezen ágazatokra vonatkozó szabályozás már megjelenik a nemzeti jogszabályi környezetben[42], így az egyik alapvető stratégiai célkitűzés a kapcsolódó szabályozási környezet teljes felülvizsgálata az ágazati szabályzókkal együtt.

b) a stratégiai célok és prioritások eléréséhez szükséges irányítási keretrendszer kidolgozása, ideértve a kapcsolódó szakpolitikákat;

c) az érdekelt felek szerepét és felelősségi körét nemzeti szinten tisztázó irányítási keretetek kidolgozása, amely alapul szolgál az illetékes hatóságok, egyedüli kapcsolattartó pontok és a számítógép-biztonsági incidenskezelő csoportok (a továbbiakban: CSIRT - Computer Security Incident Response Team) közötti nemzeti szintű együttműködéshez és koordinációhoz,

[34] Az Európai Parlament és a Tanács (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) - https://eur-lex.europa.eu (2023.05.15.)

[35] *„Az említett irányelv a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiák létrehozásával, a nemzeti képességek kialakításával …… biztosította … a nemzeti keretek teljessé tételét.”* NIS 2 irányelv (2) bekezdés

[36] NIS 2 irányelv 45. cikk

[37] NIS 2 irányelv 41. cikk

[38] NIS 2 irányelv 44. cikk

[39] NIS 2 irányelv 41. cikk

[40] nemzeti kiberbiztonsági stratégia: valamely tagállam koherens kerete, amely meghatározza a kiberbiztonság területén követendő stratégiai célokat és prioritásokat és a megvalósításukhoz szükséges irányítási intézkedéseket az adott tagállamban - NIS 2 irányelv 6. cikk 4. pont

[41] NIS 2 irányelv 7. cikk (1) bekezdés

[42] a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény és végrehajtási rendeletei - https://njt.hu/ (2023.05.15.)

valamint ezen szervek és az ágazatspecifikus hatóságok közötti koordinációhoz és együttműködéshez;

d) a releváns eszközök azonosítására szolgáló és a kockázatok értékelését tartalmazó előírások rögzítését;

e) az eseményekre[43] való felkészültségnek, az azokra való reagálási képességnek és a működés helyreállítását biztosító intézkedések azonosításának, ideértve a köz- és magánszféra közötti együttműködést is előírása;

f) a Kiberbiztonsági Stratégia végrehajtásában részt vevő hatóságok és érdekelt felek felsorolása;

g) a NIS 2 és az (EU) 2022/2557 irányelv[44] szerinti illetékes hatóságok közötti, a kockázatokkal, a kiberfenyegetésekkel és az eseményekkel, továbbá a nem kiberbiztonsági jellegű kockázatokkal, fenyegetésekkel és eseményekkel kapcsolatos információk megosztására, valamint a felügyeleti feladatok ellátását célzó fokozott koordinációra vonatkozó szakpolitikai keretek meghatározása;

h) intézkedési terv meghatározása a polgároknak a kiberbiztonsággal kapcsolatos tudatosság általános szintjének a fokozására, ideértve a szükséges intézkedéseket is.

A tagállamok által a Kiberbiztonsági Stratégia részeként a NIS 2 szerint el kell készíteni[45]:

a) a szervezetek által a szolgáltatásaik nyújtásához használt IKT-termékek[46] és IKT-szolgáltatások[47] ellátási láncához kapcsolódó kiberbiztonsági feladatok kezelésére;

b) az IKT-termékek és IKT-szolgáltatások kiberbiztonsággal kapcsolatos követelményeinek a közbeszerzésekbe történő felvételére és meghatározására, ide értve a kiberbiztonsági tanúsítás, a titkosítási követelmények és a nyílt forráskódú kiberbiztonsági termékek használatára;

c) a sérülékenységek kezelésére[48];

d) a nyílt internet nyilvános alkotóelemei általános rendelkezésre állásának, sértetlenségének és bizalmasságának fenntartására;

e) a legkorszerűbb kiberbiztonsági kockázatkezelési intézkedések végrehajtását célzó megfelelő fejlett technológiák fejlesztésének és integrációjának előmozdítására;

f) a kiberbiztonsággal, a kiberbiztonsági készségekkel, a figyelemfelkeltéssel, valamint a kutatási és fejlesztési kezdeményezésekkel kapcsolatos oktatás és képzés, valamint a helyes kiberhigiéniai gyakorlatokkal és ellenőrzésekkel kapcsolatos, a polgárokat, az érdekelt feleket és a szervezeteket célzó iránymutatások előmozdítására és fejlesztésére;

g) a tudományos és kutatóintézeteknek a kiberbiztonsági eszközök és a biztonságos hálózati infrastruktúra fejlesztése, megerősítése és bevezetésének előmozdítása terén történő támogatására;

[43] esemény: olyan esemény, amely veszélyezteti a hálózati és információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát; - NIS irányelv 6. cikk 6. pont

[44] Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről - https://eur-lex.europa.eu (2023.05.15.)

