Farkas Ádám – Gosztonyi Gergely –
Szabó Hedvig – Vikman László

A kibertér katonai és nemzetbiztonsági vonatkozásainak egyes szabályozási kapcsolódásai

Military and Intelligence CyberSecurity Research Paper
2024/3.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

BEVEZETÉS[1]

Jelen tanulmány a Katonai Nemzetbiztonsági Szolgálatnál 2022 óta zajló Tématerületi Kiválóság Program keretében elvégzett multidiszciplináris kutatások zárásának apropóján tekint ki azokra a főbb területekre, amelyek kontextusában a kibertér a katonai és nemzetbiztonsági vonatkozásokkal szabályozási szempontból aktuálisan összekapcsolódik.

A szerzők személye és affiliációja jól tükrözi a kutatás és a téma azon sajátosságát, hogy a civil-állami, nemzetbiztonsági szakmai és jogi-kormányzástani vonatkozásokat úgy kapcsolja össze, hogy a biztonsági érdekek, a technikai újdonságok, a szabályozási nehézségek és a szükségszerű korlátok és aggályok egyaránt megjelenítésre kerüljenek. Meggyőződésünk ugyanis, hogy hosszú távon is konstruktív, fejlődést hozó és eredményességet biztosító keretek csak ezzel a metodikával biztosíthatók e területen.

Az infokommunikáció robbanásszerű fejlődése, a kibertér jelentőségének reálisan nehezen átlátható felfutása a személyes, társadalmi, gazdasági, innovációs és információ-áramlási viszonyokban magától értetődő módon együtt jár a biztonsági kapcsolódások értelmezésének kihívásával és a megfelelő reagálás kialakításával. Az, hogy a hagyományos bűnözés[2] és a hadviselés[3] is alkalmazkodott a kibertér nyújtotta lehetőségekhez, nem meglepő történelmi távlatokban. Az sem, hogy egy ilyen innováció hatással van a társadalmi, gazdasági és politikai működésre is. Az azonban már figyelmet érdemlő, hogy e változások kiterjedése olyan mértékű, ami korszakos változást sejtet és még olyan fenyegetésformák kapcsán is markánsan értelmezhető, mint a terrorizmus önmagában is problémás és szabályozási nehézségekkel küzdő jelensége[4].

---

[1] A TKP2021-NVA-24 azonosítószámú projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a Tématerületi Kiválósági Program 2021 - Nemzetvédelem, nemzetbiztonság pályázati alprogram finanszírozásában valósult meg.

[2] A téma kapcsán lásd: Jon DiMaggio: The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime. San Fransisco, No Starch Press, 2022.; Kiss Tibor (szerk.): Kibervédelem a bűnügyi tudományokban. Budapest, Dialog Campus, 2020.; Nyitrai Endre: A digitális adatok és a modern technikai eszközök jelentősége a kriminalisztikában. Budapest, Ludovika Egyetemi Kiadó, 2025.

[3] Példaként lásd: Christopher Whyte - Brian Mazanec: Understanding Cyber-Warfare. New York, Routledge, 2023.; Peter Kestner: The Art of Cyber Warfare: Strategic and Tactical Approaches for Attack and Defense in the Digital Age. Wisbaden, Springer, 2024.; Kovács László: Hadviselés a 21. században: kiberműveletek. Budapest, Ludovika Egyetemi Kiadó, 2023.

[4] A téma kapcsán lásd: Julia Janson: Terrorism, Criminal Law and Politics: The Decline of the Political Offence Exception to Extradition (Transnational Criminal Justice). New York, Routledge, 2020.; Robert Taylor - Eric Fritsch - Michael Saylor - John Liederbach - William Tafoya: Cyber Crime and Cyber Terrorism. London, Pearson, 2018. Bartkó Róbert: Kritikai észrevételek a terrorcselekmény 2012. évi C. törvény szerinti szabályozásával kapcsolatosan. In: Szoboszlai-Kiss Katalin – Deli Gergely (szerk.): Tanulmányok a 70 éves Bihari Mihály tiszteletére. Győr, Universitas-Győr Nonprofit Kft., 2013., 45-58. o.; Bartkó Róbert: Az Európai Unió és hazánk büntetőpolitikájának helyzete a terrorizmus elleni küzdelemben. Jog Állam Politika 2010/2. szám, 57-71. o.; Bartkó Róbert: Gondolatok a terrorizmus fogalmáról. Belügyi Szemle 2005/6. szám, 75-88. o.; Bartkó Róbert: A

E tanulmány keretei között ennek három dimenzióját ragadjuk meg, melyek egymással is jelentős összefüggéseket mutatnak. Első megközelítésben a nemzetbiztonság tágabb megközelítésére fókuszálunk, amelyben a hálózatos jelleg, a rendszerszemléletű megközelítés és a kooperatív működés követelményei olyan specialitásként jelennek meg, melyeket a kibertér is felerősít, hiszen annak ezek differentia specificá-i. A második megközelítés a magyar nemzetbiztonsági arcélű szabályozás kereteit vizsgálja, aktuális szervezeti sajátosságok és szabályozási cselekmények mentén, összekapcsolódva az első résszel, de a nemzetbiztonság mikroszintjére[5] fókuszálva. A harmadik megközelítés a cenzúra kérdésének megújulására, különösen az online tartalmak biztonsági érdekből történő korlátozásának egyes szabályozási és intézményi kérdéseire tekint ki, hiszen az információs műveletek révén ez a 21. század egyik kulcskérdéseként azonosítható. Végül a tanulmány negyedik része a hálózatbiztonság fejlesztése és a szabályozás kapcsolódásai felől közelít, hiszen a biztonsági megközelítés, a nemzetbiztonsági fellépés lehetősége, a káros tartalmak korlátozása mit sem ér, ha az állami és államközi instrumentumok nem törekednek arra, hogy fejlesszék azokat a működési standardokat, amelyek a rendszerek biztonságos működését erősíthetik.

Természetesen ez a látkép nem teljeskörű, inkább figyelemfelhívó jellegű, azzal a szándékkal, hogy kulcsterületeket jelöljön meg mind nemzetközi, mind pedig hazai viszonylatban a kibertér jelentette kihívások állami-szabályozási reagálása kapcsán, különös tekintettel a nemzetbiztonsági vonatkozásokra, kitekintve egyúttal a nemzetbiztonság nagy rendszerének részét képező katonai sajátosságokra is.

II. A NEMZETBIZTONSÁG TÁGABB ÉRTELMEZÉSE ÉS A KIBERTÉR

A nemzetbiztonság tágabb értelmezésének alapja az Amerikai Egyesült Államok 1947-es National Security Act-je, majd ezzel a national security state, illetve a national security constitution fogalmi rendszereinek[6] kialakulása és előbb angolszász, majd kontinentális elterjedése adja. Ennek esszenciáját a kormányzás politikai dimenziója felől foglalta össze frappánsan Huntington a nemzetbiztonsági politika következő meghatározásával: „A nemzetbiztonsági politika célja az ország társadalmi, gazdasági és politikai intézményei biztonságának erősítése más független országok részéről jelentkező fenyegetésekkel szemben. A nemzetbiztonsági politika elvileg három formában és két szinten létezhet. A katonai biztonsági politika azon tevékenységek programja, amelyet arra terveznek, hogy minimalizálják, vagy semlegesítsék az ország meggyengítésére vagy megsemmisítésére irányuló erőfeszítéseket olyan fegyveres erők részéről, amelyek intézményi vagy területi határain kívül

terrorizmus és a politikai bűncselekmények kapcsolata az 1856-os Belga Merényleti Záradék relációjában. Publicationes Universistatis Miskolciensis Sectio Juridica et Politica 18. 22. 2004., 185-194. o.

[5] A makro és mikro szint szerinti tagolás kapcsán bővebben lásd: Farkas Ádám: Gondolatok a nemzetbiztonság fogalmáról. In: Szakmai Szemle 2020/3., 5-20. o.

[6] Vö.: Paul F. Scott: The National Security Constitution. London, Hart Publishing, 2018.; Douglas T. Stuart: Creating the National Security State. A History of the law that transformed America. Princeton, Princeton University Press, 2008.; Cody M. Brown: The National Security Council. A Legal History of the President's Most Powerful Advisers. Washington, Project on National Security Reform Legal Working Group, 2008.

tevékenykednek. A belbiztonsági politika a felforgatás veszélye ellen veszi föl a küzdelmet – vagyis azon erőfeszítés ellen, amely az állam meggyöngítésére vagy megsemmisítésére irányul a területi vagy intézményi határain belül tevékenykedő erők részéről. A helyzeti biztonsági politika az állam viszonylagos erejének csökkentésére irányuló, a társadalmi, gazdasági, demográfiai és politikai viszonyokban bekövetkező hosszú távú változásokból fakadó lemorzsolódás veszélyével foglalkozik. E politika mindhárom formájának van operatív és intézményi szintje. Az operatív politika a biztonsági fenyegetéssel való szembeszállás céljából tett azonnali intézkedésekből áll. Az intézményi politika azzal a móddal foglalkozik, ahogyan megfogalmazzák és megvalósítják az operatív politikát."[7]

Jól látható, hogy ez a megközelítés egyrészt szorosan összekapcsolja az államszervezési szempontból – irányítási, szabályozási, szervezeti és más szempontból is – elkülönülő fegyveres védelmi ágazatokat, vagyis a honvédelmet, a rendészetet és a nemzetbiztonsági szférát. Ezek mellett azonban biztonsági oldalról – a biztonság komplexitása és folyamatos bővülése miatt okkal[8] – bekapcsol a biztonsági döntéshozatalba és működésbe is olyan területeket, melyek korábban hagyományosan az állam civil szférára mutató, fegyveres szféráktól – háború idejét leszámítva – független hatósági tevékenységével azonosítható. E körben az élelmezés-, a közlekedés-, az energia-, az egészség-, vagy épp az iparbiztonság épp úgy megjeleníthető, mind bármely más olyan terület, amelynek kritikus biztonsági kockázatai összkormányzati hatást válthatnak ki.

Fontos kiemelni azt is, hogy a nemzetbiztonság tágabb, rendszerszerű megközelítése – melynek előképe a honvédelem, illetve azt megelőzően a háborús felkészülés és közigazgatás mindent átható jellege volt – nem csak a biztonság számos dimenziójának összekapcsolása miatt sajátos és szisztematikus, hanem azért is, mert mindezek terén szükségessé teszi a kooperatív és hálózatos működés többszintű fejlesztését. Ez a többszintűség lényegében az állam egészére, sőt annak a civil társadalommal való kapcsolataira is értendő és a katonai megközelítés szerinti (1) harcászati – végrehajtói/szervezeti | mikro –, (2) hadműveleti – szakirányítói/koordinációs | mezo –, valamint (3) hadászati – stratégiai | makro – szintjein is értelmezendő különféle intézményekkel és szabályozási keretekkel.

Ennek a megközelítésnek a szükségszerűségét, sőt megkerülhetetlenségét a komplex biztonság 20. század végi fejlettségi szintje is indokolta, de azt az ágazati önállóságok megóvására törekvés, illetve az átmenetileg a biztonságot kevéssé jelentős területként kezelő transzatlanti politikai víziók háttérbe tudták szorítani. Az információs robbanás, illetve annak hálózatos és lassan mindent átható jellege azonban elodázhatatlanná teszi az ez irányú fejlesztéseket.[9] Ezt a folyamatot jól támasztja alá akár a nemzetközi terrorizmus, akár a

[7] Samuel P. Huntington: A katona és az állam. Budapest, Zrínyi–Atlanti Kiadó, 1994., 8. o.
[8] A téma kapcsán lásd: Barry Buzan – Ole Weaveer – Japp De Wilde: A biztonsági elemzés új keretei. In: Póti László (szerk.): Nemzetközi biztonsági tanulmányok. Budapest, Zrínyi Kiadó, 2006.; Szálkai Kinga – Stepper Péter (szerk.): A biztonság szektorális értelmezése. Új kihívások a kutatás napirendjén. Pécs-Budapest, Publikon Kiadó, 2015.; Roland Dannreuther: Nemzetközi biztonság. Budapest, Antall József Tudásközpont, 2018.
[9] Bővebben lásd: Farkas Ádám – Kelemen Roland: Nemzeti biztonság és kibertér. Budapest, Médiatudományi Intézet, 2023.

szervezett bűnözés, akár a globális egészségügyi válsághelyzet összefonódása a digitalizációval, illetve a különféle gazdasági és információs vonatkozásokkal.

A nemzetközi tendenciákat követve Magyarországon is több lépcsőben megjelent ez a szemléletmód[10], annak kiteljesedése azonban még várat magára. Előbb az átfogó politikai irányítás kereteit jelölte a nemzetbiztonság tágabb megközelítése a Kormány Nemzetbiztonsági Kabinetjével, amelynek a helyét utóbb a Védelmi Tanács vette át. Ez után törekvések voltak ágazati, illetve szakterületi ernyőszervek és koordinációs fórumok kialakítására[11], majd megszületett egy összkormányzati megközelítésű, koordinatív jellegű védelmi-biztonsági szabályozás a COVID-19 járvány árnyékában, de a védelmi szabályozás egészére nézve.[12] Ez utóbbiban a kibertér egy elemként a számos biztonsági dimenzió mellett megjelenik ugyan, de egy valóban rendszerszerű, tehát a különféle területeket logikailag, megközelítésmódban és szabályozásban is összekapcsoló szisztéma kialakítása még előttünk áll.

Magyarországon a tág értelemben vett nemzetbiztonsági – hazai terminológia szerint védelmi-biztonsági – szabályozás jelenleg úgy fest egy átmeneti állapotban van. Egyik oldalról megszületett és fokozatosan fejlődik az összkormányzati szintű szabályozás[13], illetve annak intézményi keretei. Ettől részint függetlenül a politikai irányítás keretei is erősödnek az átfogó nemzetbiztonsági szemlélet oldaláról, hiszen 2022-ben ehhez igazodó tartalommal fejlődött tovább a miniszterelnök nemzetbiztonsági főtanácsadójának korábban létező, de eddig elsősorban hírszerzési fókuszú intézménye[14]. Egyik oldalról tehát indokolt lenne ezeknek az irányoknak az összekapcsolása akár az egységes védelmi-biztonsági kormányzati tájékoztatással, ami a nemzetbiztonsági szolgálatokról szóló törvény 2022-es módosításával a Nemzeti Információs Központ keretei között már lényegében létezik, de értelmezésében még inkább a nemzetbiztonság mikro – szervezeti – szintjére fókuszál. Másik oldalról az is kiemelendő, hogy az összkormányzati szabályozás úgy került be a magyar intézményrendszerbe, hogy nagyrészt érintetlenül hagyta – a kereszthivatkozásokat leszámítva – az ágazati koordinációs, illetve válságszabályozási rendszereket. Természetesen egy átmenet mindenképp szükséges, de a további fejlődéshez megkerülhetetlen lesz a koordinatív keretek felülvizsgálata, megújítása és ez által egy átláthatóbb és jobban tervezhető és működtethető keretrendszer kialakítása.

---

[10] Vö.: Urbán Attila: A koordinációs folyamatok intézményi hátterének evolúciója a magyar nemzetbiztonsági igazgatásban. In: Nemzetbiztonsági Szemle 2020/1., 5-32. o.

[11] Vö.: Farkas Ádám – Kelemen Roland i.m. 2023., 175-179. o.

[12] Ennek bázispontja volt az Alaptörvény kilencedik módosításának részeként a különleges jogrendi szabályrendszer és vele a normál jogrendi védelmi feladatrendszer szabályozásának alkotmányos szintű megújítása, majd egy évvel később a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény elfogadása.

