MTA DOKTORI ÉRTEKEZÉS

A KIBERBIZTONSÁG STRATÉGIAI MEGKÖZELÍTÉSE

Kovács László

Nemzeti Közszolgálati Egyetem
Budapest
2018

TARTALOMJEGYZÉK

BEVEZETÉS 4

Tudományos probléma 5

Kutatási célkitűzések 6

Kutatási hipotézisek 8

Kutatási módszerek 8

A kutatási terület lehatárolása 9

A DOLGOZATBAN HASZNÁLT LEGGYAKORIBB FOGALMAK MEGHATÁROZÁSA 10

1. FEJEZET KIBERTÉR ÉS KIBERBIZTONSÁG 12

1.1. A kibertér meghatározása 12

1.2. A kiberbiztonság meghatározása 13

1.3. A kibertér és a kiberbiztonság szerepe napjainkban 15

1.3.1. Függőség a kibertértől és az abban megjelenő szolgáltatásoktól 15

1.3.2. Kritikus infrastruktúrák és kritikus információs infrastruktúrák 18

1.3.3. A digitalizáció társadalmi hatásainak mérése 25

1.4. A kibertérben jelentkező stratégiai kihívások és veszélyek 36

1.5. Kiberbiztonság és kibervédelem stratégiai feladatai 49

2. FEJEZET A KIBERBIZTONSÁG STRATÉGIAI SZINTŰ MEGJELENÉSE 54

2.1. A nemzeti biztonság és a kiberbiztonság stratégiai összefüggései 54

2.2. Nagyhatalmak és a kibertér 57

2.2.1. Amerikai Egyesült Államok 57

2.2.2. Kína 72

2.2.3. Oroszország 82

2.3. Az Európai Unió és a NATO kibertérhez kapcsolódó stratégiái 92

2.3.1. Az Európai Unió stratégiai szintű kiberbiztonsági törekvései 92

2.3.2. A NATO kiberbiztonsági stratégiája 99

2.4. Egyes európai országok nemzeti kiberbiztonsági stratégiái 105

2.4.1. Ausztria 107

2.4.2. Cseh Köztársaság 111

2.4.3. Egyesült Királyság 116

2.4.4. Észtország 123
2.4.5. Franciaország 127
2.4.6. Hollandia 135
2.4.7. Magyarország 141
2.4.8. Lengyelország 150
2.4.9. Németország 153
2.4.10. Szlovák Köztársaság 159
2.5. A dolgozatban bemutatott országok egyes kibertéri jellemzői és kiberbiztonsági stratégiai céljai 163

3. FEJEZET A NEMZETI KIBERBIZTONSÁGI STRATÉGIA MODELLJE 182
3.1. Eddigi stratégiai modellalkotási példák 182
3.2. A megvizsgált kiberbiztonsági stratégiák elemzéséből levonható szintetizált következtetéseim 188
3.3. A nemzeti kiberbiztonsági stratégia modelljére tett javaslatom 198
3.4. A nemzeti kiberbiztonsági stratégia végrehajtása érdekében elkészítendő akcióterv felépítésére vonatkozó javaslatom 213
3.5 A nemzeti kiberbiztonsági stratégia végrehajtása hatékonyságának mérésére szolgáló indikátor-rendszer elvi alapjaira tett javaslatom 214

ÖSSZEGZETT KÖVETKEZTETÉSEK 226

TUDOMÁNYOS EREDMÉNYEK 228

RÖVIDÍTÉSEK JEGYZÉKE 229

ILLUSZTRÁCIÓK JEGYZÉKE 245

TÁBLÁZATOK JEGYZÉKE 246

IRODALOMJEGYZÉK 247

AZ ÉRTEKEZÉS TÉMÁJÁBAN SZÜLETETT FONTOSABB TUDOMÁNYOS PUBLIKÁCIÓIM JEGYZÉKE 273

BEVEZETÉS

A kibertér az elmúlt években társadalmi működésünk alapja és meghatározó tényezője lett. A kibertér rendszereinek, eszközeinek és az azokon keresztül megvalósuló folyamatok zavartalan működése ma már elengedhetetlen. Így a kibertér biztonsága az olyan hagyományos biztonsági tényezők sorába emelkedett, mint a katonai, a politikai, gazdasági, illetve a környezeti biztonság. Ezek a biztonsági tényezők egy adott ország nemzeti biztonságának alapvető összetevői, amelyek egymásra is kölcsönösen nagy hatással vannak. Ezeknek a biztonsági dimenzióknak a sorába lépett és vált az egyik legfontosabb faktorrá a kiberbiztonság.

A kibertér, illetve az abban lévő szolgáltatások és digitális alapú folyamatok életünk minden szegmensére kihatással vannak. Ez a hatás igaz a gazdaságra, a politikára, a kultúrára, de a magánéletünk egyes elemeire és az emberek egymáshoz való viszonyára is. Ennek megfelelően a kibertér biztonságával kapcsolatban az egyik legnagyobb kihívást az jelenti, hogy a kibertérben meglévő szolgáltatások és az ezeket lehetővé tevő rendszerek összessége egyre nagyobb függőséget jelent a számunkra. Amennyiben ezek a szolgáltatások és rendszerek akár csak időlegesen is működésképtelenné, vagy elérhetetlenné válnak, akkor azok súlyos fennakadásokat okoznak a mindennapjainkban és az anyagi károkon túl komoly veszélyt jelentenek az emberek életére is.

Mindezek alapján a kibertér és annak biztonsága a fejlett információs infrastruktúrával rendelkező országok számára meghatározó fontosságú, amely a különböző országok kiberbiztonságról való stratégiai elképzeléseiben tükröződik vissza. Azonban a nemzeti kiberbiztonsági stratégiák – legyen szó akár a nagyhatalmakról, akár a kisebb országokról – eltérő válaszokat és megoldásokat sorakoztatnak fel a kibertéri kihívásokra. Számos európai ország nemzeti szintű kiberbiztonsági stratégiája ma már a második, vagy esetenként a harmadik – néhány esetben kisebb módosításokon átesett, de több ország esetében alapjaiban újragondolt – kiadásánál tart.

Ugyanakkor kérdésként merül fel, hogy a kibertér biztonsága megteremthető-e csupán nemzeti szinten, hiszen a kibertérben nem, vagy csak nagyon nehezen értelmezhetők a földrajzi határok. Mindezek alapján az is vizsgálat és elemzés tárgyát kell, hogy képezze, hogy az olyan politikai-gazdasági szövetségek, mint az Európai Unió, vagy az olyan politikai-katonai szövetség, mint a NATO milyen megoldásokat látnak a kibertér biztonságára nézve megvalósíthatónak stratégiai szinten, hiszen – bár ezekben a szövetségekben a tagállamok sok területen autonóm megoldásokkal élnek – a közösség ereje

és egymás iránti elkötelezettsége más biztonsági dimenziókban – például a gazdasági- vagy a katonai biztonság terén – már többször is bizonyított.

Ezeknek a tényezőknek megfelelően célszerű azonosítani a szövetségi szinten megjelenő kiberbiztonsági stratégiák és politikák összetevőit és legfontosabb pontjait, majd ezeket összevetni a nemzeti szintű kiberbiztonsági stratégiákkal. Ez utóbbiakhoz segítséget nyújthatnak azok a többségében nemzetközi szervezetek által készített ajánlások, amelyek modellként szolgálhatnak egy ország nemzeti kiberbiztonsági stratégiájának felépítéséhez.

Ugyanakkor ezek korántsem teljesek és nem tökéletesek. Visszautalva a korábbi megállapításra: a nemzeti kiberbiztonság a nemzetközi környezethez igazodva, kezelve a kibertér sajátosságaiból eredő nemzetközi kihívásokat és veszélyeket az adott ország nemzeti biztonságának részét kell, hogy képezze. Ezekre az összefüggésekre azonban az eddigi nemzetközi modellek nem, vagy csak részben adtak válaszokat.

Mindezek alapján egy teljes értékű, a nemzetközi kibertér sajátosságait – legyenek azok biztonságpolitikai, katonai, vagy akár technikai kihívások – kezelni képes, az országok nemzeti szintű kiberbiztonsági stratégiájára vonatkozó modell megalkotása válik szükségessé.

Jelen értekezésben eddigi kutatásaim eredményeire alapozva egy ilyen általános – a nemzeti kiberbiztonsági stratégia alapjait meghatározó, a stratégia összetevőre és felépítésére koncentráló – modell megalkotását tűztem ki célul.

Tudományos probléma

Az olyan nemzetközi szervezetek, mint az Európai Unió vagy a NATO, csakúgy, mint a legtöbb európai ország, így Magyarország is rendelkezik kiberbiztonsági stratégiával. **Ugyanakkor ezek a stratégiák többnyire statikus dokumentumok, amelyek nem, vagy csak részben képesek kezelni azt a dinamizmust, amely a kiberteret jellemzi**. Azonban a kibertér jellegéből adódóan, azaz a globalitás, az országhatárok nélküliség, rendkívül gyors technológiai változások, mint legfőbb jellemzők igénylik azt, hogy általános, regionális vagy globális alapértékek mellett egységes modellt határozzunk meg a kiberbiztonsági stratégiák megalkotásához. **Egyes országok nemzeti szinten csak korlátozott hatású elveket és szervezeti hátteret (szabályozást) képesek ebben a határok nélküli térben megalkotni.** Nem kétséges, hogy a nemzeti kiberbiztonsági szabályozásra szükség van, de ezeknek az önálló stratégiáknak mégis szükséges meghatározni egy közös elvi alapot, amely a szövetségi tagságból, a hasonló kihívásokból, a hasonló értékekből, illetve a kibertér korábban említett jellegéből ered. Ez az alap, azaz modell nemzetközi konszenzussal kell,

hogy létrejöjjön. Ez a konszenzus elsősorban azokra a legfontosabb célokra, illetve azok elérésére kell, hogy irányuljon, amelyek a kiberbiztonság megteremtését hivatottak biztosítani. A közös elvi modell kiterjed minden olyan kérdésre, amelyeket a nemzeteknek jelenleg és a közeli jövőben a kibertérben kezelniük kell. Az egységes modell egységes válaszokat is jelent, így az e mentén megvalósuló nemzeti kiberbiztonsági stratégiák nemzetközi szinten is hatékony kiberbiztonságot eredményeznek.

Kutatási célkitűzések

Az elmúlt időszakban kutatásaim a kiberbiztonság három nagy területére terjedtek ki. Elsőként a kiberbiztonság technikai kihívásait, illetve az infokommunikációs rendszereket és eszközöket fenyegető veszélyeket, valamint az ellenük való védekezés lehetséges módszereit vizsgáltam. Ezek a kutatások már a kezdeti szakaszukban rávilágítottak arra a problémára, amelyet a digitális korszakban az ezektől a rendszerektől való társadalmi, gazdasági és politikai függőség jelent. Ezért ezt a függőséget a társadalom és a biztonság, elsősorban a nemzeti biztonság szempontjából vizsgáltam. Ennek során olyan kérdéseket kutattam kiemelten, mint a kiberterrorizmus vagy a kiberhadviselés. Ezeknek a kutatásoknak már a részeredményei is abba az irányba mutattak, hogy mindezek a veszélyforrások komoly nemzetbiztonsági kockázatként jelentkeznek mindazon országok, így hazánk esetében is, amelyek fejlett információs infrastruktúrával rendelkezik. Ennek oka a korábban említett információtechnológiai függőség. Ezekre a kockázatokra azonban nem adható úgy válasz, hogy azokat ne stratégiai szinten koordinálná az egyes ország, vagy akár az adott nemzetközi közösség. Így a kiberteret érintő kutatásaim harmadik területe a nemzeti biztonsági stratégiára épülő nemzeti kiberbiztonsági stratégiák vizsgálata volt.

Jelen értekezés célja mindezen kutatások eredményeinek az összefoglalása, majd erre az összefoglalásra építve a legfontosabb célkitűzésem egy olyan **kiberbiztonsági stratégia modelljének megalkotása**, amely tartalmazza azokat a tényezőket, alapvetéseket, amelyek mind nemzetközi, mind nemzeti szinten képesek választ adni a kibertér biztonságát meghatározó kihívásokra a közeli és a távolabbi jövőben egyaránt. A modell megalkotása során a stratégia összetevőire, felépítésére és annak életciklusára kívánok fókuszálni.

E cél elérése érdekében a következő részcélokat határoztam meg:

- bemutatni a digitalizáció társadalmi hatásait, rámutatni az infokommunikációs technika és technológia nélkülözhetetlenségére, kitérve a kibertérben megjelenő stratégiai veszélyek és kihívások felvázolására. Ezzel párhuzamosan célom bemutatni a digitalizáció társadalomra gyakorolt hatásainak mérésére már

megvalósult eszközöket, amelyekkel közvetlenül, vagy közvetett módon lehetőség lehet a kiberbiztonság helyzetének megítélésére is;

- megvizsgálni és elemezni a nemzetközi szakmai szervezetek – Nemzetközi Távközlési Egyesület (International Telecommunication Unit, ITU), Európai Unió Hálózat és Információbiztonsági Ügynökség (European Union Agency for Network and Information Security, ENISA), NATO Kibervédelmi kiválósági központ (NATO Cooperative Cyber Defence Centre of Exellence, CCDCOE) – nemzeti kiberbiztonsági stratégiára elkészítésére, illetve felépítésére tett ajánlásait, majd általános érvényű következtetések levonása, amelyek a nemzeti kiberbiztonsági stratégia általános érvényű alapjai lehetnek;
- nemzetközi szövetségek – Európai Unió, Észak-Atlanti Szerződés Szövetsége – kiberbiztonsági politikáinak és stratégiáinak az elemzése, **valamint ezekben az olyan közös elemek azonosítása, amelyek hatással vannak a nemzeti kiberbiztonsági stratégiákra**;
- nagyhatalmak – Amerikai Egyesült Államok, Kína, Oroszország – kiberbiztonságról alkotott elképzeléseinek, az elmúlt években a kibertérben megvalósított tevékenységeik elemzése, majd ezekből következtetések levonása;
- összegezni az eddig megvizsgált országok nemzeti biztonsági stratégiáit és nemzeti kiberbiztonsági stratégiáit, **ezek alapján az olyan közös elemek azonosítását elvégezni, amelyek a fenti fő cél felé mutatnak, azaz az általános nemzeti kiberbiztonsági stratégia alapjai lehetnek**;
- **egy elvi stratégiai modell felvázolása**, amely alapján egy adott ország nemzeti kiberbiztonsági stratégiája elkészíthető és a folyamatos technikai, gazdasági, társadalmi változásoktól függetlenül fenntartható;
- a nemzeti kiberbiztonsági stratégia végrehajtása érdekében **egy általános akcióterv elvi alapjainak a kidolgozása;**
- **egy olyan mérőrendszer elvi alapjainak és összetevőinek** (indikátorainak) a kidolgozása, amely alapján a nemzeti kiberbiztonsági stratégia és annak végrehajtása hatékonysága mérhetővé válik.

Kutatási hipotézisek

Kutatómunkám során az alábbi hipotéziseket állítottam fel:

1. A különböző országok jelenlegi nemzeti kiberbiztonsági stratégiáiban azonosíthatóak olyan elemek, amelyek vagy hasonlóak, vagy azonosak, és amelyek alapjai lehetnek egy nemzeti kiberbiztonsági stratégia modelljének.
2. A nemzeti kiberbiztonsági stratégiák és az abban foglaltak végrehajtása alapvetően járulnak hozzá az adott ország nemzeti biztonságának erősítéséhez. Ebből következően a kiberbiztonság megjelenítése már a nemzeti biztonsági stratégiában fontos szerepet kap.
3. A nemzeti kiberbiztonsági stratégia nem statikus dokumentum, hanem rendelkezik olyan összetevőkkel és olyan elemekkel, amelyek a kibertér dinamizmusát – legyen szó akár a technológiai, akár a nemzetközi vagy nemzeti biztonsági helyzetben bekövetkezett változások – képesek megfelelő szinten kezelni.

Kutatási módszerek

Kutatásaim során a fentiekben megfogalmazott célkitűzések elérése érdekében – építve az eddig elvégzett kutatások számos részeredményére – a következő tudományos kutatási módszereket alkalmaztam:

- kutatások másodelemzése;
- összehasonlító elemzés;
- szintézis;
- indukció;
- dedukció;
- modellezés és modellalkotás.