[45] NIS 2 irányelv 7. cikk (2) bekezdés

[46] NIS 2 irányelv 6. cikk 12. pont

[47] NIS 2 irányelv 6. cikk 13. pont

[48] ide értve a sérülékenységek NIS 2 irányelv 12. cikk (1) bekezdése szerinti összehangolt közzétételének előmozdítására és megkönnyítésére vonatkozó szabályokat;

h) a szervezetek közötti önkéntes kiberbiztonsági információmegosztás támogatása céljából történő információmegosztási eszközök beépítésére;

i) a kis- és középvállalkozások alapszintű – könnyen hozzáférhető iránymutatások és segítségnyújtás általi – kiberbiztonsági ellenállóképességének és kiberhigiéniájának megerősítésére;

j) az aktív kiberbiztonság előmozdítására

vonatkozó szakpolitikákat. Ezen dokumentumok a nemzeti stratégiai tervdokumentációk körében az R. 35. §-a szerinti szakpolitikának minősülnek, kidolgozásukra a Kiberbiztonsági Stratégia elkészítésével párhuzamosan kerülhet sor.

A NIS 2 szerint előírt[49] kiberbiztonsági tanúsítási keretrendszer alkalmazásához és kialakításához kapcsolódik a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló törvény[50] (a továbbiakban: Kibertanúsítási törvény), amely a NIS 2 szerinti megfelelés mellett az uniós kiberbiztonsági jogszabály[51] végrehajtásához szükséges rendelkezéseket állapít meg. E törvény termeti meg az Ibtv. 2022. január 1-jén hatályba lépett módosításával bevezetett európai uniós kiberbiztonsági tanúsítási rendszer alkalmazásának hazai lehetőségét, továbbá az Európai Unió tanúsítási rendszere által le nem fedett infokommunikációs termékek és szolgáltatások esetében megállapítja a hazai tanúsítási követelményeket és az ehhez kapcsolódó szabályokat. Olyan alapvető kiberbiztonsági követelményrendszert és a követelmények betartásához szükséges hatósági felügyeleti szabályokat rögzít, melyek – a NIS 2 irányelv mellett – több kiberbiztonsági stratégiai célkitűzéshez is kapcsolódnak. E körbe tartozik a társadalom és a gazdaság működése szempontjából alapvető fontosságú szektorok szereplőinek kiberbiztonsági függőség szerinti azonosítása[52] a NIS 2 szerinti kritikus ágazatok felhasználásával és a kiberbiztonsági kockázatok kezelésére szolgáló egységes követelményrendszer[53] meghatározása.

A Kibertanúsítási törvényben rögzített nemzeti kiberbiztonsági tanúsítási keretrendszer biztosítja, hogy az infokommunikációs termékek és szolgáltatások típusai, illetve fajtái tekintetében a nemzeti kiberbiztonsági tanúsító hatóság, a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH), olyan kiberbiztonsági elvárásokat és követelményeket fogalmazzon meg, melyek a termékek piaci felhasználását is elősegítik. Az SZTFH, mint hatóságnak a feladatellátása során figyelemmel kell lenni az európai kiberbiztonsági tanúsítási rendszerek fejlesztésre, a kapcsolódó szabványosítási folyamatokra és ezek alapján a nemzeti kiberbiztonsági tanúsítási rendszerek értékelésére. Ezen hatósági feladatok érvényesítése és hatékony ellátása mind a Kiberstratégiában, mind a HIRBS-ben rögzített célkitűzések teljesülését szolgálják, többek között a gazdasági szereplők motivációját és támogatását, a versenyképesség erősítését, a kiberbiztonsági szempontok érvényesítését az információs rendszerek fejlesztésével és üzemeltetésével kapcsolatosan, valamint a szabályozási környezet kialakítását.

Ez az új szabályozás nem érinti a jelenleg kijelölt nemzeti létfontosságú rendszerek és azok üzemeltetői részére előírt, az Ibtv. alapján alkalmazandó kiberbiztonsági követelményeket és felügyeleti rendszert, azonban lefedi azokat a szolgáltatókat, melyek ágazati besorolásuk vagy a

[49] NIS 2 irányelv 7. cikk (2) bekezdés b) pont

[50] a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (a továbbiakban: Kibertanúsítási törvény) - https://njt.hu/ (2023.05.15.)

[51] az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről szóló 2019. április 17-i 2019/881 európai parlamenti és tanácsi rendelet - https://eur-lex.europa.eu (2023.05.15.)

[52] Kibertanúsítási törvény 1-2. melléklete

[53] Kibertanúsítási törvény 6.-12. §-ok

követelményrendszer hiánya miatt kiesnek a kiberbiztonsági szabályozás jelenlegi hatóköréből. Megfogalmaz továbbá olyan védelmi követelményeket[54] és rögzít olyan felügyeleti eszközöket[55] – az Ibtv. rendelkezésivel összhangban –, melyek szintén olyan stratégiai célkitűzések teljesülését szolgálják, melyeket a Kiberbiztonsági Stratégiában rögzíteni kell. E körbe tartozik az IKT-termékek és IKT-szolgáltatások kiberbiztonsággal kapcsolatos, valamint a kiberbiztonsági tanúsítás követelményeinek meghatározása, illetve a Kiberbiztonsági Stratégia végrehajtásában részt vevő hatóságok meghatározása.

A Kiberbiztonsági Stratégia előkészítésénél fenti szabályok adaptálásával figyelemmel kell lenni a NIS 2-ben meghatározott kiemelten kritikus és egyéb kritikus ágazatok kiberbiztonsági követelményeinek és szabályrendszerének kidolgozására is.

