

SLRG Research Paper – Nr. 2022/1.



SmartLaw Research Group

**Gondolatok a kiberbiztonsági
stratégiák fejlesztésére vonatkozó
nemzetközi útmutató kapcsán**

Vikman László

Az „Útmutató nemzeti kiberbiztonsági stratégia kidolgozásához” témaválasztásában nem tekinthető úttörőnek, mégis átfogó képet ad a kidolgozó munkához szükséges eljárásrend és alapelvek vonatkozásában. Ez a tanulmány az útmutató legfontosabb gondolatait igyekszik megvilágítani, kiegészítve néhány olyan ponttal, amelyek figyelembevételével a stratégia alkotás hatékonysága és korszerűsége fokozható.

Kulcsszavak: *kibertér, kiberbiztonság, stratégia-alkotás, kiberbiztonsági stratégia*

The Guide to Developing a National Cybersecurity Strategy is not groundbreaking in its subject, nevertheless it gives a comprehensive perspective about the process and recommended guidelines for developing such strategy. This study tries to highlight the most important points, and gives a few thoughts about potential further key aspects for an efficient and up-to-date cyberpolicy.

Keywords: *cyber space, cyber security, strategy-making, cyber security strategy*

1. BEVEZETÉS¹

Kiberbiztonsági stratégiával az Európai Unió minden tagállama rendelkezik már, sokuk esetében már második, sőt harmadik iterációjánál tart az információs társadalmat és gazdaságot alapvetően meghatározó infokommunikációs szféra nemzeti szabályozási, adminisztratív és fejlesztési kereteit megfogalmazó dokumentum.² Ez azonban nem jelenti azt, hogy a

kiberbiztonsági stratégia alkotás folyamata már nyugalmi szakaszba érkezne, mivel számos képességfejlesztés és azok intézményi és szabályozási lekövetése, illetve az infokommunikáció és különösen a kibertér 21. századi biztonságban betöltött szerepe³ újabb és újabb kihívások elé állítja ezt a szakpolitikát. Ehhez is kötődve, a következő időszakban az EU tagállamok egyik fontos mércéje és a stratégiák revíziójának háttere lesz az Európai Bizottság által kiadott, „Digitális iránytű 2030-ig: a digitális évtized

¹ Jelen mű a Nemzeti Közszerzői Egyetem Hadtudományi és Honvédtisztképző Kar Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék keretében működő Katonai Nemzetbiztonsági Kibertér Művelési Szakcsoport keretében végzett kutatás részeként született.

² Lásd a tagállamok stratégiáit egy helyen közlő tematikus oldalt, az ENISA gondozásában: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies>

³ A téma kapcsán lásd: MERLE MAIGRE: *Cyber threat actors: how to build resilience to counter them*. In: Hybrid CoE Paper 11., Helsinki, 2022.; ANTONIO MISSIROLI: *Geopolitics and strategies in cyberspace: Actors, actions, structures and responses*. In: Hybrid CoE Paper 7, Helsinki, 2021.; WILLIAM E. LEIGHER: *Cyber conflict in a hybrid threat environment: Death by a thousand cuts*. In:

Hybrid CoE Paper 10, Helsinki, 2021.; BEN BUCHANAN: *The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics*. Cambridge, Harvard University Press, 2020.; KELEMEN ROLAND: *Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben*. In: Jog Állam Politika 2021/3. szám, 71-85. o.; KELEMEN ROLAND – FARKAS ÁDÁM: *To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare*. In: Szabó Marcel – Gyeney Laura – Lános Petra Lea (szerk.): *Hungarian Yearbook of International Law and European Law* (2019). Den Haag, Eleven International Publishing, 2020., 203-226. o.; FARKAS ÁDÁM: *A kibertér művelési képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapvonalai*. In: Jog Állam Politika 2019/2. szám, 63-79. o.;



megvalósításának európai módja”⁴ című stratégia. Ennek néhány – részben figyelemhívási céllal önkényesen kiválasztott – fontos megállapítását érdemes talán felsorolni:

- A következő időszakban jelentős lehet a dezinformáció demokratikus társadalmainkra gyakorolt hatására.
- Az EU gyakran nem uniós alapú technológiáktól való fokozott függése, és a tény, hogy a digitális csúcstechnológiákat többnyire az EU-n kívül fejlesztik egyre komolyabb versenyhátrány és egyben biztonsági kockázatok forrása is.
- A polgárokat, kkv-kat, a közszférát és a nagyvállalatokat kiszolgáló digitális infrastruktúra nagy teljesítményű számítástechnikát és átfogó adatinfrastruktúrát igényel.
- Európa digitális vezető szerepe és globális versenyképessége az erős belső és külső konnektivitástól függ, és a közösség nemzetközi szerepvállalását is meg kell határozni.
- Az EU-nak világviszonylatban élen kell járnia a kvantumszámítógépek fejlesztése terén, többek közt azért, mert a kvantumbiztonságos kommunikációs rendszerek megóvhatják az érzékeny kommunikációt.
- A digitális transzformációnak lehetővé kell tennie továbbá a modern és hatékony igazságszolgáltatási rendszereket, a

„...a következő időszakban az EU tagállamok egyik fontos mércéje és a stratégiák revíziójának hátere lesz az Európai Bizottság által kiadott, „Digitális iránytű 2030-ig: a digitális évtized megvalósításának európai módja” című stratégia.”

fogyasztói jogok érvényesítését és az állami fellépés, többek között a bűnüldözési és nyomozati kapacitások hatékonyságának növelését is

- Fontos cél olyan, mesterséges intelligencián alapuló biztonsági műveleti központok hálózatának kiépítése, amelyek képesek kellő időben észlelni egy kibertámadás jeleit, és proaktív fellépést tesznek lehetővé a nemzeti és uniós szintű közös kockázati felkészültség és reakció javítása érdekében.

A példaként felhozott témákból érezhető, hogy a kiberbiztonsági stratégiák rendszeres felülvizsgálata, a változó fenyegetésekhez igazítása, a technológiai innováció okozta

szükségességéből fakadó frissítése visszatérő, ciklikus feladat, amelyhez számos módszertani, „best practice”-alapú, vagy éppen összehasonlító jellegű útmutatót vehetnek igénybe az új iránymutatások kidolgozásával megbízott szakemberek.⁵

E cikkben röviden egy ilyen útmutató főbb javaslatait szeretném bemutatni, aminek különlegességét az elkészítésében részt vevő szervezetek sokszínűsége, a közreműködő szakemberek globális és diverz hátere adja. Ennek köszönhetően esetleg olyan perspektívák és gondolatok forrása lehet, amelyek túlmutathatnak Magyarország esetében az olyan alapvető viszonyítási pontjainkon, mint az Európai Unió, esetleg a NATO,⁶ illetőleg az egyes államok megoldásainak áttekintése.⁷

⁴ Brüsszel, 2021.3.9. COM(2021) 118 final

⁵ Példaként lásd: CLAIRE VISHIK - MIHOKO MATSUBARA - AUDREY PLONK: *Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms*. In: Anna-Maria Osula – Henry Roigas (ed.) *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn, NATO CCD COE Publications, 2016; CAROL A. SIEGEL - MARK

SWEENEY: *Cyber Strategy - Risk-Driven Security and Resiliency*. CRC Press, 2020

⁶ Lásd: KOVÁCS LÁSZLÓ: *Cyber Security Policy and Strategy in the European Union and NATO*. Land Forces Academy Review Vol. XXIII. No 1(89), 2018. 16-24. pp, DOI: 10.2478/raft-2018-0002

⁷ E körben lásd például: FARKAS ÁDÁM: *Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye? Gondolatok*



2. AZ NCS GUIDE8 - ÚTMUTATÓ EGY NEMZETI KIBERBIZTONSÁGI STRATÉGIA KIDOLGOZÁSÁHOZ

A 2021-ben publikált útmutató – melynek első verzióját 2018-ban adták ki - elkészítésében 20 kormányközi és nemzetközi szervezet, a privát szektor és az akadémiai szféra jelentős képviselői, továbbá különféle civil szervezetek szakértői működtek közre. Ezek közül – példálózó jelleggel – kiemelhető a kidolgozók sokrétűségét mutatva: az Európa Tanács, a Geneva Centre for Security Sector Governance (DCAF), a Deloitte, az International Criminal Police Organization (INTERPOL), az International Telecommunication Union (ITU), a Microsoft, a NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), a RAND Europe vagy a Világbank.

