Stratégiai Védelmi Kutatóközpont
ELEMZÉSEK 2017/3.

2017. március 3.

Beláz Annamária[1] – Berzsenyi Dániel[2]: Kiberbiztonsági Stratégia 2.0
A kiberbiztonság stratégiai irányításának kérdései[3]

Vezetői összefoglaló

- Az aktuális Nemzeti Kiberbiztonsági Stratégia kiadása (2013) óta eltelt időszak jelentős változásokat hozott a kiberbiztonság terén, amelyek indokolttá teszik a stratégia felülvizsgálatát, illetve egy új dokumentum megalkotását. A jelenlegi stratégia számos nemzetközi ajánlást és elvárást figyelmen kívül hagyott elfogadásakor, és a hazai beágyazottság tekintetében is vannak hiányosságai.
- Az új stratégiát új formában célszerű elkészíteni, kötelezően elkészítendő, rövid-középtávú stratégiai dokumentumtípusként, amelynek elfogadásához előzetes és utólagos értékelés elvégzése is szükséges lenne.
- A fenyegetettségek és a célkitűzések megalapozottságának érdekében az új stratégia kidolgozása előtt országos kiberbiztonsági kockázatelemzés és értékelés elvégzése szükséges.
- Az új stratégiához nyilvános végrehajtási terv kidolgozása, valamint a végrehajtás ellenőrzését szolgáló mérőszámok és indikátorok meghatározása kell, hogy kapcsolódjon – csak ezáltal válik eredményesen végrehajthatóvá. A mérőszámokhoz felelősöket és erőforrásokat is szükséges kapcsolni.
- A fogalmak, a célrendszer, valamint a fenyegetések meghatározását körültekintőbben szükséges elvégezni.
- Az életciklusmodell alkalmazása és a felülvizsgálatra vonatkozó szabályok ugyancsak meg kell, hogy jelenjenek a stratégiában.

Manapság egyre inkább közhelynek számít, hogy a hálózat alapú információs rendszerek létfontosságú szerepet játszanak társadalmunkban. Ezzel együtt az a nézet is egyre szélesebb társadalmi beágyazottságra talál, ami szerint ezeknek a rendszereknek a megbízható működése és biztonsága alapvető a gazdaság és a társadalom egészének működése szempontjából. Ugyanakkor az információs rendszereket érő, azok biztonságos működését veszélyeztető események nagyságrendje, gyakorisága és a hatása az elmúlt időszakban folyamatos növekedést mutat, miközben az előrejelzések szerint ez a trend a jövőben tovább erősödik. Az információs hálózatok és rendszerek transznacionális jellege miatt a működésben fellépő zavarok és azok hatásai nem állnak meg az országhatároknál, érinthetnek több országot, egy egész régiót, vagy akár a teljes Európai Uniót. Mindez felhívja a figyelmet arra, hogy az információs rendszerek biztonsága és védelme kiemelkedő fontosságú terület nemzeti és nemzetközi szinten egyaránt. A tanulmány a következő generációs kiberbiztonsági stratégia kidolgozói számára fogalmaz meg szakmai ajánlásokat elsősorban a nemzetközi elvárásoknak, valamint a kormányzati stratégiai irányítási rendszernek való megfelelés szempontjait szem előtt tartva.

Az információs rendszerek, a bennük előállított, tárolt, továbbított adatok, valamint a felhasználók által alkotott kibertér biztonsága érdekében szükséges, hogy Magyarország rendelkezzen azokkal a minimumképességekkel, amelyek biztosítani tudják a megfelelő szintű védelmet, és amelyek képessé teszik az országot a nemzetközi együttműködésekben való eredményes részvételre. A kapcsolódó, nemzeti szinten megvalósítandó feladatok legmagasabb szintű dokumentuma a Nemzeti Kiberbiztonsági Stratégia. A jelenlegi stratégiát 2013-ban fogadták el, így pusztán a „korát" tekintve egyáltalán nem számít elavult dokumentumnak még nemzetközi szinten sem – ugyanakkor a kiadás óta eltelt időszakban számos olyan változás történt, ami indokolttá teheti az eredetileg is több hiányossággal küzdő dokumentum felülvizsgálatát. Napjainkban egyre több országban jelennek meg úgynevezett „második generációs" (2.0-s) kiberbiztonsági stratégiai dokumentumok, amelyek több ponton is eltérnek első generációs társaiktól.

[1] Beláz Annamária (belazannamaria@gmail.com) a Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Kar közigazgatási szakértő (közigazgatás-tudományi szakirány) MA szakos hallgatója, a Stratégiai Védelmi Kutatóközpont szakmai gyakornoka.
[2] Berzsenyi Dániel (berzsenyi.daniel@uni-nke.hu) okleveles biztonság- és védelempolitikai szakértő, a Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola doktorandusza.
[3] A szerzők ezúton fejezik ki köszönetüket azoknak a szakembereknek, akik gondolataikkal és véleményükkel inspirálták a tanulmány elkészítését, köztük Prof. Dr. Rajnai Zoltánnak, Dr. Muha Lajosnak, Dr. Krasznay Csabának és Dr. Rain Ottisnak.

A legtöbb országban az első generációs kiberbiztonsági stratégiák arra koncentráltak, hogy a kiberteret, mint a nemzet biztonsága szempontjából fontos területet azonosítsák és jelenítsék még, ennek megfelelően kijelöljék a jelentősebb kormányzati szereplőket és felelősöket, továbbá létrehozzák és fejlesszék azokat a kormányzati szervezeteket és koncepciókat, amelyek elengedhetetlenek a kibertérből érkező kihívások és fenyegetések nemzeti szintű kezeléséhez. Sok esetben az első generációs stratégiákban leírt folyamatok megvalósítását a nulláról kellett elkezdeniük a kormányoknak, ezért tekinthetők egyfajta alapító dokumentumnak is a kibertér biztonságára vonatkozó nemzeti szintű igény és felelősség kinyilvánítása aspektusából. Ezzel szemben a következő generációs kiberbiztonsággal foglalkozó stratégiai dokumentumok már egy olyan környezetre próbálnak reagálni, ahol az alapvető kiberbiztonsági koordináció megvalósul a létrejött kormányzati álláspontoknak és szervezeteknek köszönhetően, illetve egyetlen szereplő sem kérdőjelezi meg a kiberbiztonság helyét és szerepét nemzetbiztonsági szempontból. Ennek megfelelően a következő generációs kiberbiztonsági stratégiai dokumentumok letisztult képet nyújtanak a kiberbiztonsági kihívásokról és fenyegetésekről; egyértelmű, jól definiált célkitűzéseket tartalmaznak; nagy hangsúlyt fektetnek a konkrét kiberképességek kialakítására, illetve továbbfejlesztésére; amihez a leírtak követhetőségét és a számonkérést segítő passzusok, illetve kiegészítő dokumentumok kapcsolódnak.

A tanulmány célja elsősorban a jelenleg hatályos Nemzeti Kiberbiztonsági Stratégia (továbbiakban: NKBS) vizsgálata a nemzetközi ajánlásoknak, valamint az Európai Parlament és a Tanács, a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016/1148 irányelvének (továbbiakban: NIS Irányelv) való megfelelés szempontjából. A tanulmány elkészítése közben a szerzők törekedtek arra, hogy a hazai jogszabályi környezet perspektívájából is megvizsgálják az NKBS-t, ezen belül is elsősorban a stratégiai dokumentumokra vonatkozó iránymutatások domináltak. Az analízis eredményeire alapozva a tanulmány néhány ajánlást is megfogalmaz, amelyek egy új nemzeti kiberbiztonsági stratégia megalkotása során segíthetik a folyamatban szerepet vállaló szervezetek és szakemberek munkáját annak érdekében, hogy a dokumentum minél magasabb szinten teljesítse az általános szakmai, a nemzetközi szövetségesi, valamint a hazai jogszabályi elvárásokat.