A 2008/114/EK irányelv[56] az első olyan uniós szabályozás, amely intézkedéseket tartalmazott az európai kritikus infrastruktúrák védelmére vonatkozóan és megállapította, hogy a védelemért való felelősség a tagállamokat és az infrastruktúrák tulajdonosait, üzemeltetőit terheli. Előírta olyan üzemeltetői biztonsági terv rendelkezésre állását, amely rögzíti a jelentős eszközök meghatározását, a kockázatértékelést, valamint a kockázatokkal arányos védelmi intézkedések meghatározását, kiválasztását és rangsorolását. Ezen irányelvnek való megfelelést Magyarországon a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény és végrehajtási rendeleti biztosították, melyek NIS-irányelv szerinti megfeleltetésére is sor került 2018-ban. A megfeleseltetés nem járt a tagállamok részére stratégiaalkotási kötelezettséggel.

A 2008/114/EK irányelvet 2024. október 18-ával hatályon kívül helyezi az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról[57] (a továbbiakban: CER irányelv), amely 2023. január 3-án lépett hatályba[58] azzal, hogy rendelkezéseit a tagállamoknak 2024. október 18-tól kell kötelezően alkalmazni, átültetésére 21 hónap áll rendelkezésére[59]. Az irányelv rögzíti, hogy a kritikus szervezetek fizikai biztonsága és kiberbiztonsága közötti kapcsolatot a tagállamok kötelezettsége kialakítani és biztosítani, azzal, hogy a CER irányelv és a NIS 2 végrehajtását koordináltan szükséges megvalósítani[60].

A CER irányelv célja, hogy az alapvető szolgáltatást nyújtó kritikus szervezetek rezilienciáját fokozza annak érdekében, hogy az alapvető szolgáltatásokat, mint a társadalmi funkciók és gazdasági tevékenységek fenntartásához nélkülözhetetlen szolgáltatásokat az unió belső piacán egységes és elégséges szinten biztosítsák a szolgáltatást nyújtó szervezetek[61]. A célmeghatározás értelmezéséhez és adaptálásához a CER irányelv az alábbi fogalom meghatározásokat adja:

a) kritikus szervezet[62]: olyan köz- vagy magánjogi szervezet, amely irányelv szerinti azonosítását, ágazati, alágazati besorolását, szervezeti kategóriájának azonosítását a tagállam elvégezte és kritikus szervezetként meghatározta;

[54] Kibertanúsítási törvény 19. §
[55] Kibertanúsítási törvény 22-26. §-ok
[56] az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelv - https://eur-lex.europa.eu (2023.05.15.)
[57] az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (a továbbiakban: CER irányelv) - https://eur-lex.europa.eu (2023.05.15.)
[58] CER irányelv 28. cikk
[59] CER irányelv 26. cikk (1) bekezdés
[60] CER irányelv 1. cikk (2) bekezdés
[61] CER irányelv (43) bekezdés és 1. cikk (1) bekezdés
[62] CER irányelv 2. cikk 1. pont

b) reziliencia: valamely kritikus szervezet azon képessége, hogy megelőzzön egy eseményt, azzal szemben védekezzen, arra reagáljon, annak ellenálljon, azt enyhítse, tompítsa, ahhoz alkalmazkodjon, és abból helyreálljon[63];

c) kritikus infrastruktúra: olyan eszköz, létesítmény, berendezés, hálózat vagy rendszer, vagy valamely eszköz, létesítmény, berendezés, hálózat vagy rendszer része, amely szükséges az alapvető szolgáltatás nyújtásához[64];

d) alapvető szolgáltatás: az alapvetően fontos társadalmi funkciók, a gazdasági tevékenységek, a népegészségügy és a biztonság vagy a környezet fenntartásához elengedhetetlen szolgáltatás[65].

Ezen fogalmi meghatározásokat – ahogy azt a Kiberstratégia és az Ibtv. viszonyában rendezte a jogalkotó – a kritikus szervezetek rezilienciájára vonatkozó stratégia[66] készítésénél alapvetésként kell kezelni.

A CER irányelv a kritikus szervezetek számára rögzíti azokat a kötelezettségeket, melyek teljesítésével, végrehajtásával rezilienciájukat és szolgáltatási szintjüket tudják növelni. Ennek érdekében olyan kockázatokkal arányos technikai, biztonsági és szervezeti intézkedéseket kell hozniuk, amelyekkel megelőzik valamely esemény bekövetkezését, védekezzenek azzal szemben, reagáljnak a bekövetkezett eseményre, továbbá enyhítik annak hatását és a helyreállítást támogatják[67]. Ez a követelményrendszer a NIS 2 által előírt szakpolitikák köréből is levezethető[68], amelyet szintén adaptálni kell a stratégiakészítés során az alkalmazott cél- és eszközrendszerre.

A stratégiakészítési kötelezettséghez kapcsolódóan a CER irányelv előírja, hogy minden tagállamnak a kritikus szervezetek rezilienciájának fokozására 2026. január 17-ig stratégiát kell készíteni (a továbbiakban: KRS), azzal, hogy ezen stratégiában az ágazati stratégiákra és tervdokumentációkra építve kell meghatározni a stratégiai célokat és szakpolitikai intézkedéseket a kritikus szervezetek magas szintű rezilienciájának elérése és fenntartása céljából, lefedve az alábbi ágazatokat[69]:

a) energia,

b) közlekedés,

c) banki szolgáltatások,

d) pénzügyi piaci infrastruktúra,

e) egészségügy,

f) ivóvíz,

g) szennyvíz,

h) digitális infrastruktúra,

i) közigazgatás,

j) világűr,

[63] CER irányelv 2. cikk 2. pont
[64] CER irányelv 2. cikk 4. pont
[65] CER irányelv 2. cikk 5. pont
[66] CER irányelv 4. cikk (1) bekezdés
[67] CER irányelv (29) bekezdés
[68] NIS 2 irányelv 7. cikk (2) bekezdés
[69] CER irányelv 4. cikk (1) bekezdés

k) élelmiszer- előállítás, feldolgozás és forgalmazás.