A dokumentum célja a nemzeti döntéshozók és szabályozás-formálók számára segítséget nyújtani egy korszerű nemzeti kiberstratégia elkészítésében, amely figyelemmel van a kiberbiztonságra, kiber felkészültségre és ellenállóképességre. A kiberbiztonság megteremtése összetett kihívás, amely

„A 2021-ben publikált útmutató – melynek első verzióját 2018-ban adták ki - elkészítésében 20 kormányközi és nemzetközi szervezet, a privát szektor és az akadémiai szféra jelentős képviselői, továbbá különféle civil szervezetek szakértői működtek közre.”

magába foglal számos kormányzás-technikai, szabályozási, műveleti, műszaki és jogi aspektust is. Az útmutató küldetése, hogy kifejtsse, rendszerezze és prioritizálja ezeket a területeket létező és széles körben elterjedt modellezési és keretrendszerekkel. Mint ilyen, az útmutató szellemiségében egyértelműen rámutat arra, hogy a kiberbiztonság szavatolása szervesen illeszkedik abba a 21. századi biztonságot érintő nézetrendszerbe, amely a biztonságot és annak erősítését komplex és rendszerszerű megközelítéssel tartja csak helyesen megoldhatónak.⁹

Jelen mű célja áttekinteni és bemutatni az útmutató szellemiségét és újszerűségét, így elsődlegesen annak alapvető jellegű felvetéseit érdemes kidomborítani, míg az útmutató első fő tartalmi egységében (Section 3. Lifecycle of a National Cybersecurity Strategy) kifejtett, de egyébként nagyon is értékes és hasznos stratégia-életciklusra, kidolgozási metodikára nem térnek ki, egy fontos kivételtől eltekintve. Ez pedig a későbbi implementációban ideálisan nem érintett stratégia-kidolgozási projektvezető függetlenségének és megfelelő felhatalmazásokkal való ellátásának kérdése, amely nélkül a kidolgozásban résztvevő szervezetek, érdekelték között a szakmai alapú bizalom és egyensúly megbomolhat.¹⁰

az angol National Cyber Force kapcsán. In: Military and Intelligence CyberSecurity Research Paper 2021/1.; VIKMAN LÁSZLÓ: *A német kiberbiztonsági szisztéma áttekintése. Szervezeti keretek, különös tekintettel a nemzetbiztonsági szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására.* In: Military and Intelligence CyberSecurity Research Paper 2021/2.; SPITZER JENŐ: *A francia kibervédelmi és kiberbiztonsági rendszer egyes stratégiai aspektusai.* In: Military and Intelligence CyberSecurity Research Paper 2021/3.

⁸ *Guide to Developing a National Cybersecurity Strategy*, (NCS Guide) <https://ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf>

⁹ Példaként lásd: NORA VANAGA – TOMS ROSTOKS (eds.): *Deterring Russia in Europe.* Defence Strategies for Neighbouring States. London – New York, Routledge, 2019.; PIOTR SZYMANSKI: *New Ideas for Total Defence. Comprehensive Security in Finland and Estonia.* Warsaw, Centre for Eastern Studies, 2020.; PHILIPP LANGE: *Total Defence. How Germany should implement a whole-of-government national and collective defence.* In: Security Policy Working Paper No. 2/2018, Federal Academy for Security Policy.; FARKAS ÁDÁM: *A totalitás kora?* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.; FARKAS ÁDÁM: *Az állam fegyveres védelmének alapjainak.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2020.

¹⁰ NCS Guide i.m. p. 16.



Az útmutató elsősorban a kibertér polgári vagy „civil” védelmére – vagyis nem a katonai dimenzióra – koncentrál, és a következő két érdemi része olyan fő szervező alapelveket (Section 4 Overarching Principles) és jó gyakorlatokat (Section 5 National Cybersecurity Strategy Good Practice) ad meg, amelyek mindenképpen megfontolásra érdemesek egy kiberstratégia kidolgozási folyamatában, ezért ezeket legalább említés szintjén érdemes leltárba venni.

A fő alapelveket úgy fogalmazták meg, hogy egy előre tekintő és holisztikus megközelítésű stratégia megformálásához adjanak vezérfonalat és a kidolgozási folyamat egészében irányt mutathatnak, hiszen nem korlátozódnak egy-egy lépésre. Véleményem szerint a felsorolásuk sorrendjében is inkább logikai narratívát, mint hierarchiát kell keresni. Az optimális stratégiának