Természetszerűleg a kutatásaim eddigi eredményei nagymértékben befolyásolták azokat a kutatási irányokat, amelyek a kibertér különböző területeinek vizsgálatai során követtem. E munka során az alapvető irodalmi források feldolgozásán túl a hazai nemzeti kiberbiztonsági stratégia módosításában részt vettem, mint véleményező. Ezen kívül az Európai Unió Horizont 2020 kutatás-fejlesztési programja egyes alprogramjai szakértőjeként az Európai Bizottság meghívására személyesen a gyakorlatban, közvetlen közelről tanulmányozhattam számos olyan területet, amely jelen dolgozat viszonyában is releváns.

Mindezeken túl jelen értekezés nagyban épít a 2018-ban megjelent általam 2017-ben és 2018-ban írt két monográfiára – *A kibertér védelme*, valamint a *Kiberbiztonság és -stratégia* –, amelyekben az addigi kutatásaim eredményeire építve igyekeztem bemutatni közérthető módon a kibertér egyes területeit.

A kutatási terület lehatárolása

Kutatásaim során, így jelen értekezésben megjelenő tudományos kutatómunka során szükségszerűen lehatárolásokat kellett tennem. Ennek oka a téma szerteágazósága. Ennek megfelelően nem került elemzésre mind a 28 európai uniós tagország nemzeti biztonsági, illetve nemzeti kiberbiztonsági stratégiája. Az európai országok közül csak az általam kiválasztott 10 olyan ország releváns stratégiáit elemeztem, amelyek vagy méretben (például gazdasági teljesítmény, vagy a népesség számát tekintve) összehasonlíthatók hazánkkal (például Szlovákia, Csehország, Szlovénia), vagy nagyságuk alapján meghatározóak Európa számára (például Németország, Franciaország, Egyesült Királyság).

A lehatárolást meg kellett tennem a kiberbiztonsági szervezetek esetében is. Így az egyes országok esetében csak az adott ország nemzeti kiberbiztonsági stratégiájában esetlegesen meghatározottak alapján vizsgáltam az adott ország kiberbiztonsági szervezetét, így nem elemeztem mélyrehatóan azok szervezeti felépítését, vagy azok hatékonyságát.

A DOLGOZATBAN HASZNÁLT LEGGYAKORIBB FOGALMAK MEGHATÁROZÁSA

A kibertér és annak biztonsága számos olyan fogalmat takar, amelyeket naponta használunk, de azok mégis sokszor eltérő jelentést hordoznak. Ezért szükséges a dolgozatban leggyakrabban használt fogalmakat és meghatározásokat megadni annak megfelelően, ahogy azt a vizsgálatok és elemzések során használtam.

Biztonság: az eszközök, rendszerek és hálózatok olyan megkívánt állapota, amelyben a veszélyek megfelelő szintű kezelése megtörténik.

Digitális ökoszisztéma: a nagy sávszélességű infokommunikációs infrastruktúra, a képzett felhasználók, a digitális szolgáltatásokat használó és azokra épülő üzleti szféra, a fejlett és intenzív K+F+I ipar, a digitális szolgáltató állam, az online elérhető kereskedelmi szolgáltatások, a digitális archívumok olyan összessége, amely a tudásalapú társadalom meghatározó tényezőjeként értelmezhető.

Infokommunikáció: az informatika és a kommunikáció konvergenciája révén létrejövő technológia, eszközök és rendszerek gyűjtőfogalma.

Infrastruktúra: létesítmények, hálózatok, rendszerek és üzemeltető szakemberek összessége, amelyek hozzájárulnak a társadalom alapvető szükségleteinek kielégítéséhez.

Internet: az internet egy olyan globális kiterjedésű számítógép-hálózat, amelyben számítógép-hálózati protokoll(ok) kapcsolja össze a felhasználókat és szolgáltatásokat.

Kiberbiztonság: a biztonságot meghatározó eszközök, politikák, koncepciók, technológiák, irányelvek, kockázatkezelési módszerek, tevékenységek, képzések, valamint a legjobb gyakorlatok összessége, amelyek arra irányulnak, hogy megvédjék az infokommunikációs környezetet, az ezt használó szervezetek és felhasználók eszközeit, rendszereit.

Kibertér: globálisan, közvetlenül vagy közvetett módon számítógép-hálózathoz kapcsolt, decentralizált, egyre növekvő infokommunikációs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese által alkotott tér.

Kritikus infrastruktúra: olyan eszköz, létesítmény vagy rendszer, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.

Kritikus információs infrastruktúra: olyan hálózatszerű, fizikai vagy virtuális rendszereket, eszközöket és módszereket (eljárások, szolgáltatások) foglal magában, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban kritikus rendszerek vagy más azonosított kritikus rendszer működéséhez nélkülözhetetlenek.

Védelem: olyan tevékenységeket takar, amelyek a biztonság megteremtésére és fenntartására irányulnak.

1. FEJEZET
KIBERTÉR ÉS KIBERBIZTONSÁG

1.1. A kibertér meghatározása

A kibertér biztonságát vizsgálva mindenekelőtt magát a dimenziót, azaz a kiberteret szükséges definiálnunk. Ez azonban több ok miatt sem egyszerű feladat, hiszen ahogy Munk egyik tanulmányában megfogalmazta: *„[a] kibertér és a hozzá kapcsolódó fogalmak esetében nem kérdéses, hogy ... távol állunk az együttműködéshez szükséges mértékben egységes értelmezéstől. Ez részben a 'kiber' jelzővel jellemezhető fogalmi rendszer viszonylagos újdonságából, részben az általa leírt dolgok, jelenségek, objektumok napjainkban is tapasztalható változásaiból következik"* (Munk 2018)

Ugyanakkor számos kibertér megfogalmazás eltérő szinten tárgyalja a fogalmat. A meghatározások egy része tartományt, egy másik része a környezetet érti a fogalom alatt, de egy másik részük például a hálózatok összességeként írja le magát a kiberteret. (Munk 2018, Kovács 2018b)

A kibertér biztonságának stratégiai szintű vizsgálata szükségessé teszi, hogy az eltérő kibertéri megfogalmazások közül egy olyat válasszunk ki, amely a stratégiai megközelítést tekinti kiinduló pontnak. Erre egy kis kiegészítéssel megfelelő lehet a 2013-as hazai Nemzeti Kiberbiztonsági Stratégia által megfogalmazott kibertér fogalom. Ez alapján: *„[a] kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."* [1139/2013. (III. 21.) Korm. határozat]

Az említett kiegészítés a számítógép-hálózatba kapcsolt infokommunikációs eszközök szükségszerű beemelését jelenti a definícióba. Ennek megfelelően a legfontosabb terminológiai elemeknél már említett kibertér fogalmat alkalmazom a továbbiakban, azaz a kibertér globálisan, közvetlenül vagy közvetett módon számítógép-hálózathoz kapcsolt, decentralizált, egyre növekvő infokommunikációs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese által alkotott tér.

A nemzeti kiberbiztonsági stratégiákat érintő elemzésekkor később utalni fogok arra, hogy számos ország egyedi módon határozza meg a kiberteret. A fenti magyar meghatározáshoz hasonlóan ezek között vannak jól követhetők és használhatók, de számos esetben találunk erre ellenpéldát is. Ugyanakkor a tudományos vizsgálatok során születtek

megfontolandó elképzelések is a kibertérre vonatkozólag. Sok esetben azonban ezek is egy nézőpontból kiindulva adtak egyfajta meghatározást. Ilyen kiinduló pont például a nemzetközi jog. Erre egy példa a külső űrrel kapcsolatos kibertéri meghatározás, amely az arra a területre érvényes nemzetközi jogi szabályozás kialakulását és annak kibertéri hasonlóságát vizsgálja. A külső űr és a kibertér vonatkozásában Nyman-Metcalf a következőket állapítja meg egy tanulmányában: *„[a] kibertérrel való hasonlóság az alap üzenetben megtalálható: az emberiség valami olyan teljesen új korszakba lépett, elhagyva a föld korlátait, amely egy teljesen új jövőt jelent, melyben a nemzeti határok és a földi viták nem játszanak szerepet. A kibertéren dolgozók közül sokan valószínűleg büszkék arra a felismerésre, hogy ez a nyelv nagyban hasonlít a korai kibertéri vitákban használtakra."* (Nyman-Metcalf 2018, idézi: Kovács 2018b)

1.2. A kiberbiztonság meghatározása

A kibertér meghatározása után a következő fogalom, amelyet az értekezés szempontjából, azaz a kiberbiztonság stratégiai szintű vizsgálata során szükséges megvizsgálni az maga a kiberbiztonság. A kibertér fogalmához hasonlóan ennek meghatározása sem könnyű feladat, de ebben az esetben már vannak olyan nemzetközi és akár hazai megfogalmazások, amelyek egymáshoz nagyon közel állnak. Az egyik ilyen definíciót az ITU adta. Ennek alapján a kiberbiztonság: „ *[...] az eszközök, politikák, biztonsági koncepciók, biztonsági garanciák, biztonsági technológiák, irányelvek, kockázatkezelési módszerek, tevékenységek, képzések, valamint a legjobb gyakorlatok összessége, amelyek arra irányulnak, hogy megvédjék a számítógépes környezetet, az ezt használó szervezetek és felhasználók eszközeit, rendszereit.*" (ITU 2017a)

Ezt a meghatározást felhasználva a kiberbiztonságot olyan tevékenységek sorozataként kell vizsgálnunk, amelyek során a jelenlegi és az előre jelezhető biztonsági kihívások kezelése megtörténik. Mindezek alapján tehát a kiberbiztonság azt az állapotot jelenti, amelyben a szervezet működőképessége (ez lehet akár egy adott ország működőképessége is), beleértve a felhasználó eszközeinek zavartalan és biztonságos alkalmazását, az adatokhoz és információkhoz való hozzáférést, illetve a szervezet különböző folyamatai az eredeti működési szándéknak megfelelő módon működnek, illetve valósulnak meg. (ITU 2017a)

A 2013-ban született hazai információbiztonsági törvény, azaz a 2013. évi L törvény már ezt a filozófiát követi. A törvény megfogalmazásában 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." (2013. évi L. törvény)

A kibertér és a kiberbiztonság mellett egy kapcsolódó fogalom, az információbiztonság meghatározása is szükséges. Ennek oka az, hogy a kiberteret alkotó infokommunikációs eszközök és rendszerek közvetlen biztonsága az egyik legmeghatározóbb tényező a kiberbiztonságban. Az információbiztonságot általában három – erre a területre nagyon jól alkalmazható – tényezővel tudjuk leírni. Ez a három tényező a *bizalmasság*, *sértetlenség* és *rendelkezésre állás,* amelyeket az angol nyelvű megfelelőik kezdőbetűi – azaz a bizalmasság: confidentiality, sértetlenség: integrity, valamint elérhetőség: availability – után CIA elvnek is hívnak. (Kovács 2018b)

Ezekkel a tulajdonságokkal jól jellemezhető az adott szervezet információbiztonsága, ugyanakkor a kiberbiztonság megvalósítása komplex tevékenységek sorozatát igényli. Haig szerint a komplex információbiztonság legfontosabb eleme annak céljában keresendő: „*az információs társadalom információbiztonsága szempontjából tehát a fő cél a kritikus információk megóvása.*" (Haig 2015, idézi: Kovács 2018b)

A komplex információbiztonság és ezen keresztül a kiberbiztonság is védelmi tevékenységek egymásutánisága, illetve sok esetben egymással párhuzamos elvégzése során, mint állapot alakítható ki. Ezek a tevékenységek több területre kell, hogy kiterjedjenek, amelyek a következők:

- személyi biztonság;
- fizikai biztonság;
- adminisztratív (dokumentum) biztonság;
- elektronikus információbiztonság. (Haig 2015, idézi: Kovács 2018b)

Mindezek mellett a kiberbiztonságot a kritikus infrastruktúrák szemszögéből is meg kell vizsgálni, mert a kritikus infrastruktúrák ma már nem nélkülözhetik az infokommunikációs eszközöket és rendszereket azok vezérlésének és zavartalan működésük biztosítása érdekében. Elsőként a kritikus infrastruktúra fogalmat szükséges meghatározni, amelyhez rendelkezésre áll Magyarország a kritikus infrastruktúra védelmére 2012-ben született törvény. Az ebben foglaltak szerint a kritikus infrastruktúra, illetve a törvényben használt

definíció készlet szerint létfontosságú infrastruktúra[1]: „*meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához - így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához -, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.*" (2012. évi CLXVI. törvény 1.§ f. pont)

A törvényben utalást találunk az európai értelemben vett kritikus infrastruktúra, illetve létfontosságú infrastruktúra[2] fogalmára is: „*a törvény alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős hatással lenne - az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve - legalább két EGT-államra.*" (2012. évi CLXVI. tv. 1.§ c. pont)

Mindezek azonban nem adnak eligazítást a kritikus információs infrastruktúra (létfontosságú információs infrastruktúra) fogalmi meghatározására. Ugyanakkor az említett kritikus infrastruktúra védelmére született törvény egyik végrehajtási rendelete tartalmaz erre utalást, amely a számunkra megfelelő. E szerint a kritikus információs infrastruktúra, nem más mint: „*a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek.*" (65/2013. (III. 8.) Korm. Rendelet 1. § 3. pont)

1.3. A kibertér és a kiberbiztonság szerepe napjainkban

1.3.1. Függőség a kibertértől és az abban megjelenő szolgáltatásoktól

A digitális technológia innovációja, az IKT eszközök és rendszerek elterjedése azt eredményezték, hogy a társadalom egyre nagyobb igényt támaszt az új digitális eszközökre és szolgáltatásokra.

A társadalom a technológia fejlődésével átalakult. Különösen gyors átalakulás tapasztalható az információtechnológia hatása nyomán. A 20. század végén erre az átalakulás nyomán létrejött társadalomra az egyik legtalálóbb kifejezés: *hálózatos*

[1] A törvény címéből adódóan is a kritikus infrastruktúra kifejezés helyett konzekvensen a *létfontosságú rendszerelem* megnevezést használja. (2012. évi CLXVI. tv. 1.§ f. pont)

[2] A törvény az *európai létfontosságú rendszerelem* kifejezést alkalmazza az európai kritikus infrastruktúra vonatkozásában. (2012. évi CLXVI. tv. 1.§ c. pont)

társadalom volt, amelyet Manuel Castells spanyol szociológus adott meg. E szerint az új társadalmat, mint hálózatos társadalmat tudjuk jellemezni. Castells meghatározása alapján az információs társadalom: „*olyan hálózatos társadalom, ahol a kulcsfontosságú társadalmi rendszerek és tevékenységek elektronikus információs hálózatok köré szerveződnek*." (Castells 2005, idézi: Kovács 2018a)

A 21. század elejére azonban a különböző technológiákra alapuló eszközök, rendszerek és szolgáltatások között a határok eltűnnek. Így létrejött az úgynevezett digitális ökoszisztéma, amely az IKT révén hálózatba kapcsolja a felhasználókat, és a hálózatok segítségével biztosítja a társadalom tagjai számára az egyre inkább alapvetővé váló digitális szolgáltatásokat.

Ebben a digitális ökoszisztémában a szolgáltatások, a felületek és a felhasználás módja is egyre inkább összemosódik, hiszen digitális televíziót nézünk, amely internetelérést és telefont is biztosít egyben. Olyan IKT eszközöket használunk, amelyek számos mindennapi társadalmi funkciót – például kommunikáció, információkeresés, közösségi kapcsolatok stb. – egyesítenek magukba. A határok, amelyek eddig az ember és a technológia között jól elkülöníthetőek voltak egyre inkább elmosódnak. (Kovács 2018a)

Az új digitális világban a társadalom legtöbb funkciója digitális szolgáltatásokra épül, amelyek az emberek magánéletétől kezdődően az oktatásban, a közlekedésben, az egészségügyben, a gyártásban, az energiaellátásban vagy a védelmi szférában abszolút módon jelen vannak.