Ezen ágazatok átfedésben vannak a NIS 2 szerint rögzített és a Kiberbiztonsági Stratégiában érintett ágazatokkal, így a stratégiakészítés során a Kiberbiztonsági Stratégia és a KRS rendelkezéseit összehangoltan kell megállapítani.

Kötelező, minimumkövetelménynek a CER irányelv a következőket stratégiai tartalmat rögzíti[70]:

a) a kritikus szervezetek általános reziliencájának fokozására vonatkozó stratégiai célkitűzések és prioritások, figyelembe véve a határokon átnyúló és ágazatközi, valamint a kölcsönös függőségeket;

b) a stratégiai célkitűzések és prioritások elérését szolgáló irányítási keretrendszer, ideértve a különböző hatóságok, a kritikus szervezetek és a stratégia végrehajtásában részt vevő felek szerepkörének és felelősségének a leírását is;

c) a kritikus szervezetek általános rezilienciájának fokozásához szükséges intézkedések leírása, ide értve a tagállamok részére előírt kockázatértékelés leírását is, melynek ki kell terjednie a releváns természeti és ember okozta kockázatokra, beleértve a több ágazatot érintő vagy a határokon átnyúló jellegű kockázatokat, a baleseteket, a természeti katasztrófákat, a népegészségügyi szükséghelyzeteket és a hibrid fenyegetéseket vagy egyéb ellenséges fenyegetéseket, ideértve a terrorista bűncselekményeket is[71];

d) a kritikus szervezetek azonosítására szolgáló eljárás leírása;

e) a kritikus szervezetek támogatását célzó eljárás leírása, beleértve a közszektor, a magánszektor, valamint a közjogi és magánjogi szervezetek közötti együttműködés erősítését célzó intézkedéseket is;

f) a stratégia végrehajtásában részt vevő főbb hatóságok és a kritikus szervezetektől eltérő érintett érdekelt felek jegyzéke;

g) a CER irányelv és a NIS 2 szerinti illetékes hatóságok közötti koordinációt szolgáló szakpolitikai keret a kiberbiztonsági kockázatokra, a kiberfenyegetésekre és kiberjellegű eseményekre, valamint a nem kiberjellegű kockázatokra, fenyegetésekre és eseményekre vonatkozó információmegosztás és a felügyeleti feladatok ellátása céljából;

h) a már bevezetett olyan intézkedések leírása, amelyek célja elősegíteni a CER irányelv szerinti[72], a kritikus szervezetek rezilienciájára vonatkozó kötelezettségeknek a tagállam által kritikus szervezetként azonosított kis- és középvállalkozások általi végrehajtását.

A CER irányelv kihirdetésével párhuzamosan került kiadásra a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről szóló tanácsi ajánlás[73] (a továbbiakban: ajánlás) amely a stratégiakészítéshez további iránymutatást adhat. Az ajánlás hangsúlyozza, hogy a kritikus infrastruktúrák és az általuk nyújtott alapvető szolgáltatások biztonsága a tagállamoknak és azok kritikusinfrastruktúra-üzemeltetőinek a felelőssége, azonban az uniós szintű koordináció megerősítése szükségszerű és helyénvaló akkor, amikor a fenyegetések módja és mértéke folyamatosan változik, a hibrid hadviselés teret hódit. Mindez minden uniós

[70] CER irányelv 4. cikk (2) bekezdés
[71] CER irányelv 5. cikk
[72] CER irányelv III. fejezet 12-16. cikkek
[73] A Tanács ajánlása (2022. december 8.) a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről (2023/C 20/1) - (a továbbiakban: Tanács ajánlása) - https://eur-lex.europa.eu (2023.05.15.)

tagállamot érinthet és hatással lehetnek nemcsak egy tagállam, hanem az Unió egész gazdaságának, belső piacának és teljes társadalmának a rezilienciájára és megfelelő működésére[74]. A 2008/114/EK irányelv és a NIS irányelv a kibertérben megjelenő fenyegetéseket és az ezeket kezelő védelmi intézkedéseket helyezte a középpontba, azonban a változó fenyegetettségi helyzet miatt az hálózati és információs rendszerek, a kritikus szervetek és ágazatok ellenálló képességének fejlesztése a fő cél, így és a CER irányelv és NIS 2 a kritikus infrastruktúrák és a kiberbiztonság egységesen magasabb szintű rezilienciájának és védelmének biztosítása céljából ad új jogi kereteket, amely alapja kell, hogy legyen a stratégiáknak.

Az ajánlás rámutat arra, hogy a kulcsfontosságú ágazatokban – mint például az energiaágazatban, a digitális infrastruktúrák terén, a közlekedési ágazatban és az űrágazatban –, valamint a tagállamok által azonosított egyéb releváns ágazatokban prioritásnak kell, hogy minősüljenek a rezilienciaerősítő intézkedések. Ezen intézkedések meghozatalánál különös figyelemmel kell lenni az ágazati függőségekre és átjárhatóságra, azok határon átnyúló jellegére, az ellátási láncok zavaraira, valamint a hibrid fenyegetésekre[75]. Mindez olyan adottság, amelyet a nemzeti stratégiaalkotás során zsinórmértékként kell kezelni, kiemelt figyelemmel az elmúlt időszakban bekövetkezett eseményekre (pl. egészségügyi válsághelyzet, energiaválság, természeti katasztrófák, orosz-ukrán háború).