- világos összkormányzati és össztársadalmi víziót kell meghatározni;
- a teljes digitális környezetet átfogó, mégis az adott ország körülményeihez és prioritásaihoz igazított elemzésből kell fakadnia;
- valamennyi érintett és érdekelt szereplő aktív részvételével kell készülnie, a szükségleteik és felelősségi körök meghatározásával;
- gazdasági és társadalmi fejlődést kell ösztönöznie, hogy maximalizálja az információs és kommunikációs technológiák hozzájárulását a fenntartható fejlődéshez és a társadalmi inkluzivitáshoz;
- tiszteletben kell tartania és meg kell felelnie az alapvető emberi jogokból származó követelményeknek;
- lehetővé kell tennie a kiberbiztonsági kockázatok hatékony menedzselését és ösztönöznie kell a gazdasági és társadalmi tevékenységek rezilienciáját;

- alkalmaznia kell a lehető legmegfelelőbb rendelkezésre álló szabályozási megoldásokat a kitűzött célok elérésére, figyelembe véve az adott állam sajátos körülményeit;
- a kormányzat legmagasabb szintjéről kell kiadni, innen elosztva a releváns szerepeket és felelősségi köröket, és rendelkezésre bocsátva a szükséges humán- és pénzügyi erőforrásokat;
- segítenie kell egy olyan digitális környezet kiépülését, amelyben az állampolgárok és a szervezetek megbízhatnak.

A kiberbiztonsági stratégia a társadalmi-gazdasági fejlődés számos területét érinti és több tényező is befolyásolja a nemzeti kontextusban. Ezért a stratégia átfogó jellege és hatékonysága érdekében a szerzők olyan jó gyakorlatokra is tettek javaslatokat, amelyek segíthetik a nemzeti kontextusba illeszkedő dokumentum kidolgozását. Ezeket a javaslatokat csoportokra rendezve fogalmazták meg, és az egyes kidolgozó államok saját szervezetrendszerének, szabályozásának és infrastruktúrájának fejlettségétől is függ, hogy melyek alkalmazhatók.

1. fókuszterület: kormányzat

Biztosítani kell a legmagasabb szintű támogatást, továbbá a kormányzaton belüli és a szektorok közötti együttműködést. Létre kell hozni – ha lehetőség van rá, akár ágazatonként is – egy kompetens központi kiberbiztonsági szervezetet, allokálva a szükséges erőforrásokat. A stratégia végrehajtását lépésekre lebontott akcióterv kidolgozásával és ellenőrzésével kell megvalósítani.

2. fókuszterület: kockázatkezelés a nemzeti kiberstratégiában

A kiberfenyegetettség értékelését¹¹ és a kormányzati irányvonalakat a folyamatosan szélesedő kiberfenyegetési térképhez¹² kell

¹¹ Kiberfenyegetések értékeléséhez lásd: GREGORY FALCO - ERIC ROSENBAUGH: *Confronting Cyber Risk - An Embedded Insurance for Cybersecurity*. Oxford University Press 2022, 41. o.

¹² A jövőbeni fenyegetésekhez, mint AI, közösségi média, adatvédelem, zero-trust hálózatok stb. lásd pl. HAMID JAHANKHANI - LIAM M. O'DELL - GORDON BOWEN - DANIAL HAGAN - ARSHAD JAMAL: *Strategy, Leadership, and AI in the Cyber Ecosystem - The role of digital*



igazítani. Meg kell határozni – ezzel egységesíteni – a kockázat-menedzsment megközelítéseket, valamint rögzíteni kell a kockázatkezelés egységes metodológiáját. Ki kell dolgozni szektorális kockázati profilokat, és a kiberbiztonsági szabályozás kidolgozásakor erre is figyelemmel kell lenni.

3. fókuszterület: felkészültség és reziliencia

Ki kell alakítani eseménykezelő képességeket, kiberbiztonsági incidens kezelési- és katasztrófaelhárítási terveket. Ösztönözni kell az információ-meogsztást, gyakorlatokat kell végezni, és ki kell értékelni a kiberbiztonsági eseményeket.

4. fókuszterület: kritikus infrastruktúrák és alapvető szolgáltatások

Ki kell alakítani egy kockázat-kezelő megközelítést a létfontosságú rendszerelemek és alapvető szolgáltatások azonosítására és védelmére, olyan háttérzabályozással, amely átlátható felelősségi köröket ad meg. Meg kell határozni a minimális kiberbiztonsági alapkövetelményeket, piaci ösztönzőket kell kialakítani, és a privát- és közszféra közt működőképes partnerkapcsolatokat.