A néhány éve megjelent olyan kifejezések, mint a dolgok internete, angol terminológiával Internet of Things, IoT[3], vagy mint az okos városok nem csak öncélú technológiai fejlesztéseket jelentenek, hanem például a városokban[4] élő lakosság egyre nyomasztóbb problémáinak megoldásában játszanak nagy szerepet úgy, hogy azokban már az IKT rendszerek alapvető közműnek számítanak: *„[a]z alapvető közművek városi környezetben nemcsak a villamosenergiát vagy a vezetékes vizet jelentik, hanem többek között a gyors információcserét lehetővé tevő szélessávú internetet, a városi forgalom digitalizáció révén*

[3] Az IoT (Internet of Things, azaz a dolgok internete) a hálózatba kötött érzékelők, az ezek alapján fizikai beavatkozást végző eszközök, az ezeket összekötő hálózat, valamint a mindezeket vezérlő intelligens szoftverek együttesét értjük. Az IoT eszközök a beépített szenzorok vagy külső érzékelők adatait önállóan is fel tudják dolgozni, szoftvereik ezek alapján megfelelő döntéseket hoznak, amelyek az eszköz fizikai térben történő beavatkozását eredményezik. (Kovács 2018a)

[4] 2014-ben a Föld lakosságának az 54%-a városban (ebbe beletartoznak az urbanizált területek és a városok agglomerációs területei is) élt. Ez az arány 1950-ben még csak 30% volt, viszont az ENSZ előrejelzése alapján 2050-ben már több mint 68% lesz. (UN DESA 2018, Kovács 2018a)

létrejövő optimális és hatékony szervezését vagy akár a logisztikai ellátás zökkenőmentességét, illetve akár a parkolás minél hatékonyabb lebonyolítását is." (Kovács 2018a)

Hazánkban a digitális ökoszisztéma kifejezés egyik első megjelenése a 2014-ben kiadott hazai *Nemzeti Infokommunikációs Stratégia 2014-2020* dokumentumban történt. Ez a stratégia a digitális ökoszisztémával kapcsolatosan a következő meghatározást adta: *„[a] digitális ökoszisztéma különböző összetevőinek (nagy sávszélességű elérést biztosító infrastruktúra, képzett és motivált felhasználók, az információs világ vívmányait kihasználó üzleti szféra, fejlett és intenzív K+F+I tevékenységet végző infokommunikációs és informatikai (IKT) ipar (amely ideális terület, a magyar gazdaság egyik fejlesztési fókusza), modern szolgáltató állam, online elérhető köz- és kereskedelmi szolgáltatások, digitális archívumok stb.) kiegyensúlyozott rendelkezésre állása jelentősen javítja az állampolgárok életminőségét, a vállalkozások versenyképességét és az állami működés hatékonyságát."* (Nemzeti Infokommunikációs Stratégia 2014, idézi: Kovács 2018a)

Az IKT technológia okozta átalakulás, illetve fejlődés társadalomra gyakorolt hatását vizsgálva többek között a hírekhez való hozzáférés esetén tudjuk szemléltetni. Az Európai Bizottság egyik 2015-ös felméréséből világosan kiderül, hogy az online hírek átvették a vezető szerepet még az olyan „hagyományos" médiumokkal szemben is, mint a televízió vagy a rádió, nem beszélve a nyomtatott sajtóról. (Európai Bizottság 2015a)

A digitalizáció korábban említett függőséget okozó megjelenése számos további példán keresztül válik nyilvánvalóvá, és az egyelőre töretlennek tűnő technikai fejlődés ezt a függőséget tovább növelhető. Erre talán egyik legjobb példa a mesterséges intelligencia, hiszen ez a technológia további hatalmas potenciált rejt magában, és így már a közeljövőben tovább alakíthatja az életünket[5].

A mesterséges intelligencia, amelyet röviden csak MI-nek, vagy az angol *Artificial Intelligence* kifejezésből adódóan csak AI-nak hívunk, bizonyos szinten már ma is ott van a mindennapjainkban. Az MI elemei ma már a gyártástól kezdve – például az ipari vezérlő számítógépekben, ipari és egyéb robotokban –, a közlekedésen át a logisztikáig, sok helyen megtalálhatóak. Az MI további fejlesztése és fejlődése a technikai előnyökön túl nagy anyagi haszonnal is kecsegtet, hiszen az MI számos iparágban meghatározó jelentőségre tehet szert a jövőben. Az MI alapú fejlesztés az internetes közösségi oldalak és a hozzájuk kapcsolódó

[5] Ugyanakkor a mesterséges intelligencia nem csak előnyöket, hanem veszélyeket is hordoz magába, amelyekre például Hawking is figyelmeztetett. (Cellan-Jones 2014, Kovács 2018a)

szolgáltatások fejlesztésében már ma is jelentős, de ez igaz a járműgyártástól kezdődően a logisztikán át az egészségügyig számos egyéb területre is. (Kovács 2018a)

1.3.2. Kritikus infrastruktúrák és kritikus információs infrastruktúrák

A kibertértől való függőségünknek van egy másik oldala is, amely legalább olyan mértékű, mint maga a digitalizáció teremtette függőség. Ez nem más, mint a digitális szolgáltatásokat lehetővé tevő infrastruktúra, illetve azok együttese. Ezeket ma kritikus infrastruktúráknak, illetőleg kritikus információs infrastruktúráknak, de sok esetben a korábban ismertetett módon létfontosságú elemeknek és rendszereknek is nevezzük[6]. Kritikus rendszereink olyan szoros kapcsolatban vannak egymással, hogy egy-egy rendszer vagy rendszerelem kiesése negatív hatással van egy vagy akár több kritikus rendszerre.

Mivel a rendszerek egymástól való függősége azok összetettsége miatt csak nehezen térképezhető fel, így azok esetlegesen egymásra gyakorolt valamennyi hatása is csak nagyon nehezen és nagy bizonytalanság mellett vizsgálható. Az egymásra utaltság és a rendszerek egymásra hatása a villamosenergia-szolgáltatás esetén különösen igaz, hiszen ez az egyik olyan kritikus infrastruktúra ágazat, amely minden más ágazattal és alágazattal kapcsolatban van. A villamosenergia-szolgáltatás, mint kritikus ágazat így megjelenő intra- és interdependenciája pedig ennek megfelelően szintén nagyon nehezen térképezhető fel. (Rinaldi–Peerenboom–Kelly 2001)

Mivel a kritikus infrastruktúrák a kibertéri szolgáltatások alapjai, ezért szükséges annak meghatározása, hogy melyek a legfontosabb infrastruktúrák, illetve ezeket milyen olyan veszélyek és kihívások fenyegetik, amelyek közvetve vagy közvetlen módon a kibertérre is hatással vannak.

[6] A továbbiakban a két kifejezést szinonim fogalomként használom.

A kritikus infrastruktúra védelem területén hazánkban áttörést jelentett a 2012-ben megjelent kritikus infrastruktúra védelmi törvény[7], amely a kritikus infrastruktúra[8] fogalmára a következő meghatározást adta: *„meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához - így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához -, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna."* (2012. évi CLXVI. tv. 1.§ f. pont)

A törvény megadta az európai értelmemben vett kritikus infrastruktúra[9] fogalmát is: *„a törvény alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős hatással lenne – az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve – legalább két EGT-államra*." (2012. évi CLXVI. tv. 1.§ c. pont)

Ugyanakkor a törvény nem tér ki a kritikus információs rendszerre vagy infrastruktúrára, de a jogszabály egyik végrehajtási rendelete meghatározza *a kritikus információs rendszer* és *létesítmény*[10] fogalmát. Ez alapján a kritikus információs rendszerei: „*a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek.*" [65/2013. (III. 8.) Korm. rendelet 1. § 3. pont] Ez a meghatározás megfelelő tartalommal bír dolgozatom vizsgálati szempontjaiból,

---

7 E törvény megjelenését megelőzően hazánkban a terület első jelentős jogszabálya a Kritikus Infrastruktúra Védelem Nemzeti Programról szóló (2080/2008. számú) Kormányhatározat volt 2008-ban. Ez a jogszabály előremutató módon elsőként tartalmazta hazánk kritikus infrastruktúra ágazatainak és alágazatainak felosztását. Azonban e kormányhatározat után még három évre volt szükség a katasztrófavédelmi törvény (A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény) megjelenésére. A 2011-ben megjelent törvény teremtette meg a jelenlegi szervezeti hátteret a kritikusinfrastruktúra-védelemhez. Az Országos Katasztrófavédelmi Főigazgatóság és annak három pillére, azaz a tűzoltóság, a polgári védelem, valamint az iparbiztonság szervezetrendszere ekkor jött létre. Ez utóbbi, azaz az iparbiztonsági pillér felügyeli a kritikus infrastruktúrák védelmét. Ezt követően csak 2012-ben jelent meg a 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről, amelyet gyakran csak kritikusinfrastruktúra-védelmi törvénynek hív a szakmai közösség. Ez a törvény, illetve annak végrehajtási rendeletei (például a 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról) szabályozzák ma a kritikus infrastruktúra hazai védelmét.

8 A törvény a *létfontosságú rendszerelem* megnevezést használja. (2012. évi CLXVI. tv. 1.§ f. pont)

9 A törvény az európai értelemben vett kritikus infrastruktúra vonatkozásában a korábban említettekhez hasonló módon az *európai létfontosságú rendszerelem* kifejezést használja. (2012. évi CLXVI. tv. 1.§ c. pont)

10 A Kormányrendelet *létfontosságú információs rendszer és létesítmény* megnevezést tartalmazza. [65/2013. (III. 8.) Korm. rendelet 1. § 3. pont]

mert magába foglalja, illetve keretet ad mindazon rendszerekhez és elemekhez, amelyek a kiberteret alkotják.

1. táblázat

A hazai kritikus infrastruktúra ágazatok és alágazatok

	Ágazat	**Alágazat**
1	Energia	villamosenergia-rendszer létesítményei (kivéve az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek)
2		kőolajipar
3		földgázipar
4	Közlekedés	közúti közlekedés
5		vasúti közlekedés
6		légi közlekedés
7		vízi közlekedés
8		logisztikai központok
9	Agrárgazdaság	mezőgazdaság
10		élelmiszeripar
11		elosztó hálózatok
12	Egészségügy	aktív fekvőbeteg-ellátás
13		mentésirányítás
14		egészségügyi tartalékok és vérkészletek
15		magas biztonsági szintű biológiai laboratóriumok
16		egészségbiztosítás informatikai rendszere
16a		gyógyszer-nagykereskedelem
17	Pénzügy	pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei
18		bank- és hitelintézeti biztonság
19		készpénzellátás
26	Infokommunikációs technológiák	internet-infrastruktúra és internethozzáférés-szolgáltatás

27		vezetékes és vezeték nélküli elektronikus hírközlési szolgáltatások, vezetékes és vezeték nélküli hírközlő hálózatok
28		rádiós távközlés
29		űrtávközlés
30		műsorszórás
31		postai szolgáltatások
32		kormányzati informatikai, elektronikus hálózatok
33	Víz	ivóvíz-szolgáltatás
34		felszíni és felszín alatti vizek minőségének ellenőrzése
35		szennyvízelvezetés és -tisztítás
36		vízbázisok védelme
37		árvízi védművek, gátak
38	Jogrend − Kormányzat	kormányzati rendszerek, létesítmények, eszközök
39		közigazgatási szolgáltatások
40		igazságszolgáltatás
41	Közbiztonság − Védelem	rendvédelmi szervek infrastruktúrái
42	Honvédelem	honvédelmi rendszerek és létesítmények

Forrás: 2012. évi CLXVI. tv., szerkesztette a szerző

A kritikus infrastruktúrák területén az egyik legnagyobb problémát az infrastruktúrák azonosítása jelenti. (Haig et al. 2009, Kovács 2018a) Az azonosításhoz szükséges azoknak a kritériumoknak a meghatározása, amelyek alapján egy-egy infrastruktúráról, illetve annak egyes elemeiről eldönthető, hogy az kritikus infrastruktúrának minősül-e.

A kritikusság meghatározásához szükséges elveket és kritériumokat határozza meg a már említett *65/2013. (III. 8.) Kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról* című jogszabály. A kormányrendelet alapján a kritikus infrastruktúra vonatkozásában az azonosítás *„az a folyamat, amely során a lehetséges létfontosságú rendszerelemeket kockázatelemzés, valamint az ágazati és horizontális kritériumok alapján meghatározzák.”* [65/2013. (III. 8.) Korm. rendelet 1. § 1. pont]

Ennek érdekében, azaz az azonosításhoz, vagy a besoroláshoz meg kell határozni az adott rendszerrel vagy rendszerelemmel szemben megjelenő kockázatokat, amely természetesen megfelelő kockázatelemzési megoldást is igényel. Ez azonban nem egyszerű folyamat és sok esetben komoly kihívás elé állítja az azonosítást végzőket. Az említett kormányhatározat szerint a kockázatelemzés: *„fenyegetettségi és kockázati tényezők vizsgálata a rendszerelemek sebezhetőségének, valamint a megzavarásuk vagy megsemmisítésük által okozott következmények értékelése céljából."* [65/2013. (III. 8.) Korm. rendelet 1. § 2. pont]

Az igazi kihívás az említett megfelelő kockázatelemzési módszertan kiválasztása mellett a kritériumok meghatározása. Ezt a meghatározást maga a kormányhatározat is megteszi öt fő csoportban, amely szerint a veszteségek kritériuma, a gazdasági hatás kritériuma, a társadalmi hatás kritériuma, a politikai hatás kritériuma, valamint a környezeti hatás kritériuma csoportokban lehetséges azonosítani ezeket a kritériumokat [65/2013. (III. 8.) Korm. rendelet 1. melléklet], de ezek csak nagyon tág kereteket adnak az egyes esetekben használható kritériumokhoz.

A hazai kritikusinfrastruktúra-védelem megfelel az Európai Unió területi szabályozásának, és illeszkedik az Unió kritikus infrastruktúra védelem irányelveihez. Az EU kritikusinfrastruktúra-védelem konkrét, szabályozásokban is megjelenő tevékenysége a 2000-es évekre datálható. A legfontosabb első lépések egyike a 2006-ban megjelent *Kritikusinfrastruktúra-védelem Európai Program*, amely hivatalos angol címéből *European Programme for Critical Infrastructure Protection* adódóan az EPCIP-program nevet viseli. Ez a program a kritikus infrastruktúrák védelmét tagállami hatáskörben tartja, ugyanakkor ebben a feladatban az Unió koordináló, felügyelő és tanácsadó szerepet tölt be, azaz minden tagállam maga gondoskodik nemzeti szinten a saját infrastruktúráinak védelméről, amelyhez az EU-tól nemzetközi szintre lépve koordinációs segítséget kap.