A fogalmi keretek tisztázása

Tekintettel arra, hogy a tudományos gondolkodás és kutatás kiindulópontját mindig a vizsgált terület fogalomrendszerének áttekintése adja, érdemes megvizsgálni legalább a kiberbiztonság fogalmát anélkül, hogy a fogalmi keretek tisztázása kapcsán túl mélyre merülnénk a kérdésben. „Kézenfekvőnek tűnhet, hogy a kölcsönös megértés, a világos és egyértelmű kommunikáció, vagy éppen a félreértések elkerülése céljából az azonos területen megfogalmazott politikák és stratégiák terminológiája egyforma, és az egyes fogalmakat ugyanolyan jelentéstartalommal tölti meg minden érintett. Azonban ez koránt sincs így, az államok gyakran használnak eltérő fogalmakat különböző dokumentumaikban (jogszabályok, stratégiák, ajánlások, iránymutatások, stb.), ami nemzeti és nemzetközi szinten is értelmezési problémákhoz vezethet.”[4] Mivel napjainkban a legtöbb kiberbiztonsághoz kapcsolódó dokumentum eltérő fogalmakat használ nem csak nemzetközi, de nemzeti szinten is, gyakran a fogalmi keretek tisztázása az egyik legnehézkesebb feladat a kiberbiztonság területén tevékenykedő stratégák számára. Mindez érthetővé teszi azon szakemberek álláspontját, akik szerint a terminológiai kérdéseket célszerű félretenni és más területekre koncentrálni, amelyek gyorsabb, látványosabb eredményeket hozhatnak. Ugyanakkor a nemzetközi ajánlásoknak és elvárásoknak való megfelelés szempontjából kifejezetten fontos, hogy ismerjük a kiberbiztonság meghatározásának különböző aspektusait, hiszen a későbbiekben is látható lesz, hogy a terminológiai definíciók és a következetes alkalmazás egyre nagyobb szerepet kap.

A kibertér (cyberspace) és a biztonság közötti összefüggések meghatározására alakult ki a kiberbiztonság (cybersecurity) kifejezés, amelyet az informatikai szakembereken túl ma már tanácsadók, elemzők, lobbisták és politikai szereplők is egyaránt használnak egyre szélesebb körben. Ezen a ponton számtalan kérdés merülhet fel a kifejezés tartalma, használata, vagy akár az érintett folyamatok, eszközök és felhasználók tekintetében. A kiberbiztonság fogalmi kereteinek megállapítását nem könnyíti meg az a folyamat, aminek nyomán az utóbbi időben egyre elterjedtebb a kifejezés használata a médiában is. A tömegtájékoztatásban a kiberbiztonság kifejezést túl általános és sokszor leegyszerűsített formában használják minden olyan eseménnyel kapcsolatban, amely a számítógépek működését megzavarja.

Az Amerikai Egyesült Államok Belbiztonsági Minisztériuma által működtetett kormányzati számítógépes eseménykezelő szervezet honlapján egyből két definíció is található a kiberbiztonságra vonatkozóan. A rövidebb meghatározás

[4] BERZSENYI Dániel: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbztonsági stratégiák összehasonlító elemzése, *Nemzet és Biztonság – Biztonságpolitikai Szemle*, VII. évf., 2014/6., 130. o.

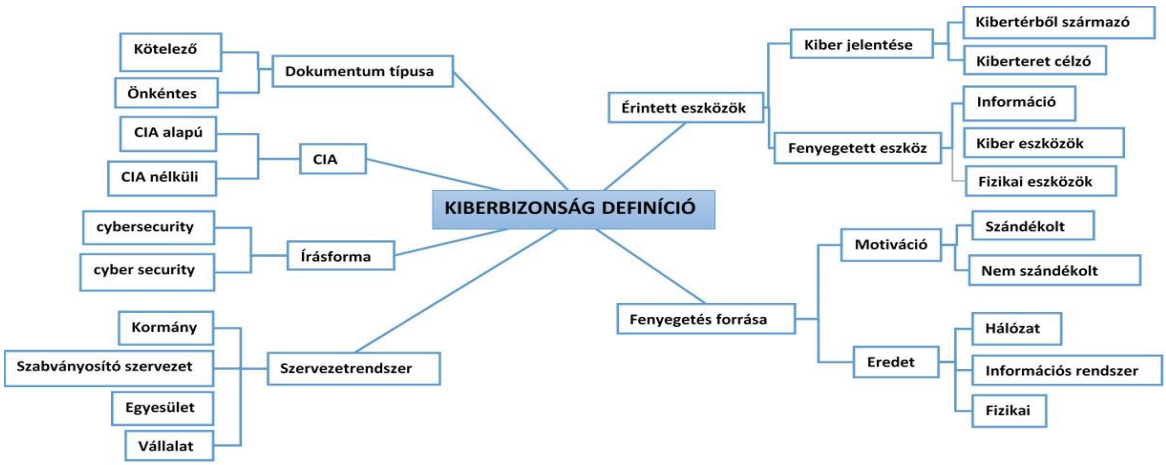
értelmében a kiberbiztonság olyan tevékenység, folyamat, lehetőség, képesség, vagy állapot, ahol az információs és kommunikációs rendszerek és a bennük található információ védettek a károsodástól, az illetéktelen hozzáféréstől és módosítástól, valamint a kihasználástól.[5] Az, hogy közvetlenül a meghatározás mellett szerepel egy bővebb, sok szempontból átfogóbb leírása is, illetve számos kormányzati dokumentumot és direktívát is feltüntettek forrásként, arra enged következtetni, hogy az amerikai kormányzati lexikon összeállítói számára is nehézséget okozott a kiberbiztonság definiálása. A helyzet nem válik egyszerűbbé akkor sem, ha a kiberbiztonságot valamilyen specifikus ágazati nézőpontból vizsgálva próbáljuk meghatározni, mint amilyen a kritikus infrastruktúrák üzemeltetése, vagy a katonaság.

Katonai megközelítésben a kiberbiztonság például egy tágabb és többnyire a stratégiai nézőpontot sem nélkülöző fogalom, ami szoros kapcsolatban áll a kibervédelem (cyberdefense) és a kiberháború (cyberwar) kifejezésekkel. Az Amerikai Egyesült Államok Védelmi Minisztériuma által kiadott katonai szótár alapján a kiberbiztonság nem más, mint a számítógépek, elektronikus kommunikációs rendszerek és szolgáltatások, valamint a vezetékes kommunikáció és elektronikus kommunikáció sérülésének megelőzése, védelme és visszaállítása a bennük található információkkal együtt, továbbá a rendelkezésre állás, az integritás, a bizalmasság, a letagadhatatlanság és a hitelesítés biztosítása.[6]

Tekintettel a fent leírtakra, a kiberbiztonság meghatározásakor érdemes számításba venni az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (továbbiakban: ENISA) által megadott[7] 5 fő területet, amit a szervezet szerint a kiberbiztonság fogalma lefed:

1. A kommunikáció biztonsága: Az információs rendszer technikai infrastruktúrájának védelme.
2. A működés biztonsága: A munkafolyamatok szándékos megzavarása, megváltoztatása elleni védelem.
3. Az információs biztonsága: Az információs rendszerben tárolt vagy továbbított adat lopással, törléssel vagy megváltoztatással szembeni védelme.
4. A fizikai biztonság: Az információs rendszer védelme a fizikai veszélyektől (például: számítógépekhez való hozzáférés, fertőzött hardver beépítése a hálózatba, stb.)
5. Közbiztonság/Nemzetbiztonság: A kibertérből származó olyan fenyegetések elleni védekezés, amelyek egyaránt veszélyeztethetik a fizikai rendszereket és a kiberteret (például: Stuxnet, vagy kiterjedt szolgáltatás megtagadással járó támadás egy kritikus információs infrastruktúra ellen), egyúttal a támadó számára politikai, katonai vagy stratégiai előny megszerzését jelentik.