5. fókuszterület: képesség és kapacitás építése, a tudatosság növelése

Stratégiai szemlélettel szükséges megtervezni a képességek és különösen ezek

teherbírásának kialakítását. Ki kell építeni a kiberbiztonsági képzések kereteit, ösztönözni kell a munkaező képzését. Koordinált kiberbiztonsági tudatosság-növelő programot kell indítani. Támogatni kell a kiberbiztonsági innovációt és kutatás-fejlesztést. Pályázatokat, támogatási programokat kell indítani a sérülékeny és forráshiányos szektorok és csoportok részére.

6. fókuszterület: törvényalkotás és részletszabályozás

Ki kell alakítani a kiberbiztonság, és ehhez kapcsolódóan a kiberbűnözés és a digitális forenzikus terület nemzeti jogi keret- és részletszabályozását.¹³ Védeni kell az emberi szabadságjogokat, ki kell alakítani a szabályok betartását ellenőrző compliance-mechanizmusokat. Ösztönözni kell a bűnüldözés releváns képességeinek

fejlesztését, és a szervezetek közötti információcsere és közös munka alapjait jelentő eljárások bevezetését. Támogatni kell a nemzetközi kooperációt a kiberfenyegetések és kiberbűnözés elleni küzdelemben.

7. fókuszterület: nemzetközi kooperáció

A kiberbiztonságot a külpolitika fontos elemeként kell kezelni és ehhez kell igazítani a hazai és nemzetközi erőfeszítéseket.¹⁴ Részt kell venni a nemzetközi eszmecserékben és a közösen kialakított irányelvek implementációjában.¹⁵ Ösztönözni kell a

„A kiberbiztonsági stratégia a társadalmi-gazdasági fejlődés számos területét érinti és több tényező is befolyásolja a nemzeti kontextusban. Ezért a stratégia átfogó jellege és hatékonysága érdekében a szerzők olyan jó gyakorlatokra is tettek javaslatokat, amelyek segíthetik a nemzeti kontextusba illeszkedő dokumentum kidolgozását. Ezeket a javaslatokat csoportokra rendezve fogalmazták meg, és az egyes kidolgozó államok saját szervezetrendszerének, szabályozásának és infrastruktúrájának fejlettségétől is függ, hogy melyek alkalmazhatók.”

societies in information governance and decision making. Academic Press, 2021.

¹³ A témához lásd pl.: DAMIEN VAN PUYVELDE - AARON F. BRANTLY: *Cybersecurity - Politics, Governance and Conflict in Cyberspace*. Polity Press, 2019, p. 54.

¹⁴ A kiberkonfliktusok jövőjéhez lásd: CHRISTOPHER WHYTE - BRIAN MAZANEC: *Understanding Cyber Warfare - Politics, Policy and Strategy*. Routledge, 2019, p. 272.

¹⁵ A nemzetközi kibertér és kiberbiztonság vonatkozásában a nemzetközi jog vonatkozásában bőven akadnak fejleszthető aspektusok, nem véletlen,



hivatalos és informális kooperációt a kibertérben, és a nemzetközi kooperációhoz szükséges képességek kiépítését, növelését.

ÉSZREVÉTELEK ÉS GONDOLATOK AZ ÚTMUTATÓ KAPCSÁN

Bármely nemzeti stratégia ritkán áll egymagában, mivel az adott ország kormánya által kialakított szakpolitikák közvetlen manifesztációi, fejlesztésük csak más területekre tekintettel lehetséges.¹⁶ Az állami költségvetés kialakítása, az egyes társadalmi érdekek megjelenítése a táblázat soraiban az erőforrások és lehetőségek végessége miatt egy zéró összegű játszma eredménye, a prioritások meghatározásával lehet garantálni azt, hogy ami fontos az mindenképpen kapjon erőforrást. Ezért az útmutató is több esetben hangsúlyozza, hogy a stratégiát a nemzeti sajátosságok és a már meglévő képességek ismeretében kell kialakítani.¹⁷ Emellett nem szabad elfelejteni, hogy a

redundanciák a biztonság és így a kiberbiztonság területén sem feltétlenül jelentenek pazarlást, sőt a hálózatos elvű védekezés tekintetében komoly előnyökkel is járhatnak. Emellett az is igaz, hogy a megfelelő összkormányzati egyeztetéssel, az akciótervek alapján az előrehaladás rendszeres értékelésével, kontrollmechanizmusok alkalmazásával, az esetleges gyakorlati tapasztalatok feldolgozása eredményeként az esetlegesen valóban indokolatlan, vagy a lekötött erőforrásokkal arányban nem álló hozadékokkal párosuló „vadhajtások” korrigálhatók.