[13] Bővebben lásd: Kádár Pál: A védelmi-biztonság szabályozási reform rendszer alapelgondolásának elemzése és perspektívái. In: Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2022/8.; Farkas Ádám: A védelmi és biztonsági tevékenységek összehangolásáról szóló törvény helye, szerepe a jogrendszerben. In: Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2022/39.

[14] Vö.: A miniszterelnök nemzetbiztonsági főtanácsadójával kapcsolatos kormányrendeletek módosításáról szóló 57/2024. (III. 13.) Korm. rendelet.

Ez utóbbi gondolatkörbe a kibertér és annak biztonsága is beletartozik. Egyik oldalról szükséges lehet az összkormányzati szabályozásban is részletezni az azzal kapcsolatos felhatalmazásokat és intézkedéseket, másik oldalról pedig az ágazati szabályozásokat is indokolt jobban szinkronizálni, mint ahogy jelenleg vannak. A honvédelmi törvény kibertér műveleti szabályai és a nemzetbiztonsági törvény hasonló szabályozása ugyanis bizonyos hasonlóságokat mutat, de jellegében és szellemiségében mégis jelentősen eltér egymástól, miközben az összkormányzati keretekhez való kapcsolódást nem tükrözik. Ezt kiegészítendő, a jövőben vizsgálandó lesz az is, hogy a kiberbiztonsági szabályozás – amely önálló területté fejlődött – hogyan kapcsolható megfelelően a tág értelemben vett nemzetbiztonsági szabályozáshoz, külön kitérve a tanulmányunkban később még tárgyalásra kerülő koordináció kérdéskörére is. Ez a terület ugyanis megkerülhetetlen a biztonság szavatolása szempontjából a 21. században és ha ágazati vagy szervezeti érdekek miatt lényegében teljesen elkülönül az összkormányzati keretrendszertől, akkor jó eséllyel kollíziókat fog generálni a tervezés, az összehangolt fejlesztés majd a reagálás tekintetében is. Ehhez pedig a kiberbiztonság területe mellett fontos bekapcsolni mindazokat a sajátos területeket és szabályozási szegmenseket, amelyek az információs tér biztonságos kiaknázását segíti. Ide értendő tehát a tartalomszabályozás és szükség esetén -korlátozás is, illetve mindazok a hálózatbiztonsági vonatkozások, melyekre a tanulmány a következőkben szintén kitekint.

A tág értelemben vett nemzetbiztonsági szisztéma fejlesztésében tehát még számos tennivaló áll előttünk az információs korszak sajátosságaira figyelemmel. Ehhez a védelmi és biztonsági szabályozási reform az alapokat, a főbb kereteket fektette le, amelyekre a jövőben ráépíthető lenne egy amerikai típusú nemzetbiztonsági szabályozás. Ehhez azonban a pillanatnyi politikai és biztonsági környezeti indikátorok mellett egy komolyabb felkészülés, rendszerszerű megközelítés és a nemzetbiztonság tág értelmezéséhez igazodóan széles spektrumú – ebből következően szükségképpen multidiszciplináris – döntéselőkészítés is szükséges, aminél a társadalmi bázis és bizalom építése, erősítése sem kerülhető meg. Ezt a külföldi minták[15] egyértelműen alátámasztják, a nemzeti ellenállóképesség fejlesztésére való EU és NATO szintű törekvés, illetve annak hazai jogszabályi implementálása pedig keretbe tudja foglalni. Fontos azonban rögzíteni, hogy a döntéselőkészítéseben szükséges lenne egy a nemzetbiztonság tág megközelítéséhez illeszkedő hazai kutató-szakértő képességhálózat és intézményi keretrendszer kialakítása is, mivel a feladat sokrétűsége, perspektivikus és konstruktív kritikai jellege túlmutat a kormányzati igazgatás napi dinamikáján és ágazati tagoltságú szemléletmódján egyaránt. Mindezeket számításba véve pedig fontos, hogy a nemzetbiztonság tágabb megközelítéséhez a szűkebb, tehát a titkosszolgálati eszközökre és módszerekre, illetve a nemzetbiztonsági szolgálatokra és azok szerepére irányuló szabályozást, illetve az erre irányuló kutatásokat is megfelelően kapcsoljuk.

[15] Vö.: Kelemen Roland – Petruska Ferenc – Spitzer Jenő – Vikman László: Nemzetközi minták vizsgálata sz összehangolt válságkezelésre, az arra való felkészülésre és a különleges jogrendi szabályozásra. In: Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2022/30.; Farkas Ádám: A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022., 65-121. o.

III. A KIBERTÉR NEMZETBIZTONSÁGI ARCÉLÚ SZABÁLYOZÁSA MAGYARORSZÁGON

III.1. A KIBERTÉR FEJLŐDÉSÉNEK ALAPHATÁSAI AZ ÁLLAMI-JOGI KERETEKRE

A biztonság területén az információs állam fejlődése, evvel egyidejűleg a jogállamiság erősödése hozzájárultak egy olyan fejlődési irány kialakulásához, amely az állami biztonság garantálásának katonai dominanciájától egy sokrétegű és több ágazatra bontott védelmi rendszer felé való elmozdulást eredményezett.[16] Annak ellenére, hogy a katonai védelem jelentősége ma is vitathatatlan – a fenyegetések sokrétűsége, a védelmi ágazatok közötti szoros együttműködés és a nemzetközi együttműködésben való részvétel miatt – szem előtt kell tartanunk, hogy a rendészet és a nemzetbiztonsági ágazat a biztonság garantálásának letéteményese különösen, hogy intenzív fejlődésen és differenciálódáson ment keresztül a 20. század óta.

A nemzetbiztonsági területek azok, amelyek elsődlegesen érintettek a globalitás és az információs kor új kihívásaiban, miközben a változó, de mégis hagyományait megőrző katonai védelem főszabályként kiegészítő szerepet tölt be.

A megváltozott társadalmi környezet az analóg világon túlmutatva egy új térben, a kibertérben hozott megoldandó biztonsági kérdéseket. A kibertér egy rendkívül komplex, sui generis jelenség, amely mára az életünknek annyira meghatározójává vált, mint a fizikai tér. A kibertér már önmagában is többes jellegű entitásként jelenik meg, ezen belül további, megszámlálhatatlan részt és jelleget öltve. Hiszen egyrészről a kibertér alapjait tekintve fizikai eszközökből álló rendszer, a fizikai egységei is dinamikusan és exponenciálisan növekednek. Az információs-kommunikációs-technológiai infrastruktúra felől közelítve a határai meghatározhatók, a tenger alatti kábelektől, az űrben lévő kommunikációs eszközökön át. Másrészről, ha a biztonsági ágazat oldaláról közelítjük, a kibertér egy állandóan változó fizikai, adat és információs ökoszisztéma, amely olyan lehetőségeket és egyben kihívásokat teremt a társadalom valamennyi szektorában, amelyre a történelem folyamán eddig nem volt példa.

Alapvetően befolyásolja a mindennapokat, olyan felforgató változásokat eredményezve, hogy maga a kibertér tovább evolválódik és az olyan „hétköznapi kérdéseken" túlmutató entitássá válik, amely egyben szimbolikus definíciók sorozatában, eszmék hálózatában is kiteljesedik.[17]

A kibertér kezdeti, szabályozatlan világához képest az államok egyre inkább törekednek arra, hogy befolyásukat kiterjesszék erre a területre is. Ennek egyik, de nem kizárólagos eszköze a jogi szabályozás kialakítása, amelynek kapcsán normaalkotó és normakövető államokról beszélhetünk. Egy a globális kibertér jellegéhez illeszkedő globális kiberszabályozás minden érdekelt fél bevonásával valósulhatna meg.[18] De az egységes szabályozás helyett, a geopolitikai érdekek alapján három fő tábor alakult ki: az egységes kibertér szabályozás koncepciót

[16] Farkas Ádám: Gondolatok a 21. századi biztonságról, államról, védelemről. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA, 28(E-szám) 2018., 241-256. o.
[17] Whittaker, Jason: The cyberspace handbook. Routledge, 2004.
[18] Dornfeld László: A kibertér szabályozási modelljei Európában. geotan.hu

támogató, elsősorban Európai Uniós államok; a nemzeti szuverenitás alapjára helyezkedő autoriter államok (Kína, Oroszország), valamint az egyik irányba sem elkötelezett államok. Így egyelőre a nemzetközi szabályozásra várni kell, hiába globális maga a kibertér. Ennek különösen biztonsági aspektusból van jelentősége, mert a kibertér egy olyan komplex megkerülhetetlen rendszer.

III.2. Kibertér és Magyarország biztonsággal kapcsolatos stratégiái

Ha létezik egy olyan rendszer, amely globális, megkerülhetetlen, folyamatosan evolválódik, akkor az azt eredményezi, hogy a biztonsággal foglalkozó szektoron belül a nemzetbiztonsági ágazattal kapcsolatosan megjelennek mindenhol, így Magyarországon is, azok a kormányzati elvárások, hogy kibertér védelmében aktívan vegyenek részt a nemzetbiztonsági szolgálatok.[19] A nemzetbiztonság fogalmát, nemzetbiztonsági szabályozás kérdését ebben a tanulmányban többnyire a Farkas Ádám-féle felosztás mikroszintjének feleltetem meg és a jelenleg ismert jogi és szervezeti keretek talaján kerül elemzésre a kibertér nemzetbiztonsági kezelésének kérdése.[20]

A szervezeti szint elemzése azt is megmutatja, hogy a magyar állam milyen biztonság percepciót képvisel, ezek milyen feladatokat képeznek le a nemzetbiztonság szervezeti szintjén és melyek lehetnek az állam nemzetbiztonsági prioritásai a kibertér vonatkozásban. Magyarország két biztonsági stratégiája részletesen foglalkozik a kibertér jelentette kihívásokkal és lehetőségekkel, kiemelve a kiberbiztonság fontosságát.[21]

Magyarország Nemzeti Katonai Stratégiája kiemeli, hogy a modern konfliktusoknak jelentős kiberbiztonsági összetevői vannak, azaz egyértelműen deklarálásra kerül, hogy a biztonságot nem csak katonai veszélyek fenyegetik. Emiatt cél a kibervédelmi feladatok integrálása és a kiberhadviselésre való felkészülés, beleértve a védelmi és támadó képességek egyensúlyának megteremtését. A kibertérben végzett műveletek szolgálhatnak a kinetikus műveletek végrehajtásának támogatására, de irányulhatnak a kormányzati informatikai rendszerek, az e-közigazgatás, a közműszolgáltatók, a stratégiai jelentőségű vállalatok, a közlekedési ágazat és más, a gazdaság működése szempontjából fontos ágazat létfontosságú rendszerelemeinek, a társadalom működéséhez nélkülözhetetlen szervezetek digitális hálózatainak megzavarására. A Magyar Honvédség aktívan közreműködik a nemzeti kibervédelmi feladatokban, felkészülve a különleges jogrendi helyzetekben történő feladatvégrehajtásra is. A katonai kibertérműveleti erők, beleértve az offenzív műveleteket is, hozzájárulnak a szárazföldi és légi erők kinetikus műveleteinek hatékonyságához.[22] Ezen képességek támogatják a harci és harctámogató műveleteket, valamint aktívan részt vesznek a nemzeti kibervédelmi feladatokban. A kibertérműveleti képességek biztosítják a kibertérből

[19] Szenes Zoltán: A hibrid fenyegetések elleni szakpolitika Magyarországon. Hadtudomány 31(4), 2021., 39-56. o.
[20] Farkas Ádám: A magyar védelmi és biztonsági szabályozási séma kibertér fókuszú áttekintése. Nemzeti Biztonság és Kibertér Médiatudományi Intézet, 2023., 174-192. o.
[21] Magyarország Nemzeti Katonai Stratégiájáról 1393/2021. (VI. 24.) Korm. határozat.
[22] Kovács László: Hadviselés a 21. században: kiberműveletek. Budapest, Ludovika Kiadó, 2023.

érkező fenyegetések és veszélyek azonosítását, hatékony kezelését, valamint az azokkal kapcsolatos válaszlépések és ellenintézkedések végrehajtását. A kibertérben végrehajtott műveletek támogatják a hagyományos katonai műveleteket, beleértve a felderítést, a stratégiai kommunikációt és az információs hadviselést.

A Katonai Stratégia elemzéskor megállapíthatjuk, hogy a kibertér kérdésében nemcsak a katonai, hanem a polgári aspektus is megjelenik. A stratégia megerősíti, hogy a kibertérben végzett műveletek fontos szerepet játszanak a nemzetbiztonság egészében és a kiberbiztonság nemzeti jelentőségű, amely túlmutat a szigorúan vett katonai aspektusokon. A nemzeti ellenállóképesség (reziliencia) fejlesztése különösen fontos a komplex és kiszámíthatatlan biztonsági környezetben. A rezilienciába értendőek a kritikus fontosságú rendszerek működésének biztosítása. Továbbá elvárásként jelenik meg a polgári képességek támogatása, polgári felkészültség fejlesztése és a civil-katonai együttműködés erősítése.

Magyarország Nemzeti Biztonsági startégiája megerősíti a kibertér jelentőségét átfogó feladatként meghatározva, a kibertérből érkező fenyegetésekre való megfelelő reagáló képességet és a nemzeti létfontosságú információs infrastruktúra védelmét.[23] Ennek érdekében alapvető feladat a kibertérben jelentkező kockázatok azonosítása és nyomon követése, ami magában foglalja a fenyegetések folyamatos monitorozását és elemzését. Ehhez elengedhetetlen a kormányzati koordináció erősítése, amely biztosítja az érintett kormányzati szervek hatékony együttműködését és információmegosztását. A kibertér jogi szabályozásának fejlesztése szintén központi szerepet játszik a stratégiai célok elérésében. Az átfogó és korszerű jogi keretek megteremtése hozzájárul a kiberbiztonsági intézkedések hatékonyságának növeléséhez és a jogszerűség biztosításához. A felhasználók biztonságtudatos viselkedésének elősegítése érdekében szükséges a lakosság és a szervezetek kiberbiztonsági ismereteinek bővítése, valamint a biztonságtudatosság növelése. Ennek érdekében edukációs programokat és kampányokat kell indítani, amelyek célja a megfelelő biztonsági gyakorlatok elterjesztése. A kormányzati infokommunikációs rendszerek, a nemzeti létfontosságú információs infrastruktúra, a minősített információk és a nemzeti adatvagyon védelmének erősítése kiemelt fontosságú. Ennek érdekében szükséges a technikai és szervezeti védelmi intézkedések folyamatos fejlesztése és korszerűsítése. A kiberbiztonsággal kapcsolatos nemzetközi együttműködés bővítése szintén elengedhetetlen. Magyarország aktívan részt vesz a globális kibertérben való felelősséget szabályozó normák és a globális kiberbiztonság fokozására szolgáló bizalomerősítő intézkedések kidolgozásában és végrehajtásában.

Végül, Katonai Stratégia mellett a Nemzeti Biztonsági Stratégiában is alapvető stratégiai cél kibertérben alkalmazható offenzív képességek kiépítése és fejlesztése, amely magában foglalja a Magyar Honvédség kibervédelmi és kiberműveleti erőinek folyamatos fejlesztését, hogy képesek legyenek hatékonyan támogatni a haderő kinetikus műveleteit és reagálni a kibertérből érkező támadásokra.

Ezek az intézkedések együttesen biztosítják Magyarország kiberbiztonsági képességeinek megerősítését és a kibertérből érkező fenyegetések hatékony kezelését,

[23] Magyarország Nemzeti Biztonsági Stratégiájáról 1163/2020. (IV. 21.) Korm. határozat.

hozzájárulva a nemzetbiztonság magas szintjének fenntartásához. Egyben iránytűként szolgálnak, hogy lássuk az állam elvárásait a biztonsági feladatok vonatkozásában.