Az ajánlás számos olyan célzott uniós és nemzeti szintű intézkedést, ajánlást határoz meg, melyek a kritikus infrastruktúrák rezilienciájának önkéntes alapon történő támogatását és fokozását ösztönzik és teszik lehetővé. Ezek közül a kiberbiztonsági stratégiaalkotás során a célok, eszközök és intézkedések rendszere mentén az alábbiak figyelembevétele indokolt:

a) szakértői képzések támogatása és a szakértők közötti információmegosztás erősítése, a nemzeti és nemzetközi képzési platformokon való részvétel ösztönzése[76],

b) elkülönített pénzügyi források biztosítása a kiberbiztonsági kapacitások megerősítésére, mind a hatósági feladatellátás (CSIRT hálózatban történő részvétel), mind az eseménykezelés tekintetében (helyreállítási költségek megtérítése)[77],

c) szakpolitika elkészítése azon űrágazati szereplők számára, amelyek az űralapú szolgáltatások nyújtását támogató földi infrastruktúra rezilienciájának növelését célozzák, és egy összes veszélyre kiterjedő megközelítésen és egy kockázatalapú megközelítésen alapulnak[78],

d) a nemzetközi együttműködés erősítése, kiemelt figyelemmel az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközponttal, valamint a Veszélyhelyzet-reagálási Koordinációs Központtal, egyrészt tudástranszfer lehetőségeinek felhasználása, másrészt a korai előrejelzés és a reagálóképesség javítása céljából[79].

e) az ágazatközi együttműködés erősítése a megfelelő uniós szintű reagálás biztosítása érdekében, rendszeres képzések és gyakorlatok szervezése a tagállamokkal az együttműködés tesztelésére[80],

[74] Tanács ajánlása (3) bekezdés
[75] Tanács ajánlása (5) bekezdés
[76] Tanács ajánlása II. fejezet 5. pont
[77] Tanács ajánlása II. fejezet 7. pont
[78] Tanács ajánlása II. fejezet 10. pont
[79] Tanács ajánlása II. fejezet 12. pont és III. fejezet 25/b pont
[80] Tanács ajánlása III. fejezet 30/c pont

f) a kiberbiztonsági stratégiák felülvizsgálata és naprakésszé tétele, ennek keretében a tagállami CSIRT-ek képességeinek fokozása és a kiberbiztonsági eseményekre és válságokra vonatkozó nemzeti reagálási tervek elfogadása[81].

A kiberbiztonságra vonatkozó nemzeti stratégiai örökség (Kiberstratégia és HIRBS) és a stratégiaalkotási kötelezettséget előíró NIS2 és CER irányelv szellemiségéből és előírásaiból következik, hogy a Kiberbiztonsági Stratégia elkészítésénél az ellenálló- és reagálóképesség két olyan követelményként jelenik meg, melyek hatékony és összehangolt jogalkotást és végrehajtást követelnek meg.

A szabályozási környezet kialakításához szükséges fogalmi keretekhez – a CER irányelv fentebb rögzített fogalmi rendelkezései mellett – a Vbö. értelmező rendelkezése ad iránymutatást, amely rögzíti a nemzeti ellenálló képesség fogalmát[82]. E szerint nemzeti ellenálló képesség *„az Észak-atlanti Szerződés 3. cikkével összhangban, a nemzetet alkotó lakosság, gazdaság és állam képessége arra, hogy külső vagy belső, a közrendet és közbiztonságot, valamint az állam honvédelmi és nemzetbiztonsági érdekeit, továbbá stabilitását sértő vagy veszélyeztető törekvések, támadások, természeti vagy ipari katasztrófák, járványok hatékony előrejelzését, megelőzését, a kockázatok lehető legkisebbre csökkentését, illetve bekövetkezésük esetén azok kezelését és azt követően a mielőbbi és hatékony helyreállítást a polgári és katonai felkészültségen keresztül – a biztonságtudatosság fejlesztésével, a felkészültség fokozásával és a szükséges védelmi intézkedések foganatba vételével – megfelelően biztosítsa”.* Ezen fogalmi meghatározás mellett a Vbö. alapelvi szinten rögzíti, hogy Magyarország védelme, biztonságának fenntartása és fejlesztése olyan összetett feladatrendszer, amelynek ellátása során az érintett szervezetek és természetes személyek összehangoltan a szükségesség és arányosság elve mentén, kölcsönösen együttműködnek egymással[83].

A Vbö. előírja a védelmi és biztonsági célú tervezés rendszerének kialakítását, amely célja a védelmi és biztonsági szervezetek, az ezen feladtok ellátásában részt vevő kormányzati szervek együttműködési kereteinek biztosítása, eseménykezelésre való felkészítése, továbbá az eseménykezeléshez kapcsolódó működésük, fejlesztésük stratégiai szempontú meghatározása. Ezen tervrendszerben kormányzati szinten összehangolt, központilag meghatározott szempontrendszer mentén, ágazati sajátosságokat rögzítő stratégiai dokumentumok kerülnek elkészítésre[84]. A tervkészítés alapelveit és folyamatát a VböR. rögzíti, hangsúlyozva az összkormányzati tervrendszerhez illeszkedés és a tervdokumentációk egymásra épülésének alapkövetelményét[85]. A főbb tervdokumentumok körébe az alábbiak sorolhatók[86]:

a) a Biztonság- és Védelempolitika Alapelvei,

b) a Nemzeti Biztonsági Stratégia,

c) az Integrált Védelmi és Biztonsági Iránymutatás, valamint

d) ágazati törvényben és a Kormány rendeletében előírt ágazati, illetve kihívás- vagy fenyegetésközpontú, továbbá kockázatelemzésen alapuló stratégiák, alaptervek, illetve intézkedési tervek.