Néhány egyéb gondolat felvethető még, ami a meglévő szabályozási rend, intézményrendszer, aktuális fenyegetések tükrében hangsúlyt kaphat. Ilyenek például a következők:

- A digitális közegben működő közösségi média kapcsán az ellenérdekelt szereplők információs műveleteivel szemben hatékony eszközök kialakítására van szükség,¹⁸ mivel az ilyen fenyegetések a társadalmi, diplomáciai és

hogy a leginkább elfogadott témához kapcsolódó szakkönyv is már korábban meglévő nemzetközi szerződésekből, jogelvekből, szokásjogi szabályokból épített analógiákkal operál túlnyomórészt: MICHAEL N. SCHMITT (ed.): *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, Cambridge, Cambridge University Press, 2017

¹⁶ Ha Magyarországot tekintjük, a kiberbiztonság területét a következő – bizonyos vonatkozásokban egymásra is épülő - stratégiák közvetlenül érintik: 1139/2013. (III. 21.) Korm. határozat, Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 1838/2018. (XII. 28.) Korm. határozat, Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiájáról, 1573/2020. (IX. 9.) Korm. határozat, Magyarország Mesterséges Intelligencia Stratégiájáról, valamint a végrehajtásához szükséges egyes intézkedésekről, 1163/2020. (IV. 21.) Korm. határozat, Magyarország Nemzeti Biztonsági Stratégiájáról, 1393/2021. (VI. 24.) Korm. határozat, Magyarország Nemzeti Katonai Stratégiájáról. A szóban forgó stratégiák mellett látni kell azt is, hogy a vonatkozó jogszabályi környezet alakítása, különösen a feladatrendszerek és felhatalmazások változása is komoly hatással lehet a stratégiákban meghatározottak megvalósítására.

Ezen felül lényeges, hogy külön szakirodalma van már az egyes nemzeti kiberbiztonsági stratégiák összehasonlításának is, lásd pl.: SCOTT N. ROMANUK

- MARY MANJIKIAN (ed.): *Routledge Companion to Global Cyber-Security Strategy*. Routledge, 2021

¹⁷ Az USA-ban a National Defense Authorization Act alapján, 2019-ben létrehozott Solarium Bizottság végzett kiterjedt háttér munkát az USA kiberbiztonsági stratégia kidolgozásának előkészítéséhez, lásd: BRANDON VALERIANO – BENJAMIN JENSEN: *Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report*. In: T. Jancárková, L. Lindström, G. Visky, P. Zotz (szerk.): 13th International Conference on Cyber Conflict: Going Viral, Tallinn, NATO CCD COE Publications, 2021

¹⁸ A téma kapcsán lásd: VÉGH KÁROLY: *Információs és befolyásolási műveletek a nemzetközi jog „szürke zónájában”*. In: Farkas Ádám – Végh Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020., 191-212. o.; QUARESHI, WASEEM AHMAD: *Information Warfare, International Law, and the Changing Battlefield*. In: Forsham International Law Journal 2020/4., 901-937. o.; FARKAS ÁDÁM – SPITZER JENŐ: *Az információs korszak és az állami reziliencia egyes kérdései*. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/18.; VIKMAN LÁSZLÓ: *A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra*. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/14.



gazdasági – sőt szélsőséges esetben a katonai – kohéziót és cselekvőképességet is alááshatják.

- Az államműködés és ebből következően kormányzás, az irányítás és vezetés folytonossága legalább olyan fontos, mint a létfontosságú rendszerelemek és alapvető szolgáltatások működtetése, az ehhez szükséges infrastruktúrák biztosítása és ennek részeként szükséges mértékű és hálózatos szervezési elven nyugvó redundanciája alapvető biztonsági érdek.

- A kiberbiztonság összkormányzati tevékenység, de az egyes részterületek felelősei között adott esetben a feladatok és hatáskörök, felelősségi területek vonatkozásában lehetnek súrlódások, amelyek gyors és hatékony rendezésére megfelelő mechanizmusok és felhatalmazások szükségesek, hogy a gyors esemény-kezelés minden esetben garantálható legyen és a fejlesztések során se alakuljon ki a működést nehezítő egyensúlytalanság a nemzeti rendszer egészére vetítve.