Az államnak - a két stratégiai dokumentuma alapján is - a kibertérrel kapcsolatos elvárásai jól behatárolhatóak, hogy ebből mennyi feladat kerül delegálásra a nemzetbiztonsági szolgálatoknak megmutatja, hogy a kibertérrel kapcsolatos biztonsági kihívások mennyire válnak összetett kezelést igénylő feladattá.[24]

III.3. Kiberbiztonsági Ökoszisztéma Magyarországon

A kibertérből érkező biztonsági események kezelése érdekében az egyik elsődleges feladata a kormányzatnak, hogy kialakítsa az a kollaborációs keretrendszert, melynek keretében lehetőség van a kiberbiztonság szereplőinek az egymással való egyeztetésre. A Kormány 2013-ban alkotta meg Magyarország kiberstratégiáját, mely kimondja, hogy Magyarországon „a kibertér szabadságának és biztonságának szavatolása a kormányzat, a tudományos, a gazdasági és a civil szféra közös felelősségvállaláson alapuló, szoros együttműködésével, összehangolt tevékenységével valósul meg”.[25] A kiberökoszisztéma kialakításának egyik indoka kifejezetten nemzetbiztonsági volt, mert „a nemzeti biztonsági szempontok szerinti hatékonyabb gyakorlati alkalmazás, az eszközök megerősítése és hatékonyabb felhasználásának érdekében szükséges egy koherens együttműködési rendszer kialakítása és működtetése a kormányzati és nem-kormányzati szektorok között.” Bár 2013. évi kiberstratégia már idejétmúlt (NIS2 irányelvnek megfelelően, előkészület alatt az új kiberstratégia)[26], de az ökoszisztéma kialakításának megadta az alapját. Ugyanis még ebben az évben megkezdte működését a kollaborációs rendszer két szerve.[27] Stratégiai szinten Nemzeti Kiberkoordinációs Tanács működik, amelynek nemzetbiztonsághoz való kötődése, hogy a Nemzetbiztonsági Szakszolgálat (NBSZ) főigazgatója vezeti. Szervezetében az állandó tagokat a miniszterek jelölik ki, míg a Tanács munkáját segítők között több, egyéb állami szerv vezetői által kijelölt tag kap helyet.[28] A Koordinációs Tanács nemzetbiztonsági szerepét erősítheti, hogy a Katonai Nemzetbiztonsági Szolgálat főigazgatója – külön megjelenítve - is az állandó tagok közé tartozik, azonban a többi nemzetbiztonsági szolgálat nem delegál tagot a testületbe.

---

[24] Cavelty, Myriam Dunn - Egloff, Florian J.: The politics of cybersecurity: Balancing different roles of the state. St Antony's International Review.15(1) 2019., 37-57. o.

[25] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról 1139/2013. (III. 21.) Korm. határozat.

[26] Az Európai Parlament és a Tanács 2022. december 14-I (EU) 2022/2555 Irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/Eu rendelet és az (EU) 2018/1972 Irányelv módosításáról és az (EU) 2016/1148 Irányelv hatályon kívül helyezéséről (NIS2 Irányelv).

[27] A Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről484/2013. (XII. 17.) Korm. rendelet.

[28] Állami Számvevőszék, Magyar Nemzeti Bank, Nemzeti Adatvédelmi és Információszabadság Hatóság, Nemzeti Hírközlési és Informatikai Tanács, Nemzeti Média- és Hírközlési Hatóság, Magyar Energetikai és Közmű-szabályozási Hivatal.

A Tanács feladata a kormányzati tevékenység koordinációjának elősegítése és a végrehajtás figyelemmel kísérése. A Tanács nagy mozgástérrel rendelkezik a különböző kibertér vonatkozású kérdések kezelésében és a Tanács lehetőségeit mutatja, hogy „soft law" kiadására is van lehetősége, így jogi kötelező erővel nem rendelkező ajánlásokat adhat ki a kibertámadások kezelése és az elektronikus információbiztonság területén alkalmazandó legjobb gyakorlatokról. Az ökoszisztéma befolyásoló képességét tovább erősíti az a kötelezettsége, hogy Nemzeti Kiberbiztonsági Akciótervet kell készítenie és éves szinten felülvizsgálnia, továbbá a Tanács munkájáról legalább félévente be kell számolnia a Miniszterelnöki Kabinetirodát vezető miniszternek.

A Tanács koordinációs tevékenységét, valamint döntéseinek végrehajtását a Nemzeti Kibertér Munkacsoport és a Nemzetközi és Európai Uniós Kibertér Munkacsoport segíti.

A Kiberbiztonsági Fórum lehet az igazi ökoszisztéma teremtő szervezet, mert az akadémiai és a magánszféra szakmai véleményének kormányzati döntéshozatalba történő becsatornázásnak szervezetéül szolgál, amelynek szakmai koordinálását a kiberkoordinátor látja el.

A szervezetek működéséről és tevékenységéről nem állnak rendelkezésre nyilvánosan hozzáférhető információk, emiatt a kiberbiztonság erősítésének legegyszerűbb útja lehetne, ha a Tanács által hozott „legjobb gyakorlatokról" szóló ajánlások megismerhetőek lennének, valamint rendszeres és mindenki számára hozzáférhető jelentések készülnének a kiberbiztonsággal kapcsolatos információkról. A „legjobb gyakorlatok" ajánlásai közvetlenül hasznosíthatóak lennének valamennyi szervezetben. A Kiberbiztonsági Fórum (esetleg a Nemzeti Kiberkoordinációs Tanács minősített adatot nem tartalmazó) munkájáról és döntéseiről készült jelentéseket nyilvánosan hozzáférhetővé lehetne tenni, hogy az érintettek tájékozódhassanak a kibervédelem aktuális helyzetéről és a tervezett intézkedésekről. Ez növelni tudná az átláthatóságot és a bizalmat a kiberbiztonsági rendszer iránt, valamint lehetőséget biztosítana az érintettek számára a visszajelzések megfogalmazására és egy iteratív folyamat indulhatna meg, amely úgyszintén előremutató lehetőséget jelentene a kiberökoszisztéma fejlesztésében.

A kiberökoszisztéma állami szereplői 2013-ban kezdték meg - a Kiberbiztonsági Stratégia elfogadásával egyidejűleg - a működésüket.[29] Az elmúlt évtized alatt számos változást élt meg a struktúra, de az állam következetesen végigvitte azt a megoldási módot, hogy elkülönült egymástól az operatív irányításban részt vevő közigazgatási szervezetrendszer és a Kormány munkáját stratégiailag támogató szervek működése.[30] A kibertérrel összefüggő feladatok végrehajtásában a folyamatos centralizáció jelent meg, melynek első állomása 2015-ben történt meg, mikor a hatósági feladatokat végző szerv, az Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH), a szakhatósági feladatokat ellátó hivatal, a Nemzeti Biztonsági Felügyelet (CDMA), továbbá az informatikai biztonsági eseménykezelés, NBSZ

[29] Orbók Ákos. Rövid áttekintés a Nemzeti Kibervédelmi Intézet megalakulásáról, működéséről és előzményeiről. Hadmérnök, X. évf, 2015., 4: 247-251. o.
[30] Kovács Zoltán: Kibervédelem és biztonság. In: Kibervédelem a bűnügyi tudományokban. Budapest, Ludovika Kiadó, 2020., 65-90. o.

(GovCERT) egy irányítás alá került a Nemzeti Kibervédelmi Intézethez (NKI), amely az egyik nemzetbiztonsági szolgálat, a Nemzetbiztonsági Szakszolgálat szervezeti egységeként működik. A következő centralizáció irányába ható intézkedés 2019-ben történt, mikor az Országos Katasztrófavédelmi Főigazgatóság Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (LRL IBEK) feladatok is a Nemzeti Kibervédelmi Intézethez (NKI) kerültek.[31] A Nemzeti Kibervédelmi Intézet látja el az elektronikus információbiztonsági hatóság feladatokat, biztosítva ezzel, hogy mind az állami, mind a magánszektor megfeleljen a biztonsági előírásoknak. A kiberincidensek kezeléséért a Kiberincidens Kezelő Központ (CERT-Hungary) felel, amely foglalkozik a kibertérből érkező fenyegetések kezelésével. Ez a központ az események azonosítása és elemzése mellett koordinálja a válaszintézkedéseket, segítve ezzel a gyors és hatékony reagálást. A sérülékenység vizsgálatokat végző szerv az informatikai rendszerek potenciális biztonsági réseinek feltárásával és a rendszerek védelmi képességeinek tesztelésével foglalkozik. Ezek a vizsgálatok létfontosságúak az esetleges biztonsági hiányosságok azonosításához és a megfelelő védelmi intézkedések kidolgozásához. Emellett, a 2001. évi CVIII. törvény értelmében, bizonyos online szolgáltatásokat – mint például online piactér, internetes keresőszolgáltatás és felhőszolgáltatás – nyújtó szolgáltatóknak bejelentési kötelezettségük van az NKI irányába, valamint az eseménykezelési feladataikat a Nemzeti Kibervédelmi Intézet látja el.[32] A Nemzeti Kibervédelmi Intézet működteti a „nemzeti kapcsolattartó pontot", amely kulcsszerepet játszik az Európai Unión belüli jelentős zavart okozó kiberincidensek kezelésének hazai koordinálásában.[33] Az NKI, mint kapcsolattartó pont fogadja és továbbítja az incidensekkel kapcsolatos jelentéseket a nemzetközi partnerszervezetek felé, erősítve ezzel a nemzetközi együttműködést és információcserét a kiberbiztonsági kérdésekben. [34]

2021-ben azonban a centralizációs tendencia megfordult és a digitális termékek kiberbiztonság tanúsító hatósági feladatait a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) kapta meg. A SZTFH tevékenysége kiterjed a digitális termékek és szolgáltatások kiberbiztonsági tanúsítási folyamatának felügyeletére. Ez magában foglalja az akkreditált megfelelőségértékelő testületek, vizsgálólaboratóriumok, gyártók és forgalmazók ellenőrzését is. Az auditok és egyéb vizsgálatok révén a hatóság biztosítja, hogy a tanúsítványok birtokosai, valamint a megfelelőségi nyilatkozatok kibocsátói megfeleljenek a vonatkozó előírásoknak.

A kibertanúsításról szóló törvény kiterjeszti a SZTFH jogkörét azon vállalatokra és szervezetekre, amelyek a társadalom és gazdaság szempontjából kritikus szolgáltatásokat nyújtanak. Ez magában foglalja azokat a szolgáltatásokat is, amelyek a digitalizáció

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

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

[33] Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 87/2015. (VII. 13.) Korm. rendelet.

[34] Európai Unió (EU) 2019/881 Rendelete.

előrehaladtával váltak nélkülözhetetlenné. A hatóság feladata, hogy ellenőrizze és garantálja ezeknek a szolgáltatásoknak a kiberbiztonsági megfelelőségét.[35]

III.4. KIBERTÉR BIZTONSÁGÁNAK GARANTÁLÁSA: NEMZETBIZTONSÁGI SZEREPLŐK, NEMZETBIZTONSÁGI FELADATOK

A kiberökoszisztéma egyik nemzetbiztonsági szereplőjeként azonosítására került a Nemzetbiztonsági Szakszolgálat, amelynek kibertérrel összefüggő feladatai és hatásköre a nemzetbiztonsági ágazatra vonatkozó jogszabályban (Nbtv.) is megjelennek.[36] Az Nbtv. előírja, hogy az NBSZ az elektronikus információbiztonsággal kapcsolatos feladatokat lát el, kivéve a katonai kibertér műveleteket. Feladatkörébe tartozik az állami és önkormányzati szervek elektronikus információbiztonságának védelme a kibertérből érkező fenyegetésekkel és támadásokkal szemben. Emellett irányítja a kibertérből érkező fenyegetésekre való felkészülést és a kapcsolódó biztonsági feladatokat, a honvédelmi ágazat kivételével. Ezek a tevékenységek a klasszikus információbiztonsággal összefüggő feladatok, amelynek végrehajtását széleskörű hatáskör biztosítja, hogy az NBSZ képes legyen átfogó és hatékony védelmet nyújtani a kibertérből érkező fenyegetésekkel szemben és lehetőséget ad az egységes és összehangolt válaszintézkedések kidolgozására és végrehajtására. Ha a nemzetbiztonság oldaláról vizsgáljuk kijelenthető, hogy ezek a feladatok nem klasszikus nemzetbiztonsági tevékenységek.[37] Az, hogy a nemzetbiztonsági szolgálatok közül miért a Nemzetbiztonsági Szakszolgálathoz kerültek telepítésre ezek a feladat- és hatáskörök, könnyen indokolhatóak az NBSZ szerepével a rendvédelmi és nemzetbiztonsági közösségen belül, mivel az NBSZ a felderítő szervezeteknek nyújt - részben - technológiával összefüggő titkos felderítéshez köthető „szolgáltatásokat”. Az, hogy miért a nemzetbiztonsági ágazathoz kerültek delegálásra ezek a feladatok, magyarázhatóak avval, hogy a kibertér számtalan megoldandó aspektusa közül a biztonsági kérdések a legmarkánsabbak.

A klasszikus információbiztonsági feladatokon túlmutat már az a komoly kihívást jelentő elvárás, mely szerint az NBSZ ellenőrzi – az azon folytatott kommunikáció megismerése nélkül – az elektronikus hírközlési hálózatok forgalmát, észleli a kibertérből érkező fenyegetéseket és támadásokat. Ha párhuzamot keresünk az NBSZ egyéb feladataival, könnyen megtalálhatjuk azt a kizárólag a titkos felderítéshez köthető rendeltetését, mely szerint az NBSZ az elektronikus hírközlési szolgáltatások és az információs rendszerek tekintetében hajt végre információgyűjtést, ha azonban mélyebben vizsgáljuk a két tevékenységet egyértelmű, hogy a kettő között nem sok átfedést találunk. Ez a feladat nem kapcsolódik sem a klasszikus információbiztonsághoz, sem a titkos felderítés technológiai szolgáltatásához, hanem az államok kiberbiztonsági kapacitásépítési feladata közé tartozik. Kiberbiztonsági kapacitásépítés keretében az állam kiépíti saját kiberbiztonsági technológiai rendszereit, amelyek alkalmasak

[35] A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény.
[36] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény.
[37] Börcsök András - Vida Csaba: A nemzetbiztonsági szolgálatok rendszere (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására), Nemzetbiztonsági Szemle 2.1, 2014., 63-100 o.

arra, hogy a kormányzati IKT rendszerek rezilienciáját tudja fokozni. A hálózati forgalom monitorozás, támadások észlelése segíti a proaktív, megelőző jellegű kibervédelem megvalósítását.