Az ENISA említett elemzése szerint a kiberbiztonság fogalmát további építőelemekre és komponensekre bonthatjuk:



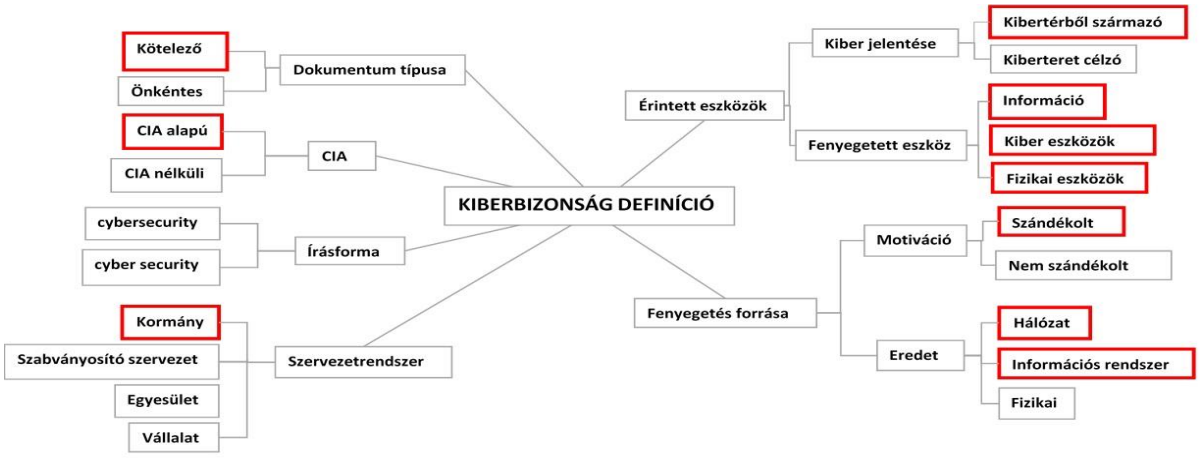
1. ábra: A kiberbiztonság fogalmát alkotó komponensek

[5] „Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.” Department of Homeland Security: National Initiative for Cybersecurity Careers and Studies – Glossary, [online], NICCS [2017. 02. 18.]

[6] „Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.” Department of Defense: Dictionary of Military and Associated Terms, [online], Dtic.mil [2017. 02. 18.]

[7] Charles BROOKSON (et al.): Definition of Cybersecurity – Gaps and overlaps in standardization v1.0, [online], 2015, ENISA [2017. 01. 08.]

A tanulmány vizsgálatának középpontjában álló NKBS az alábbiak szerint definiálja a kiberbiztonság fogalmát: „A kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez."[8] A definíció és az NKBS „Magyarország kiberbiztonsági környezete" című része alapján az ENISA ábráját követve az alábbiak szerint adhatók meg a magyar kiberbiztonsági fogalom komponensei:



2. ábra: A kiberbiztonság fogalmának (piros színnel jelölt) komponensei az NKBS definíciója alapján

Bár jelen esetben az ENSZ szakosított ügynöksége, az International Telecommunications Union (ITU) és a NATO vonatkozó ajánlásaiban szereplő meghatározások fentiekhez hasonló részletes ábrázolására nem kerül sor, elmondható, hogy az NKBS a két szervezethez képest valamivel tágabb, általánosabb definíciót használ. Ez önmagában nem jelentene problémát, azonban a nemzetközi ajánlásokban az egyes komponensek részletesen kifejtésre kerülnek, míg az NKBS ebben a tekintetben nem sok támpontot biztosít a stratégia megvalósításához, hiányoznak a gyakorlati iránymutatások és konkrétumok. Más országokban és nemzetközi szinten is gyakran alkalmazott megoldás, hogy a kereteket meghatározó felső szintű dokumentumokhoz olyan, szintén nyilvános akciótervek készülnek[9], amelyek részletesen tartalmazzák a kitűzött célokhoz vezető folyamatokat és azok megvalósításának lépéseit a hozzárendelt erőforrásokkal együtt. Mindez elvezet a tanulmány következő témaköréhez, amely az NKBS részletesebb elemzésével továbbra sem szakad el a fogalmi problémáktól.

A kiberbiztonsági stratégiaalkotás nemzetközi keretrendszere

Az NKBS elemzéséhez és értelmezéséhez, valamint a stratégiai dokumentumok hierarchiájában betöltött szerepének meghatározásához a kiberbiztonság után szükséges a stratégia fogalmára is röviden kitérni. Közpolitikai szempontból a stratégia egy meghatározott cél, állapot elérése érdekében végrehajtandó cselekvések, akciók hosszú távú terve.[10] A stratégiai dokumentum a cselekvések végrehajtása érdekében felelősöket jelöl ki, az akciókhoz erőforrásokat rendel. A stratégiai tervezés során a cél eléréséhez szükséges cselekmények részletes és módszertani szempontból következetes kidolgozása történik meg, beleértve a stratégia értékeléséhez és finomhangolásához szükséges folyamatokat is.[11]

[8] 1139/2013. (III. 21.) Kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 5. pont
[9] Lásd az Amerikai Egyesült Államokban az Obama-adminisztráció által kiadott: 2015 Cybersecurity Strategy and Implementation Plan c. dokumentumot [online], 2015, Obamawhitehouse.archives.gov [2017. 02. 05.], vagy Koszovó esetében a National Cyber Security Strategy and Action Plan 2016 – 2019 stratégiát, [online], 2015, Kryeministri-ks.net [2017. 02. 05.]
[10] George A. STEINER: *Strategic Planning*, Simon&Schuster, New York, 1979, 12-34. oldal
[11] A stratégiaalkotás európai tapasztalatairól és értékelési szempontjairól lásd: CSIKI Tamás: Az új Nemzeti Katonai Stratégia a nemzetközi tapasztalatok tükrében, *Nemzet és Biztonság – Biztonságpolitikai Szemle*, VII. évf., 2014/2., 46-47. o.

A Magyary-program keretében[12] 2012 elején sor került a stratégiai tervezés és irányítás teljes hazai rendszerének átalakítására. Ezt a változást az a felismerés indukálta, hogy a korábban létrehozott strukturálisan és módszertanilag heterogén, tartalmilag összeegyeztethetetlen stratégiaszerű dokumentumok végrehajtása lehetetlennek bizonyult. A stratégiaalkotási és irányítási tevékenység megújítását és a stratégiák tartalmi összehangolásához szükséges keretek kialakítását a kormány új kormányzati stratégiai irányításról szóló rendelete[13] valósította meg. A rendelet egyik célja, hogy hozzájáruljon ahhoz, hogy a stratégiai szemlélet a kormányzati tervezés részévé váljon, a stratégiai dokumentumok pedig egy átlátható, hierarchikus rendszerbe illeszkedjenek.

Bár az első magyar kiberbiztonsági stratégia már az új stratégiai tervezési rendszer kialakítását és hatályba lépését követően, 2013-ban került kiadásra, annak szabályait és elvárásait figyelmen kívül hagyta. A stratégia nem hivatkozik a stratégiai tervezési rendszerről szóló rendeletre, és jelenlegi állapotában nem feleltethető meg egyetlen, a rendeletben említett stratégiai dokumentum típusnak sem. Annak ellenére, hogy az NKBS a stratégiák elkészítésére vonatkozó hazai szempontrendszernek nem felel meg és nemzetközi összehasonlításban is számos hiányossága felróható, a dokumentum rámutatott számos olyan területre és kérdésre a kiberbiztonság kapcsán, amelyek napjainkban már nem csak a szakembereket, hanem egyre inkább a közvéleményt is foglalkoztatják. Az NKBS-sel együtt elfogadott és azóta módosított 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban: Ibtv.) megteremtette azt a jogszabályi környezetet, amely elősegítette a kiberbiztonság területén működő állami szervezetek kialakítását és megszilárdítását. Többek között ezeknek a stratégiai és jogszabályi törekvéseknek köszönhetően volt Magyarország 2013-ban nemzetközi szinten 6., az Európai Unió országaihoz viszonyítva a 3. helyen a kiberbiztonsági felkészültség világranglistáján (Global Cybersecurity Index).[14]

Bár az NKBS-hez kapcsolódó stratégiákat és jogszabályokat hosszasan lehetne sorolni, jelen tanulmány szempontjából fontosabbak azok a nemzetközi irányelvek és ajánlások, amelyeket a nemzeti kiberbiztonsági stratégiák készítői számára írtak azzal a céllal, hogy a nemzeti szintű dokumentumok struktúrája és terminológiája egyfelől illeszkedjen a nemzetközi trendekhez – ezáltal is növelve a beágyazottságukat –, másfelől minél inkább illeszkedjenek az adott nemzet képességeihez és lehetőségeihez. A következőkben ezen ajánlások alapján értékeljük az NKBS-t.