- Az útmutatóban is hangsúlyozott állami és civil szféra közötti információcsere valóban ösztönzendő, de bizonyos adatok a minősített, vagy üzleti titok jellegük, esetleg más ok miatt kizárólag a kezelésükhöz előírt csatornákon mozoghatnak, amihez a szükséges adminisztratív és műszaki háttér is biztosítandó, egyébként egyes kérdésekről csak absztrakt, konkrétumok nélküli egyeztetések folytathatók, ami a biztonság-szavatolás konkrét végrehajtási szintjén képességcsökkenést eredményez.

- Az EU Iránytű is említi, hogy az EU-s érdekkörben történő kritikus fejlesztések kulcsfontosságúak, nincs ez másként nemzeti szinten sem, mivel a kereskedelmi

megoldások biztonsági színvonala nem minden feladathoz megfelelő.

Az előzőekben áttekintett és felvetett gondolatokat egybe vetve az is kiemelendő, hogy a legrészletesebb és mindenre kiterjedő stratégia és akcióterv is csupán annyit ér, amit ténylegesen végre is hajtanak belőle. Ahhoz, hogy az adott intézkedés hatást érjen el,

„...a legrészletesebb és mindenre kiterjedő stratégia és akcióterv is csupán annyit ér, amit ténylegesen végre is hajtanak belőle. Ahhoz, hogy az adott intézkedés hatást érjen el, szükséges az érintettek hozzáértése, szakértelme mellett azok hivatástudata és elkötelezettsége is, továbbá a biztonság-tudatosság – feladatellátáson túlmutatóan – széles körű erősítése.”

szükséges az érintettek hozzáértése, szakértelme mellett azok hivatástudata és elkötelezettsége is, továbbá a biztonság-tudatosság

– feladatellátáson túlmutatóan – széles körű erősítése. Ekkor van ugyanis esély a célok irányába történő eredményes előre lépésre. Amellett, hogy az útmutató igényes részletességgel veszi végig a valóban tisztázandó témaköröket,

legfontosabb értékeként a szerkesztők által alkalmazott rugalmas megközelítést, a jó gyakorlatokból leszárt alapelvek rendszerezését tekinthetjük. Tudományos igényességét pedig jól jelzi, hogy az elmélyülést, az egyes résztemák részletes feltárását a dokumentum végén egy részletes és aktuális forrásgyűjtemény segíti, ami a témával kapcsolatos szakpolitikai tevékenységek során épp úgy használható a jövőben, mint a kapcsolódó tudományos kutatások tekintetében.

FELHASZNÁLT IRODALOM

- [1] Ben BUCHANAN: *The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics*. Cambridge, Harvard University Press, 2020.;
- [2] Gregory FALCO - Eric ROSENBAUGH: *Confronting Cyber Risk - An Embedded Insurance for Cybersecurity*. Oxford University Press 2022



- [3] FARKAS Ádám: *A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapvonalai.* In: Jog Állam Politika 2019/2. szám, 63-79. o.;
- [4] FARKAS Ádám: *Kibertér művelet: hírszerző, rendészeti és katonai műveletek elege? Gondolatok az angol National Cyber Force kapcsán.* In: Military and Intelligence CyberSecurity Research Paper 2021/1.;
- [5] FARKAS Ádám: *A totalitás kora?* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.;
- [6] FARKAS Ádám: *Az állam fegyveres védelmének alapvonalai.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2020.
- [7] FARKAS Ádám – SPITZER Jenő: *Az információs korszak és az állami reziliencia egyes kérései.* In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/18.;
- [8] *Guide to Developing a National Cybersecurity Strategy,* <https://ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf>
- [9] Hamid JAHANKHANI - Liam M. O'DELL - Gordon BOWEN - Danial HAGAN - Arshad JAMAL: *Strategy, Leadership, and AI in the Cyber Ecosystem - The role of digital societies in information governance and decision making.* Academic Press, 2021
- [10] KELEMEN Roland: *Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben.* In: Jog Állam Politika 2021/3. szám, 71-85. o.;
- [11] KELEMEN Roland – FARKAS Ádám: *To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare.* In: SZABÓ Marcel – GYENEY Laura – LÁNCOS Petra Lea (szerk.): *Hungarian Yearbook of International Law and European Law* (2019). Den Haag, Eleven International Publishing, 2020., 203-226. o.;
- [12] KOVÁCS László: *Cyber Security Policy and Strategy in the European Union and NATO.* In: Land Forces Academy Review Vol. XXIII. No 1(89), 2018. 16-24. pp, DOI: 10.2478/raft-2018-0002
- [13] Philipp LANGE: *Total Defence. How Germany should implement a whole-of-government national and collective defence.* In: Security Policy Working Paper No. 2/2018, Federal Academy for Security Policy.;
- [14] William E. LEIGHER: *Cyber conflict in a hybrid threat environment: Death by a thousand cuts.* In: Hybrid CoE Paper 10, Helsinki, 2021.;
- [15] Merle MAIGRE: *Cyber threat actors: how to build resilience to counter them.* In: Hybrid CoE Paper 11., Helsinki, 2022.;
- [16] Antonio MISSIROLI: *Geopolitics and strategies in cyberspace: Actors, actions, structures and responses.* In: Hybrid CoE Paper 7, Helsinki, 2021.;
- [17] Damien VAN PUYVELDE - Aaron F. BRANTLY: *Cybersecurity - Politics, Governance and Conflict in Cyberspace.* Polity Press, 2019
- [18] Waseem Ahmad QUARESHI: *Information Warfare, International Law, and the Changing Battlefield.* In: Forsham International Law Journal 2020/4., 901-937. o.;
- [19] Scott N. ROMANIUK - Mary MANJIKIAN (ed.): *Routledge Companion to Global Cyber-Security Strategy.* Routledge, 2021
- [20] Michael N. SCHMITT (ed.): *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations,* Cambridge, Cambridge University Press, 2017
- [21] Carol A. SIEGEL - Mark SWEENEY: *Cyber Strategy - Risk-Driven Security and Resiliency.* CRC Press, 2020
- [22] SPITZER Jenő: *A francia kibervédelmi és kiberbiztonsági rendszer egyes stratégiai aspektusai.* In: Military and Intelligence