Az Nbtv-ben megjelenítésre kerül a kiberbiztonság speciális lehetősége, amely túlmutat a hagyományos megelőzést előtérbe helyező biztonságfelfogáson és egy aktív, eshetőlegesen represszív felhatalmazást kap az NBSZ, avval a feladattal, mely szerint „végrehajtja vagy kezdeményezi a kibertérből érkező támadás megszakításához szükséges intézkedéseket". Ebben a lehetőségben világosan megjelenik az az állami kiberbiztonsági funkció, melyben az állam fenyegető szereplőként tud megjelenni, kibertámadó képesség kialakításával. Elsődlegesen a kibertámadó képesség gyakorlásának sem, a döntések meghozatalának meg végképp nem az NBSZ a fő letéteményese. De az államok a kibertér fejlődésével páhuzamosan katonai, védelmi szempontok alapján eljutottak az elrettentés elvének alkalmazásáig a kibertérben is. Cél itt is az – csakúgy, mint a nukleáris elrettentés esetén – hogy akadályozza a rossz szándékú támadókat a kibertámadások indításában azáltal, hogy visszatartó erejű intézkedésekkel fenyeget.[38] Noha az elrettentés elsősorban akkor lehet hatékony, ha a fenyegetés állami szereplőktől ered, ami a kibertámadások csak egy részére igaz.[39]

Magyarországon a Nemzeti Biztonsági Stratégia tartalmazza az állam különleges szerepét a kibertérben, mely az offenzív képességek kiépítését jelenni. Ennek érdekében előírja, hogy fejleszteni kell a Magyar Honvédség kibervédelmi és kiberműveleti erőit. Magyarország Nemzeti Katonai Stratégiája meghatározza, hogy Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat pedig akár fegyveres támadásnak tekinti, amelyre adott esetben katonai válaszadás is lehetséges.[40]

De visszatérve az NBSZ által végrehajtható, aktív kiberintézkedésről dönteni, azaz a támadást megszakítani, a Kormány által kijelölt személy (nemzetbiztonsági főtanácsadó) döntése alapján lehet. A támadás leállítása után szükséges a további védelmi intézkedések és ország védelmével összefüggő döntések szükségességének felülvizsgálata.[41] Az aktív támadás megszakításához szükséges kiberintézkedés esetén az Nbtv. előírja, hogy intézkedésnek az okozott sérelemmel vagy közvetlen fenyegetéssel arányosnak és szükséges mértékűnek kell lennie, és törekedni kell arra, hogy a támadás megszakításán túli eredményre vagy sérelemre ne vezessen. Bár, ahogy az előbbiekben már megállapításra került, ez a típusú kibertérből érkező támadással összefüggő intézkedés, nem a titkos felderítéssel összefüggő feladat. Ennek ellenére, az intézkedés végrehajtása előtt egy alapvető jogkorlátozással összefüggő teszt elvégzését írja elő a jogszabály. Az Alaptörvényben meghatározott teszt elvégzése akkor

[38] Soesanto, Stefan - Smeets, Max: Cyber deterrence: the past, present, and future. NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice. 2021., 385-400. o.

[39] Ugyanakkor Katonai Stratégia szerint: „Az elrettentés és védelem eszköztára a Magyarországot fenyegető kihívások kezelése során elsősorban azok esetében lehet hatékony, amelyek állami szereplőktől eredeztethetők."

[40] Magyarország Nemzeti Katonai Stratégiájáról szóló 1393/2021 (VI. 24) határozat.

[41] A miniszterelnök nemzetbiztonsági főtanácsadójával kapcsolatos kormányrendeletek módosításáról szóló 57/2024. (III. 13.) Korm. rendelet.

indokolt (egyben kötelező), ha egy intézkedés alapvető jog korlátozását jelentheti,[42] ami egy kibertérből érkező támadás esetén előfordulhat, de vélhetően nem ez a jellemzője.[43] További kötelezettség kibertámadás megszakítása esetén, hogy biztosítani kell az összhangot a nemzetbiztonsági, honvédelmi, bűnüldözési és külpolitikai érdekekkel és törekvésekkel, valamint a külföldről érkező jelentős kibertámadás esetén a foganatosított intézkedésekről és azok okairól tájékoztatni kell a külpolitikáért felelős minisztert a további intézkedések megtétele céljából. Az összkormányzati megközelítés indokolt a kibertérből érkező fenyegetések esetén, különösen, ha azok támadó jellegűek és a megszakítás érdekében intézkedéseket szükséges tenni, az azonban már kétséges, hogy az Nbtv. szabályai elegendőek-e egy valós szituáció megoldására. Felmerül, hogy a katonai aspektus miért csak annyiban kerül megjelenítésre, hogy az NBSZ „a katonai kibertér műveletek kivételével hajtja végre", ezt a feladatot, annak ellenére, hogy (akár külföldről érkező) támadásról beszélünk. Az egyértelmű, hogy az NBSZ-nél megjelenített feladat nemzetbiztonsági vonatkozású, de hogy az Nbtv.-ben, mely elsősorban a nemzetbiztonsági szervezetek jogállását, feladatait és a titkos információgyűjtést szabályozza, indokolt-e a kibertér biztonságának néhány szeletét szabályozni újragondolást érdemel. Kockázatot jelenthet, hogy a jogalkalmazás – jelenlegi szabályozás mellett – bármikor kerülhet olyan helyzetbe, mikor téves döntésekkel nagyobb kárt tud katonai, diplomáciai és gazdasági téren okozni, mint amilyen kárnak az elhárítására törekedett.

A nemzetbiztonsági szféra másik szereplője a Katonai Nemzetbiztonsági Szolgálat, ahol dedikáltan megjelennek a kibertérrel összefüggő feladatok, mely szerint „információkat gyűjt a honvédelmi érdeket veszélyeztető kibertevékenységekről és -szervezetekről, észleli a kibertérből érkező fenyegetéseket és támadásokat, jogszabály keretei között ellátja a honvédelmi ágazat elektronikus információbiztonsági feladatait, biztosítja a honvédelemért felelős miniszter által vezetett minisztérium, valamint a Honvéd Vezérkar tervező munkájához szükséges, kibertérrel összefüggő nemzetbiztonsági jellegű információkat, továbbá kibertér műveleti képességeivel ellátja a honvédelmi érdekek nemzetbiztonsági jellegű védelmét és együttműködik a Magyar Honvédség kiberműveleti erőivel".[44] A jogalkotás meglehetősen vegyes feladatkört szabályozott egy pontban. Láthatunk ebben a rendelkezésben hagyományos hírszerző feladatot (információt szerez), elhárító feladatot (védelmet lát el), tájékoztató feladatot (miniszter, vezérkar tervező munkájához szükséges információkról), de nem marad ki a hatósági információbiztonsági feladat sem. A KNBSZ hatáskörének alapja a hagyományos nemzetbiztonsági tevékenység esetén a honvédelmi érdek, míg az információbiztonsági feladatkörben a honvédelmi ágazat, amely a jogalkotás oldaláról tankönyvszerű megoldás, azonban a hálózatos, konvergáló IKT rendszerek, valamint az információs társadalom világában a jogalkalmazásnak kihívást jelenthet.[45]

[42] Alaptörvény Szabadság és Felelősség 1. cikk (3)
[43] Titkosszolgálati eszközök és módszerek alkalmazása esetén kötelező elvégezni.
[44] Nbtv. 6. §. g)
[45] Castells, Manuel: An introduction to the information age. City, 2(7) 1997., 6–16. o.

A többi nemzetbiztonsági szolgálat feladatkörében kifejezett módon nem jelenik meg a kibertérhez kapcsolódó tevékenység. Ugyanakkor nem lehet figyelmen kívül hagyni, hogy az Alkotmányvédelmi Hivatal feladatai között szerepel a „felderíti és elhárítja a Magyarország függetlenségét, politikai, gazdasági, védelmi vagy más fontos érdekét sértő vagy veszélyeztető külföldi titkosszolgálati törekvéseket és tevékenységet, felderíti és elhárítja a Magyarország tudományos-technikai, biztonságát veszélyeztető leplezett törekvéseket."[46] Az Információs Hivatal „megszerzi, elemzi, értékeli és továbbítja a kormányzati döntésekhez szükséges, a külföldre vonatkozó, illetőleg külföldi eredetű, a nemzet biztonsága érdekében hasznosítható információkat, felderíti a Magyarország függetlenségét, politikai, gazdasági vagy más fontos érdekét sértő vagy veszélyeztető külföldi titkosszolgálati törekvéseket és tevékenysége, továbbá Magyarország érdekeinek érvényesítését szolgáló tevékenységet folytat, felderíti az ország gazdasága biztonságának és pénzügyi helyzetének veszélyeztetésére irányuló külföldi szándékokat és cselekményeket."[47]

Mindezen rendelkezések alapján, noha dedikáltan nem jelenik meg a kibertérrel összefüggő feladatkör, mind a két szolgálatnak lehetősége, mi több kötelessége, hogy részt vegyen a kibertér „nemzetbiztonsági védelmében". Erre utal az a rendelkezés is, mely szerint „a nemzetbiztonsági szolgálatok külső engedély alapján a kibertérből érkező fenyegetés elhárítása céljából az információs rendszerbe beavatkozhatnak".[48] Ebből a rendelkezésből egyenesen le lehet vezetni a szolgálatok hatáskörét a kibertér feladatokra. Az egyértelmű, hogy ez a rendelkezés - hasonlóan az NBSZ felhatalmazásához - a legerősebb kibertérben végzett tevékenységre ad felhatalmazást, mert az állam kibertérben megnyilvánuló fenyegető szerepéhez kapcsolódóan ad jogosultságot.

IV. AZ INTERNET SZABÁLYOZÁS KIHÍVÁSAI ÉS EGYES MEGOLDÁSAI

Az internet térhódítása alapvetően átalakította a kommunikációs szokásokat, a társadalmi kapcsolattartást, a gazdasági működést és a politikai véleménynyilvánítást is. A kétezres években láthattuk az internet kapcsán, hogy (1) megjelent egy jelentős számú, immár aktívan részt vevő felhasználó, (2) megszülettek azok az alkalmazások, amelyek ezen felhasználók véleménynyilvánítási igényeit képesek voltak kiszolgálni (elsősorban természetesen a közösségi médiát értve ezen), és (3) mindezek körül az első időszakban egy szinte légüres jogi tér lebegett. A hálózat nyújtotta globális szabadság ugyanakkor új jogi problémákat szült: a véleménynyilvánítás szabadsága, a dezinformáció elleni küzdelem és az állami-, illetve a platform-cenzúra kérdései mára központi témákká váltak az internetes szabályozásban. Az új média teljesen átalakította az életünket: mind a privát életet, mind a közösségi életet, és a változás ekkora mértékére senki nem volt felkészülve. „A korai hozzászólók megkérdőjelezték, hogy a kormányok miként reagálnak az internet elterjedésére, és hogy kialakul-e az internet

[46] Nbtv. 5. §.
[47] Nbtv. 4. §.
[48] Nbtv. 56. §. e)

irányításának nemzetközi megközelítése."[49] Ráadásul ki kell emelni, hogy míg az internet az Amerikai Egyesült Államokban született, és az alapja a szólásszabadság és a magánszféra legteljesebb körű biztosítása volt, Európában még csak-csak elfogadták ezeket (bár módosításokkal), de az internet hamarosan elterjedt olyan (jogi) kultúrákban is, ahol mindezen értékeknek más a fokmérője.

Így tehát a jogi kihívás többdimenziós: egy olyan, immár milliók és milliárdok által – több kontinensen – használt tömegkommunikációs eszközt kell jogi keretek közé szorítani, amit (alapvetően) amerikai megközelítést alkalmazó (többnyire) amerikai cégek működtetnek és tulajdonolnak, és olyan (jogi) kérdések kezelésére kell vállalkozni, amelyekre az eltérő jogi kultúrák (de akár hasonló jogi kultúrájú országok között egyes eltérő jogszabályok) eltérően reflektálnak. Ezáltal a szabályozó államok könnyen találhatták magukat olyan helyzetben, amikor a szabályozás tárgyát csak „különböző és olykor átfedő szinteken: a helyi szinttől a nemzetek feletti és globális szintig"[50] lehetett értelmezni. Így „a hagyományos szabályozás vertikális, központosított és államalapú módszereit kiegészítik az együttműködő horizontális elrendezések, amelyek „egymásra épülő struktúrák komplex ökológiájához" vezetnek, „a formális és informális mechanizmusok széles skálájával, amelyek sokféle helyszínen működnek".[51]

A kétezres évek közepére a politikai szereplők és az általuk vezetett államok már nem nézhettek többet félre: nem engedhették meg, hogy folytatódjon a közösségimédia-cégek által végzett úgynevezett „privatizált" szabályozás, azaz az állam szabályozási igényének kiszervezése. Ahogy Jack M. Balkin fogalmazott: „Ezt megértve, az országok kidolgozták a véleménynyilvánítás szabályozásának új technikáit. Nemcsak közvetlenül a megszólalókat célozzák, hanem a magánkézben lévő infrastruktúra tulajdonosait is, azt remélve, hogy rákényszeríthetik vagy felkérhetik őket arra, hogy az állam helyett ők szabályozzák a szólásszabadságot."[52]

Az Európai Unió (a továbbiakban: EU) és Magyarország egyaránt szembesült e kihívásokkal az elmúlt években, így az internetes szolgáltatások szabályozása Európában sem volt problémamentes. A kilencvenes évek végére formális megkülönböztetés alakult ki a hagyományos médiaszolgáltatások között, amelyeknél a szolgáltató határozza meg a tartalom fogyaszthatóságának idejét és az internetalapú szolgáltatások között, ahol a fogyasztó határozhatja meg mindezt. Ennek alapján született meg az „információs társadalommal összefüggő szolgáltatások" fogalma, amely 2000. június 8-a – az elektronikus kereskedelemről

[49] Paslawsky, Alexandra: The Growth of Social Media Norms and Government's Attempts at Regulation. Fordham International Law Journal. 2017/5. sz., 2017., 1487. o.
[50] Raboy, Marc – Padovani, Claudia: Mapping Global Media Policy: Concepts, Frameworks, Methods. Communication, Culture & Critique. 2010/2. sz., 2010., 162. o.
[51] Hintz, Arne: Social media censorship, privatized regulation, and new restrictions to protest and dissent. In: Dencik, Lina – Leistert, Oliver (szerk.): Critical Perspectives on Social Media and Protest: Between Control and Emancipation. London, Rowman & Littlefield, 2015., 111. o.
[52] Balkin, Jack M.: Szólásszabadság az algoritmusos társadalomban. A big data, a magánszabályozás és a véleménynyilvánítás szabályozásának új iskolája. In Medias Res, 2018/2, 2018., 199. o.

szóló irányelv (Eker. irányelv)[53] elfogadása – óta eltelt húsz év egyik kulcsfogalmává vált. Az EU és tagállamai különös figyelmet fordítanak arra, hogy az alapvető jogok, köztük a véleménynyilvánítás szabadsága érvényesüljön, miközben fellépnek a káros tartalmakkal, például az álhírekkel és a gyűlöletbeszéddel szemben. Az ilyen típusú tartalmakat megtalálni az adatok rengetegében nem könnyű feladat, és ezt nehezíti, hogy az Eker. irányelv 15. cikkében foglaltak szerint[54] a tagállamok nem állapítanak meg a szolgáltatókat terhelő olyan általános kötelezettséget, amely alapján *a)* az általuk továbbított vagy tárolt információkat nyomon kellene követniük, vagy amely szerint b) a jogellenes tevékenységre utaló tényeket vagy körülményeket kellene kivizsgálniuk („általános monitorozási vagy nyomonkövetési kötelezettség tilalma").[55] Ez a szabály tehát nem kötelezi a szolgáltatókat, és így a közösségi médiát sem arra, hogy folyamatosan nyomon kövessék a rájuk felkerülő tartalmakat.[56]

A fentebb vázolt többdimenziós jogi kihívás abban rejlik, hogy egyszerre kell:

- biztosítani az internet szabad használatát,
- garantálni a véleménynyilvánítás szabadságát,
- megvédeni a társadalmat a manipulációtól, álhírektől és káros dezinformációtól, és
- szabályozni a nagy technológiai platformok hatalmát, anélkül, hogy azok önkényes privát cenzúrához folyamodjanak.

A fenti folyamatban egyre nyilvánvalóbbá vált minden résztvevő számára, hogy az egységes európai piac szabályrendszerét a digitális térbe is szükséges átültetni. Ez egyfajta az aktív, kezdeményező szerepbe helyezteaz Európai Uniót, amivel „az internet történetében először tereli az erőviszonyokat az Egyesült Államoktól és Európa felé".[57] Ugyanakkor a probléma, amivel szembesülni kellett, hogy „az elektronikus kereskedelemről szóló irányelv végrehajtásának módja az EU-ban nagyon eltérő, és hogy az online felelősségre vonatkozó nemzeti ítélkezési gyakorlat ma továbbra is nagyon széttagolt".[58] Mindezt tetézi a „jó szamaritánus paradoxon"[59] is, azaz az a gyakorlat, hogy a platformszolgáltatók inkább passzívak

[53] Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (elektronikus kereskedelemről szóló irányelv), Hivatalos Lap L 178, 17/07/2000, 0001–0016.