Az International Telecommunications Union (ITU) ajánlásai

Az NKBS elemzésekor meghatározó szervezet az ITU, amely 1947 óta működik az ENSZ szakosított szerveként, 193 tagállamában közel 700 ágazati és társult tagja van. Elsődleges feladata a nemzetközi együttműködés megteremtése az infokommunikációs szabványosításban a hálózatok problémamentes összekapcsolása érdekében, különösen a rádióspektrum és a műholdas pályapozíciók globális felosztása területén.[15] Világértekezletein, kutató- és munkacsoportjain keresztül nem kötelező jellegű, de tudományosan megalapozott eredményeket és jó gyakorlatokat tartalmazó, egységes módszertant és tervezési rendszert biztosító ajánlásokat és jelentéseket fogalmaz meg.

Az ENSZ Közgyűlés jóváhagyásával 2001-ben az ITU Tanácsa döntött az Információs Társadalom Világtalálkozójának megszervezéséről. A találkozó első szakasza 2003-ban Genfben, második fázisa 2005-ben Tunéziában zajlott. A csúcstalálkozó lezártával az ITU új alapvető funkciójává lépett elő az információs és kommunikációs technológiák használói közötti bizalomépítés, valamint az infokommunikációs és távközlési rendszerek biztonságának erősítése.[16] 2007-ben a szervezet felállította a Globális Kiberbiztonsági Napirendet (Global Cybersecuirty Agenda[17]), amely nemzetközi keretként szolgál a kiberbiztonság területén keletkező kihívások leküzdésére. A nemzeti kiberbiztonsági stratégiák elkészítésének, tartalmi elemeinek és fejlesztésének elősegítésére 2011-ben a szervezet kiadott egy gyakorlati kézikönyvet[18], amely napjainkig alapul szolgál a kiberteret érintő stratégiák elemzésekor.

---

[12] A Magyary Program Stratégiai Irányítási Rendszerrel kapcsolatos intézkedési tervéről bővebb információ: http://magyaryprogram.kormany.hu/strategiai-iranyitasi-rendszer, [online], 2017, Magyaryprogram.kormany.hu [2017. 01. 08.]

[13] 38/2012. (III. 12.) Kormányrendelet a kormányzati stratégiai irányításról

[14] Global Cybersecurity Index & Cyberwellness Profiles 2015 Report, [online], 2015, ABI Research – ITU [2017. 01. 08.]

[15] A globalizálódó világ újabb és újabb beavatkozási területeket hoz létre az ITU számára. Napjainkban a szabványosítási tevékenységen túl speciális programjai, cselekvési és akciótervei vannak, melyek magukba foglalják a kiberbiztonság, a klímaváltozás, a digitális szakadék, a nyílt internet, az esélyegyenlőség, a fiatalok képzésének és a fejlődő országok felzárkóztatásának kérdéseit.

[16] UN General Assembly Resolution 56/183 (2001. 12. 21.), [online], 2001, Itu.int [2017. 01. 08.]

[17] Bővebb információért lásd: Global Cybersecurity Agenda, [online], 2017, Itu.int [2017. 01. 08.]

[18] Frederick WAMALA: The ITU National Cybersecurity Strategy Guide, [online], 2012, Itu.int [2016. 10. 22.]

Az European Union Agency for Network and Information Security (ENISA) ajánlásai

Hazánk Európai Uniós tagságából fakadóan a kiberbiztonságban fontos szerepet tölt be az Európai Unió döntése alapján, a működését 2005 szeptemberében Krétán megkezdő[19], az EU-tagállamok és az üzleti szféra hálózat- és információbiztonságának erősítését, a felmerülő problémáik kezelését segítő és a területen tudományos tevékenységet folytató szervezet, az ENISA. Az ügynökség feladatai között szerepel többek között a kockázatelemzéshez szükséges információk gyűjtése, a biztonsági problémák megelőzésére szolgáló közös módszerek kidolgozása, a tudatosság növeléséhez való hozzájárulás, a biztonsági szabványok kialakításának követése, saját iránymutatásainak megfogalmazása, valamint tanácsadó tevékenység ellátása az Európai Bizottság mellett.

A szervezet számos iránymutatást, ajánlást, útmutatót és kézikönyvet adott ki, amelyek közül a nemzeti kiberbiztonsági stratégiák fejlesztésére és végrehajtására vonatkozó, 2012 decemberében elkészült gyakorlati útmutató[20] meghatározó a nemzeti kiberbiztonsági stratégiák nemzetközi beágyazottságának vizsgálatakor. A nemzeti kiberbiztonsági stratégiák elemzéséhez, felülvizsgálatához és tovább fejlesztéséhez egy további gyakorlati kézikönyvet[21] adott ki a szervezet. A kézikönyvben foglaltak segítséget nyújtanak a tervezők számára a kiberbiztonsági stratégia hiányosságainak feltárásában, valamint a stratégia végrehajtásának ellenőrzéséhez nélkülözhetetlen indikátorok kijelölésében. Az elmúlt időszakban számos a kiberbiztonságra vonatkozó az Unió egészét érintő jogi, közpolitikai változás ment végbe,[22] ennek eredményeként az ügynökség egy új kézikönyvet adott ki[23] a tagállamok nemzeti kiberbiztonsági stratégiájának elkészítéséhez. Az útmutató részletesen elemzi a kiberbiztonsági stratégiák javasolt tartalmi elemeit, megalkotásuk és fejlesztésük módját, főbb fázisait, az egyes lépésekhez kapcsolódó jó gyakorlatokat, ajánlásokat és politikákat.

A NATO ajánlásai

Az Észak-atlanti Szerződés Szervezetében a kiberbiztonsági kihívásokkal kapcsolatos tevékenységek egyik legfőbb letéteményese a 2008-ban létrejött és a szervezet által akkreditált Kooperatív Kibervédelmi Kiválósági Központ.[24] A központ a kiberbiztonság területén oktatással, konzultációval, kutatással és fejlesztéssel foglalkozik, számos online és nyomtatott formában is elérhető kiadványuk kötődik a kiberkonfliktusok és kiberhadviselés etikai, illetve jogi kérdéseihez, a megfelelő kibervédelem kialakításához. Foglalkoznak technológiai témákkal, valamint a kiberbiztonsági stratégiák elkészítésével és fejlesztésével.

[19] A szervet Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról című jogi aktus révén jött létre, amelyet 2008-as és 2011-es módosítását követően 2013-ban helyezett hatályon kívül az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA).

[20] Nicole FALESSI (et al.): National Cyber Security Strategies – Practical Guide on Development and Execution, [online], 2012, Enisa.europa.eu [2016. 10. 22.]

[21] Dimitra LIVERI – Anna SARRI: An Evaluation Framework for National Cyber Security Strategies, [online], 2012, Enisa.europa.eu [2016. 10. 22.]

[22] Többek között: Közös Közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Az Európai Unió Kiberbiztonsági Stratégiája: Nyílt, megbízható és biztonságos kibertér, [online], 2013, Eur-lex.europa.eu [2016. 10. 22.]; Az Európai Parlament és a Tanács 910/2014/EU Rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről, [online], 2014, Eur-lex.europa.eu [2016. 11. 25.]; Az Európai Parlament és a Tanács 2013/40/EU Irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról, [online], 2013, Eur-lex.europa.eu [2016. 10. 22.]

[23] ENISA National Cyber Security Strategy experts group: NCSS Good Practice Guide – Desingning and Implementing National Cyber Security Strategies, [online], 2016. november, Eur-lex.europa.eu [2016. 11. 25.]

[24] A NATO Kooperatív Kibervédelmi Kiválósági Központ (*NATO Cooperative Cyber Defence Centre of Excellence* – NATO CCDCOE) alapítására vonatkozó koncepciót 2006-ban hagyta jóvá a Szövetséges Erők Transzformációs Parancsnokságának parancsnoka, 2007-ben kezdődtek meg a szponzornemzetek közötti tárgyalások. 2008 májusában Észtország, Németország, Olaszország, Lettország, Litvánia, Szlovákia és Spanyolország aláírta az alapításról szóló egyetértési megállapodást. Az alapító tagokon túl a központ jelenlegi szponzor államai: Amerikai Egyesült Államok, Ausztria, Csehország, Egyesült Királyság, Finnország, Franciaország, Görögország, Hollandia, Lengyelország, Magyarország és Törökország.