[81] Tanács ajánlása III. fejezet 26 pont
[82] Vbö. 5. § 7. pont
[83] Vbö. 4. §
[84] Vbö. 20. §
[85] a védelmi és biztonsági célú tervezés szabályairól szóló 400/2022. (X. 21.) Korm. rendelet (a továbbiakban: VböR.) 2-5. §-ok
[86] Vbö. 22. § (1) bekezdés

A Biztonság- és Védelempolitika Alapelvei (a továbbiakban: BVA) – mint az R. szerinti tervdokumentáció közül az országelőrejelzéshez leginkább kapcsolható dokumentum – a Kormány által előkészített, az Országgyűlés által meghatározott és elfogadott, hosszú távra vonatkozó, elvi szintű, nyilvános védelmi és biztonsági fő tervdokumentum. Ezen tervdokumentum, mint a Nemzeti Biztonsági Stratégia alappillére meghatározza:

a) az ország és a nemzet helyzetének és fenyegetettségének értékelése alapján,

b) a védelmi és biztonsági képességek és az ezzel összefüggésben tervezett fejlesztések alapulvételével,

c) az ország geostratégiai lehetőségeire figyelemmel

a Kormány számára, hogy az irányítása alá tartozó szervek irányítása, valamint a védelmi és biztonsági feladatok ellátásában részt vevő szervekkel, szervezetekkel való együttműködés keretében mely fő elvek, irányok és célok szerint tervezze és hajtsa végre az ország védelmi és biztonsági célú felkészítését, illetve képességeinek fejlesztését, fenntartását és működtetését[87].

A tervdokumentációk közül – az R. rendelkezéseivel összhangban - a Nemzeti Biztonsági Stratégia követelményeit is rögzíti a Vbö., amely tervdokumentum a BVA-ban foglaltaknak megfelelően hosszú távra fogalmazza meg:

a) az ország biztonsági helyzetének általános értékelését,

b) a védelmi és biztonsági képességek által védendő értékeket,

c) az ország védelmi és biztonsági helyzetét meghatározó kihívásokat, fenyegetéseket, potenciális válságokat, valamint

az ezekkel összefüggő főbb fejlesztési irányokat, és a végrehajtáshoz kapcsolódóan meghatározott cselekvési irányokat[88].

Az Integrált Védelmi és Biztonsági Iránymutatás olyan hosszú távú tervdokumentáció, amely a BVA-ban foglaltak, valamint a Nemzeti Biztonsági Stratégia alapján – a nemzetbiztonsági érdekek és minősített adatok védelmének elsőbbségére figyelemmel –hosszú távra határozza meg:

a) az ország védelmi és biztonsági érdekeinek érvényesítéséhez szükséges képességcélokat,

b) az ország biztonságának fenntartásához és megerősítéséhez szükséges részletes cselekvései irányokat,

c) az ország védelmével és biztonságával összefüggő átfogó feladatrendszerben érintett szervek együttműködésének főbb irányait, valamint

a fentiekhez kapcsolódó főbb ágazati feladatokat[89].

Ezen főbb tervdokumentációk fentiekben részletezett tartalmi elemeit tovább bontja és az elkészítéshez kapcsolódó részletszabályokat maghatározza a Vbör.[90], amellett, hogy rögzíti azon kötelezettséget is, mely szerint a tervdokumentációkat nyomon követni és időszakonként értékelni kell annak érdekében, hogy a meghatározott cél és eszközrendszer teljesülését elemezni és értékelni, az elvégzett felülvizsgálat alapján a szükséges beavatkozásokat megtenni lehessen[91].

[87] Vbö. 22. § (3) bekezdés
[88] Vbö. 22. § (4) bekezdés
[89] Vbö. 22. § (5) bekezdés
[90] VböR. 13-17. §-ai
[91] VböR. 6-12. §-ok

A Kiberbiztonsági Stratégia készítésénél a védelmi és biztonsági célú tervdokumentumokban meghatározott cél és eszközrendszerhez kell igazítani a kiberbiztonsághoz kapcsolódó – fentebb részletezett és kötelezően előírt – stratégiai célkitűzéseket, amellett, hogy a Vbö. szerint stratégiai tervrendszer bevezetése miatt a kiberbiztonsághoz kapcsolódó részstratégiák és szakpolitikák felülvizsgálata is indokolt.

4. A módosítás lehetséges irányai és lépései

Rögzíthetjük azt a tényt, hogy NIS2 és a CER irányelv, valamint az ajánlás előírásai alapján a Kiberstratégia felülvizsgálata, újraírása tagállami kötelezettség, amellett, hogy a Vbö. által bevezetett védelmi és biztonsági célú tervrendszer is a felülvizsgálatot indokolja. Mindezek a módosítás lehetséges irányait és lépéseit is meghatározzák.

a) Első lépésként a stratégiai hierarchiának megfelelő, rendszertani elhelyezést szükséges vizsgálni. A védelmi és biztonsági tervrendszernek való megfelelés mellett az NBS-sel való összhang tételes felülvizsgálatát kell elvégezni.

b) Második lépésként a NIS 2 által előírt Kiberbiztonsági Stratégia szerinti tartalmi megfelelőséget kell ki(be)építeni, azzal, hogy a stratégiai örökségek adaptálása mellett, a fejlesztendő területek meghatározását és az új irányok kijelölését is el kell végezni.

c) Harmadik lépésként a részstratégiákat és a szakpolitikákat kell kidolgozni, figyelemmel a CER irányelv és az ajánlás által előírt KRS kötelezettségekre is.