[54] Oster, Jan: European and International Media Law. Cambridge, Cambridge University Press, 2017. 234–236. o.

[55] Ki kell ugyanakkor hangsúlyozni – ahogy a későbbi bírósági joggyakorlat is foglalkozott vele –, hogy az Eker. irányelv 47. cikke kijelenti, hogy mindez „nem érinti azonban az egyedi esetben alkalmazandó nyomon követési kötelezettségeket".

[56] Van Hoboken Joris et al.: Hosting intermediary services and illegal content online. An analysis of the scope of article 14 ECD in light of developments in the online service landscape: final report. Luxembourg, European Commission, 2018., 45–47. o.

[57] Reynolds, Matt: The strange story of Section 230, the obscure law that created our flawed, broken internet. Wired, Elérhető: https://www.wired.co.uk/article/section-230-communications-decency-act

[58] Madiega, Tambiama: Reform of the EU liability regime for online intermediaries. Background on the forthcoming Digital Services Act. European Parliamentary Research Service, Elérhető: https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRSIDA(2020)649404EN.pdf

[59] Strömback, Per: Good Samaritan Paradox Paradox. Netopia, 2020. Elérhető: http://www.netopia.eu/good-samaritan-paradox-paradox

maradnak, mert aktivitásuk esetén elveszítik a felelősség alóli mentesülés lehetőségét. Egy ennyire gyorsan változó piacon azon szabályozási megoldások, amelyek 2000-ben előremutatónak tűntek, huszonpár év alatt már sokszor elvesztik relevanciájukat.

Az Európai Unió jogrendszere pedig csak fokozatosan reagált ezekre a kihívásokra. E korábbi modell ugyan ösztönözte az internetes innovációt, ám a 2010-es évek közepére világossá vált, hogy a nagy platformok – különösen a közösségi média szolgáltatók – olyan gazdasági és társadalmi hatalomra tettek szert, amely új szabályozási megközelítést igényel. Ennek eredményeként az Európai Unió 2022-ben elfogadta a Digitális szolgáltatásokról szóló rendeletet[60] (a továbbiakban: DSA) és a Digitális piacokról szóló rendeletet[61] (a továbbiakban: DMA). Az első szembetűnő jogi különbség a terület korábbi szabályozásához képest, hogy – a GDPR megoldásával analóg módon – nem irányelvként, hanem rendeletként léptették életbe azt. A DSA (egyik) központi eleme az online óriásplatformok (VLOP-ok) eltérő szabályozása.[62] E platformok kötelesek rendszeres kockázatértékeléseket végezni, a kockázatcsökkentés érdekében megfelelő intézkedéseket tenni, átláthatósági jelentéseket közzétenni, és biztosítani kell a felhasználók számára a döntéseik elleni hatékony jogorvoslati lehetőségeket. A rendelet külön hangsúlyt fektet az algoritmusok átláthatóságára és a tartalommoderálási gyakorlatok elszámoltathatóságára.[63] A DSA célja, hogy harmonizált szabályokat hozzon létre a digitális szolgáltatások működésére vonatkozóan, különös figyelemmel az illegális tartalmak eltávolítására, a platformok átláthatóságára, valamint a felhasználók jogainak védelmére. A DMA kapcsolódó központi eleme pedig a kapuőr fogalma, amely olyan szolgáltatókat takar, amik jelentős hatást gyakorolnak a belső piacra, állandósult és tartós pozíciót élveznek, és emellett legalább egy alapvető platformszolgáltatást működtetnek.[64] E szolgáltatókra ugyanúgy emelt szintű kötelezettségek vonatkoznak.[65] Ahogy Török Bernát megfogalmazta: „az elsődleges szabályozási cél: a szolgáltatónak felelősséget kell vállalnia azokért az aspektusokért, amelyekben kialakítja a saját felületén a kommunikáció szerkezetét, és ahogyan irányít bennünket a szükségszerűen korlátozott befogadású túlburjánzó tartalmak között.”[66] Az audiovizuális médiaszolgáltatásokról szóló irányelv[67] (a továbbiakban: AVMS) 2018-as

[60] Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet), PE/30/2022/REV/1, HL L 277., 2022.10.27., 1–102. o.

[61] Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló rendelet), PE/17/2022/REV/1, HL L 265., 2022.10.12., 1–66. o.

[62] DSA 33. cikk.

[63] DSA 34–42. cikkek.

[64] DMA 3. cikk.

[65] DMA 4–15. cikkek.

[66] Török Bernát (2021): Platforms and Fundamental Rights. Hungarian Conservative. 2021/2. sz.

[67] Az Európai Parlament és a Tanács 2010/13/EU irányelve (2010. március 10.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról (audiovizuális médiaszolgáltatásokról szóló irányelv), HL L 95., 2010.4.15., 1–24. o.

módosítása[68] szintén új követelményeket támasztott a videómegosztó platformokkal szemben, például a gyűlöletkeltő tartalom elleni védelem terén. Ezek az intézkedések azonban sokszor az egyensúlyozás nehézségét mutatják: miközben védik a társadalom sérülékeny csoportjait, fennáll a véleménynyilvánítás túlzott korlátozásának veszélye is.

A szabályozás másik fontos dimenziója a magánszereplők, elsősorban a platformok önszabályozása. Az Európai Bizottság (a továbbiakban: EB) több alkalommal is önkéntes magatartási kódexek megalkotását ösztönözte. Ilyen volt például „A jogellenes online gyűlöletbeszéddel szembeni fellépést szolgáló magatartási kódex”,[69] amelynek elfogadása során az aláírók – többek között – vállalták, hogy a jogellenes gyűlöletbeszédre vonatkozó érvényes bejelentéseket 24 órán belül felülvizsgálják, és az ilyen tartalmat eltávolítják vagy hozzáférhetetlenné teszik. A másik ilyen “A dezinformáció visszaszorítását célzó uniós gyakorlati kódex”[70] volt, amelyben az aláírók által vállalt kötelezettségek között szerepel például a reklámelhelyezések ellenőrzése, a politikai és témafókuszú hirdetések vizsgálata, a szolgáltatások integritása, a tudatos fogyasztói magatartás megerősítése; illetve a kutatói közösség szerepének erősítése. E dokumentumok célja, hogy a platformok proaktívan lépjenek fel a problémás tartalommal szemben, ugyanakkor kritikák érték őket amiatt, hogy nem biztosítanak elégséges jogvédelmet a felhasználók számára.[71]

Az Európa Tanács (Council of Europe, a továbbiakban: CoE) is aktívan részt vesz az internet szabályozására irányuló nemzetközi törekvésekben. A 2022-ben elfogadott CM/Rec(2022)13[72] külön kiemeli, hogy a szabályozásnak tiszteletben kell tartania az Emberi Jogok Európai Egyezményének (a továbbiakban: EJEE) 10. cikkében foglalt véleménynyilvánítási szabadságot. A dokumentum hangsúlyozza, hogy “Ha az internetes közvetítők a véleménynyilvánítás szabadságát korlátozzák, az ilyen korlátozások által közvetlenül vagy közvetve érintett felhasználók számára egyértelmű tájékoztatást kell nyújtaniuk arról, hogy milyen szabályozás alapján korlátozták jogaikat. Az internetes közvetítőknek továbbá olyan időszerű és hatékony jogorvoslati mechanizmusokat kell biztosítaniuk, amelyek lehetővé teszik az érintettek számára, hogy indokolatlan költségek, késedelmek vagy nehézségek nélkül fellebbezést nyújtsanak be. E célból az internetes közvetítőknek egyértelmű iránymutatásokat kell nyújtaniuk a felhasználóknak arra vonatkozóan, hogy miként fellebbezhetnek, és tájékoztatást kell adniuk arról, hogy a fellebbezéseket hogyan és mikor bírálják el. Az internetes

---

[68] Az Európai Parlament és a Tanács 2018/1808 irányelve (2018. november 14.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról szóló 2010/13/EU irányelvnek (audiovizuális médiaszolgáltatásokról szóló irányelv) a változó piaci körülményekre tekintettel való módosításáról. PE/33/2018/REV/1, HL L 303, 28.11.2018, 69–92. o.

[69] Elérhető: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_20_1134/IP_20_1134_EN.pdf

[70] Elérhető: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_21_4945/IP_21_4945_EN.pdf

[71] Douek, Evelyn: The Rise of Content Cartels. New York, Columbia University, 2020.

[72] Recommendation CM/Rec(2022)13 of the Committee of Ministers to member States on the impacts of digital technologies on freedom of expression (Adopted by the Committee of Ministers on 6 April 2022 at the 1431st meeting of the Ministers’ Deputies)

közvetítőknek ezt a rendelkezést az Európa Tanács a tartalomszabályozás önszabályozó és társszabályozó mechanizmusainak hatékony jogi és eljárási keretei felé vezető legjobb gyakorlatokról szóló iránymutatásával összhangban kell végrehajtaniuk."[73] A CoE szerint a platformoknak biztosítaniuk kell az átláthatóságot, a független felülvizsgálati mechanizmusokat, valamint a felhasználók jogorvoslathoz való jogát.

Magyarországon az internet szabályozása több jogi területen valósul meg: a médiaszabályozás, a büntetőjog, az adatvédelem és a polgári jog területén is találunk releváns rendelkezéseket. A legfontosabb törvények közé tartozik az Alaptörvény, amely garantálja a véleménynyilvánítás szabadságát, de meghatározza a korlátait is. Az Alaptörvény IX. cikk (1) bekezdése szerint "Mindenkinek joga van a véleménynyilvánítás szabadságához", ám az alapvető jogok védelme nem abszolút, hiszen a közérdek és más alapvető jogok, például mások jogvédte érdekei vagy a személyes adatok védelme korlátozhatják a véleménynyilvánítás szabadságát. Az Alkotmánybíróság (a továbbiakban: AB) több határozatában is megerősítette, hogy a véleményszabadság a demokratikus társadalom egyik alappillére. 2015-ben az AB kifejezetten kimondta, hogy "a politikai véleményszabadság fókuszában elsősorban maguk a közügyek, nem pedig a közszereplők állnak, a közügyekre vonatkozó szólások mindegyike fokozott védelem alá tartozik",[74] és csak kivételesen, szűk körben korlátozható. 2023-ban az AB elvi éllel kimondta, hogy "a közösségi média felületei olyan fórumot kínálnak a szólás szabadságához és a közügyek szabad vitathatóságához, amely kulcsfontosságú szerepet játszik abban, hogy a közvélemény és a politikusok számára ellenőrizhetővé válhassanak a közhatalmat gyakorlók, illetve a köztisztséget vállalók",[75] ezzel elismerve a közösségi média, mint a demokratikus diskurzus színterének különleges státuszát.

A dezinformáció – különösen a COVID-19 járvány és egyes európai választások idején – új dimenziókat nyitott a szabályozási kérdésekben. Az EU célja, hogy minden egyes tagállam aktívan vegyen részt az álhírek és a dezinformáció elleni küzdelemben, és hogy a platformok maguk is felelősséget vállaljanak a hamis információk gyors eltávolításában. A fentebb említett 2018-as "A dezinformáció visszaszorítását célzó uniós gyakorlati kódex", amelyet az adott év végén a félretájékoztatással szembeni cselekvési terv elfogadása követett.[76] Ebben kiemelik, hogy "a félretájékoztatási akciók (főként azok, amelyeket harmadik országok folytatnak) gyakran a hibrid hadviselés keretei közé illeszkednek, és kibertámadásokkal, illetve hálózatok feltörésével párosulnak. Az adatok szerint a külföldi szereplők egyre gyakrabban folyamodnak félretájékoztatáshoz a társadalmi viták befolyásolása, a társadalom megosztása és a demokratikus döntéshozatali folyamatokba való beavatkozás céljából." Ezzel kapcsolatban négy pillért emeltek ki, ahol az Európai Uniónak teendői vannak:

1. az uniós intézmények képességeinek javítása a félretájékoztatás eseteinek észlelése, elemzése és leleplezése területén;

[73] Uo. 4.5.
[74] 1/2015. (I. 16.) AB határozat, [68].
[75] 3234/2023. (VI. 2.) AB határozat, [38].
[76] Közös lözlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Cselekvési terv a félretájékoztatással szemben. JOIN(2018) 36 final.

2. a félretájékoztatással kapcsolatos koordinált és együttes válaszlépések megerősítése;
3. a magánszektor mozgósítása a félretájékoztatás elleni küzdelem érdekében;
4. tudatosságnövelés és a társadalom rezilienciájának javítása.[77]

A cselekvési terv következtében az uniós országok és intézmények 2019-ben felállították a Gyorsriasztási rendszert[78] (Rapid Alert System, RAS), a dezinformációval kapcsolatos ismeretek megosztása céljából. 2022-ben részletesebb és szigorúbb előírásokkal megerősítették a kódexben foglaltakat,[79] majd 2025-ben az EB hivatalosan is integrálta azt a DSA-ba.[80] A rendelet kötelezi a nagy platformokat arra, hogy hatékonyan kezeljék a jogellenes tartalmakat, például az álhíreket és a gyűlöletbeszédet. A DSA új szabályai alapján az EB gyorsan beavatkozhat, ha egy tagállamban nem működik megfelelően a dezinformációval kapcsolatos szabályozás. A rendelet emellett az átláthatóságot is növeli: a platformoknak nyilvánosságra kell hozniuk, hogyan moderálják a tartalmakat, milyen algoritmusokat alkalmaznak, és hogyan mérik a moderálás hatékonyságát. Ezzel az EU célja, hogy megelőzze az önkényes cenzúrát, és biztosítsa, hogy a véleménynyilvánítás szabadságának védelme a dezinformáció és a gyűlöletbeszéd elleni küzdelemmel egyensúlyban maradjon. Az Európai Unió Bíróságának (a továbbiakban: EUB) ítélkezési gyakorlata is segíti az egységes szabályozás kialakítását. A Glawischnig-Piesczek kontra Facebook Ireland Limited ügyben[81] az EUB kimondta, hogy a közösségi platformok kötelezhetők arra, hogy ne csak a konkrétan kifogásolt tartalmat, hanem az azzal azonos vagy hasonló tartalmakat is eltávolítsák.[82]

Ki kell ugyanakkor emelni elvi éllel, hogy a tartalommoderálás kapcsán az állami szabályozás és a platformok önszabályozása nem mindig egyezik. Míg az államoknak alkotmányos kötelezettségük van a véleménynyilvánítás védelmére, addig a platformok gyakran üzleti érdekek mentén, saját szabályzataik alapján korlátoznak tartalmakat. Ez konfliktushoz vezethet, különösen akkor, amikor politikai véleményeket, kisebbségi hangokat vagy vitatott tényállításokat moderálnak.