2012 decemberében jelent meg az a nemzeti kiberbiztonsági keretrendszert bemutató kézikönyv,[25] amely részletes háttérinformációkat és elméleti kereteket biztosít a nemzeti kiberbiztonság különböző vetületeinek megértéséhez. Az ITU és az ENISA kézikönyvéhez hasonlóan iránymutatást nyújt a nemzeti kiberstratégia megalkotásához, az alkalmazási terület kijelöléséhez, az együttműködés dimenzióinak meghatározásához és a szabályozásra szoruló kritikus kérdések azonosításához.

A Nemzeti Kiberbiztonsági Stratégia értékelése

A bemutatott szervezetek ajánlásai és vonatkozó dokumentumai alapján összeállított mátrix eredményeit az alábbi táblázatok összesítik, amelyekből kiderülnek a nemzetközi szinten megjelenő legfontosabb elvárások egy nemzeti kiberbiztonsági stratégiával szemben, illetve látható, hogy ezekből az NKBS mely elvárásokat és ajánlásokat teljesíti.

A Nemzeti Kiberbiztonsági Stratégia alapvető tulajdonságai és beágyazottsága a nemzetközi ajánlások és elvárások tükrében	
Kiadás éve	2013
Első kiberstratégia?	Igen
Hossza	4 oldal (12 pont)
IKT mely típusait érinti?	Elektronikus információs rendszerek, és azokon keresztüláramló adatok formájában megjelenő társadalmi és gazdasági folyamatok
Utal a következőre?	
Nemzeti Biztonsági Stratégia	■ (annak 31. pontjára)
Kritikus infrastruktúra védelmi stratégia	□
Nemzeti digitális menetrend	□
EU digitális menetrend (EC, 2010)	■
Nemzeti Katonai Stratégia	□
Egyéb	Alaptörvény, Budapesti Konvenció, EU Kiberbiztonsági Stratégia, NATO Stratégiai koncepció

1. táblázat: A Nemzeti Kiberbiztonsági Stratégia és a nemzetközi ajánlásoknak való megfelelés a stratégiai dokumentumok kapcsolódása szempontjából. *(Jelmagyarázat: Az adott komponenseket tartalmazza-e a Nemzeti Kiberbiztonsági Stratégia? ■ = igen, □ = nem)*

Az 1. táblázatból kiderül, hogy az NKBS logikai szempontból szoros összefüggésben áll több felső szintű dokumentummal is, így hivatkozik az Alaptörvényre, a Budapesti Konvencióra, az EU Kiberbiztonsági Stratégiájára és a NATO Stratégiai Koncepciójára is, illetve a Nemzeti Biztonsági Stratégia 31. pontjára hivatkozva, *„abból kiindulva kifejti […] a meghatározott törekvéseket és megfogalmazott kormányzati felelősséget”*.[26] Nincsenek letisztázva a közvetlen kapcsolódási pontok olyan területekkel, mint például a kritikus infrastruktúrák védelme, vagy a digitális társadalom nemzeti szintű fejlődése. Előbbi területet ugyan megnevezik a célrendszerben, de a vonatkozó kormányrendeletet nem említi az NKBS, ahogyan az utóbbi területhez történő kapcsolódás sem megoldott, mivel Nemzeti Infokommunikációs Stratégia és a Digitális Nemzeti Fejlesztési Program is később jelent meg. Bár a Nemzeti Katonai Stratégia három hónappal korábban jelent meg, az NKBS ehhez sem kapcsolódik közvetlenül. Mivel az eltelt időszakban a NATO hivatalosan is a hadviselés ötödik dimenziójává nyilvánította a kiberteret, ez a tény indokolttá tenné a stratégiák közötti összefüggések és kapcsolatok explicit megjelenítését.

[25] Alexander KLIMBURG (szerk.): National Cyber Security Framework Manual, [online], 2012. december, Ccdcoe.org [2016. 10. 22.]
[26] 1139/2013. (III. 21.) Kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 2. pont

A Nemzeti Kiberbiztonsági Stratégia fenyegetésekre és célrendszerre vonatkozó komponensei a nemzetközi ajánlások és elvárások tükrében	
A fenyegetések a következő területeket érinthetik	
Kritikus infrastruktúra	Explicit
Védelmi képességek	Explicit
Gazdasági teljesítőképesség	Explicit
Globalizáció	□
Nemzetbiztonság	Explicit
Közbizalom az infokommunikációs technológiákban	Implicit
Polgárok szociális élete	Explicit
Kiberfenyegetés fajtái (motiváció)	
Aktivisták/szélsőséges csoportok	□
Bűnözők, szervezett bűnözés	□
Kémkedés	□
Kiberhadviselés	■
Terrorizmus	□
Célrendszer, vízió	
Katonai kiberképességek	□
Kiberbűnözés elleni fellépés	□
Hírszerzés és elhárítás	□
Kritikus infrastruktúra védelme, válságkezelés	■
Kiberdiplomácia	□
Internetszabályozás és igazgatás	□

2. táblázat: A Nemzeti Kiberbiztonsági Stratégia és a nemzetközi ajánlásoknak való megfelelés a fenyegetések és intézkedési célrendszer szempontjából. *(Jelmagyarázat: Az adott komponenseket tartalmazza-e a Nemzeti Kiberbiztonsági Stratégia? ■ = igen, □ = nem)*

Az NKBS a fenyegetési formákra vonatkozóan viszonylag kevés egzakt ténymegállapítást tartalmaz. Bár a kiberfenyegetések és azok formái többféle szempontrendszer alapján is csoportosíthatók, az NKBS meg sem próbál kísérletet tenni arra, hogy a különböző fenyegetési formákat kategorizálja, vagy még tovább menve, esetleg osztályozza azokat a fenyegetés mértékének, illetve hazai percepciónak megfelelően. A kiberfenyegetések formái között a modern hadviselés egyik legfontosabb dimenziójaként szóba kerül a kibertér és a kiberháború. Ennek lehetőségét nem is lehet kizárni, azonban kiberháború hiányában, békeidőben is akad számos olyan fenyegetés a kibertérben – többek között a terrorizmus, a kémkedés vagy a szervezett bűnözés kifejezetten erre a dimenzióra specializálódott fajtái – amelyekkel szemben a hatékony fellépés egyre sürgetőbb. Hasonlóan szűkszavú az NKBS a célrendszer, illetve a vízió tekintetében. A kritikus infrastruktúrák védelmén és a válságkezelésen túlmenően nincs olyan célterület, ahol a dokumentum konkrétumokat jelölne meg a végrehajtók számára.

A Nemzeti Kiberbiztonsági Stratégia komponensei az alapelvek, a definíciók, az érintettek körének és a kormányzati struktúra meghatározására vonatkozó nemzetközi ajánlások tükrében	
Alapelvek	□
Definíciók és legfontosabb kihívások, veszélyek azonosítása	■
Kormányzati struktúra	Említésre kerül: Koordinációs Tanács és összkormányzati koordináció, CERT-ek Nem kerül megemlítésre: Koordinációs Fórum, Kibervédelmi Koordinátor vagy más szervezetek

Érintettek	
Polgárok	■
Kis- és középvállalkozások, nagyvállalatok	(Gazdasági társaságok általában)
Internet szolgáltatók	□
Kritikus infrastruktúra szolgáltatók	□
Nemzeti biztonság	■
Globális infrastruktúrák, ügyek	■
Operatív szintű cselekvési tervek	
SMART (specifikus, mérhető, elérhető, realisztikus, időszerű)	□
Jövőbeli veszélyekhez való alkalmazkodás	□

3. táblázat: A Nemzeti Kiberbiztonsági Stratégia és a nemzetközi ajánlásoknak való megfelelés. *(Jelmagyarázat: Az adott komponenseket tartalmazza-e a Nemzeti Kiberbiztonsági Stratégia? ■ = igen, □ = nem)*

Az NKBS tartalmazza a kiberbiztonság definícióját és azonosít néhány kiemelten fontos kihívást és veszélyt, (többek között a kritikus adatok, információk illegális megszerzését, a kommunikációs és informatikai rendszerekben történő károkozást, az információs hadviselést; az informatikai és hírközlési rendszerek üzembiztonsági szabályozása körében tapasztalható hiányosságokat, a megjelenő új technológiákat (például az informatikai felhőt vagy a mobilinternetet), továbbá kitér a dokumentum által érintett szereplőkre is. Az NKBS ugyanakkor nem határoz meg alapelveket, amelyek mentén a stratégia készült, vagy amelyeket a végrehajtás közben követni lehetne. Az operatív szintű cselekvési tervek és összességében az egész stratégia tekintetében a legfájóbb pont az úgynevezett SMART[27] (Specific, Measurable, Achievable, Realistic, Timely) elemek hiánya, amelyek a specifikusság, mérhetőség, elérhetőség, realisztikusság és időszerűség kritériumrendszere mentén nyújtanának egyértelmű iránymutatást a stratégia végrehajtói számára.