A Kiberbiztonsági Stratégia és a KRS kötelező tartalmi elemeinek tételes meghatározására az előző fejezetben már sor került, amellett, hogy azoknak a főbb adaptálható céloknak és eszközöknek a felsorolása is rögzítésre került, amelyek más szabályzókból eredeztethetőek (pl. stratégiai örökség, ajánlás, törvényi előírások), így ezek ismétlésétől itt eltekintünk.

Fentiektől függetlenül álláspontom szerint van néhány olyan visszatérő témakör, melyeket egy új kiberbiztonsági stratégia megalkotása során nem szabad figyelmen kívül hagyni. Ezek az alábbiak.

a) A kibertér, mint önálló műveleti tér megjelenéséből eredő kockázatok egységes kezelése. Az NBS a kiberteret védelmi szempontból olyan önálló műveleti térként definiálja, amely a szervezet bűnözés mellett az állami hírszerzési tevékenységeknek is teret ad. Ettől függetlenül a kibertérben megjelenő fenyegetések hatása többrétű. Egy rosszindulatú szoftver használatával a kiberbűnözők átvehetik az irányítást személyes IT eszközeink felett, ellophatnak vagy megsérthetnek személyes adatokat és on-line csalást követhetnek el vele. Egyénre, szervezetre, közösségre, államra vonatkozó jogellenes tartalmakat terjeszthetnek az interneten és a közösségi média különböző platformjain, ezáltal súlyos erkölcsi, pszichológiai és anyagi, vagy éppen nemzetbiztonsági károkat okozva az áldozatoknak. A „darkneten” keresztül tiltott árukkal kereskedhetnek és elektronikus hackelési szolgáltatásokat nyújthatnak, ezáltal jelentős anyagi kárt okozhatnak gazdasági szereplőknek és az állami költségvetésnek (üzleti haszon és adóbevételek elmaradása). Mindez rámutat arra, hogy a kibertér, mint önálló műveleti tér definiálása polgári és rendvédelmi szempontból egyaránt szükséges, ezáltal az NBS mellett a Kiberbiztonsági Stratégiában történő definiálása is időszerű.

b) Az ellenállóképesség növelése az egyén, a szervezet, az állam és a társadalom oldalán. Ehhez a reziliencia fogalmát a stratégiaalkotás során úgy kell alkalmazni, mint a megelőzésre, védekezésre, reagálásra, ellenállásra, enyhítésre, alkalmazkodásra vagy helyreállításra való képességet, amely

képességek hiánya jelentős mértékben befolyásolja az egyén életminőségét, a szervezetek, az állam, a társadalom és a gazdaság működőképességét és fenntarthatóságát. Figyelemmel arra, hogy a fizikai és a digitális infrastruktúrák között fennálló, egyre nagyobb mértékű kölcsönös függőségéből adódóan a kiberbiztonság megteremtése alapvető társadalmi, gazdasági és állami érdekké vált, emellett az egyének biztonságtudatosságának meghatározó tényezője lett, a stratégiai válaszok a problémára szükségszerűek.

c) Új szabályozási célkitűzések meghatározása. A tárgyalt stratégiai elvekből is levezethető, azonban ha ettől elvonatkoztatva számbavételezzük azokat a jogszabályokat, amelyek a generális, Ibtv. és végrehajtási rendeletei szerinti szabályozás mellett információbiztonsági szabályelemeket tartalmazva speciális ágazati szabályzóként az elmúlt években megjelentek azt látjuk, hogy olyan szerteágazó és mennyiségét tekintve számos jogszabály áll rendelkezésre, amely a jogalkalmazás és a jogérvényesítés oldaláról hatékonysági és átláthatósági kérdéseket vet fel. Hosszútávon egy egységes, személyi hatályát tekintve az Ibtv. közvetlen hatályától szélesebb kört felölő információbiztonsági törvény megalkotása szükséges, amely stratégiai célkitűzésként – az Ibtv. megalkotásánál nóvumnak számító megoldáshoz képest – előremutató még európai szinten is.

d) Biztonságtudatosság fejlesztése. Az NBS rögzíti a biztonságtudatosság alacsony szintjét, mint az általános biztonsági környezet átrendeződésének egyik következményét, emellett azonban az elmúlt években a biztonsági események növekvő tendenciája, a kiberbűnözői csoportok szaporodása és a kibertér kriminalizálódása is arra mutat rá, hogy az egyének mellett, a szervezetek, - nemzetbiztonsági szempontok mentén az államok – ez irányú képességét is erősíteni kell. Az oktatási szintek és tartalmak specializálása is olyan célkitűzés, amely nem maradhat el egy megújult stratégiai környezetben.