A bonyolult (jogi) helyzet kezeléséere a CoE külön ajánlásokat is megfogalmazott a tagállamok számára a tartalommoderálással kapcsolatban. A CM/Rec(2018)2[83] hangsúlyozza, hogy az online tartalommoderáció során is tiszteletben kell tartani az emberi jogokat, különösen a szólás- és véleményszabadságot. Ráadásul az ajánlás megjegyzi, hogy a közvetítő szolgáltatók "valamennyi alkalmazottjának megfelelő alapképzést és folyamatos továbbképzést

[77] Uo. 3.
[78] Elérhető: https://www.eeas.europa.eu/node/59644_en
[79] Elérhető: https://ec.europa.eu/newsroom/dae/redirection/document/87585
[80] Elérhető: https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation
[81] Eva Glawischnig-Piesczek v. Facebook Ireland Limited (C-18/18). ECLI:EU:C:2019:821.
[82] Bővebben lásd: Gosztonyi Gergely: Cenzúra Arisztotelésztől a Facebookig. A közösségi média tartalomszabályozási gyakorlatának komplexitása. Budapest, Gondolat Kiadó, 205–208. o.
[83] Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies)

kell biztosítani az alkalmazandó jogszabályokról és nemzetközi emberi jogi normákról, azoknak a közvetítők szolgáltatási feltételeivel és belső normáival való összefüggéseiről, valamint az esetleges konfliktusok esetén teendő intézkedésekről."[84]

A CoE a CM/Rec(2022)4[85] ajánlásában kiemeli, hogy mind az államok, mind egyes platformok jelentős erőfeszítéseket tettek a dezinformáció elleni küzdelemben, de "ezeknek az intézkedéseknek a demokratikus társadalmakban az információ és ötletek szabad áramlására gyakorolt hatását alaposan meg kell vizsgálni."[86] A CoE álláspontja szerint – a nemzetközi emberi jogi normákkal és joggyakorlattal egyhangúan – a jogsértő tartalmak eltávolítására irányuló intézkedéseknek átláthatónak, arányosnak és jogorvoslattal támadhatónak kell lenniük. Az EU 2023-ban útjára indította az „EU vs Disinfo" kampányt is, amely kifejezetten az orosz dezinformációs kampányok elleni küzdelmet célozza.[87] A kampányban naprakész elemzéseket és tényellenőrzéseket tesznek közzé.

Magyarországon a dezinformáció elleni jogi fellépés erőteljesen a büntetőjogra támaszkodik.[88] A 2024. évi LXIV. törvény alapján 2025. március 1-től módosul a 2012. évi C. törvény a Büntető Törvénykönyvről, amelynek új 332/A. § (1) bekezdése alapján: "Aki nagy nyilvánosság előtt elektronikus hírközlő hálózat útján olyan kifejezést, ábrázolást vagy kép- és hangfelvételt használ vagy tesz közzé, amely beazonosítható személlyel vagy személyekkel szembeni erőszakos a) halált okozó, vagy b) különös kegyetlenséggel elkövetett büntetendő cselekményre irányuló szándékot vagy kívánságot fejez ki, ha súlyosabb bűncselekmény nem valósul meg, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő."

A törvény ugyanakkor nem rendeli büntetni azt, aki a fentieket ismeretterjesztő, oktatási, tudományos, művészeti célból vagy a történelem, illetve a jelenkor eseményeiről szóló tájékoztatás céljából követi el, feltéve, hogy a cselekmény félelemkeltésre nem alkalmas.

Az online környezetben a cenzúra kérdése is élesebben merül fel. A platformok algoritmikus moderációja gyakran vezet átláthatatlan döntésekhez. A DSA új szabályai előírják, hogy a felhasználók számára biztosítani kell az eltávolított vagy korlátozott tartalmakkal szembeni fellebbezési lehetőséget,[89] továbbá a platformok kötelesek indokolni a moderációs döntéseiket.[90] A jövő kihívásai között az állami szabályozás és a platformok globális működése közötti feszültség kiemelt helyet foglal el. Mivel a nagy platformcégek multinacionális szereplők, akik egyszerre több joghatóság alatt működnek, a nemzeti szabályozások gyakran nem bizonyulnak elegendőnek.

---

[84] Uo. 2.3.4.
[85] Recommendation CM/Rec(2022)4 of the Committee of Ministers to member States on promoting a favourable environment for quality journalism in the digital age (Adopted by the Committee of Ministers on 17 March 2022 at the 1429th meeting of the Ministers' Deputies).
[86] Uo. 6.
[87] Elérhető: https://euvsdisinfo.eu
[88] Mezei, Kitti – Szentgáli-Tóth, Boldizsár: Az online platformok használatában rejlő veszélyek: a dezinformáció és a kibertámadások jogi kockázatai. In: Chronowski Nóra (szerk.): Demokrácia-dilemmák. Alkotmányjogi elemzések a demokráciaelv értelmezéséről az Európai Unióban és Magyarországon. Budapest, ELTE Eötvös Kiadó, 2022.
[89] DSA 16. cikk (5).
[90] DSA 17. cikk

Emellett az Európai Unió a mesterséges intelligencia (a továbbiakban: MI) fejlődésével is számol a szabályozás kialakításában. Az EU MI rendelete[91] jelentős mértékben kapcsolódik az algoritmikus tartalommoderáció és a dezinformáció elleni fellépés kérdéseihez. Az EU álláspontja szerint az MI által támogatott moderációs rendszereknek átláthatónak, auditálhatónak és elszámoltathatónak kell lenniük, hogy biztosított legyen az emberi jogok védelme az online térben is.[92]

Összességében megállapítható, hogy az internet szabályozása az Európai Unióban és Magyarországon is folyamatos fejlődésben van. A jogalkotók, az igazságszolgáltatás és a nemzetközi szervezetek – mint az EU, a Coe vagy az EJEB – közös célja, hogy olyan keretrendszereket alakítsanak ki, amelyek egyszerre biztosítsák a véleménynyilvánítás szabadságát és védjék a társadalmat a káros tartalmaktól. Magyarország számára különösen fontos kihívás lesz, hogy a nemzetközi emberi jogi normákkal összhangban, átlátható és jogállami módon fejlessze tovább az internetes szabályozási rendszerét, hiszen szerte a világban pedig egyre több autoriter vagy erősen autoriter jellegű állam próbálgatja az internet határokon átnyúló jellegének és a globális közösségnek határait. A kérdés pedig így az, hogy az államok hagyományos területi szuverenitása milyen mértékben érvényesül és érvényesíthető a kibertérben. Ahogy Pia Hüsch fogalmazott a kérdés kapcsán: "A kibertér egyedi jellemzői még egy újabb nehézségi szintet adnak az állami szuverenitás megértésének kihívásához, így az államok alapvetően nem értenek egyet abban, hogyan közelítsék meg a szuverenitást a kibertérben."[93]

E bonyolult – jogi, politikai és gazdasági szempontokat egyszerre tartalmazó – keretrendszer megalkotása még így várat magára. És bár a Tim Berners-Lee által javasolt[94] világméretű „Internet Magna Carta" megalkotása a különféle kormányzatok eltérő megközelítései miatt nem reális, mindenképpen gondolatébresztő. Ugyanakkor nem válaszolja meg a fő kérdést: kinek kell(ene) lépnie? Az bizonyosnak tűnik, hogy a három főszereplő egyike sem lesz képes a helyzetet egyedül kezelni. Sem az államok – bár a szándék, mint láthattuk, egyre erősebben jelenik meg a részükről –, sem a techcégek, sem pedig a civil szféra vagy a felhasználók. Paulina Wu így írta ezt le: „Bár a magánszereplők önmagukban nem elegendőek

[91] Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2024. július 12.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet), PE/24/2024/REV/1, HL L, 2024/1689, 12.7.2024.

[92] Gyetván, Dorina – Gosztonyi, Gergely: Garanciális elemek az online platformok véleménynyilvánítást korlátozó moderálási gyakorlatával szemben a digitális szolgáltatásokról szóló rendelet (DSA) előtt és után. Magyar Jog, 2025/4. sz., 2025., 226–236. o.

[93] Hüsch, Pia: Error 404: No Sovereignty Analogy Found. In: Golia, Angelo Jr. – Kettemann, Matthias C. – Kunz, Raffaela (szerk.): Digital Transformations in Public International Law. Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden, 2022., 29. o.

[94] Berners-Lee, Tim: We Need a Magna Carta for the Internet. New Perspectives Quarterly. 2014/3. sz., 2014., 39–41. o.

a sikeres szabályozáshoz, őket is be kell vonni a szabályozási folyamatba",[95] azaz a „platformszabályozási háromszög"[96] mindhárom szereplőjének részt kell vennie a folyamatokban. Az állami és az önszabályozást fel kellene váltania vagy ki kellene egészítenie a társszabályozási megoldásoknak.

V. AZ EURÓPAI UNIÓ KIBERBIZTONSÁGI SZABÁLYOZÁSA ÉS ANNAK HATÁSA A MAGYAR KERETEKRE

V.1. A VÁLTOZÓ KIBERBIZTONSÁGI SZABÁLYOZÁS ELŐZMÉNYEI

A 2016/1148 irányelv (NIS) megalkotásakor nagy eredményeket hozott azzal, hogy EU-szinten meghatározta a kiberbiztonság alapvető kereteit, de irányelvi jellegéből fakadóan a benne lévő mozgástér meglehetősen sokféle nemzeti megoldást hozott magával, amelyek mostanra akadályává váltak a folyamatosan romló biztonsági környezet által is megkövetelt magas szintű koordinációnak, és az egyes kérdések nemzeti sajátosságok elismerése melletti, de korreláló megközelítésének. A tágabb hálózatbiztonság és a szűkebb kiberbiztonság szabályozásának fejlődése az új irányelvek unió szintű implementációjával olyan evolúciós lépés, amelynek eredményeként a tagállamok szabályozása egyenszilárdabb, szakmaibb és a kiberfenyegetettségi térkép számos vektorának adekvátabb válaszokat adó lesz.

Hosszú előkészítés után, 2022. decemberében – tekintettel az orosz-ukrán háború tapasztalataira is – a tagállamok kiberbiztonságát alapjaiban meghatározó és alakító új szabályozók jelentek meg: a NIS 2 irányelv[97], és a pénzügyi szféra szempontjából meghatározó „lex specialis", a DORA rendelet[98], valamint NIS 2-vel szorosan együtt mozgó, a kritikus infrastruktúrák/létfontosságú rendszerelemek szempontjából fontos CER irányelv[99]. A már meglévő szabályok újragondolását a fokozó fenyegetésekre hozott nemzeti intézkedések ismételt közös nevezőre hozása, az együttműködés, de egyúttal a szabályozási fókusz kibővítése is magával hozta.

Az állami szféra szempontjából fontos, kiemelkedő újítás, hogy – összhangban egyébként az EU 2020-as kiberbiztonsági stratégiájával, amely a bevezetőjében is említi – uniós szinten bevonta a személyi hatálya alá a közigazgatási szerveket, amelyek ezt megelőzően nem

[95] Wu, Paulina: Impossible to Regulate? Social Media, Terrorists, and the Role for the U.N. Chicago Journal of International Law. 2015/1. sz., 2015., 309. o.
[96] Gorwa, Robert: The Politics of Platform Regulation. How Governments Shape Online Content Moderation. Oxford, Oxford University Press, 2024.
[97] Az Európai Parlament és a Tanács 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2).
[98] Az Európai Parlament és a Tanács 2022/2554 rendelete a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (DORA).
[99] Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (CER).

tartoztak a NIS irányelv alá. Azt is le kell szögezni, hogy az általános kivételszabályt itt is alkalmazta a közösségi jogalkotás, azaz a védelmi, nemzetbiztonsági és rendészeti szervezeteket nem vonta be a szabályozott személyi körbe. Ez azonban nem jelenti azt, hogy önmagában ne lenne pozitív lépés a közszféra bevonása, hiszen a védelmi és biztonsági szervezeteknek alapvető feladata ezen szervezetek védelme, amit egy tervszerű, módszeres és kidolgozott eljárásokkal működő elektronikus információbiztonsági menedzsement tevékenység jobban megalapoz.

Magyarország vonatkozásában a nemzeti jogalkotó ennél évekkel korábban már tett lépéseket a közszférában kezelt elektronikus információs rendszerek és az ezekben kezelt adatok védelme érdekében. Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat 8. pontja már rögzítette, hogy a jelen és a jövő kihívásaihoz igazodva a magyar kibertér nyújtson biztonságos és megbízható környezetet az elektronikus közigazgatás számára, hozzájárulva az állami szolgáltatások innovatív és előremutató fejlesztéséhez. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény preambuluma kihangsúlyozta, hogy a kiberfenyegetések miatt a nemzeti elektronikus adatvagyon, az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága nemzeti érdek. A kormányzati elektronikus szolgáltatások biztonságának növelésével a Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat is részletesen foglalkozott.

V.2. Az új uniós keretek

A NIS 2 irányelvnek való megfelelést a tagállamoknak 2024. október 17-ig kellett biztosítaniuk. Preambulumában reagálva az aktuális fenyegetésekre új elemként az irányelv kiemeli, hogy az ellátási láncokban komoly szerepet játszó kis- és középvállalkozások válnak egyre inkább támadások célpontjaivá, ezért az ő fokozottabb kiberbiztonságuk is fontos cél. Konkrét technikai-műszaki intézkedésekről, mint a kockázatelemzés, eseménykezelés és jelentéstételi-kötelezettség, üzletmenet-folytonosság, ellátási-lánc biztonság és kockázatértékelés, szabályzatok és eljárások, kriptográfia és HR-biztonság a 24. cikk rendelkezik, biztosít kereteket. A beszállítói rendszerek kapcsán a tagállamok felelősségévé teszi, hogy az irányelv hatálya alá tartozó szervezetek, amikor mérlegelik az egyes intézkedések megfelelőségét, figyelembe vegyék az egyes közvetlen beszállítókra és szolgáltatókra jellemző sérülékenységeket, valamint a beszállítóik és szolgáltatóik termékeinek és kiberbiztonsági gyakorlatainak – többek között biztonságos fejlesztési eljárásaiknak – az általános minőségét. A tagállamoknak biztosítaniuk kell, hogy a szervezetek – amikor azt mérlegelik, hogy az említett pontban említett intézkedések közül melyek megfelelők – kötelesek legyenek figyelembe venni a kritikus ellátási láncok vonatkozásában, a tagállamok közötti stratégiai együttműködés és információcsere céljából

létrehozott tagállami együttműködési csoport által elvégzett összehangolt biztonsági kockázatértékelések eredményeit[100].

A 13., 23. és 29. cikk szerinti széles körű értesítési és jelentéstételi kötelezettség valamint információmegosztás szabályozása a határokon átnyúló vagy ágazatközi jelentős események vonatkozásában EU-szintre emeli az eseményekről, kiberfenyegetésekről való értesülést, sőt újításként behozza a majdnem bekövetkezett eseményt is, így a gyártók és beszállítók szempontjából sem mindegy, hogy bármely jelentős biztonságot érintő minőségi probléma nagyon gyorsan közismertté válik, ezzel növelve a hanyag fejlesztés reputációs kockázatait. Az együttműködés lehető legszélesebb körének kialakítása érdekében a nemzeti CSIRT-hálózat, az uniós szintű válságok kezelésére létrejött EU-CyCLONe és a már említett tagállami együttműködési csoport kerül létrehozásra.

A szabványosításról szóló 25. cikk előírja a tagállamoknak, hogy – részrehajlás nélkül - ösztönözzék a hálózati és információs rendszerek biztonsága tekintetében releváns európai és nemzetközi szabványok és műszaki előírások alkalmazását. Az Európai Kiberbiztonsági Ügynökség (ENISA) pedig ebben a témában a tagállamokkal együttműködve és adott esetben az érintett érdekelt felekkel folytatott konzultációt követően tanácsokat és iránymutatásokat dolgozhat majd ki. Az irányelv tudatosan és következetesen többször hivatkozik[101] a folyamatosan fejlődő műszaki szabványkörnyezetre, ezzel nyilván elkerülve, hogy fontos részei valamely innováció következtében anakronisztikussá, meghaladottá, vagy egyenesen alkalmazhatatlanná váljanak.