Az EU kritikus infrastruktúrákkal kapcsolatos jelenlegi szabályozása[11] összhangban van a 2015-ben megjelent *Európai Biztonsági Menetrenddel*[12] (Európai Bizottság 2015c), az *Egységes Digitális Piaci Stratégiával* (Európai Bizottság 2015b), valamint a *Kiberbiztonsági Stratégiával*. (Az Európai Unió kiberbiztonsági stratégiája 2013) Ezek az említett stratégiák közvetlenül, vagy közvetett módon erősítik az egységes európai biztonságot, amelyben az egyik legfontosabb tényező a kritikus infrastruktúrák, illetve kritikus információs infrastruktúrák területe. Ehhez járul hozzá az EU úgynevezett *NIS*[13] irányelve is, amely részben a kritikus infrastruktúrákra, illetve az abban lévő információs és hálózati rendszerekre is vonatkozik. *„A NIS direktíva 2018 májusában életbe lépve, bár közvetlenül nem a kritikus infrastruktúrákra vagy a kritikus információs infrastruktúrákra vonatkozik elsősorban, mégis a kiberbiztonság megteremtésével, illetve annak növelésével közvetett*

[11] Uniós szinten a kritikus infrastruktúrák védelmének első meghatározó szabályozási lépése a 2004-ben az európai terrortámadások hatására *A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben* című, az Európai Bizottság által kiadott közleménnyel történt. Ebben a dokumentumban határozta meg az EU elsőként a kritikus infrastruktúra fogalmát: *„A kritikus infrastruktúrák magukban foglalják mindazon fizikai és információs technológiai létesítményeket, hálózatokat, szolgáltatásokat és eszközöket, amelyek megzavarása vagy pusztítása komoly hatással lenne az állampolgárok egészségére, biztonságára, gazdasági jólétére, vagy közvetlen hatással lenne a tagállamok kormányzati működésére."* (Európai Bizottság 2004) Ezt követően 2005-ben jelent meg az Európai Bizottság *Zöld Könyve* a kritikus infrastruktúrák európai szintű védelméről. Ebben a Bizottság már megnevezi azt a 11 szektort és 37 szolgáltatást, amely az európai kritikus infrastruktúrák besorolását jelenti. (Európai Bizottság 2005) A kritikus infrastruktúra védelem területen mégis az igazi áttörést a 2006-ban elfogadott *Kritikusinfrastruktúra-védelem Európai Programjával (European Programme for Critical Infrastructure Protection, EPCIP)* következett be. (Európai Bizottság 2006) Az EPCIP már nem csak a terrorizmust tekintette fő fenyegetésnek, hanem az a kritikus infrastruktúrákat fenyegető egyéb bűncselekményeket, valamint a természeti és ipari katasztrófákat is besorolta ezek közé. Nagyon előremutató módon az EPCIP kritikus infrastruktúra védelmi kapcsolattartó pontokat is előírt az EU-tagállamok között a rendszeres információcsere biztosítása érdekében. (Európai Bizottság 2006) 2017 a következő mérföldkő az EU kritikus infrastruktúra védelem területén *az Európai Kritikusinfrastruktúra-direktíva (Directive on European Critical Infrastructures, ECI)* kiadásával. Az ECI célja az európai kritikus infrastruktúrák azonosítására és kijelölésére, valamint azok védelmére szolgáló eljárások kialakítása. Az irányelv hátránya azonban az, hogy ez csak az energia- és közlekedési ágazatra vonatkozik. Ezekben az ágazatokban a kijelölt kritikus infrastruktúra tulajdonosainak és üzemeltetőinek biztonsági terveket kell készíteniük, valamint ki kell jelölniük biztonsági összekötőket. Ezek az összekötők a tulajdonos és/vagy üzemeltető kapcsolatát biztosítják a kritikus infrastruktúra védelméért felelős nemzeti hatósággal. (Európai Bizottság 2018a) Ugyanakkor ez korábban már EU-s szinten is megteremtődött azzal, hogy az Európai Bizottság meghatározta egy, a tagországok kritikus infrastruktúrákat érintő kommunikációját segíteni hivatott információs hálózat létrehozását, amely a *Kritikus infrastruktúrák figyelmeztető információs hálózata* (*Critical Infrastructure Warning Information Network, CIWIN)* nevet kapta. A CIWIN beintegrálásra is került az EPCIP-be. (Európai Bizottság 2018b)

[12] Az Európai Biztonsági Menetrend (2015−2020) az Európai Bizottság politikai irányelveit fordítja le végrehajtható akciótervekké az európai biztonság megteremtése érdekében. (Európai Bizottság 2015c)

[13] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről. (NIS Direktíva 2016)

módon hozzájárulhat a kritikus információs infrastruktúrák védelméhez is." (Deighton 2017, idézi: Kovács 2018a)

A NIS meghatározza azokat az alapvető szolgáltatásokat nyújtó szereplőket, amelyek: *„a szervezet a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújt; az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ; és az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában."* (NIS Direktíva 2016 5. cikk 2. pont, idézi: Kovács 2018a)

Ennek megfelelően a NIS – hasonlóan a kritikus infrastruktúrák hazai szabályozásánál már bemutatotthoz – a kritikus szolgáltatásokat ágazatokra és alágazatokra osztja, amelyeket a következő táblázatban foglalok össze.

2. táblázat

A NIS-direktíva által meghatározott alapvető szolgáltatásokat nyújtó szereplők

Ágazat	**Alágazatok**
Energia	a) Villamos energia b) Kőolaj c) Földgáz
Közlekedés	a) Légi közlekedés b) Vasúti közlekedés c) Vízi közlekedés d) Közúti közlekedés
Banki szolgáltatások	
Pénzügyi és piaci infrastruktúrák	
Egészségügy	Egészségügyi ellátó létesítmények (beleértve a kórházakat és a magánklinikákat is)
Ivóvízellátás és -elosztás	
Digitális infrastruktúra	IXP-k DNS-szolgáltatók TLD-névnyilvántartók

Forrás: NIS Direktíva 2016 II. melléklet, szerkesztette: szerző

A NIS tehát számos szempontból fontos egységes európai szabályozás. Az abban foglalt rendelkezések egyes elemei a nemzeti kiberbiztonsági stratégiákra is komoly hatással vannak, mert sok olyan elemet határoz meg, amelyeket a nemzeti szintű stratégiákba kötelező érvényűen be kell építeni.

A kritikus infrastruktúra hazai és európai szabályozását elemezve megállapítható, hogy a kritikus infrastruktúrákon belül ugyan megjelenik az infokommunikációs szektor, mint kritikus ágazat, de a kritikus információs infrastruktúrákról sokáig nem volt egységes szabályozás. Ezt részben pótolja a NIS irányelv, illetve részben az EU ehhez szervezetrendszert[14] is hozzárendel, amely feladata a kiberbiztonság különböző kérdéseinek, így a kritikus infrastruktúrák és kritikus információs infrastruktúrák szerteágazó területeinek koordinációja. (ENISA 2017a)

1.3.3. A digitalizáció társadalmi hatásainak mérése

A digitalizáció társadalomra gyakorolt hatása ma már olyannyira elvitathatatlan, hogy gyakran magára a társadalomra is a digitális jelzőt használjuk[15]. Ahogy az Európai Bizottság elnöke az Unió 2015-ben kiadott *Európai digitális egységes piaci stratégiájában* megfogalmazta: *„[a]z internet és a digitális technológiák a gazdaság és a társadalom valamennyi szektorába való intenzív beágyazódás révén minden szinten átalakítják életvitelünket és munkamódszereinket: egyénenként, az üzleti világban és a közösségben is."* (Európai Bizottság 2015b, idézi: Kovács 2018a)

Mielőtt azonban megvizsgáljuk azokat a mérési metódusokat, amelyekkel a digitális technika és technológia társadalomra gyakorolt egyes hatásai mérhetőek, célszerű egy pillantást vetni azokra a statisztikákra, amelyek az internethasználatra nyújtanak képet[16].

A világ népessége 2018-ra elérte a 7,6 milliárd embert. A 2016-os statisztikai adatok még azt mutatták, hogy a világon közel 3,7 milliárd ember használta az internetet, ugyanakkor ez az arány 2018 év közepére már 4,2 milliárdra nőtt, amely a teljes népesség 55,1 %-a. A 2000-től eltelt időszakban ez a szám, azaz internetet rendszeresen használók száma

[14] E szervezetrendszer egyik eleme az ENISA.

[15] Az információtechnológia társadalomra gyakorolt hatásai bemutatására az 1990-es évek óta számos kifejezést használtunk, mint például a tudástársadalom, vagy információs társadalom. Az információs társadalom meghatározását korábban így adtuk meg: *„[a] tudomány eredményeinek intenzív és folyamatos felhasználására alapozott, új típusú termelési és társadalmi alapmodell, amelyet tartalma alapján intenzív tudásgazdaságnak és tudástársadalomnak neveznek."* (Haig–Kovács 2012)

[16] A dolgozatban megvizsgálni kívánt országok vonatkozásában az internethasználók számát és teljes lakossághoz viszonyított arányát a 2.5. fejezetben az országok nemzeti kiberbiztonsági stratégiáinak legfontosabb elemeit összefoglaló táblázatokban adom meg.

megtízszereződött. (Internet World Stats 2018) Azonban az internethasználók számának régiónkénti eloszlása nem homogén. Hatalmas különbségek vannak a kontinensek, illetve azokon belül is a különböző régiók között a felhasználók számában. (Kovács 2018a) Ezeket az arányokat szemlélteti a következő táblázat.

3. táblázat
A világ internetpenetrációja

Régiók	**Népesség** (2018) *millió fő*	**A világ népességének %-a**	**Internethasználók száma** (2018.06.30.) *millió fő*	**Internet-penetráció aránya** (népesség %-ában)
Ázsia	4207	55,1%	2062	49,0%
Európa	827	10,8%	705	85,2%
Latin-Amerika	652	8,5%	438	67,2%
Afrika	1287	16,9%	464	36,1%
Észak-Amerika	363	4,8%	345	95,0%
Közép-Kelet	254	3,3%	164	64,5%
Óceánia, Ausztrália	41	0,6%	28	68,9%
Összesen	**7634**	**100%**	**4208**	**55,1%**

Forrás: Internet World Stats 2018, szerkesztette: szerző

A DESI index

Az, hogy a digitális technológia mennyire van jelen a társadalom hétköznapjaiban ma már pontosan – ráadásul országok összehasonlítását lehetővé tevő módon – mérhető, akár földrajzi területenként, akár országonként. E mérések eredményei alapján lehetséges a fejlesztési források megfelelő allokációja, a befektetések támogatása és ösztönzése, valamint ahol erre valódi szükség van ott a társadalmi ösztönzés kiemelten kezelhető, amely közvetett módon a versenyképesség növeléséhez is hozzájárulhat. (Kovács 2018a)

Erre a mérésre az Európai Unió kidolgozta az úgynevezett digitális társadalom és digitális gazdaság indexet (Digital Society and Economy Index, DESI). A DESI egy többelemű, kompozit index, amely összefoglalja a tagországok digitális teljesítményét, így nyomon

követhető az EU tagországainak fejlődése, valamint digitális versenyképessége. (Európai Bizottság 2017, Kovács 2018a)

A DESI öt, a digitalizációval összefüggő területen méri a gazdaság és a társadalom fejlettségét, amelyekhez további harminc indikátor kapcsolódik[17]. Az öt fő teljesítménymutató és az azokhoz tartozó főbb mérendő területek:

- összekapcsoltság: ez az indikátorcsoport méri a hálózati, és ebben kiemelten a szélessávú internetes infrastruktúrát és annak minőségét, a 4G mobilszolgáltatások meglétét, annak igénybevételét, de a szélessávú internetelérés árát is. A gyors és szélessávú internetalapú szolgáltatások szükséges feltételei a gazdasági és társadalmi versenyképesség elérésének;
- humán tőke: ez az index azokat a mutatókat méri, amelyek az egyén vagy társadalmi csoport legalapvetőbb digitális készségeit, valamint a digitális társadalom által nyújtott lehetőségeket kihasználását jellemzik, illetve mutatják meg. Ezekbe a készségekbe többek között az olyan alapvető felhasználói ismereteket tartoznak, amelyek lehetővé teszik az egyénnek az online térben való eligazodást, a digitális termékek és szolgáltatások megvásárlását, vagy azok használatát. Ide sorolják azokat a fejlett digitális készségeket is, amelyek alapján a munkaerő képessé válik a fokozott termelékenységre, így járulva hozzá a gazdasági növekedéshez;
- internetes szolgáltatások használata: ez az index nem csak az adott ország internethasználóinak számát méri, hanem azt is, hogy ez az internethasználat a felhasználók részéről milyen internetes tevékenységeket jelent, azaz például milyen szolgáltatásokat használ, mennyire van jelen a távmunkában, milyen korszerű online kommunikációs eszközöket, online vásárlás és e-banki szolgáltatásokat vesz igénybe;
- digitális technológiák integráltsága: ez az index a vállalkozások digitalizációját mutatja meg például az online értékesítési csatornák használatának mérésével. Ez azért fontos, mert a digitális technológia alkalmazása, valamint annak az üzletbe való beépítése hozzájárul a vállalkozások hatékonyságához, csökkentheti a vállalkozás költségeit, de az online kereskedelmi felület szélesebb körű piaci

[17] Ennek az öt fő indikátorcsoportnak a kiegészítésére 2018-ban már az IKT szektorban megvalósuló kutatás-fejlesztést, valamint a Horizont 2020 programban megvalósuló IKT projektekben való részvételt is alkalmazzák. (Európai Bizottság 2018c)

hozzáférést is biztosít, így az adott vállalkozás növekedési potenciálját direkt módon is emeli;

- digitális közszolgáltatások: ez az index az e-kormányzati megoldásokat és szolgáltatásokat, illetve az azokhoz való állampolgári (amelybe természetesen a vállalatok ilyen lehetősége is beletartozik) hozzáférés lehetőségét, valamint azok használatát méri. A digitális közszolgáltatások hozzájárulnak a közigazgatás hatékonyságának növeléséhez, amely közvetlen módon hat az állampolgárok és a vállalkozások állammal való viszonyára. (Európai Bizottság 2018c, Kovács 2018a)

3. ábra

A DESI fő mérőszámcsoportjai

Forrás: Európai Bizottság 2016, Kovács 2018a, szerkesztette: szerző

Egy adott ország DESI értéke a fő területek pontszámainak és a részterületek pontszámainak egyedileg súlyozott átlagából tevődik össze. A kompozit indexben a kapcsolati sebesség és a digitális készségek az adott ország átlagos pontszámának 25%-25%-át, a digitális technológia integrációja 20%-át, az internethasználat és a digitális közszolgáltatások pedig 15%-15%-át adják. A DESI 0 és 1 közötti értéket vehet fel. Minél jobb egy ország teljesítménye, azaz a mutatószámok alapján minél fejlettebb az adott ország digitális gazdasága és társadalma, az eredmény annál közelebb áll az 1-hez. (Európai Bizottság 2016, Kovács 2018a)

A DESI összegzett értékeit az Európai Unió az előző évek fejlődési trendjeit is figyelembe véve összegzi, amely során a tagállamok teljesítménye az EU-s átlaghoz való viszonyként is bemutatásra kerül. Az évenként elvégzett számítások és összegzés szerint 2018-ban digitális társadalom és gazdaság tekintetében kiemelkedően fejlett[18] országok Dánia, Svédország, Finnország, Hollandia és Luxemburg voltak, míg a gyengén teljesítő országok Románia, Görögország, Bulgária, Lengyelország, Magyarország[19], Horvátország, Ciprus és Szlovákia voltak. (Európai Bizottság 2018c)

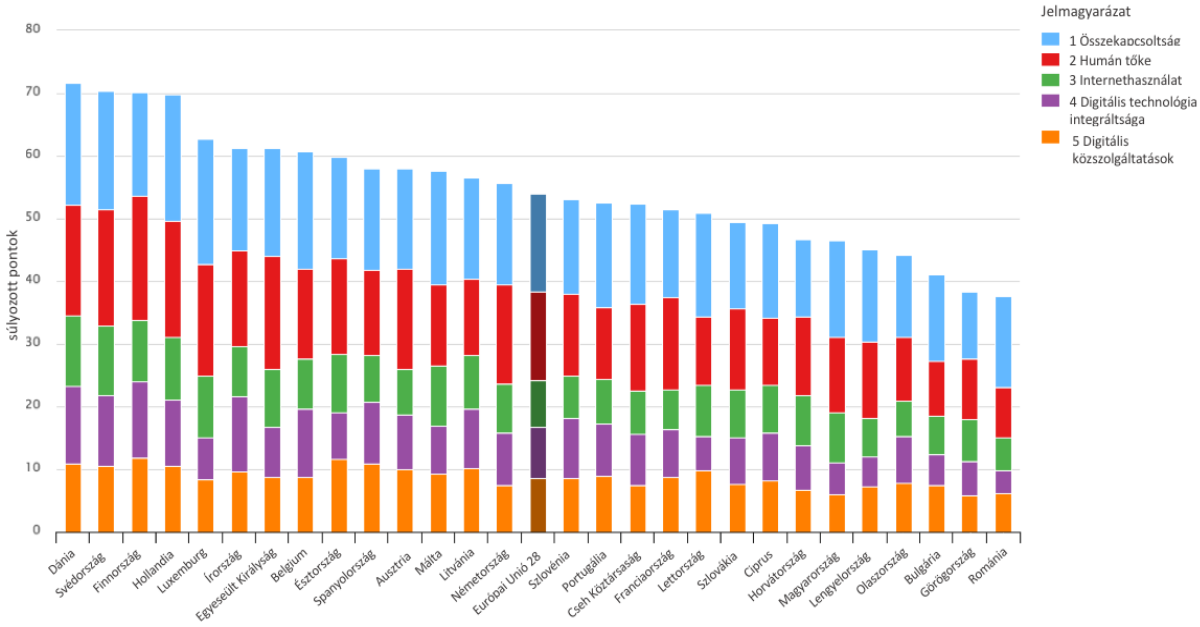
Minden évben új friss adatok alapján számítják ki öt indikátorcsoportban az adott évre érvényes DESI indexet. Magyarország DESI indexe 2016-ban 0,43 volt, amely a 20. helyre volt elegendő a 28 uniós tagállam között, ugyanakkor 2017-ben hazánk az előző évi helyezéséhez képest már két helyet rontva a 22. helyen állt a DESI ranglistán.