A Nemzeti Kiberbiztonsági Stratégia cselekvési tervekre és végrehajtásra vonatkozó komponensei a nemzetközi ajánlások és elvárások tükrében	
Részletes cselekvési terv	
Dinamikus biztonsági mérőszámok	□
Figyelemfelkeltés és oktatás	■
Veszélyhelyzeti és folytonossági tervek	□
Kritikus infrastruktúra védelem	Részben
Kriptográfiai védelem	□
Kibervédelmi műveletek, képzés, gyakorlatok	■
Jó gyakorlatok gyűjtése és megosztása	□
Infokommunikációs technológiát (IKT) alkalmazó termékek biztonságának erősítése	■
Információmegosztás	■
Nemzetközi együttműködés	■
Jogi keretrendszer, szabályozás	■
Biztonsági standardok, alapvető előírások	„Legmagasabb szintű”, érje el a legjobb nemzetközi gyakorlatokét, feleljen meg a hazai és nemzetközi szabványoknak
Nemzeti észlelési képességek	□
IKT válságmenedzsment, incidens jelentési rendszer	□
Személyes adatok védelme	Részben (nemzeti adatvagyon védelme)

[27] Kelvin F. CROSS, Richard L. LYNCH: The “SMART” way to define and sustain success. *National Productivity Review*, VIII. évf., 1988-89/1., 23-33 o.

Köz- és magánszektor együttműködése	■
Kutatás-fejlesztés	■
Fenyegetettségek csökkentése	■
Kiberbűnözés visszaszorítására tett lépések	□
Protokoll és szoftver biztonság	□
Kormányzati szféra védelme	Csak „kormányzati koordináció”
Stratégiai kiberbiztonsági tanács	□
Fenyegetettség és sérülékenység vizsgálat	□
Stratégia végrehajtása és felülvizsgálata	
Végrehajtási ideje, irányításáért felelős személyek, szervezetek	□
Végrehajtás mérése (mutatók, indikátorok)	□
Végrehajtás költségvetése	□
Felülvizsgálat ideje, rendszere	□

4. táblázat: A Nemzeti Kiberbiztonsági Stratégia és a nemzetközi ajánlásoknak való megfelelés a cselekvési tervek, a végrehajtás és a felülvizsgálat szempontjából. *(Jelmagyarázat: Az adott komponenseket tartalmazza-e a Nemzeti Kiberbiztonsági Stratégia? ■ = igen, □ = nem)*

A cselekvési tervek kapcsán jól látszik, hogy az NKBS, még ha sokszor csak említés szintjén is, de számos nemzetközi elvárásnak és ajánlásnak eleget tesz a jelenlegi formájában, ugyanakkor több szempont még csak említésre sem kerül, vagy érdemben nem reflektál a stratégia az adott területre. Bár irreális elvárás lenne egy kiberbiztonsági stratégiával szemben, hogy a létező összes ajánlásnak és elvárásnak megfeleljen, a SMART elemek hiányához hasonlóan fontos lenne az olyan kritikus fontosságú komponensek megjelenítése, mint a végrehajtásra és a felülvizsgálatra vonatkozó követelmények, amelyek pótlása már rövidtávon is szükséges lehet.

A nemzetközi szakmai ajánlások és elvárások alapján az egyik legnagyobb hiányossága az NKBS-nek, hogy a kiberbiztonsági környezet értékelése rendkívül elnagyolt, a Magyarország elleni kibertérből származó fenyegetések kapcsán csak a kiberhadviselés kerül említésre, nincs szó például a kémkedés vagy a terrorizmus kibertérben jelentkező hatásairól, ahogy az ellenük való védekezésről sem. A dokumentum nem tartalmaz részleteket arra vonatkozóan, hogy milyen program keretében és milyen eszközökkel kívánja növelni a társadalmi-felhasználói tudatosítás és az oktatás szerepét, de arról sem derülnek ki részletek, hogy a nemzetközi együttműködést, vagy – az egyik legkritikusabb területet – az információmegosztást milyen módon képzeli el a kormány. Utóbbihoz szorosan kapcsolódó kérdésként szintén tisztázatlanul maradnak a magánszektor és az állami szféra együttműködésére vonatkozó elképzelések, csakúgy mint a kutatás és fejlesztés lehetőségei. Az analízis eredményei alapján a tanulmány következő része megfogalmaz néhány ajánlást, amelyek egy új kiberbiztonsági stratégia elkészítésekor a folyamatban résztvevő szakemberek és szervezet munkáját segíthetik.

Egy új kiberbiztonsági stratégia

A tanulmány elkészítéséhez felhasznált dokumentumok és elkészített interjúk alapján a témában járatos szakembereket két csoportra lehet bontani a stratégiaalkotással kapcsolatban. Az egyik csoport álláspontja szerint a mai Magyarországon nincs szükség új kiberbiztonsági stratégia elkészítésére. Véleményük szerint egy a kibertérrel és annak biztonságával foglalkozó stratégiának nem csak négy évre kell készülnie, illetve a jelenlegi NKBS elfogadása óta nem változott a kiberbiztonság olyan mértékben, ami indokolttá tenné egy új stratégia megírását. Az új stratégia elkészítését ellenzők további érvként hozzák fel, hogy a stratégiai dokumentumoknak nem kell részletekbe menő konkrét cselekvési tervet tartalmazniuk, inkább a „stratégia stratégiáját” szükséges elkészíteni. Ez alatt egy olyan részletes, mérhető végrehajtási és költségvetési tervezetet kell érteni, amely konkrét célokat és mérföldköveket határoz meg, kijelöli a szükséges eszközöket és a végrehajtás felelőseit a stratégiában meghatározott biztonsági állapot elérésének érdekében.

A kiberbiztonsági stratégiával kapcsolatban megkérdezett szakértők másik csoportja támogatja egy új NKBS elkészítését, amit elsősorban azzal indokolnak, hogy az Európai Unió jogi környezete az elmúlt időszakban jelentősen megváltozott, köszönhetően a tagállamok közötti hosszú egyeztetés után elfogadott NIS Irányelvnek.[28] Tekintettel arra, hogy a kiberbiztonsághoz szorosan kapcsolódik a magánszféra és az adatok védelme, szintén fontos változásokat hoz a területen az Európai Unió Általános Adatvédelmi Rendelete (*General Data Protection Rules* – GDPR)[29], melyet 2018. május 25-től kell alkalmazni a tagállamokban. A küszöbön álló és a folyamatban levő változások tehát álláspontunk szerint mindenképpen indokolttá tesznek egy új kiberbiztonsági stratégia megalkotására vonatkozó szakmai eszmecserét, amit csak tovább erősít a jelenlegi NKBS hazai szabályozással kapcsolatban fennálló konfliktusa.

A korábban már említett, kormányzati stratégiai irányításról szóló rendelet alapján, főszabály szerint a stratégiai tervdokumentumokat a nyomon követés során felmerülő hiányosságok kiküszöbölését szolgáló felülvizsgálatra való tekintettel automatikusan módosítani kell. A NIS Irányelv számottevően több elemet tartalmaz, mint az aktuális NKBS, azonban ezeknek az elemeknek a beillesztését nem lehet a stratégia felülvizsgálata során megvalósítani, mivel a módosítási folyamat szétfeszítené a jelenlegi stratégia tartalmi kereteit.