A DORA rendelet különlegességét az adja, hogy az IKT-technológiák alkalmazásában élenjáró, tevékenysége miatt örök célpont pénzügyi szféra biztonsági színvonalát – digitális működési rezilienciáját[102] – emelje és egységesítse az EU-ban egy magas szintre és működési alapelveken túl konkrétabb intézkedések megtételét is előírja. Ennek egyik legfontosabb eszközrendszere a közösségi pénzügyi piacot felügyelő európai felügyeleti hatóságok[103] által 2024. július 17-ig kiadott szabályozástechnikai-standardok és végrehajtás-technikai standardok

[100] Aminek előképeként hivatkozza a telekommunikációs 5G-hálózatok kiberbiztonsága kapcsán korábban kiadott (EU) 2019/534 Bizottsági ajánlást.

[101] A felhőszolgáltatásokkal kapcsolatban az ISO/IEC 17788:2014, a sérülékenységkezeléssel kapcsolatban az ISO/IEC 30111, ISO/IEC 29147, a kiberbiztonsággal kapcsolatban általánosságban az ISO/IEC 27000 szabványsorozat kerül megemlítésre hivatkozási pontként.

[102] 3. cikk 1. pont: „a pénzügyi szervezet képessége arra, hogy kiépítse, biztosítsa és felülvizsgálja működési integritását és megbízhatóságát azáltal, hogy harmadik fél IKT-szolgáltatók által nyújtott szolgáltatások igénybevételével közvetlenül vagy közvetetten biztosítja azon hálózati és információs rendszerek biztonságának kezeléséhez szükséges IKT-vonatkozású képességek teljes körét, amelyeket a pénzügyi szervezet használ, és amelyek a pénzügyi szolgáltatások folyamatos nyújtását és minőségét támogatják, többek között zavarok fennállásakor is;”

[103] Ezek az 1093/2010/EU európai parlamenti és tanácsi rendelettel létrehozott európai bankfelügyeleti hatóság (Európai Bankhatóság, EBA), az 1094/2010/EU európai parlamenti és tanácsi rendelettel létrehozott európai felügyeleti hatóság (Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság, EIOPA) és az 1095/2010/EU európai parlamenti és tanácsi rendelettel létrehozott európai felügyeleti hatóság (Európai Értékpapírpiaci Hatóság, ESMA).

lesznek[104]. A rendelet alapján elvárás az IKT-kockázatok kezelése, az események osztályozása és jelentése, a sérülékenység ellenőrzése, a beszállítói kockázatok kezelése (a rendeletben harmadik féltől eredő IKT-kockázat), és a piaci szereplők között kiberfenyegetésekre vonatkozó információmegosztás – mindezek egy szinttel konkrétabban és részletesebben, mint a NIS 2 esetében, így az azonosításra, védelemre, reagálásra és helyreállításra, sőt a mentési gyakorlatra is szabályok megadásával. A rendelet 2024. január 16-án lépett hatályba és rendelkezéseit 2 év felkészülési idő után kell alkalmazni.

V.3. A NEMZETI IMPLEMENTÁCIÓ FOLYAMATA

A NIS magyar implementációja elsődlegesen a már több mint 10 éve hatályban lévő Ibtv-ben és kormányrendeleteiben jelent meg, de természetesen a teljes kiberbiztonsági szabályozási háttér ennél jóval szélesebb és sokszínűbb, amelynek áttekintése és koncepcionális, stratégiai értékelését követő módosítása a NIS2-ből származó feladat lesz, amelyet a magyar jogalkotó már részben el is végzett a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény elfogadásával (a továbbiakban: Kibertantv.). A kiberbiztonsági tanúsítás szabályait[105] az Ibtv. III/A. Fejezetéből emelték át és fejlesztették tovább. A NIS 2 kiberbiztonsági felügyeletre vonatkozó cikkeinek implementációját végrehajtó rendelkezések lépcsőzetesen, jövő év január 1-én, illetve október 18-án lesznek alkalmazandók. A személyi hatály igazodik az irányelvhez (a törvény mellékletében meg is jelennek az irányelvi mellékletek), kivételt az Ibtv. szerinti honvédelmi célú elektronikus információs rendszerek és hálózatok, a kijelölt európai vagy nemzeti létfontosságú rendszerelemeknél, illetve az atomenergia alkalmazása körében használt elektronikus információs rendszerek.
A szervezeteknek az okozható károk mértékével arányos módon kell gondoskodniuk az elektronikus információs rendszereik fizikai környezetének védelméről, valamint az elektronikus információs rendszereken kezelt, tárolt és továbbított információk, alamint az általuk nyújtott szolgáltatások bizalmasságát, sértetlenségét és rendelkezésre állásáról (CIA-elv: confidentiality, integrity, availability).

A kiberbiztonsági felügyeletet hatóságként a Szabályozott Tevékenységeket Felügyeleti Hatósága (a továbbiakban SZTFH) látja el, ahol minden a törvény hatálya alá tartozó szervezetnek regisztrálnia magát (2024. június 30-ig). A szervezeteknél elektronikus információs rendszerek felügyeletét biztosító személyt kell kinevezni, folyamatosan együtt kell működni a hatósággal, felügyeleti díjat kell fizetni, valamint az elektronikus információs rendszereiket biztonsági osztályokba kell sorolniuk. Az SZTFH elnöke rendeletében meghatározhatja majd, hogy a szervezetek milyen kiberbiztonsági tanúsítással rendelkező IKT-

[104] Ezek kidolgozása már folyamatban van, az első nyilvános anyagok már elérhetők: https://www.eba.europa.eu/esas-consult-first-batch-dora-policy-products

[105] Továbbra is biztosítva 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 (kiberbiztonsági jogszabály) szóló (EU) 2019/881 európai parlamenti és tanácsi rendeletnek való megfelelést.

terméket, IKT-szolgáltatást vagy IKT-folyamatot használhatnak a rendszereikben – ami biztosan jelentős hatással lesz egyrészt a biztonsági színvonalra, másrészt a beszállítói piacra.

Szintén az objektíven igazolható magas színvonalat szolgálja, hogy a szervezet köteles a tevékenység végzésére jogosult, független auditor által két évenként kiberbiztonsági auditot végeztetni, az elsőt 2025. június 30-ig kell végrehajtani. Ha pedig az elektronikus információs rendszerben biztonsági esemény történt vagy annak közvetlen bekövetkezése fenyeget, a szervezet köteles haladéktalanul a nemzeti eseménykezelő központnak jelenteni az eseményt. A kijelölt magyar CSIRT a Nemzetbiztonsági Szakszolgálat keretei közt működő Nemzeti Kibervédelmi Intézet, amely egyben a kijelölt kapcsolattartó (Single Point of Contact a NIS 2-ben) szervezet is nemzetközi kiberbiztonsági kérdésekben.

Az Országgyűlés által éppen tárgyalt T/9716. számú, Magyarország kiberbiztonságáról szóló törvényjavaslatból már tudható, hogy egyrészt kódex-jellegű jogszabály készül az Ibtv. és a Kibertantv. is hatályon kívül lesz helyezve, de a jogalkotó nem fogja elvetni az alapvetően bevált intézményi kereteket, rendező elveket, szereplőket, eljárásokat, és feladatokat, inkább bővülésre kell számítani a hatósági-felügyeleti hatáskörök és konkrét biztonságosnak tekinthető, elvárt üzemeltetési rendek vonatkozásában. A végrehajtási rendeletek szintjén is várható, hogy egy koncentráltabb, összefogottabb szabályozásban jelenik majd meg a hatósági, incidenskezelési, sérülékenységvizsgálati, korai előrejelzési és más tematikus részletszabályok.

Az új uniós szabályozók kapcsán már érintett témák megjelenése mellett várható a közigazgatási térben is egyre komolyan szerepet játszó felhőalapú szolgáltatási modellek explicitebb megjelenése, ideértve az infrastruktúra-szolgáltatást (IaaS), a platformszolgáltatást (PaaS), a szoftverszolgáltatást (SaaS), valamint a hálózatszolgáltatást (NaaS). A felhőszolgáltatásokkal kapcsolatban szükséges lesz a NIS 2-nek megfelelően rendezni a szolgáltatást nyújtó, és igénybevevő felelősségi körét, és azt is, hogy a személyes adatok, esetleg más privilegizált adatkörök milyen előfeltételekkel, üzemeltetési rendben, és ellenőrzés mellett kezelhetők nemzeti joghatóságon kívül az új szabályozási keretekben. Szintén várható, hogy a felügyeleti jogkörök mellé olyan, kifejezetten a kiberbiztonság területére szóló ajánlás/útmutató-kibocsátó felhatalmazást is kapnak majd a magyar hatóságok, amelyek megfeleltethetőek az uniós szinten meglévő hasonló specifikus és néha eseti jellegű szabályozóknak, ezzel téve reakcióképesebbé, rugalmasabbá és egységesebbé a felügyelt szervezetek közös és egyéni működését, felkészültségét.

A további szabályozási lépéseknél a jogalkotóra nagy teher hárul, hiszen a kiterjedt hatósági-felügyeleti feladatokat ellátó szervezeti kör, az érintettek széles spektruma, a hatáskörök és a kapcsolódó kötelezettségek gyarapodása szükségessé teszi, hogy a módosítás folyamán körültekintően járjon el a hatásköri összeütközések elkerülése és a pontos lehatárolások érdekében, nem lényegtelen az sem, hogy milyen mélységű szabályozás milyen jogforrási hierarchia-szinten jelenik meg, és arra is nagy szükség van, hogy kellő hangsúlyt fektessenek a széles körű tájékoztatásra abban a vonatkozásban, hogy kihez kell/lehet fordulni. A szabályozási modell változása természetesen az egyes rendszerüzemeltetők részéről szintén magával hozza azt a feladatot, hogy előzetesen és folyamatában is karbantartott naprakész információi legyenek a rá vonatkozó szabályozási környezetről. Az IT folyamatokat értékelő

kötelező audit, és a belső szabályozással foglalkozó governance mellett az IT compliance is egyre hangsúlyosabb lesz a jogi keretek szofisztikálódásával, olyan szervezetknél is, ahol eddig ezek a folyamatok nem képezték a napi gyakorlat részét.

V.4. A KIBERBIZTONSÁG SOFT-ESZKÖZÖKKEL VALÓ SZABÁLYOZÁSA

Az uniós és nemzeti jogi keretrendszerek mellett még két kategóriát mindenképpen érdemes érinteni a teljesebb kép érdekében, különösen mivel ezek egyre szélesebb körű megjelenése, és elvárt követése várható. Az első a NIS 2 kapcsán már tárgyalt ENISA, illetve a közösségi pénzügyi piacot felügyelő európai felügyeleti hatóságok és hazai megfelelőjükként az MNB kiberbiztonságra vonatkozó már meglévő tájékoztató, ajánlásokat kibocsátó, útmutató tevékenysége, amihez a jövőben az SZTFH elnöke által rendeletben kiadásra kerülő – így kötelező – szabályok (amelyeknek valamilyen ekvivalens formája a NBSZ NKI és a honvédelmi ágazat vonatkozásában a KNBSZ részéről sem lenne ok nélküli). A másik lényegesen nagyobb és sokszínűbb halmaz az informatikai mérnök-szakmai szabályokat és jó gyakorlatokat rögzítő szabványok csoportja.

Az ENISA részéről a téma szempontjából kiragadható a kiberbiztonsági beszállítói láncokkal kapcsolatos jó gyakorlatokat összefoglaló jelentés[106] 2023. júniusából, a mesterséges intelligencia kiberbiztonságáról és a szabványosításról szóló jelentés 2023. márciusából[107], vagy egy hazánkban még kevésbé forgó téma, a kiberbiztonsági biztosítások kereslet oldali elemzése[108]. A EU-s pénzügyi felügyeleti hatóságok korábbi iránymutatásai és ajánlásai közül kiemelhető az EBA „Iránymutatások a felügyeleti felülvizsgálati és értékelési eljárás (SREP) során végzendő IKT-kockázat értékeléshez”[109], az „Iránymutatás a kiszervezésről”[110], az EIOPA „Az információs és kommunikációs technológiák biztonságára és irányítására vonatkozó iránymutatások”[111], az "Iránymutatások a felhőszolgáltatókhoz történő kiszervezésről"[112] valamint az ESMA felhőszolgáltatókhoz történő outsourcing-ról szóló irányelvei[113]. Az MNB ajánlásai közül kettőt emelnék ki, a 4/2019. (IV.1.) számú ajánlást, a közösségi és publikus

[106] Elérhető: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity
[107] Elérhető: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation
[108] Elérhető: https://www.enisa.europa.eu/publications/demand-side-of-cyber-insurance-in-the-eu
[109] Elérhető: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1954038/68542d41-1585-4228-891f-259bba26a64c/Guidelines%20on%20ICT%20Risk%20Assessment%20under%20SREP%20%28EBA-GL-2017-05%29_HU.pdf?retry=1
[110] Elérhető: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/71c44093-b908-4532-b464-1efa8818458e/EBA%20revised%20Guidelines%20on%20outsourcing_HU.pdf?retry=1
[111] Elérhető: https://www.eiopa.europa.eu/system/files/2021-04/eiopa-gls-ict-security-and-governance-hu.pdf
[112] Elérhető: https://www.eiopa.europa.eu/system/files/2020-04/guidelines_on_outsourcing_to_cloud_service_providers_cor_hu_0.pdf
[113] Elérhető: https://www.esma.europa.eu/document/guidelines-outsourcing-cloud-service-providers

felhőszolgáltatások igénybevételéről[114] és a 8/2020. (VI.22.) számú ajánlást az informatikai rendszer védelméről[115].

A de jure (valamely nemzetközi szabványtestület által hivatalosan kiadott) és de facto (szakmai szervezet által összeállított szabályok, legjobb gyakorlatok) szabványok[116] közül a legfontosabbak és gyakran a jogi szabályozásra is közvetlen hatást gyakorlók kettőt érdemes kiemelni.

Az ISO 27000-es szabványcsalád[117] eredete 1995-ig vezethető vissza, a brit Kereskedelmi és Ipari Minisztérium által kiadott BS 7799 szabványra, amely menedzsment szemszögből foglalt rendszerbe informatikai biztonsági követelményeket. Mára egy egész szabványcsaláddá vált[118], számos biztonsági aspektust érintve (kiberbiztonság, személyes adatok védelme, szervezetek között kommunikáció, auditálás, monitoring, kriptográfia). A megfelelőségüket igazolni kívánó szervezetek szempontjából várhatóan az egyik legnépszerűbb megoldás lesz az információbiztonsági menedzsment rendszereik auditáltatására

A másik jelentős szabványcsalád az USA Szabványügyi és Technológiai Intézete által kiadott NIST 800-as szabvány-sorozat[119], amely komoly jelentőséggel bír világszerte (részben az IKT-szektorban betöltött domináns szerep miatt is). Hazánkban már korábban is szakmai hátterét adta az elektronikus információbiztonsági kontrollok meghatározásának, így a 41/2015. BM rendeletet leváltó 7/2024. MK rendelet tartalma is innen származtatható.

V.5. A HAZAI IMPLEMENTÁCIÓT KÖVETŐEN VÁRHATÓ TOVÁBBI FELADATOK

A szuprancionális, nemzeti és szakmai keretek változása minden bizonnyal több lényegi változást, fejlődést hoz majd magával. Állami, szakpolitikai szinten a NIS 2 7. cikke által is érintett nemzeti kiberbiztonsági stratégia átdolgozása lesz szükséges, amely az alapvető és fontos szervezetekre koncentrálva, részletes ágazati és tematikai alábontásaiban is konzekvens módon, egy központi víziót követve, határoz meg intézkedési irányokat és stratégiai törekvéseket. Időhorizontját tekintve a stratégia nem szaladhat 5 évnél sokkal előbbre az állandóan változó, innovatív közeg miatt, amely a stratégia helyzetértékelési, fenyegetettség-elemző, és prioritás-mátrixát is gyorsan elavulttá teszi.