- CyberSecurity Research Paper 2021/3.
- [23] Piotr SZYMANSKI: *New Ideas for Total Defence. Comprehensive Security in Finland and Estonia*. Warsaw, Centre for Eastern Studies, 2020.;
- [24] Brandon VALERIANO – Benjamin JENSEN: *Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report*. In: T. JANCÁRKOVÁ, L. LINDSTRÖM, G. VISKY, P. ZOTZ (szerk.): 13th International Conference on Cyber Conflict: Going Viral, Tallinn, NATO CCD COE Publications, 2021
- [25] Nora VANAGA – Toms ROSTOKS (eds.): *Deterring Russia in Europe. Defence Strategies for Neighbouring States*. London – New York, Routledge, 2019.;
- [26] VÉGH Károly: *Információs és befolyásolási műveletek a nemzetközi jog „szürke zónájában”*. In: FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020., 191-212. o.;
- [27] VIKMAN László: *A német kiberbiztonsági szisztéma áttekintése. Szervezeti keretek, különös tekintettel a nemzetbiztonsági szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására*. In: Military and Intelligence CyberSecurity Research Paper 2021/2.;
- [28] VIKMAN László: *A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra*. In: Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2021/14.
- [29] Claire VISHIK - Mihoko MATSUBARA - Audrey PLONK: *Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms*. In: Anna-Maria Osula – Henry Roigas (ed.) *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn, NATO CCD COE Publications, 2016
- [30] Christopher WHYTE - Brian MAZANEC: *Understanding Cyber Warfare - Politics, Policy and Strategy*. Routledge, 2019.



IMPRESSZUM

Szerző(k):

Dr. Vikman László

Kézirat lezárásának ideje:

2022. Február 28.

Szerkesztők:

Dr. Farkas Ádám PhD
Dr. Glavanits Judit PhD
Dr. Karácsony Gergely PhD
Dr. Kelemen Roland

Dr. Keserű Barna Arnold PhD
Dr. Király Péter Bálint
Dr. Spitzer Jenő
Németh Richárd

Kiadó:

Smart Law Research Group

Elérhetőségek:

<http://smartlawresearch.hu/>

ISSN:

2732-3846

A borító a <https://wallpaperaccess.com/download/iot-3246253> címen elérhető ingyenes háttérkép felhasználásával 2021. február 15-én készült.

A sorozat egyes számaiban foglalt vélemények, állásfoglalások a szerzők saját véleményét tükrözik. Azok nem tekinthetők sem a kiadó, sem a szerzőt foglalkoztató intézmények hivatalos álláspontjának.

A sorozat célja a SmartLaw Reseach Group, illetve annak tagjai és esetleges külső együttműködők által végzett kutatások részeredményeinek közzététele a szakmai, tudományos megvitathatóság érdekében, illetve a későbbi publikációk előkészítésének támogatása érdekében.