2017-ben Magyarország DESI-indexe 0,44 volt, amely bár magasabb pontszám volt, mint a 2016-ban kapott eredmény, de az EU-s DESI-átlag értéke is nőtt a 2016-os 0,49-ről 0,51-re 2017-ben. Ebben az évben is megállapítható volt, hogy hazánk az összekapcsoltság területén messze az EU-s átlag fölött van a nagy sebességű vezetékes széles sávú és a 4G-s mobilrendszerek elterjedtségének köszönhetően, így ebben a mutatóban magas pontszámot kapott. Hazánk javított a digitális készségek területén is, de ezen a területen még mindig alaposan elmarad az EU-s átlagtól. A 2017-ben a DESI jelentés Magyarország vonatkozásában a legnagyobb kihívásoknak a vállalkozások IKT-eszközök, rendszerek és

18 Az EU ezekre az országokra az angol *running ahead* kifejezést használja.

19 Hazánk DESI index alapján elfoglalt helye az Unió tagországai között annak tükrében tűnik nagyon gyengének, hogy Magyarországon már 2001-ben megszületett a Nemzeti Információs Társadalom Stratégia (NITS), amelyben több olyan programpont volt, amelyek az egyes – most a DESI által is mért – területek fejlesztését szolgálták. Ilyen program volt például az infrastruktúra-fejlesztési, vagy az elektronikus kormányzati program. Ezt követően számos további stratégia is született az információs társadalom építése és fejlesztése területen, például a 2003-ban kiadott Magyar Információs Társadalom Stratégia (MITS). (Haig – Kovács 2012) Az ezekben foglalt stratégiai elképzelések európai szinten csak a 2010-ben született Európai Digitális Menetrend céljai között jelennek meg. Azaz hazánk információs társadalmat érintő stratégiai tervei jónéhány évvel megelőzték az európai közös gondolkodást, ugyanakkor ez mégsem vezetett oda, hogy hazánk ma a digitális gazdaság és társadalom európai összehasonlításában az élen szerepeljen. (Kovács 2018a) Mindezeken túl hazánk DESI index alapján mért helyezése azért is nehezen érthető, mert 2014-ben megszületett a már említett Nemzeti Infokommunikációs Stratégia 2014-2020, amely fő célja pont a DESI-ben is mért egyes területek fejlesztése. (Nemzeti Infokommunikációs Stratégia 2014) Ugyanakkor fontos hangsúlyozni, hogy a kormány 2016-ban Digitális Jólét Program (DJP) névvel a digitális gazdaság és társadalom fejlesztése érdekében számos stratégiát magába foglalva széleskörű koncepciót dolgozott ki. A DJP magába integrálja a Digitális Magyarország programot is, amely egy olyan átfogó infokommunikációs fejlesztési elképzelést takar, amely alapján minden háztartás számára lehetőség lesz a szélessávú internetelérésre. A DJP számos olyan pályázati lehetőséget is takar, amely hátrányos helyzetű társadalmi rétegek vagy elmaradott, fejletlen régiók számára tesz lehetővé digitális eszközökhöz és szolgáltatásokhoz való hozzáférést. (Digitális Jóléti Program 2017, Kovács 2018a)

szolgáltatások használatának csekély mértékében és a digitális közszolgáltatások alacsony fejlettségi szintjében azonosította. (Európai Bizottság 2017d, Kovács 2018a)



1. ábra
Az Európai Unió országainak DESI indexe 2018-ban
Forrás: Európai Bizottság 2018c, szerkesztette: szerző

A DESI 2018-as éves felmérése alapján hazánkra vonatkoztatva sajnos jórészt ismét csak a kihívások azonosíthatóak, ugyanis Magyarország még hátrébb került a 28 tagország DESI ranglistáján. 2018-ban már csak a 23. helyet foglalja el Magyarország a DESI alapján. Hazánk csak Lengyelországot, Olaszországot, Bulgáriát, Görögországot és Romániát előzte meg. (Európai Bizottság 2018c)

4. táblázat
Magyarország DESI indexe 2017-ben és 2018-ban

	Érték*/helyezés	**EU átlag***
2017	44,2 / 22	50,8
2018	46,5 / 23	54,0

** Megjegyzés: 100-as értékben megadva*

Forrás: Európai Bizottság 2018d, szerkesztette: szerző

Magyarország vonatkozásában az indikátorok között továbbra is jó az összekapcsoltság, amely a nagysebességű és szélessávú hálózati elérés lehetőségének és használatának

köszönhető. Ugyanakkor a humán tőke vonatkozásában már elmaradunk az Uniós átlagtól. Ennek oka az, hogy a lakosság fele nem rendelkezik az alapvető digitális készségekkel.[20] A legnagyobb lemaradás mégis az e-közszolgáltatások terén van, mert ebben a szegmensben hazánk csak a 27. helyet szerezte meg a 28 tagország között. (Európai Bizottság 2018d)

5. táblázat

Magyarország DESI indexe indikátorcsoportonként 2018-ban

Indikátorcsoport	**Érték*/helyezés**	**EU átlag***
Hálózati összekapcsoltság	61,7 / 18	62,6
Humán tőke	48,0 / 21	56,5
Internetes szolgáltatások használata	53,6 / 12	50,5
A digitális technológiák integráltsága	25,1 / 25	40,1
Digitális közszolgáltatások	40,4 / 27	57,5

***** *Megjegyzés: 100-as értékben megadva*

Forrás: Európai Bizottság 2018d, szerkesztette: szerző

A DESI index számítási metodikájából jól látszik, hogy az közvetlen módon nem tartalmazza a kiberbiztonság mérését. Ugyanakkor a DESI egyes elemei közvetett módon kifejezhetik a kibertérben megvalósuló biztonságot. Ilyen mutató lehet például az e-közigazgatást használók száma, hiszen amennyiben ezek a szolgáltatások biztonságosak, akkor a velük – és nem utolsó sorban az állammal – szembeni állampolgári bizalom erősödik. Mindezek alapján kijelenthető, hogy a DESI indexre építve, az abban foglalt egyes elemek fejlődési trendjén keresztül közvetett módon mérhető a biztonság, mint állapot változása, mert a kiberbiztonság hozzájárul a gazdaság jobb teljesítőképességéhez, a kereskedelemhez, valamint az állampolgárok állam és közigazgatással szembeni bizalmához

Ugyanakkor a bemutatott DESI értékek világosan rámutatnak, hogy Európa nem egységes a digitális gazdaság és társadalom építésében, illetve az abban elért eddigi eredményekben. Ennek kiküszöbölésére, illetve a területen valamennyire is egységes szint

[20] Ehhez nyilvánvalóan a műszaki tudományokat és matematikát (Science, Technology, Engineering and Mathematics, STEM) tanulók és/vagy diplomások alacsony száma is hozzájárul.

elérése érdekében az Európai Bizottság 2015-ben életre hívta az európai *Digitális Egységes Piaci Stratégiát (Digital Single Market)*. A stratégia célját jól mutatja az a jelmondat, amelyet az Európai Bizottság fogalmazott meg ezzel kapcsolatban: *„[b]ontsuk le a korlátokat, hogy feltárjuk az online lehetőségeket."* (Európai Bizottság 2017e)

A *Digitális Egységes Piaci Stratégia* legfontosabb célja a digitális gazdaság kiterjesztése révén a szolgáltatók versenyre kényszerítése és a kis- és középvállalkozások növekedési potenciáljának emelése, a fogyasztók és a vállalkozások számára Európa-szerte egységes elvek szerinti termékekhez és szolgáltatásokhoz való hozzáférés[21]. A dokumentumban foglaltak alapján az EU hozzá kíván járulni a digitális hálózatok és szolgáltatások növekedési és terjeszkedési feltételeinek megteremtéséhez, így az európai digitális gazdaság növekedéséhez. A stratégiában a digitális szabad piac[22] mellett markánsan megjelenik a biztonság. (Európai Bizottság 2015a)

A biztonsággal kapcsolatban az egyik nagyon fontos feladat a felhasználók személyes adatainak kezelése, annak biztonságosabbá, megbízhatóbbá és a felhasználók számára átláthatóbbá tétele a digitális szolgáltatások használata során. Ez a feladat az uniós adatvédelmi szabályozásban is megvalósult, hiszen elfogadásra került az úgynevezett GDPR-irányelv, azaz az EU általános adatvédelmi irányelve, amelyet az Európai Unió kiberteret érintő stratégiáinál külön is bemutatok.

A személyes adatok kezelése során megjelenő bizalom kiépítése a jogszabályi háttér megalkotása mellett a kiberbiztonság emelésével érhető el. Ennek érdekében az Európai Unió megalkotta az *Európai Digitális Menetrend*[23] részét képező *EU kiberbiztonsági*

---

21 A stratégia céljainak elérése érdekében az Európai Bizottság olyan intézkedéseket fogalmazott meg, mint például a határokon átnyúló online értékesítés szabályainak megreformálása. Ez együtt jár a fizikai termékek határokon átnyúló online értékesítésével kapcsolatos jogok és a fogyasztói jogok egységesítésével is. A Bizottság javasolta a határokon átnyúló csomagküldés egyszerűbbé tételét, valamint a területi alapú tartalomkorlátozás megszüntetését, amely jelenleg azt eredményezi, hogy a fogyasztók eltérő árat fizetnek egy-egy szolgáltatásért, függően tartózkodási helyüktől. (Európai Bizottság 2015a, Kovács 2018a)

22 A szabad, de egységes piacon azonban kiemelten fontos a szerzői jogok védelme. Ennek érdekében az európai szerzői jogi szabályozás reformja sem váratott magára túl sokat, hiszen a terület 2016-os szabályozása felülvizsgálatra szorult. Bár azt az Európai Parlament 2018 júniusában még elutasította annak egyes rendelkezései miatt, de 2018 szeptemberében megszavazta az új szerzői jogokról szóló egységes európai szabályozást. (Európai Parlament 2018) A vegyes érzelmeket kiváltó szabályozás a biztonság szempontjából sem elhanyagolható, mert többek között a színvonalas újságírásra is ad számos szabályozási pontot. Így a később bemutatni kívánt hamis hírek elleni védelem egyik közvetett jogszabályi alapjának is tekinthető ez a szabályozás.

23 A 2008-as gazdasági válság után az Európai Bizottság 2010-ben *Európa 2020* címmel stratégiát hirdetett, amely egyik fontos pillére az *Európai Digitális Menetrend.* (Europe 2020 Strategy 2010) Az Európai Digitális Menetrend egyik legfontosabb célja az unió tagországai számára egységes digitális piac létrehozása, amely fenntartható gazdasági és szociális előnyökhöz juttatja a tagországokat. Ennek egyik alapfeltétele a nagy sebességű internet és az interoperabilitás kialakítása. A menetrend feltárja az

stratégiát[24] (2013), valamint az úgynevezett *NIS irányelveket*[25] (2016). Ezeket a stratégiákat, illetve direktívákat az Európai Unió kiberteret érintő szabályozását bemutató alfejezetben szintén elemzem.

A GCI index

A GCI index, azaz a *Global Cybersecurity Index*, magyarul Globális Kiberbiztonsági Index az ITU által megalkotott referenciaszámítás, amelyhez a szükséges adatokat a résztvevő országok önkéntesen szolgáltatják. Ezzel nemzetközi téren válik lehetővé az egyes országok kiberbiztonság iránti elkötelezettsége összehasonlítása, illetve annak felmérése, hogy az adott ország a kibertérben jelentkező veszélyeket és kihívásokat mennyire hatékonyan képes kezelni[26]. A GCI mérése és így az országok összehasonlítása is öt pillér mentén történik:

- jogi intézkedések;
- technikai intézkedések;
- szervezeti intézkedések;
- kapacitásépítés;
- együttműködés. (ITU 2017b)

A GCI a DESI-hez hasonlóan egy kompozit index, amely az 5 fő területen 25 indikátor alapján kerül kiszámításra. Az ezeken a területeken elért pontszámok súlyozott átlaga egy

Unióban meglévő gazdasági és társadalmi hiányosságokat (többek között például a digitális piac szétaprózottsága, az interoperabilitás hiánya, a kiberbűnözés terjedése, hálózati beruházások alacsony volumene, kevés és nem hatékony K+F, digitális írástudatlanság magas szintje). Ezek kiküszöbölésére és az EU digitális területeinek fejlesztésére számos olyan intézkedést határoz meg, mint például az egységes digitális piac létrehozása, a tartalomhozzáférés könnyebbé tétele, a nemzetközi pénzügyi tranzakciók egyszerűsítése, a távközlési szolgáltatások egységes piacának erősítése, törekvés a közös szabványok kialakítására, a digitális szolgáltatásokkal kapcsolatos bizalomerősítés, a nagysebességű internet és hálózati szolgáltatások kialakítása, valamint aktívabb és hatékonyabb K+F támogatása. (Európai Bizottság 2017c. Kovács 2018a)

24 Az EU kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér. (Az Európai Unió kiberbiztonsági stratégiája 2013)

25 A NIS irányelv hivatalos címe: Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. (NIS Direktíva 2016)

26 Az itt bemutatott GCI indexhez nagyban hasonlító egyéb mérési metodológiák is napvilágot láttak. Az egyik ilyen igen előremutató index az úgynevezett Nemzeti Kiberbiztonsági Index (National Cyber Security Index, NCSI), amelyet egy többségében észt szakértőkből álló csoport alkotott és fejleszt. Az NCSI célja, hogy az elérhető legtöbb ország esetén összehasonlítható módon megmérje a kibertéri fenyegetettségek megelőzésére és a kiber incidensek kezelésére való felkészültségüket. Az NCSI egy nyilvános adatbázis, amelyben nyomon követhetők az adott ország említett területeken meglévő kapacitásai és képességei. Hazánk ebben a listában globálisan az előkelő 17. helyet szerezte meg 2018-ban. (NCSI 2018)

összpontszámot eredményez, amely így lehetőséget ad az országok kiberbiztonsági helyzetének összehasonlítására. A GCI legfontosabb célja elsősorban azonban nem csak az összehasonlítás és ennek megfelelően egy rangsor előállítása, hanem a kiberbiztonság területén megvalósuló nemzetközi együttműködés és a tudáscsere előmozdítása. Ez a tudáscsere lehet az alapja az adott ország kiberbiztonsági elköteleződésének és így a kiberbiztonság növelésének. A GCI-hez az ITU Globális Kiberbiztonsági Programja (Global Cybersecurity Agenda, GCA) biztosítja a megfelelő keretet. Az ITU kezdeményezésére 2007-ben elindított GCA az információs társadalom biztonságának fokozására irányuló nemzetközi együttműködés keretrendszere. A GCA öt pillére épül: jogi intézkedések, műszaki és eljárási intézkedések, szervezeti struktúrák, kapacitásbővítés, nemzetközi együttműködés elősegítése és fokozása. A program fő célja az információs társadalom biztonságának hatékony, a különböző területek és tevékenységek között meglévő átfedéseket minimalizáló nemzetközi együttműködésre épülő fejlesztése. (ITU 2018a, Kovács 2018b)

2. ábra
Az ITU GCI indexének mérőszám-csoportjai

Forrás: ITU 2018b, szerkesztette: szerző

A GCI öt fő pillére a fentieknek megfelelően a következő indikátorokat foglalja magába:

- jogszabályi megfelelőség:
  - kiberbűnözés elleni tevékenység szabályozottsága;
  - kiberbiztonság szabályozottsága;
  - kiberbiztonsági képzés szabályozottsága;
- technikai megfelelőség:
  - nemzeti CSIRT (Computer Incident Response Team, azaz számítógépvészhelyzeti-reagáló csoport) meglévősége;
  - kormányzati CSIRT meglévősége;
  - ágazati CSIRT(ek) meglévősége;
  - a szervezetek számára kiadott működési normák meglévősége;
  - szakemberek minősítési normáinak megléte;
  - gyermekek online védelme;
- szervezeti megfelelőség:
  - stratégia meglévősége;
  - felelős szervezet meglévősége;
  - a kiberbiztonság mérésének meglévősége;
- képességépítés:
  - szabványosítási szervezet megléte;
  - jógyakorlatok megléte;
  - kiberbiztonsági K+F programok megléte;
  - felhasználói tudatosságot növelő kampányok megléte;
  - szakmai képzési programok megléte;
  - kiberbiztonság megjelenése a nemzeti oktatási programokban;
  - kiberbiztonsági ösztönző rendszer(ek) megléte;
  - hazai kiberbiztonsági ipar megléte;
- együttműködés:
  - államok közötti együttműködések;
  - többnemzeti megállapodások;
  - nemzetközi fórumokban való részvétel;
  - állami- és magánszféra együttműködései;
  - kiberbiztonsági szervezetek közötti együttműködések. (ITU 2017b)

A GCI index alapján számított ranglistán a világ első három országa 2017-ben Szingapúr, az Egyesült államok és Malajzia voltak. Európában az első három ország Észtország 0,84 GCI ponttal, globálisan az 5. helyezéssel; Franciaország 0,81 ponttal, globálisan a 8. helyezéssel; valamint Norvégia 0,78 ponttal, globálisan a 11. helyezést elérve voltak. (ITU 2017b)

Magyarország GCI indexe 2017-ben 0,53 pont volt, amely globálisan az 51. helyre volt elegendő. (ITU 2017b)

1.4. A kibertérben jelentkező stratégiai kihívások és veszélyek

A kiberbiztonsági fenyegetések felmérése kiemelten fontos, ugyanakkor nagyon nehezen megvalósítható feladat is egyben. Ennek oka kettős. Egyrészt naponta jelennek meg újabb és újabb olyan támadási módok, amelyek az infokommunikációs rendszerek sérülékenységeit kihasználva kompromittálják azokat, másrészt sok esetben nehéz különbséget tenni a fenyegetések különböző szintje, illetve volumene között. Stratégiai szinten is jelentkezhetnek olyan támadások, amelyek alapvetően technikai jellegű sérülékenységeket kihasználva, egyes felhasználók eszközeit támadva fejtik ki hatásukat és okoznak károkat[27].