A cél nemzeti szinten az EU-s keretek között mozgó, rugalmas és az iparági jó gyakorlatokat bátorító regulatív modellek felépítése, amely az IKT fejlesztésben és

[114] Elérhető: https://www.mnb.hu/letoltes/4-2019-felho.pdf
[115] Elérhető: https://www.mnb.hu/letoltes/8-2020-informatikai-rendsz-vedelmerol.pdf
[116] A szabványok áttekintéséhez lásd: SZÁDECZKY Tamás: Információbiztonsági szabványok, Budapest, NKE, 2014.
[117] A kiberbiztonság szempontjából kiemelt szabványcsalád alkalmazási gyakorlatához lásd pl: Heinrich KERSTEN, Gerhard KLETT, Jürgen REUTER, Klaus-Werner SCHRÖDER: IT-Sicherheitsmanagement nach der neuen ISO 27001, Wiesbaden, Springer 2020, 2. kiadás; Alan CALDER, Steve WATKINS: IT Governance - An International Guide to Data Security and ISO27001/27002, London, Kogan Page, 2020, 7. kiadás; Abhishek CHOPRA, Mukund CHAUDHARY: Implementing an Information Security Management System - Security Management Based on ISO 27001 Guidelines, New York, Springer, 2020.
[118] Lásd az ISO oldalán: https://www.iso.org/standard/iso-iec-27000-family
[119] Elérhető: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

üzemeltetésben közreműködő minden szakemberrel szemben – az adott feladat által megkövetelt biztonsági szinthez és az üzemeltetett rendszerhez igazított – szakmai elvárásokat támaszt, ellenőriz és számonkér. A NIS 2 által megfogalmazott együttműködések erősítése érdekében élő és folyamatosan működő kommunikációs csatornák kialakítására van szükség az IT ipar (kooperáció a biztonság növelése érdekében), az egyetemi és szakképzési szféra (K+F+I, az iparági szakemberigények közvetítésére, a szükséges HR-erőforrás rendelkezésre állásának előmozdítására) és a fogyasztói csoportok tudatosságának növelésére (szemléletformálás, tudatos és kockázatcsökkentő online működés érdekében).

Hatósági-felügyeleti oldalról jól kommunikáló, ügyfélorientált, szükséges erőforrásokkal rendelkező, gyorsan reagáló (nem bürokratikus), személyes bizalomra is építő kibervédelmi szervezetrendszer kialakítása szükséges, amely a kibervédelmi termékek tanúsításától az eseménykezelésen át a felügyeleti/hatósági funkciók ellátásáig kompetens módon látja el feladatait. Annak, hogy az SZTFH nagyobb bevonódásával egy újabb szervezet kapott fontos feladatokat a kiberbiztonság területén több következménye is van. Egyrészt valószínűleg szükség lesz előbb-utóbb a határokon átnyúló, vagy potenciálisan nagy károkat okozó fenyegetések kezelésére valamilyen felső szintű, operatív kiberbiztonsági ernyőszervezetre, ami a területen hatás- és feladatkörrel rendelkező szerveket (SZTFH, NBSZ NKI, BM OKF, NMHH, KNBSZ, TEK, NVSZ, ORFK (KR NNI Kiberbűnözés Elleni Főosztály), KKM, BM, HM, MK VIH, BM OKF) összefogja, képes a koordináció és információáramlás biztosítására, és a felsővezetői tájékoztatásra, a központi döntések becsatornázására. Példaként erre felhozható a német Nemzeti Kiber-elhárítási Centrum[120]. Ez lehetőséget adna a jelentős beruházási értéket képviselő (és gyorsan avuló…) technikai infrastruktúra és a különösen értékes magas tudásszintű és nehezen megszerezhető (még nehezebben megtartható) emberi erőforrás koncentrálására is. Másrészt hosszabb távon egyébként az sem kizárható, hogy nem csak a korszerű hardver- és szoftver technika ára miatt, de egy esetleg feszesebb költségvetési helyzet, és a piacon is nagyon értékes és jól fizetett emberi erőforrás megtartása miatt felmerül majd a szervezeti racionalizálás is – esetleg egy német Szövetségi Információtechnikai Biztonsági Hivatalhoz (Bundesamt für Sicherheit in der Informationstechnik)[121] hasonló szervezetben.

Az illetékes hatóságok útmutatóival és ajánlásaival nálunk is jelentős szerepet játszanak már az alacsonyabb szintű jogi szabályozók és az inkább a „soft law" kategóriájába eső dokumentumok. Szinte biztos, hogy a jövőben az egyre komplexebb elvárások miatt több szervezet is ad majd ki specifikus szektorális szabályokat, iránymutatásokat[122].

Az új szervezetrendszer felállásával, a hatósági felügyelet alá kerülő szervezeti kör kialakulásával és az auditok lebonyolításával kialakuló, remélhetőleg magasabb biztonsági

[120] Bővebben lásd: VIKMAN László: A német kiberbiztonsági szisztéma áttekintése, Military and Intelligence Cybersecurity Research Paper, 2/2021., Elérhető: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/2_2021_MIC_RP.pdf

[121] Elérhető: **https://www.bsi.bund.de/DE/Home/home_node.html**

[122] Példaként lásd a BSI IT-Grundschutz gyűjteményt, Elérhető: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

színvonalat rendszerszintű, átfogó, reális és súlyos következményekkel fenyegető gyakorlatok tervezésével és végrehajtásával tesztelni kell majd, az aktuális nemzetközi tapasztalatok ismeretében is.

A tanúsított termékek kötelező használatának előírása primer módon érzékelhető lesz kereskedelmi oldalról, a tanúsításra alkalmas, és a kiberbiztonsági auditok elvégző cégek száma is növekedni fog, ennek kapcsán ilyenkor – főleg az árérzékenyebb szervezeteknél – oda kell majd figyelni a dokumentált és a valós színvonal közötti esetleges eltérésekre. Ezek a változások beszállítói oldalról jelentős fejlesztési, kereskedelmi kihívásokat, beszerzői irányból beszerzési és üzemeltetési megfelelőségi, compliance, governance kérdéseket vet majd fel.

Növekedni fog a folyamatos képzés és továbbképzés jelentősége, a teljes szervezet szintjén, hiszen a munkatársak szemléletformálásától a vezetői felkészítésen át az IKT szakmai munkatársak folyamatos magas szintű tudását és garantálni kell (fel fognak még inkább értékelődni a nemzetközi biztonsági vizsgák, pl. CISA, CISM, Comptia+…)[123], mivel a biztonságos rendszer nem megvásárolható, a biztonság legalább annyira szemléletmód és alapvető működési irányelv, mint egy termék vagy szolgáltatás képessége vagy minősége.

Jogi szempontból tehát egy korszerű és biztonságos szervezeti IKT-környezethez az alábbiakra lesz mostantól szükség:

- széles spektrumú felmérésen, kockázatelemzésen alapuló, folyamatosan naprakészen tartott szervezeti kiberbiztonsági compliance és governance (jogi megfelelőség, stratégiaépítés és belső szabályozottság), rendszeres felülvizsgálatok
- a szervezet menedzsmentje által meghatározott elvek és a rendelkezésre álló erőforrások mentén optimalizált, szakmai-beszerzési-jogi szempontok szerint kialakított beszerzési gyakorlat;
- több irányból ellenőrzött, jogilag is támogatott üzemeltetés;
- megfelelő kapcsolati háló és bizalom kialakítása minden jelentős partner irányában (így a felügyeleti hatóságok felé is);
- a beszállítók szűrése, az engedélyezett termékek nyomonkövetése (közbeszerzésköteles szervezetek esetében ez további jogalkotással jár majd várhatóan).

A magyar implementációra vonatkozóan érdemes megfontolni, hogy az olyan kiemelt EIR-ek esetében, amelyek pénzügyi, adat-osztályozási, vagy rendelkezésre állási szempontból magas szintű kockázatokkal működnek, azok esetében sokkal kisebb mértékben lehet teret engedni az egyes kontrollintézkedések megvalósításának és a pénzügyi ágazatnál már ismert szorosabb, előíróbb és szigorúan ellenőrzött követelményeket kell támasztani. A hatósági/felügyeleti munkában a közigazgatási szféra vonatkozásban fontos, hogy valós tartalmú kockázatértékelések készüljenek, naprakészen tartott biztonsági szabályozókkal.

A NIS2 nem terjed ki az egyébként közigazgatáshoz tartozó rendészeti, nemzetbiztonsági és honvédelmi ágazatra, ezért az újra-szabályozásnál ezek esetében is olyan standardeket kell meghatározni, amelyek a lehetőségekhez mérten legmagasabb biztonságot szavatolják – ismét

[123] Elérhető: https://www.isaca.org/credentialing/certifications ; https://www.comptia.org/

utalva a pénzügyi ágazat minta-jellegére vélhetően kevés magyar közigazgatási szervezet tud ekvivalens vagy jobb védelmi színvonalat felmutatni egy átlagos magyar pénzintézethez viszonyítva.

A közelmúltban ismertté vált biztonsági események figyelembevételével is megfontolandó egy olyan költségvetési tartalékkeret elkülönítése a központosított beszerzéseket bonyolító tárca költségvetési fejezetében, amely alkalmas lehet katasztrofális rendszerhibák és leállások gyors kezelésére, illetve olyan tartalékok (eszköz és üzemelési helyszín) biztosítására, amelyekre ilyenkor szükség lehet. Minisztériumi szinten az ágazati szervezetek elektronikus információbiztonságát felügyelő, támogató, költségvetési tervezésben érdekeit képviselő szervezeti egységek felállítása nagy segítséget jelentene a költségvetés végső formálásában szerepet nem kapó szervezetek szempontjából.

A nemzeti adatvagyon fokozottabb védelme, megőrzésének szavatolása érdekében a felhő-szolgáltatások kiterjedt igénybevétele mellett érdemes lehet megvizsgálni az állami alapnyilvántartások biztonságba helyezését, akár az észt adat-nagykövetség mintájára[124] külföldön, de akár belföldön is.

A közbeszerzési szabályozást érdemes lenne áttekinteni (beszerzési tárgyak, kivételek, eljárási könnyítések, bírálati szempontok vonatkozásában mindenképp), hogy mennyiben szükséges és lehetséges a magasabb szintű kiberbiztonságot célzó beszerzési követelmények lehetővé vagy kötelezővé tétele. A közszférával kötött beszállítói szerződések vonatkozásában a biztonsági színvonalat emelő kötelező elemek előírása mindenképpen szükséges lenne azért, hogy legyen egy megkövetelt minimum-tartalom (az építési beruházások esetében például elvárás.) Érdemes lenne egyre inkább kiválasztási szemponttá tenni a vásárolt termékek, szolgáltatások kiberbiztonsági tanúsítottságát, előírni felelősségbiztosítások alkalmazását. Az eljárások szerződéstervezeteiben a klasszikus rendelkezésre állási kérdések (SLA szintek) mellett mind a biztonsági frissítések, mind a biztonsági események konkrét alkalmazást érintő kérdéseire is ki kell térni és konkrét EIR-től is függő mértékben a beszállítói lánc biztonságát emelő intézkedéseket kell tenni.

Az irányelvben erősen hangsúlyozott vezetői felelősséget konzekvensen érvényesíteni kell a szervezeti vezetők vonatkozásában, ha szándékosságról, súlyos gondatlanságról, vagy a hibák elfedéséről van szó. Maradványkockázatként azonosított hiányosságok esetében, zero-day sérülékenységeknél, vagy központi szolgáltatások esetén nem méltányos a felelősségre vonás (különösen, ha a megoldást már jelzett, tervezett, de költségvetési finanszírozással nem lefedett fejlesztések jelenthették volna), de a foglalkoztatási, polgári jogi, büntetőjogi következmények nem maradhatnak el az alapvető biztonsági intézkedések súlyosan gondatlan figyelmen kívül hagyásáért, szándékos megsértéséért, hiszen a közigazgatásban nem a piac „büntet”. Az elektronikus információbiztonságért felelős vezető belső szervezeti függetlenségét továbbra is garantálni kell törvényi szinten is, és biztosítani kell a közvetlen jelentési lehetőséget a szervezeti vezetés felé – megfontolható lehet hierarchikus szervezetben (regionális-központi-kormányzati szintek esetén) a „szolgálati utat” megkerülő szignalizációs lehetőség biztosítása az ágazati felsővezetés irányába.

[124] Elérhető: https://e-estonia.com/wp-content/uploads/2020mar-facts-a4-data-embassy.pdf

A COVID-járvány melléktermékeként a távoktatás is jelentős mértékben fellendült, a közigazgatásban pedig egyébként is nagy hagyományai vannak a munkakörökhöz kapcsolódó vizsgáztatásnak, ezért nem tűnik lehetetlennek és idegennek sem egy egységes online-oktatási rendszer kialakítása, valamint a munkakörök betöltésének vizsgaeredményekhez való kötése. A bonyolult biztonsági szabályzatok teljes számonkérése helyett elképzelhető a legfontosabb biztonsági rendszabályok és magatartásformák kivonatolása (katonai Rules of Engagement-kártyák mintájára), ami gyorsan ellenőrizhető, plakátokon is kirakható, a fiókban tartható.

VI. Zárszó

Jól látható, hogy az internet világa átfogó módon érinti a nemzetbiztonságot, illetve a társadalmi biztonság számos aspektusát. Ez a kihívás azonban találkozik a már meglévő értelmezési kérdésekkel, illetve a nemzeti intézményi sajátosságokkal is, ami a változó biztonsági és nemzetközi politikai környezetben tovább nehezíti az adaptációt a kérdéskörben. Jelen tanulmány ezért arra tett kísérletet, hogy az info-kommunikációs robbanás és az információs társadalom jelentette kihívás-halmazt a nemzetbiztonság értelmezése, intézményi és szabályozási sajátosságai, valamint az internetszabályozás és a kiberbiztonsági szabályozás elegyítésével közelítse meg.

A tanulmány nem csak arra kívánta felhívni a figyelmet, hogy az egyes szakterületek közti fokozott kommunikáció, illetve együtt gondolkodás megkerülhetetlen az ilyen komplexitású témák feldolgozása, jobb megértése és megértetése tekintetében, hanem arra is, hogy a szabályozás kapcsán rávilágítson arra, hogy a párhuzamos, elkülönült, kevéssé szinkronizált megoldásokat ideje meghaladni a változó környezetben.

Jelen keretek között persze a cél elsődlegesen az összefüggések megvilágítása, az eltérő nézőpontok láttatása volt, ami lehetőséget teremthet további kutatások elvégzéséhez és az eredmények tanulmányokban történő feldolgozásához. Bízunk abban, hogy a felvázolt gondolatok segíteni tudják a megcélzott kérdések körüli diskurzus további élénkülését, mivel a jelen szerzők szakterületi látásmódját további megközelítésmódokkal lehet és szükséges kiegészíteni a jövőben. Egy ilyen szakmai-tudományos diskurzusból úgy véljük, középtávon olyan megállapítások és javaslatok is következhetnek, amelyek a hazai szabályozási és intézményi rendszer fejlesztését is segíthetik.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Military and Intelligence CyberSecurity Research Paper 2024/3.

Szerző(k) / Author(s):
Farkas Ádám PhD | Gosztonyi Gergely PhD
Szabó Hedvig PhD | Vikman László

Kézirat lezárásának ideje / Manuscript closing time:
2024.12.20.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD | Dr. Magyar Sánor PhD
Dr. Vikman László | Krizsán Bence

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Dr. Magyar Sándor PhD

Elérhetőségek /Contacts:
https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. | 9-11. Hungária Blvd., Budapest, H1011

ISSN: *2786-3778*

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.
The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.