Ennek alátámasztására a NIS Irányelvben a nemzeti stratégia legfontosabb témáira vonatkozó rendelkezések szolgálnak, az alábbiak szerint:

1. A nemzeti stratégia céljai és prioritásai
2. A nemzeti stratégia céljainak és prioritásainak teljesítését szolgáló irányítási keretrendszer, beleértve a kormányzati és egyéb érintett szereplőket és felelősségüket
3. Felkészültségre, reagálásra és helyreállításra vonatkozó intézkedések azonosítása, ideértve a köz- és magánszféra közötti együttműködést
4. Hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiához kapcsolódó oktatási, tájékoztató és képzési programok megjelölése
5. Hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiához kapcsolódó kutatás-fejlesztési programok megjelölése
6. Kockázatok feltárására szolgáló kockázatértékelési terv
7. A stratégia végrehajtásába bevont különböző szereplők jegyzéke

Jól látható, hogy a NIS Irányelvben több olyan előírás is szerepel a nemzeti kiberbiztonsági stratégiák tartalmára vonatkozóan, amelyek jelentős hányada nem található meg a jelenlegi NKBS-ben.

Az Irányelv legfontosabb rendelkezése a tanulmány témája szempontjából a 7. cikk, amely előírja az EU-tagállamok számára az Irányelv rendelkezéseivel harmonizáló stratégiaalkotás kötelezettségét.[30] A cikk alapján a tagállamoknak rendelkezniük kell az államuk biztonságára szolgáló minimumképességekkel, valamint konkrét stratégiai célokat és részletes szakpolitikai intézkedéseket kell megfogalmazniuk. Az Irányelv átültetésének határideje 2018. május 9., tehát eddig az időpontig a tagállamoknak vagy egy új stratégiát kell elfogadniuk, vagy a harmonizáció érdekében módosítaniuk kell a meglévő stratégiáikat.[31]

A NIS Irányelvben rögzített szempontokon túlmenően egy új stratégia megalkotásakor érdemes lehet figyelembe venni a hazai beágyazottságra vonatkozó szempontokat is.

---

[28] Az Európai Parlament és Tanács (EU) 2016/1148 Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, [online], 2016, Eur-lex.europa.eu [2016. 10. 22.]

[29] Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), [online], 2016, Eur-lex.europa.eu [2016. 10. 22.]

[30] Az Európai Parlament és Tanács (EU) 2016/1148 Irányelvének 7. cikke: *„Valamennyi tagállam elfogad egy hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát, amelyben meghatározza a stratégiai célokat, valamint a hálózati és információs rendszerek magas szintű biztonságának megteremtéséhez és fenntartásához szükséges megfelelő szakpolitikai és szabályozási intézkedéseket, legalább a II. mellékletben említett ágazatokra és a III. mellékletben említett szolgáltatásokra vonatkozóan."*

[31] Az Európai Parlament és Tanács (EU) 2016/1148 Irányelvének 25. cikke: *„(1) A tagállamok 2018. május 9-ig elfogadják és kihirdetik azokat a törvényi, rendeleti és közigazgatási rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek megfeleljenek. Erről haladéktalanul tájékoztatják a Bizottságot. … Amikor a tagállamok elfogadják ezeket az intézkedéseket, azokban hivatkozni kell erre az irányelvre, vagy azokhoz hivatalos kihirdetésük alkalmával ilyen hivatkozást kell fűzni. A hivatkozás módját a tagállamok határozzák meg. (2) A tagállamok közlik a Bizottsággal nemzeti joguk azon főbb rendelkezéseinek szövegét, amelyeket az ezen irányelv által szabályozott területen fogadnak el."*

A kormányzati stratégiai irányítási rendszer az alábbi elveket követi:[32]

1. Biztosítani kell a stratégiai tervdokumentumok és a kapcsolódó kormányzati intézkedések, célkitűzések összhangját.
2. A stratégiai tervdokumentumok előkészítésének, elfogadásának és megvalósításának, a stratégiai tervdokumentumok elfogadását követően a nyomon követésnek és értékelésnek, valamint a felülvizsgálatnak a meghatározott ciklikus eljárásrend szerint kell megvalósulnia.
3. Biztosítani kell a hosszú távú, a középtávú és a rövid távú stratégiai dokumentumok összhangját, hierarchikus egymásra épülését.
4. A stratégiai tervdokumentumok előkészítésénél figyelemmel kell lenni a területi adottságokra, továbbá kidolgozásuk során érvényesíteni kell a területi és területi felzárkózási szempontokat.
5. A stratégia megalkotása során támaszkodni kell az állami és a nem állami szereplőknél felhalmozódott tudásra és tapasztalatokra.
6. A stratégia megvalósítható (rendelkezzen megfelelő forrással), fenntartható (illeszkedjen a stratégiai rendszerbe) legyen; releváns és megalapozott adatokra épüljön; a benne szereplő célokhoz mutatók legyenek rendelve; továbbá jelenjenek meg benne a nemzetpolitikai, az európai uniós és nemzetközi összefüggések.

A vonatkozó rendelet alapján a stratégiai dokumentumok jellegük szerint több kategóriába sorolhatók. Időhorizontjuk szerint hosszú (10 évet meghaladó), közép- (4-10 éves időtartamot felölelő) és rövidtávú (1-4 évet felölelő) stratégiáról, az elkészítési kötelezettség szempontjából kötelezően elkészítendő és nem kötelezően elkészítendő stratégiai tervdokumentumokról beszélhetünk. Egyes szakértői vélemények alapján nemzeti kiberbiztonsági stratégiát 10 éves időtartamra ajánlott tervezni, ugyanakkor fontos megjegyezni, hogy a nemzetközi gyakorlat ettől eltérő tendenciát mutat (lásd az 5. táblázatot).

A kiberbiztonság területén bekövetkező gyors változásoknak és a terület stratégiai kérdésként történő megközelítésének újszerűsége következtében a kiberbiztonsági stratégiák rövidebb időszakonként változnak.[33] Felépítését tekintve az első 5 évre vonatkozó cselekményeket, akciókat, valamint a hozzájuk rendelt erőforrásokat részletesen, a hatodik évtől pedig átfogó jelleggel érdemes kidolgozni a hazai vélemények alapján. Utóbbiakra figyelemmel a kiberbiztonsági stratégia a középtávú stratégiák közé tartozna. A stratégiai irányításról szóló rendelet három dokumentumtípust sorol a középtávú stratégiák közé:[34] a nemzeti középtávú stratégiát, a szakpolitikai stratégiát és a fehér könyvet. Tekintettel arra, hogy a három típus közül csak a nemzeti középtávú stratégia előkészítése és elfogadása kötelező, ahol előzetes értékelést kell végezni, illetve a megvalósítást követő egy éven belül utólagos értékelést is készíteni kell, egy új NKBS-nek nemzeti középtávú stratégiaként kellene megjelennie, hogy a célkitűzéseket kielégítően szolgálhassa, és a stratégiai dokumentumok hierarchiájába megfelelően illeszkedjen.

A fenti megállapítást fontos kiegészíteni azzal, hogy kötelezően elkészítendő és rövidtávú, átfogó, horizontális megközelítésű társadalmi, gazdasági, környezeti célrendszert leíró, a célok elérését bemutató stratégiai dokumentum nem létezik a vonatkozó rendelet értelmében. Olyan nem kötelezően elkészítendő tervdokumentum, amely rövidtávra is készülhet, a fehér könyv, azonban ennek elkészítése alapvetően más stratégiai dokumentumok megalapozását szolgálja. A rövidtávú stratégiai tervdokumentumok másik használható formája a szakpolitikai program, azonban ennek esetében más vonatkozó stratégiák alapján kell a tervdokumentumot kidolgozni. Ebből kifolyólag a kormányzati stratégiai irányítási rendszer szabályai alapján az átfogó, horizontális megközelítés helyett témaspecifikus, vertikális megközelítésű stratégia készülne el – azonban a kiberbiztonság jellegéből fakadóan egy ilyen dokumentum nem lenne alkalmas a kitűzött célok megvalósításához.