e) Együttműködés szélesítése és erősítése. A jelenleg működő nemzeti és nemzetközi együttműködés a kiberbiztonságban érintett szakmai szervezetek és hatóságok között hatékony és előremutató. Ettől függetlenül ha az együttműködési lehetőségeknek a mélységét és minőségét vizsgáljuk, fellelhetünk továbblépési irányokat. Az egyének, gazdasági szereplők, közösségek irányába az állami szereplők (hatóságok, eseménykezelő központok) és a szakmai szövetségek részéről egyirányú, de az igényeken alapuló nyílt és biztonságos kommunikációt kell erősíteni, ahogy a közszféra és a magánszféra közötti kétirányú viszonyrendszerben is, előtérbe helyezve a tudatosságfejlesztést és a kiberhigiénia széles körű elterjesztését.

f) Költségvetési források allokációjának kérdésköre. Az éves költségvetési tervezés során a védelmi kiadások keretein belül a kiberstratégiai cél és eszközrendszerhez igazítva arányosítani szükséges a biztonsággal összefüggő központi költségeket, mind az összvédelmi költségvetés, mind a kibervédelmi költségvetés szerkezetén belül egyaránt. Emellett figyelemmel kell lenni a tagállami finanszírozás során az uniós törekvésekre is. Ehhez kiinduló stratégiai alap lehet, hogy az Európai Unió kiberbiztonsági helyzetének javításáról szóló, 2022. május 23-i tanácsi következtetésekkel összhangban a Tanács felszólította a Bizottságot, hogy terjesszen elő javaslatot egy kiberbiztonsági vészhelyzeti alapra vonatkozóan[92].

Megítélésem szerint ezen témaköröket egy új, változó kiberbiztonsági környezetben stratégiai alapvetésként célszerű és szükségszerű kezelni annak érdekében, hogy változó környezet változó kihívásaira tekintettel a jogalkotás megfelelő választ adjon.

[92] Kiberbiztonság: hogyan kezeli az EU a kiberfenyegetéseket? https://www.consilium.europa.eu/hu/policies/cybersecurity/#challenges – letöltés ideje: 2023.05.15.

5. Zárszó

Az elmúlt időszak biztonsági eseményeinek hatására és az Európát ért változó intenzitással és kiterjedtséggel rendelkező kibertámadások eredményeképpen felértékelődött és aktuális témává vált szakpolitikai és politikai szintéren egyaránt a kiberbiztonság. Ennek egyik eredménye, hogy a tagállamok és az unió egyaránt stratégia szintre emelte a kérdés- és problémakört, azonos szintű válaszokat szorgalmazva. Alapvetésként került meghatározásra, hogy a kiberbiztonság területére vonatkozó stratégiaalkotás uniós és nemzeti színtere egymással szoros összefüggésben van. A megváltozott uniós irányok, új irányelvek, rendeletek a tagállamok részéről jogalkotási kötelezettségeket keletkeztetnek, ezáltal meghatározzák az aktuális mérföldköveket és az egységes kereteket. Olyan kérdéskörök kerültek a végrehajtás szintjére, mint a sebezhetőség, az ellenálló- és a reagáló képesség. Az elkövetkezendő időszakban megalkotásra kerülő tagállami stratégiáknak az uniós jogi normák által előírt kötelező tartalmi elemek mellett fenti kérdésköröket és nemzeti sajátosságaikat egyaránt tartalmazniuk kell. A kibertérből érkező fenyegetések nem ismernek országhatárokat, észrevétlenül, a másodperc tört része alatt tudják elektronikus információs rendszereinket, létfontosságú rendszerelemeinket működésképtelenné tenni, amely elhárítására a felkészülést megkezdeni és a biztonság iránti elköteleződést rögzíteni a lehető legmagasabb szintű tervdokumentumok körében kell kezdeni. Stratégia nélkül tehát nem megy és ahogy azt fenti mottó is szemlélteti a stratégiát folyamatszemlélettel kell kidolgozni és megérteni.

Irodalomjegyzék

1. A hálózati és információs rendszerek biztonságára vonatkozó Stratégia – URL: https://nki.gov.hu/wp-content/uploads/2020/11/Strat%C3%A9gia-a-h%C3%A1l%C3%B3zati-%C3%A9s-inform%C3%A1ci%C3%B3s-rendszerek-biztons%C3%A1g%C3%A1ra.pdf – letöltés ideje: 2023.05.15.
2. Bodó Attila Pál – Haddad Richárd – Marsi Tamás - Pongrácz Péter: Kritikus információs infrastruktúrák védelme – Nemzeti Közszolgálati Egyetem 2019
3. John L. Thompson: Strategic Management – International Thomson Business Press, London 1997.
4. Kiberbiztonság: hogyan kezeli az EU a kiberfenyegetéseket? - az Európai Unió kiberbiztonsági helyzetének javításáról szóló, 2022. május 23-i tanácsi következtetések – URL: https://www.consilium.europa.eu/hu/policies/cybersecurity/#challenges – letöltés ideje: 2023.05.15.

Jogszabályok:

Letöltés helye és ideje: https://njt.hu/ (2023.05.15.) és https://eur-lex.europa.eu (2023.05.15.)

1. a kormányzati stratégiai irányításról szóló 38/2012. (III. 12.) Korm. rendelet
2. Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat
3. Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III.21.) Korm. határozat
4. Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat
5. 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról - Biztonságos Magyarország egy változékony világban
6. az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
7. a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény
8. a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény
9. a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016. július 6-i 2016/1148 (EU) európai parlamenti és tanácsi irányelv
10. az Európai Parlament és a Tanács (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
11. az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről
12. a Tanács ajánlása (2022. december 8.) a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről (2023/C 20/1)