Ennek megfelelően ezen a helyen célom az, hogy a kiberbiztonság stratégiai környezete szempontjából releváns kihívások és veszélyek bemutatásra, illetve röviden elemzésre kerüljenek. Mindezek olyan trendekre kívánja a figyelmet fókuszálni, amelyek összefüggenek a kiberbiztonság stratégiájának kialakításával és amelyek alapvetően befolyásolják egy-egy nemzeti kiberbiztonsági stratégia tartalmát[28].

Fontos hangsúlyozni, hogy a kiberbiztonság csak stabil, nemzetközi együttműködésre alapozott kibertérben valósítható meg. Ennek azonban van egy másik oldala is, amely a nemzetek kiber autonómiájában, illetve az arra való törekvésben nyilvánul meg. Az autonómia meghatározott keretek között és meghatározott szintig – a hatályos nemzetközi

[27] Erre az egyik legjobb példa a 2016-os amerikai elnökválasztás során bekövetkezett – alapvetően orosz támogatású, befolyásolást elérni kívánó – támadások egész sor, amely során például a Demokrata Nemzeti Konvenció szerverei kompromittálódtak. A támadások alacsony szintű technikai támadások voltak, de az így megszerzett több ezer e-mail megfelelő módon és megfelelő időben történő nyilvánosságra hozatala hatását tekintve stratégiai jelentőségű következményeket jelentett. (Kovács–Krasznay 2017)

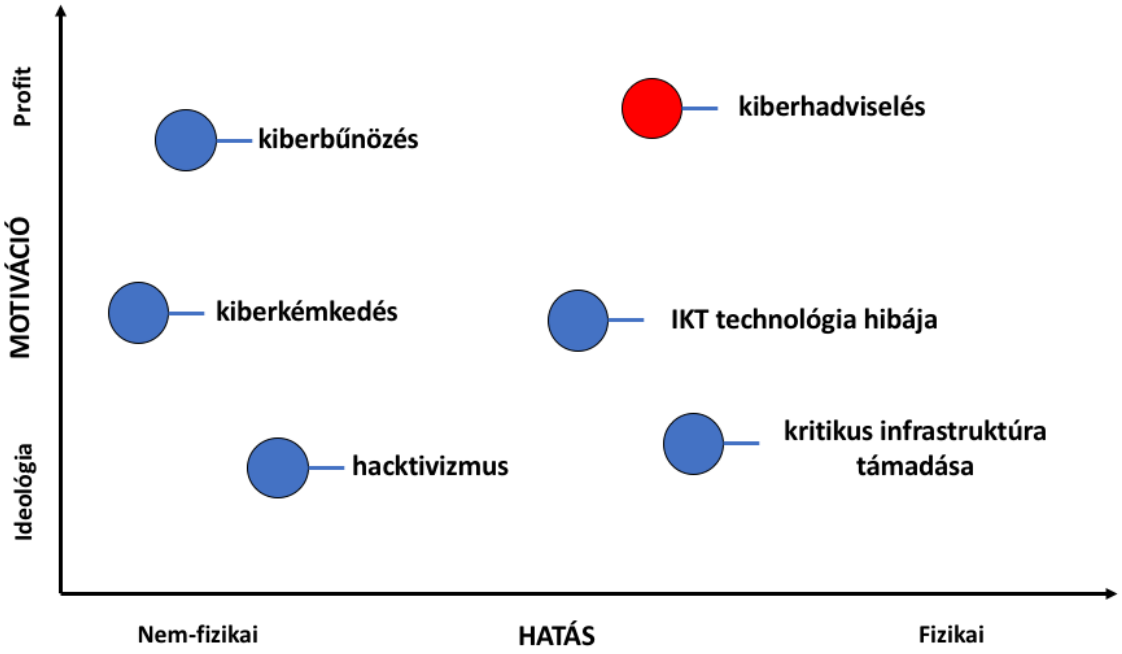
[28] Itt utalnom kell arra, hogy bár a dolgozatban csak később kerülnek bemutatásra az egyes országok nemzeti biztonsági stratégiái, de az azokból levonható következtetések azt mutatják, hogy számos ország nem csak statikus módon felsorolja ezeket a veszélyeket és kihívásokat, hanem az azokra adandó megfelelő stratégiai szintű válaszok mentén határozza meg a kiberbiztonság szervezeti- és együttműködési rendszerét is. Ennek megfelelően célszerű a legfontosabb stratégiai kihívások, illetve azok lehetséges következményeit, egymásra, valamint a kiberbiztonságra gyakorolt hatásait bemutatni.

szabályokat betartva, azokat tiszteletben tartva, azok alkalmazása mellett – biztosítható, de nagyon sok olyan kérdés van, amely csak a nemzetközi térben – akár kompromisszumos megoldásokat keresve – oldható csak meg.

Eddigi kutatásaimra építve a fentiekben említett kiberbiztonsági kihívások és fenyegetések trendjei stratégiai szinten a következők lehetnek:

- kiberbűnözés;
- hacktivizmus;
- kiberkémkedés;
- kiberhadviselés;
- politikai befolyásolás;
- kiberfegyverek terjedése;
- a kritikus infrastruktúrák és a kritikus információs infrastruktúrák támadhatósága.

A fenti kihívások a jelen és a közeljövő várható kihívásai és veszélyei. Ugyanakkor a kibertér biztonságának stratégiai megvalósítása csak akkor lesz sikeres, ha az nem csak a jelenlegi veszélyekre, hanem a távolabbi jövő lehetséges kihívásaira is képes megfelelő válaszokat adni. Mivel a kibertér – leszámítva a nemzetek egyelőre elfogadható kibertéri autonómia igényeit – nemzetközi jelleggel bír, így a fenti kihívásokra adandó válaszok megoldása nem történhet meg kizárólag csak nemzeti szinten. Ennek megfelelően nemzetközi, akár globális együttműködés szükséges a kiberbiztonság megteremtése és növelése érdekében. (Kovács 2018b)



3. ábra
A kibertérben megjelenő kihívások és veszélyek hatás és következmény szerinti interpretálása

Forrás: CRC-ICS 2015, szerkesztette: szerző

Kiberbűnözés

A kiberbűnözés fogalmát az Európai Unió kiberbiztonsági stratégiája a következőképpen adja meg: *„[a] számítástechnikai bűnözés számos különböző bűncselekményt jelenthet, amelyek során a számítógépek és az információs rendszerek az elsődleges eszközök, illetve ezek az elsődleges célok. A számítástechnikai bűnözés hagyományos szabálysértéseket (például csalás, hamisítás és személyazonosság-lopás), tartalmakhoz kapcsolódó szabálysértéseket (például gyermekpornográfia internetes terjesztése vagy fajgyűlöletre uszítás), illetve csak számítógépekre és információs rendszerekre korlátozódó szabálysértéseket (például információs rendszerek elleni támadások, hozzáférés megtagadása vagy rosszindulatú szoftverek) is magában foglal.”* (Az Európai Unió kiberbiztonsági stratégiája 2013, idézi: Kovács 2018a)

A kiberbűnözés által alkalmazott módszerek ma már egyre inkább egymásra épülnek, és ezekben egyre inkább a komplexitás figyelhető meg. A felhasználókat célozza a személyiséglopás, de a célzott phishingtámadás[29] is. Ugyanakkor ezeket a módszereket sok

[29] A phishing olyan adathalász technika, amely során a támadó az áldozatot megtévesztéssel – például egy hamis weboldalra mutató linkre való kattintással – veszi rá érzékeny adatainak (például bankszámlaadatok) megadására. A célzott phishing (spear phishing) ennek szofisztikált változata,

esetben a bonyolultabb, így nehezebben felderíthető szofisztikáltabb technikai és hálózati eszközökkel megvalósított elkövetésekkel kombinálják, amelyek célja nem a felhasználó, hanem azon keresztül az adott vállalat, legyen szó ipari vállalatról vagy akár pénzintézetről. Az elkövető, azaz a kiberbűnöző ma már nem feltétlenül magányos elkövető, mert az összetett védelmi megoldások miatt komplex tudásra, és így több elemből álló összetett támadási módszerre van szükség egy-egy bűncselekmény elkövetéséhez. Így egyre inkább szervezett csoportok az elkövetők. A kiberbűnözés az említett fejlett és egyre összetettebbé váló védelmi rendszerek miatt sok esetben komoly anyagi befektetést is igényel. Így sokszor a hagyományos bűnözői körök azok, amelyek ezeket a befektetéseket eszközölik, azaz megveszik vagy bérlik azt a tudást és/vagy technikai hátteret, amely a bűncselekmények megvalósításához szükséges. (Kovács 2018a)

Ugyanakkor a kiberbűnözés és azok a csoportok, akik hosszú évek munkáját fektetik az akcióikba nem csak nagy technikai tudásra tesznek szert, hanem olyan információk birtokába is kerülnek, amelyek stratégiai szinten is érdeklődésre tarthatnak számot. A kiberbűnözés során összegyűlt adatok, illetve az azok elemzéséből levonható következtetések alkalmasak lehetnek egy másik ország politikai és/vagy gazdasági befolyásolására, valamint felhasználhatóak a kiberhadviselés során annak tervezési fázisától kezdve a kibertámadások kivitelezéséig számos helyen.

Hacktivizmus

A hacker és az aktivizmus szavak összevonásából keletkezett hacktivizmus eredete az 1990-es évek közepére, illetve második felére tehető. Mégis a hackerszintű informatikai tudással rendelkező, majd valamely politikai, gazdasági, vallási vagy kulturális ügy mellé álló aktivisták a 2010-es években lettek világszinten is ismertek, amely jórészt az *Anonymous*[30] nevű csoportnak köszönhető. A csoport több igen nagy visszhangot kiváltott támadást intézett 2008 és 2015 között többek között a Szcientológiai egyház, vagy a WikiLeaks

amely során már nem nagytömegű felhasználót céloznak meg a támadások, hanem csak egy-kettő, nagyon tudatosan kiválasztott olyan áldozat a célpont, amelyről előzőleg már sok információ áll a támadó rendelkezésére, amely birtokában könnyebben rá tudja venni az áldozatot adatai megadására.

30 A csoport jellemzésére korábban a következő meghatározást adtam: *„[a]z Anonymous nagyon nehezen beazonosítható szervezet, önnön hitvallásuk szerint is hacktivistacsoportok lazán kapcsolódó nemzetközi szervezete. A csoportok nem hierarchikus felépítésűek, nincsenek igazi vezetők, nincs taglista, és nincsenek irodák. Csak elvek és ötletek vannak. Az Anonymousnak mindenki tagja lehet, aki követi azokat az irányelveket, amelyeket a szervezet önmagáénak vall. A szervezet nagyon jól használja az internetes médiumokat a saját akcióik beharangozására, vagy az akciók következményeinek a tálalására."* (Kovács 2018a)

melletti szimpátiájukat kifejezve a Julian Assagne által vezetett szervezet pénzügyeit blokkoló Visa és Mastercard cégek ellen. (Kovács 2018a)

Ugyanakkor a hacktivizmus említése a stratégiai veszélyek és kihívások során nem véletlen, ugyanis a hacktivista megmozdulásokat nagyon nehéz szétválasztani az állami támogatású akcióktól. Ebben az esetben arról van szó, nagyon sok olyan nemzetközi konfliktus van, amelyben egy-egy adott állam a diplomáciai megoldások mellett valami olyan egyéb eszközt is be kíván vetni, amely közvetlenül nem köthetők össze az adott ország kormányával, vagy hivatalos szervezeteivel. Ilyen támadássorozat történt 1999-ben, amikor az Egyesült Államok vezette szövetséges NATO-csapatok Szerbiát bombázták. Ennek során bombatalálat érte a belgrádi kínai nagykövetséget, amely azonnal kínai hackerek kibertámadásait nyitotta meg amerikai szerverek ellen. (Haig–Kovács 2012, Kovács 2018a)

Kiberkémkedés

Kezdetben a kiberkémkedés az ipari és gazdasági kémkedéssel mutatott hasonlóságot, hiszen a számítógépeket és IKT eszközöket felhasználó vagy azok segítségével végzett információszerzés egyik legfontosabb célja a szellemi termékek eltulajdonítása volt. Mára azonban ezen a téren is egyre markánsabb változásoknak vagyunk tanúi, ugyanis a gazdasági információk megszerzése mellett a kiberkémkedés célpontjai között a közigazgatás, a politika és a védelmi szféra szervezetei is szerepelnek. A kiberkémkedés egyik megnyilvánulási formája az APT támadással végrehajtott információszerzés.

Az APT (Advanced Persistent Threat, sokáig fennálló fejlett támadások) nevéből eredően kibertámadások együttesét jelenti. Ez egy összetett és számos támadási formát magába foglaló eljárást takar, amelyet célzott támadásoknak is hívnak a magyar szakterminológiában. (Kovács 2018a)

Az APT-támadások egyik legfontosabb attribútuma az, hogy ezek jelentős részben sokáig felfedezetlenek és észrevétlenek maradnak. A támadásokra jellemző, hogy ezek nem véletlenszerűen kiválasztott célpontokat támadnak, hanem előre pontosan kiválasztott, a támadó számára értékes politikai, üzleti, katonai, vagy közigazgatási információkat kezelő rendszereket támadnak. Egy APT támadások sorozatából áll, amelyek jól előkészítettek és jellemzően sokáig – 1-2 héttől kezdődően akár évekig is – fennállnak. (Kovács 2018a)

Az APT támadásokat nem véletlenszerű célpontot kiválasztó szoftverrobotok hajtják végre, hanem tudatosan kiválasztott célpontok ellen tervezett, az azok gyenge vagy sérülékeny pontjait kifinomult eljárásokkal feltáró, majd ezeken keresztül a rendszerbe

behatoló olyan programok, amelyek valódi célja az ott tárolt adatok észrevétlen megszerzése és a támadó számára való kijuttatása.

Az APT támadások során alkalmazott módszerek kifejlesztése ennek megfelelően nagy anyagi és humán energiabefektetést igényel. Ennek alapján nem túlzás kijelenteni a következőket: *„[...] amennyiben az APT-támadások mögött álló – alapvetően államilag támogatott – elkövetőkkel kombináljuk a kémkedést, és ezt tekintjük a támadások fő motivációjának, akkor eljuthatunk addig a megközelítésig, hogy államilag támogatott kiberkémkedéssel állunk szemben nagyon sok APT-támadás esetében is."* (Kovács 2018a)

Kiberhadviselés

Az állami támogatású kibertámadások egyre növekvő száma az egyik legnagyobb fenyegetés és az egyik legnagyobb biztonságpolitikai kihívás lett napjainkra.

Amennyiben leegyszerűsítjük a kérdést, akkor kijelenthetjük, hogy kiberhadviselés az állami támogatású olyan kibertámadások együttese, amelyek mögött politikai és/vagy katonai célok állnak[31]. Bár a kiberhadviselés definíciójára ma még nem találunk egységesen elfogadott meghatározást, de az előre jelezhető, hogy az országok által támogatott kibertámadások számának növekedése, valamint azok egyre súlyosabb következményei miatt a kifejezés pontos meghatározása már a közeljövőben meg fog jelenni szövetséges szinten (például a NATO-ban, vagy az EU-ban), de az egyes országok is stratégiai szinten fognak erre a területre többé-kevésbé egységes meghatározással szolgálni.