A tanulmány szerzőinek véleménye alapján egy, a nemzetközi trendeket követő, valamint az ajánlásoknak és elvárásoknak megfelelő NKBS a kormányzati stratégiai irányítási rendszerről szóló rendeletben található tervdokumentum típusok közül egyik kategóriába sem fér bele. Ezen megállapítás elvezet a stratégiai dokumentumtípusok felülvizsgálatának igényéhez, ami azonban jelentősen túlmutat az elemzés és a tanulmány keretein. Összességében egy új kiberbiztonsági

[32] A 38/2012. (III. 12.) Kormányrendelet 6. § alapján
[33] Vö.: Litvánia, Szlovákia és Hollandia szabályozása évente, Ausztria kiberbiztonsági stratégiája pedig kétévente ismétlődő felülvizsgálati kötelezettséget ír elő.
[34] A nemzeti középtávú stratégiára vonatkozó szabályokat a 27. §, a szakpolitikai stratégiára a 35. § és a fehér könyvre a 34. § tartalmazza.

stratégia akkor szolgálná a leginkább a nemzeti érdekeket, ha kötelezően elkészítendő, rövid-középtávú stratégiai dokumentumtípus lenne, amelynek elfogadásához előzetes és utólagos értékelés elvégzése is szükséges lenne.

A stratégiai tervezés működési elve a ciklikusság, amely önmagába visszatérő fejlesztési folyamatot jelent, miközben a végrehajtás során, illetve azt követően lehetővé teszi a visszacsatolást és értékelést. Bár a stratégiaalkotási folyamat időszükséglete jelentős mértékben függ az adott szakpolitikai terület méretétől, kiterjedtségétől, környezetétől, a vonatkozó jogszabályoktól és nemzetközi ajánlásoktól, általánosságban kijelenthető, hogy 4-6 hónap alatt optimálisan elkészíthető a stratégiai tervdokumentum. Ezt követően lehet sort keríteni a szakmai és társadalmi véleményezésre. Mindez persze csak az ideális állapot váza, miközben hazai tekintetben a vonatkozó szabályozás ellenére a stratégiai irányítás rendszere bizonytalan lábakon áll. A stratégiai irányításról szóló rendelet, valamint a nemzetközi ajánlások értelmében is az NKBS-nek követnie kell a ciklikusság elvét,[35] azonban a jelenleg hatályos stratégia nem tartalmaz a nyomon követésre és értékelésre vonatkozó rendelkezéseket. Az NKBS-ből hiányoznak az indikátorok és a területre vonatkozó mutatók, de számos más nemzetközi ajánlás és szempont érvényre juttatását sem sikerült maradéktalanul megvalósítani.

Következő generációs kiberbiztonsági stratégiával rendelkező EU tagállamok				
Ország	**Első stratégia**	**Hatály**	**Új stratégia**	**Hatály**
Csehország	Cyber Security Strategy of the Czech Republic for the 2011 – 2015 Period.	2011-2015	National Cyber Security Strategy of The Czech Republic for the Period from 2015 to 2020	2015-2020
Egyesült Királyság	The UK cyber Security Strategy: Protecting and promoting the UK in a digital world.	2011-2016	National Cyber Security Strategy 2016-2021	2016-2021
Észtország	Cyber Security Strategy. Tallinn.	2008-2013	Cyber Security Strategy 2014-2017	2014-2017
Franciaország	Information Systems Defence and Security: France's Strategy	2011-2015	French National Digital Security Strategy	2015 – napjaink
Hollandia	The National Cyber Security Strategy (NCSS): Success through cooperation	2011-2013	National Cyber Security Strategy 2: From Awareness to Capability	2014-2016
Luxemburg	Stratégie nationale en matière de cyber sécurité	2011-2015	National Cyber Security Strategy II.	2015-2017
Németország	Cyber Security Strategy for Germany	2011-2016	Cyber-Sicherheitsstrategie für Deutschland	2016 – napjaink
Portugália	National Strategy for the Security in Cyberspace	2013-2015	National Cyberspace Security Strategy Portugal	2015 – napjaink
Spanyolország	National Cyber Security Strategy	2008-2015	National Cyber Security Plan	2014 – napjaink
Szlovákia	National Strategy for Information Security in the Slovak Republic	2008-2015	Cyber Security Concept of the Slovak Republic for 2015 - 2020	2015 – 2020

5. táblázat: Néhány európai ország első és második nemzeti kiberbiztonsági stratégiája, valamint a dokumentumok hatálya.

Összegzés és ajánlások

A következő generációs kiberbiztonsági stratégia elkészítésében résztvevő szervezetek és szakemberek számára az elvégzett elemzés alapján az alábbi ajánlásokat javasoljuk megfontolásra:

- Az NKBS módosítása nem lenne hatékony, helyette új stratégia kidolgozására van szükség.
- Az új stratégiát új formában célszerű elkészíteni, ami jobban illeszkedik a hazai és nemzetközi elvárásokhoz.

[35] A stratégiai tervdokumentumok nyomon követése, értékelése, felülvizsgálata kapcsán lásd a 38/2012. (III. 12.) Kormányrendelet 20-23. §-át.

- A jogszabályi környezet, valamint a nemzetközi megfelelés tekintetében a NIS Irányelv és a GDPR mellett a nemzetközi dokumentumok szerepe legyen meghatározó.
- A fenyegetettségek és a célkitűzések megalapozottságának érdekében az új stratégia kidolgozása előtt országos kiberbiztonsági kockázatelemzés és értékelés elvégzése szükséges.
- Nyilvános végrehajtási terv kidolgozása, valamint a végrehajtás ellenőrzését szolgáló mérőszámok és indikátorok meghatározása nélkül ne kerüljön új stratégia kiadásra.
- A mérőszámokhoz felelősöket és erőforrásokat is kapcsoljon a dokumentum.
- A fogalmak, a célrendszer, valamint a fenyegetések meghatározását körültekintőbben kell elvégezni.
- Az életciklusmodell alkalmazása és a felülvizsgálatra vonatkozó szabályok jelenjenek meg a stratégiában.

Ahhoz, hogy a jelenlegi NKBS-ben szereplő merész kijelentés, mely szerint „Magyarország kiberbiztonsági helyzete alapvetően szilárd”,[36] ne csak üres frázis legyen, a jelenleginél jóval nagyobb körültekintéssel megírt, stabilabb beágyazottsággal és megalapozottsággal rendelkező, új stratégia elkészítése indokolt. Az új kiberbiztonsági stratégia előkészítése során, bár a körültekintő eljárásnak figyelembe kell vennie a politikai és lobbi érdekeket is, azok torzító hatásának kiküszöbölésére jóval nagyobb hangsúlyt kell fektetni. Markánsabbá kell váljanak az ország kiberbiztonsági környezetének értékelésére vonatkozó bekezdések, ezen belül is az ország biztonsága szempontjából leginkább releváns fenyegetések strukturált megjelenítése szükséges. Az új stratégia időtávja kapcsán a hazai keretrendszer nem tartalmaz ideális megoldást, ugyanakkor a kiberbiztonság terén megfigyelhető rendkívül gyors technológiai fejlődés, illetve a bűncselekmények és az információs rendszerek rosszindulatú felhasználásának új formáira való tekintettel a stratégia felülvizsgálata egy-két évente indokolttá válhat. Egy az elemzés következtetései alapján kidolgozásra kerülő, a nemzetközi trendekhez és a hazai környezethez is jobban illeszkedő stratégia olyan kiberbiztonsági indikátorrá válhat, amely az egyéni felhasználó biztonságát és a nemzetbiztonságot egyaránt növeli.

[36] 1139/2013. (III. 21.) Kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 10. pont

Az „SVKK Elemzések” 2003 óta a Kutatóközpont munkatársainak tematikus szakpolitikai elemzéseit megjelentető időszakos kiadvány, melyben a szerzők független kutatói álláspontjukat közlik.

Az NKE Stratégiai Védelmi Kutatóközpont független szakpolitikai kutatóintézet, a kiadványaiban megjelenő elemzések, álláspontok, vélemények nem feltétlenül tükrözik a szerkesztőség vagy a kiadó véleményét. Az elemzésben foglalt információk, adatok, megállapítások tájékoztatás céljából készültek.

Kiadó: Nemzeti Közszolgálati Egyetem

Szerkesztés és tördelés:
Bazsó Márton, Csiki Tamás

A kiadó elérhetősége:

1581 Budapest, Pf. 15.

Tel: 00 36 1 432-90-92

E-mail: svkk@uni-nke.hu

2012– : NKE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4862)

2011–2012: ZMNE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4854)
2007–2011: ZMNE Stratégiai Védelmi Kutatóintézet Elemzések (ISSN 2063-4854)
2003–2007: ZMNE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4854)