Korábban több kísérlet született a kiberhadviselés átfogó értelmezésére, amelyek közül az egyik – a 2011-ben született Haig, Kovács, Ványa által alkotott – megfogalmazás a következő: *„[c]yberhadviselésnek nevezhetjük mindazon tevékenységeket, amelyekben a számítógép-hálózati hadviselés, a számítógép-hálózati műveletek, az elektronikai hadviselés, bizonyos esetekben a SIGINT, valamint a cyberterrorizmus, illetve az ellene folyatott tevékenységek közösen jelennek meg."* (Haig–Kovács–Ványa 2011, idézi: Kovács 2018a)

Ez azonban még egy meglehetősen technikai alapú megközelítés volt, amelyből ráadásul hiányzott az egyik legfontosabb tényező is. Ez nem más, mint annak a felismerése, hogy kiberhadviselésről – a hagyományos hadviseléssel analóg módon – akkor beszélhetünk,

[31] Ez azonban nem jelenti azt, hogy egy-egy ilyen kibertámadás mögött feltétlenül állami apparátus áll. A kiberhadviselés veszélyességét pont az jelenti, hogy olyan kis létszámú csoportok is – állami támogatás mellett, de nyilvánvalóan akár annak hiányában is – el tudják követni ezeket a támadásokat, amelyek tagjai nem feltétlenül az adott országban, hanem akár több eltérő (esetleg pont a célországban) vannak.

amennyiben egy adott ország vagy országcsoport stratégiai fontosságú rendszerei (például kritikus infrastruktúrai) ellen indított kibertámadások mögött egy másik ország vagy ország csoport (esetleg ezekkel egyenértékű gazdasági vagy politikai hatalom) áll. (Kovács 2018a)

Ugyanakkor a kiberhadviselés, illetve maguk az államilag támogatott kibertámadások jelenleg nagyon is új elemet képviselnek a biztonságpolitikában, ezért azok hagyományos hadviselés rendszerében történő elhelyezése az egyik megoldás. Így a kibertámadások és a kiberhadviselés is sok esetben a hibrid, azaz a hagyományos hadviselési elemeket az újabb nem konvencionális, de a hadviselési célokat is alkalmazó olyan tevékenységekkel, mint a média műveletek, a politikai befolyásolás eszközeit egyszerre megvalósító, politikai és katonai célokat egyaránt elérni kívánó tevékenységként jellemzik. (Fleming–Qualkenbush–Chapa 2017, Kovács 2018a)

Azonban ez a hibrid jelző egyre inkább megfoghatatlan és egyre inkább csak az olyan gyakorlati példákon keresztül érthető, mint az ukrajnai konfliktus. De pont ezeken a példákon keresztül kapunk bizonyítékot arra, hogy ma már a kiberhadviselés a hagyományos hadviselés integráns részét képezi, amelyben a katonai célok elérése érdekében, legyen szó felderítésről, ellentevékenységről, vagy akár a siker kiterjesztéséről, elengedhetetlenül fontos elemként jelentkezik.

Politikai befolyásolás a kibertérben

A kibertér globális, a nemzetközi gazdaság mára egyik legfontosabb pillérévé válásáról korábban már említést tettem. Ugyanakkor politikai értelemben is jelentős a kibertér, hiszen ahogy korábban szintén említettem egy ország, annak lakossága kibertéri műveletekkel nagymértékben befolyásolható. A 2016-os amerikai elnökválasztás vagy a közvetlenül ezt követő német és francia választások körüli kibertéri események mind-mind azt mutatják, hogy az így megvalósított politikai befolyásolás rendkívül hatékony eszköz lehet egyes országok kezében. (Kovács–Krasznay 2017)

A politikai befolyásolással kapcsolatban nagyon gyakran két ország – Kína és Oroszország – merül fel, pedig a másik oldalról például az Egyesült Államok is él hasonló módszerekkel.

A kérdésben Kori Annan volt ENSZ főtitkár is megfogalmazta markáns véleményét 2018 februárjában a müncheni biztonságpolitikai konferencián elmondott beszédében. A volt diplomata kifejezte azt a meggyőződését, hogy sok számos politikai vezető, beleértve globális hatalmak vezetőit is, a kiberteret politikai célokra használják: *„[s] végül ezek a*

rezsimek a saját szolgálatukba állították az online médiát. Közismert, hogyan próbált Oroszország beavatkozni a választásokba Ukrajnában, Franciaországban, Németországban, és az Egyesült Államokban. A Facebook saját becslése szerint az orosz tartalom, beleértve a fizetett reklámokat, 126 millió amerikait ért el – a lakosság negyven százalékát!" (Annan 2018, idézi: Kovács 2018b) Majd Annan azt a megjegyzést is hozzátette, hogy a nyugati országok hasonló eszközökkel élnek: *„[e]mlékezzünk itt a korábbi orosz vádakra, melyek szerint a nyugati országok szervezték az úgynevezett színes forradalmakat Ukrajnában és Grúziában. Az internet új csatatér lett, a manipulátorok terepe."* (Annan 2018, idézi: Kovács 2018b)

Az idézett beszédében Kofi Annan a demokrácia oldaláról világítja meg a kiberteret és az internetet, arra is választ keresve, hogy az ilyen fajta politikai manipulációval szemben mennyire is védtelenek a demokratikus országok. (Kovács 2018b)

Mindezekkel Annan rávilágított és remekül érzékeltette a kiberbiztonság alapvető összefüggéseit. A fenti nyilatkozat arra is utalt, hogy *„akár a terrorista propaganda, akár a politika, akár a faji vagy akár a nemi gyűlöletbeszéd nagyon könnyen kiléphet a virtuális térből és az a fizikai dimenzióban jelenik meg, sajnos hatványozott hatással. Ezek a hatások nem kerülhetik el a legfejlettebb országokat, nemzetközi szövetségeket, a gazdaságot, a politikát, a kultúrát, valamint az emberek mindennapjait sem."* (Kovács 2018b)

A fentiek abszolút módon érzékeltetik a korábban a tudományos problémában megfogalmazott kérdést, nevezetesen azt, hogy bár a kibertér biztonságának megteremtése minden országban stratégiai kérdés kell, hogy legyen, de az nemzetközi összefogás nélkül pont a fentiekben bemutatott új kihívások megjelenése miatt nem képzelhető el. Ennek megfelelően az egyes országok saját stratégiai útkeresése mellett, meg kell, hogy jelenjen egy globális elképzelés is, amely mentén az előbb említett kihívások és veszélyek egységesen és hatékonyan kezelhetők. (Kovács 2018b)

Kiberfegyverek

A kiberfegyverek a fizikai dimenzióban működő és kinetikus energián alapuló fegyverekkel[32] szemben olyan szoftver és hardver eszközöket, illetve ezek kibertérben történő alkalmazását jelentik, amelyekkel a kijelölt célpontok számára – közvetlen vagy közvetett módon – valamilyen mértékű kár okozható.

[32] Természetesen léteznek egyéb, nem kinetikus energián alapuló fegyverek is, amelyek nem kiberfegyverek. Ilyen fegyverek például az irányított energiájú fegyverek, amelyek lézer, elektromágneses, akusztikus stb. energiát használnak hatásuk kifejtésére.

Egy ilyen korai kiberfegyver volt az említett Anonymous hacktivista csoport által előszeretettel használt Low Orbit Ion Cannon nevű szoftver. Ez hatását tekintve: *„[...] tömeges DDoS-támadást idéz elő, azaz a nyers erőt használja a briliáns programozói megoldások helyett. Maga a program nyilvánosan elérhető és bárki által letölthető az internetről, azóta, hogy megalkotója – a Praetox Technologies – 2008 év végén [...] a Project Chanology akció után közzétette."* (Kovács 2011, idézi: Kovács 2018b)

Az ilyen és az ehhez hasonló eszközök azonban a hagyományos fegyverek esetében már ismert kiberfegyverkezési versenyhez vezetnek. Bruce Schneier, az információbiztonság nemzetközi szinten is ismert és elismert szakértője fogalmazta meg ezzel kapcsolatban a következőket 2012-ben: *„[a] kiberfegyverkezési verseny korai éveiben járunk. Bár ezek drágák, de destabilizálják, és veszélybe sodorják az internet minden olyan részét, amelyet minden nap használunk."* (Schneier 2012, idézi: Kovács 2018b)

A kiberfegyverek jelentette veszély megoldását ekkor még Schneier is a nemzetközi együttműködésben kialakított szabályozásban látta: *„[a] nemzetközi együttműködés és a nemzetközi szerződések jelentik az egyetlen módját ennek megfordítására. A kiberfegyverek betiltása jó cél, de szinte biztosan elérhetetlen. Nagyobb a valószínűsége az olyan szerződéseknek, amelyekben a felek vállalják a kiberfegyverek elsőként történő alkalmazásának tiltását, vagy amelyek tiltják az illegális vagy széles körben, nem meghatározott célpont ellen használt ilyen fegyvereket, illetve olyan fegyvereket írnak elő, amelyek a támadások végén megsemmisítik önmagukat. A következő lépés lehet az olyan szerződések kidolgozása, amelyek a kiberfegyverek alkalmazása, illetve az ilyen fegyverek felhalmozásának a korlátozására irányulnak. Meg tudnánk tiltani az olyan polgári infrastruktúra elleni kibertámadásokat, mint például a nemzetközi bankrendszer."* (Schneier 2012, idézi: Kovács 2018b)

Többek között ez a Schneier által is szorgalmazott nemzetközi együttműködés elősegítése és felgyorsítása hívta életre a Microsoft által meghirdetett *Digitális Genfi Konvenció* (Digital Geneva Convention) elképzelést. Ennek egyik legjelentősebb célja a felhasználók állami támogatású kibertámadásokkal szembeni védelme érdekében kialakítandó nemzetközi összefogás.[33] (Microsoft 2018, Kovács 2018b) Ennek a kezdeményezésnek az alapját jelentő

[33] Ezzel kapcsolatban az államok felelős magatartására hívta fel a figyelmet Lété és Chase egyik írásukban 2018-ban. A Microsoft Digitális Genfi Konvencióján alapuló, és az olyan szervezetek mint például az EBESZ, az OECD vagy az ENSZ GGE (United Nations Group of Governmental Experts, UN GGE), valamint a magánszektor közreműködésével az országoknak olyan nemzetközi jogi szabályozás felé kell haladniuk, amelyek a kibertérben valóban alkalmazhatóak a támadások, illetve a hadviselés szabályozására. (Létél–Chase 2018)

nemzetközi együttműködés kialakítása és hatékony működtetése be kell, hogy kerüljön az egyes országok nemzeti kiberbiztonsági stratégiáinak legfontosabb célkitűzései közé.

A kiberfegyverek és azok esetleges nemzetközi szabályozásának szükségességére a 2010-es iráni atomlétesítmények elleni Stuxnet ügy[34] is felhívta a figyelmet. A Stuxnet elkészítése, annak stratégiai célpontjainak kijelölése, és maga a kibertámadás kivitelezése is állami támogatással történt. (Brown–Metcalf 2014) Ennek megfelelően az állami kibertámadás másik ország stratégiai célpontjai ellen már nem példa nélküli. Ezért a kiberhadviselés fentiekben bemutatott definíciós készlete ezzel a kiberfegyverrel, valamint az állami támogatás meglétével bizonyítást nyer.

Erre a bizonyításra számos más példát is fel tudunk mutatni. Ilyen a NoPetya zsarolóvírus[35] támadássorozata is 2017-ben. A NoPetya[36], ellentétben a néhány héttel korábban világszerte hatalmas károkat okozó WannaCry[37] vírussal, nem véletlenszerűen támadott meg számítógépeket, hanem célzott támadásokat hajtott végre – az elemzések eredményei szerint – alapvetően Ukrajnában lévő számítógépek ellen. A háttérben ebben az esetben is egy másik ország – nevezetesen Oroszország – jelölhető meg támogatóként. (Ivanov–Mamedov 2017, Kovács 2018a)

---

34 2010-ben Irán bushehri atomerőművének és natanzi urándúsító centrifugáinak ipari vezérlő szoftvereit – köztük a Siemens által gyártott PLC-ket (Programmable Logic Controller, azaz programozható logikai vezérlők) – amerikai és izraeli támogatással gyártott féreg-vírussal kompromittálták. A Stuxnet névre keresztelt malware kibertámadás kivitelezésével fizikai károkat okozott az urándúsító centrifugákban, így lassítva illetve akadályozva meg az iráni atomfegyverek előállítását. (Kovács–Sipos 2010, Kovács 2018a)

35 A zsarolóvírusok – angol terminológiából eredő szóhasználattal ransomware-ek – a megfertőzött számítógépre jutva titkosítják a felhasználó fájljait. A támadó a titkosítás feloldásáért gyakran nehezen lenyomozható kriptovalutában kér váltságdíjat cserébe.

36 2017 június végén a NoPetya (egyes híradásokban PetrWrap) nevű ransomware terjedése kezdődött meg Ukrajnában a MeDoc nevű, elsősorban Ukrajnában használt könyvelőszoftver automatikus frissítésével. Később a fertőzés több európai országra is kiterjedt. A vírus a Windows SMB (Server Message Block, szerver üzenet blokk) egyik sérülékenységét használta ki, és már e-mailek csatolmányaként is terjedt, amely a WannaCry esetében még nem volt jellemző. (Kovács 2018a)

37 2017 tavaszán egy WannaCry, illetve WanaCrypt0r 2.0 névre keresztelt zsarolóvírus és annak számos mutánsa több tízezer, később pedig százezer számítógépet fertőzött meg. A vírus terjedése és intenzitása hatalmas volt elsősorban az olyan vállalati környezetben, ahol nagyon sok számítógép volt a hálózaton belül. A WannaCry elsőként az olyan számítógépeket támadta, amelyeken létfontosságú, azonnali hozzáférést igényló adatok voltak, mint például a kórházak vagy egészségügyi intézmények. A vírus egy olyan Windows sérülékenységet használt ki, amelyet korábban az NSA (National Security Agency, Nemzetbiztonsági Ügynökség) fedezett fel, de az erről szóló adatokat az Ügynökségtől korábban ellopták. (Goodin 2017, Kovács 2018a)

Kritikus infrastruktúrák és kritikus információs infrastruktúrák támadhatósága

A kritikus infrastruktúrák és a kritikus információs infrastruktúrák szerepe, azok fontossága és a rendszerelemek egymástól való függősége korábban bemutatásra került. Mivel ezek a rendszerek a digitális korszakunk legfontosabb olyan összetevői, amelyek nélkül nem, vagy csak nehezen képzelhető el a mindennapi élet, ezek támadhatóságát – az esetleges támadások következményeinek a felbecslésével – szükségszerűen meg kell vizsgálnunk.

Ahogy a kritikus infrastruktúrák úgy a kritikus információs infrastruktúrák is ki vannak téve a fizikai veszélyeknek, így azok kezelése, illetve az azokra való felkészülés elengedhetetlenül fontos[38]. Mivel az infokommunikációs rendszerek is a fizikai térben kerülnek kiépítésre, így azok teljes vagy részleges fizikai sérülése a rendszerek leállásához és a szolgáltatások rövidebb-hosszabb ideig tartó kieséséhez vezet. Ez tehát az elsődleges veszélyforrás.[39]

Ugyanakkor ezeket az infrastruktúrákat nem csak fizikai, hanem kibertéri veszélyek is fenyegetik. Ez a második legfontosabb veszélyforrás kategória, mert a kibertér korábban többször is említett sajátosságai – például határtalanság, nyitottság, globalitás, szoftver és hardver sérülékenységek – miatt nem csak a globális és regionális, hanem nemzeti vagy akár alacsonyabb szintű kritikus infrastruktúrák esetében is támadhatóvá válnak[40].

Ahogy az iráni atomlétesítményekkel szemben alkalmazott Stuxnet féregvírus esete is bizonyítja, a kritikus infrastruktúrák támadása közvetett módon is lehetséges, ezeken belül

38 A kritikus infrastruktúrákkal kapcsolatban gyakran elhangzik az ellenállóképesség (angolul: resilience) kifejezés, amellyel a különböző – fizikai és/vagy kibertérből – érkező támadások elleni felkészültséget jellemezhetjük. Ugyanakkor ez a felkészültség nem csak a különböző veszélyek – például amelyek sok esetben természeti katasztrófák, hiszen eredetileg a kifejezés is az ezekkel kapcsolatos kritikus infrastruktúra védelem területéről származik –, illetve az azokkal szemben kialakított ellenállóképességet jelenti, hanem az esetlegesen bekövetkező károk után a helyreállítás és a normál működésbe való visszatérés képességét is magába foglalja.

39 2010-ben Digitális Mohács címmel egy olyan gondolatkísérletre alapozott forgatókönyvet készítettünk, amelyben Magyarország kritikus infrastruktúrái, valamint kritikus információs infrastruktúrái ellen elkövetett különböző támadási módszereket, illetve ezeknek a támadásoknak a lehetséges következményeit vázoltuk fel. A forgatókönyv alapján levonható legfontosabb megállapítás az volt, hogy a hazai kritikus infrastruktúrák esetében a fizikai támadások okoznák a legnagyobb rendszerkieséseket. (Kovács–Krasznay 2010)

40 A korábban említett Digitális Mohács forgatókönyv második részét 2016-ban a *Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint* címmel a kibertámadásokra, illetve azok kezelésére építettük fel. A forgatókönyvben négy – kibertámadásokat magába foglaló – fázist mutattunk be és azt vizsgáltuk, hogy ezekre a támadásokra az információbiztonsági szakemberek hogyan reagálnának. A szakértői válaszok alapján megállapítottuk, hogy *„a kritikus infrastruktúráinkkal, ezen belül is a kritikus információs infrastruktúráinkkal szemben fennálló függőségünk továbbra is megköveteli azok koordinált és centralizált védelmét."* (Kovács–Krasznay 2017)

is elsősorban a kritikus információs infrastruktúrák elleni kibertámadások azok, amelyek a legnagyobb mértékű és legnagyobb területre kiterjedő károkat okozhatják. (Kovács 2018a)

A kritikus infrastruktúrák legsúlyosabb sebezhetőségei okainak feltárása során arra a következtetésre kell jutnunk, hogy ezek a rendszerek, illetve a rendszerelemek rendkívül heterogén összetételűek. Ez a korábbi és a legújabb technológiát képviselő rendszerelemek – sok esetben kényszerűség szülte – egymással párhuzamos üzemeltetésében érhető tetten a leginkább. Erre az egyik legjobb példát a SCADA[41] (Supervisory Control and Data Acquisition, azaz felügyeleti, irányító és adatgyűjtő) rendszerek esetében találhatunk. A régi és az új rendszerelemek egymás melletti alkalmazása és napi szintű használata a kritikus infrastruktúrákon belül az energiaszektorban a leglátványosabb, hiszen *„az új technológia alkalmazása a költséghatékonyabb energiaelőállítás, -tárolás, és -szállítás esetében egyre inkább a fontos szempontok és a prioritások elején található."* (Kovács 2018a) A kritikus infrastruktúrákban – elsősorban azok vezérlésében – megjelenő IoT eszközök a veszélyeztetés oldaláról tovább növelik a rendszerek kitettségét, hiszen így méginkább igaz, hogy nem csak a korábbi, hanem az új technológia egyszerre van jelen az infrastruktúrákban és az új technológia a távoli elérést lehetővé tevő kapcsolatain keresztül támadhatóvá válik.

Mindezekre számos kutatás rávilágított. Ezek közül kiemelkedik az EU által támogatott szakértői csoport vizsgálata, amelynek hivatalos neve Energy Expert Cyber Security Platform (EECSP) Expert Group, azaz kiberbiztonság az energiaszektorban. A platform 2017-ben született jelentése szerint az energiaszektor analóg rendszereit hatalmas ütemben felváltó digitális rendszerek kommunikációs megoldásaikban és intelligens komponenseikben is új filozófiát jelentenek. Az új digitális mérőberendezések, digitális szelepek, szivattyúk és számos más eszköz távolról is elérhető és így sebezhető. (ECCS 2017, Kovács 2018b)

Az EECSP Expert Group az energiaszektorban tíz olyan területet azonosított, amelyekben komoly kiberbiztonsági kihívások vannak:

- a határokon átnyúló villamosenergia-átviteli hálózatok nem stabilak;
- a jelenlegi védelmi koncepciók nem mindegyike tartalmazza a kibertéri kihívásokat és azok kezelését;

[41] A SCADA-rendszerek egyik legfontosabb felhasználási területe az ipar. Ugyanakkor ezek a rendszerek sebezhetőek többek között azok decentralizáltsága, számtalan hálózati kapcsolata, valamint hosszú életciklusuk miatt. A korábban telepített SCADA-rendszerek még soros portokat is használnak az RTU-kommunikációhoz (Remote Terminal Unit vagy Remote Telemetry Unit, azaz távoli telemetria egység), de ezzel párhuzamosan már jelen vannak a digitális SCADA rendszerek is, amelyek esetében a veszélyt azok kompromittálhatósága, vagy az azokhoz történő jogosulatlan hozzáférés jelenti. (Kovács 2018a)

- az EU tagországok eltérő kiberbiztonsági gyakorlatot folytatnak;
- a villamosenergia-rendszer elleni kibertámadások kezelésére nincsenek teljes egészében kidolgozott szabályok;
- az említett új technológiák és szolgáltatások megjelenése, illetve azok régi rendszerek üzemeltetésével párhuzamos bevezetése;
- az alkalmazott eszközök és rendszerek integritása sok esetben hiányzik;
- számos helyen kiszervezik az infrastruktúrák üzemeltetését;
- kölcsönös és egyre növekvő függőség a piaci szereplők között;
- a valós idejű, igen kiélezett szolgáltatás és rendelkezésre állás, valamint a kiberbiztonsági intézkedések közötti ellentmondás. (ECCS 2017, Kovács 2018b)

Az energiaszektor, ezen belül is a villamosenergia alágazat elleni kibertámadásokra az egyik legmarkánsabb példa 2015 decemberében történt Ukrajnában. Az egyik ukrán regionális villamosenergia-elosztó és villamosenergia-átviteli vállalat rendszereiben üzemzavar keletkezett, amely a cég számítógépeibe és SCADA-rendszereibe történt illetéktelen behatolás következményeként állt elő. A szolgáltatáskiesések több mint három órán keresztül tartottak, miután a támadók több 110 kV-os és 35 kV-os alállomást kapcsoltak le. A támadás után indult vizsgálatok kiderítették, hogy a támadók az elosztóhálózat más számítógépeibe és más villamosenergia-vállalat rendszereibe is behatoltak. Ehhez rendkívül szofisztikált eszközöket – például az úgynevezett BlackEnergy[42] rosszindulatú szoftvert – és eljárásokat alkalmazva. A támadások következtében előállt villamosenergia-átviteli rendszer kiesése miatt 225 ezer fogyasztó nem jutott áramhoz. (SANS 2016)

A 2015-ös támadás 2016 decemberében megismétlődött. Ezekből a támadásokból levonható egyrészt az a következtetés, hogy azok volumene és kifinomultsága, valamint az elkövetés módja állami támogatásra utal. Egy másik következtetés, amelyre részben már utaltam korábban, az az, hogy állami támogatással elkövetett olyan támadások, mint a 2015-ös, vagy 2016-os ukrán energiaszektort ért támadás egyrészt hatalmas felderítő[43] munka

[42] A BlackEnergy-nek nevezett malware olyan trójai program, amelyet DDoS (Distributed Denial of Service, azaz elosztott túlterheléses) támadásokra, kiberkémkedésre, valamint olyan kibertámadásokra használnak, amelyek során a legfontosabb cél az elért információ megsemmisítése. Számos elemzés arra a következtetésre jutott, hogy a programot 2008-ban a Grúzia elleni DDoS-támadások során már bevetették. (Kaspersky 2016)

[43] Ez a felderítés nem csak célpontok – ebben az esetben az ukrán energiaszektor egyes technikai elemeinek feltérképezésére irányul –, hanem az energiaellátó vállalatok vezetői, mérnökei és fontos beosztásokat betöltő munkatársai vonatkozásában történő adatgyűjtést is jelent. (Kovács 2018a) Mindezek mellett működik a nyílt forrású felderítés is, amely során a SCADA és ICS (Industrial Control System, ipari irányítási rendszerek) gyártó vállalatok internetes publikációi a források. A SANS egyik

előzi meg (így ebben a vonatkozásban ez nagy hasonlóságot mutat a hagyományos katonai konfliktusokkal), másrészt a kibertérben megvalósuló elrettentést is demonstrálják ezek a képességek. (Takacs 2017)

1.5. Kiberbiztonság és kibervédelem stratégiai feladatai

A kiberbiztonság megvalósítása érdekében szükségesek mindazok technikai, szabályozási és humán eszközök, illetve képességek megléte, amelyek a digitális ökoszisztéma, benne az infokommunikációs eszközök és rendszerek alkalmazása és működtetése során, mint védelmi megoldások tevékenységek egész sorával járulnak hozzá a biztonság kialakításához és annak fenntartásához.

Ezek közül a védelmi mechanizmusok közül ezen a helyen elsősorban a stratégiai szintű tevékenységek közül emelek ki néhányat a teljesség igénye nélkül. Ennek oka az, hogy a későbbiekben megvizsgálni kívánt nemzeti biztonsági stratégiák esetében majd ezeknek a védelmi megoldásoknak a megjelenését elemzem, kitérve azok tartalmi elemeire is, valamint az, hogy a védelmi megoldás technikai jellegű feladatait – ahogy korábban is – nem tárgyalom, mert azok a stratégiai feladatokra csak marginális hatással vannak.

Felsorolás jelleggel a stratégiai kiberbiztonsági, illetve kibervédelmi feladatok[44]:

- stratégiai szintű információszerzés és felderítés a potenciális kiberveszélyek, illetve kibertámadások területére fókuszálva;
- korai előrejelzés jogszabályi és technikai feltételeinek kialakítása, a korai előrejelzés működtetése;
- kritikus infrastruktúrák és kritikus információs infrastruktúrák védelme;
- nemzetközi együttműködés a kibervédelem területén;
- kiberelrettentés.

elemzése bizonyította, hogy az ukrán villamosenergia-elosztó cégeknek szállított távoli elérést biztosító terminálok (Remote Terminal Unit, RTU) típusát és verziószámát a gyártó közzétette. Ezeknek az információknak a birtokában pedig a nyílt interneten olyan információk voltak fellelhetőek, amely ezeknek a rendszereknek a sérülékenységeit és kompromittálhatóságát írták le. (SANS 2016, ICS-CERT 2016, Kovács 2018a)

[44] Az itt felsorolt stratégiai szintű kibervédelmi feladatok alapvetően defenzív jellegűek. Az offenzív jellegű tevékenységekre azonban a védelem teljessé tétele érdekében szükség van. Ugyanakkor ezek a tevékenységek a kiberhadviselés fogalmi körébe illenek bele, ezért tárgyalásukat ott teszem meg.

Kiberfelderítés[45]

Olyan technikai és humán összetevőkről gyűjt információkat, amelyek egy kiberfenyegetettségi térképen ábrázolva jelenítik meg a kiber veszélyeket és ezekkel párhuzamosan a saját, nem utolsó sorban a potenciális támadó vagy szembenálló fél sérülékeny és támadható pontjait. A kiberfelderítés nem csak a technikai és humán, hanem a politikai, gazdasági és kulturális területekre is ki kell, hogy terjedjen. A potenciális támadások motivációinak feltérképezéséhez ezek a területek is szükségesek. A K+F tevékenységek korai szakaszától kezdve folytat technikai felderítést, valamint esetlegesen ezzel párhuzamosan a gyártás időszakában – akár a későbbi támadásokat is lehetővé tevő – hardver és szoftver elemek rejtett beépítését.[46]

A kiberfelderítést élesen külön kell választani a kiberkémkedéstől. A különbség a két tevékenység által megszerzett információk felhasználási céljában keresendő. A fentieknek megfelelően a kiberfelderítés alapvetően a kibertérben lévő, a potenciális támadások kivitelezésére alkalmas eszközökről (szoftverekről és hardverekről) és támadásra alkalmas módszerekről szerez információt, miközben feltérképezi azokat a feleket, akik ilyen eszközökkel támadásokat terveznek vagy szándékoznak megtenni. Ezzel szemben a kiberkémkedés számítógép-hálózatokba, illetve az azok számítógépeibe történő illetéktelen behatolást jelent, amely után a megszerzett és kiértékelt információkat politikai, gazdasági vagy egyéb – például katonai – célra használják. Amíg tehát a kiberkémkedés támadó, addig a kiberfelderítés védelmi jellegű tevékenységként értékelhető.

Korai előrejelzés a kibertérben

A kibertámadások elleni védekezés akkor lehetne igazán hatékony, ha azok bekövetkezése előtt már ismert lenne a támadás célpontja, a támadás kivitelezésének a technikája.

A támadások bekövetkezésekor az idő az egyik legfontosabb tényező, mert minél gyorsabban világossá válnak a célpontok (a támadások több célpontot is érhetnek, így fontos annak megállapítás, hogy azok sérülése, illetve esetleges kiesése milyen mértékben befolyásolja más rendszerek működését), illetve minél gyorsabban ki lehet értékelni a

[45] A kiberfelderítés itt leírt magyarázatát az angol terminológia threat intelligence, azaz veszélyfelderítés kifejezéssel egyenértékűként adom meg.

[46] Erre a fajta tevékenységre már szakmai terminológia is létezik: suply chain attack, azaz a beszállítói lánc támadása. Ebben a támadásban a beszállítói lánc kevésbe védett, illetve kevésbé biztonságos eleme lesz a célpont. 2016-ban az Apple esetében, illetve annak egyik beszállítójánál a SuperMicronál már történt ilyen eset. A SuperMicro az Apple számára szervereket szállított, amelyek firmware-jei rosszindulatú programokkal voltak fertőzöttek. (Gallagher 2017, Kovács 2018a)

támadás kivitelezésének technikáját – azaz milyen sérülékenységet használ ki, milyen kiterjedt maga a támadás – annál nagyobb eséllyel lehetséges más, hasonló sérülékenységekkel rendelkező rendszerek védelmét időben megvalósítani, és annál hatékonyabb lehet a támadás által okozott károk következményeinek a felszámolása.[47]

A támadások bekövetkezése esetén tehát a védekezés és a következmények csökkentése nagyban függ az időtényezőtől. Ezért hatékonyabb lehet a támadások megelőzésére fókuszálni, azaz a potenciálisan bekövetkező támadások felderítése és azok előrejelzése lehet a megoldás korai figyelmeztető és előrejelző rendszerek kialakításával. (Kovács 2018a)

A korai kiberelőrejelzés részben átfedést mutat a kiberfelderítéssel. A korai kiberelőrejelző rendszerek komplex rendszerek, amelyek működése és hatékonysága nagyban függ a különböző forrásokból származó adatok és információk összegyűjtésétől, feldolgozásától és azok elemzésétől. A potenciális támadásra utaló adatok és információk gyűjtése és feldolgozása automatizált rendszeren történik, amely a védendő IKT rendszerek különböző helyein olyan telepített szenzorokat – hardver és szoftver kivitelben egyaránt – tartalmaznak, amelyek folyamatos monitorozással többek között a hálózat anomáliáit jelzik. Ezek a szenzorok lehetnek akár a közigazgatás vagy akár az ipar IKT rendszereiben és hálózataiban. Ezek a korai előrejelző rendszerek akár mesterséges intelligencia-támogatással nem csak anomáliákat keresnek a hálózatban, hanem a korábbi támadások módszereinek elemzései során már rendelkezésre álló mintákkal hasonlítják össze a hálózat eseményeit. Összességében kijelenthető, hogy: *„[a] szenzoroktól származó adatok párhuzamos feldolgozása, azok összevetése a hálózati forgalom – például az abban megjelenő, a megszokottól eltérő jelek – elemzése eredményeként megjelenő információkkal a biztonsági központokban (Security Operation Center, SOC), illetve a központok munkatársainak elemzéseivel kiegészítve, grafikus megjelenítéssel társítva hozzájárulhatnak a potenciális támadások időbeni (előre)jelzéséhez."* (Kovács 2018b)

A korai előrejelző rendszerek esetében azonban – legyen szó akár az ipari folyamatokban lévő SCADA- és PLC-rendszerekről, akár a közigazgatás rendszereiről – elengedhetetlen, hogy maguk az alap folyamatok ne sérüljenek. Ennek érdekében a szenzorok adatai általában nem helyben, hanem emulálva kerülnek feldolgozásra. (Kovács 2018) Ugyanilyen fontos ezen rendszerek esetében az adatok biztonságos szállítása és kompromittálás elleni védelme, még abban az esetben is, ha nem minősített adat az, amely a szenzorokon keresztül az

[47] Ebben a munkában nyújtanak segítséget azok az ajánlások, amelyeket például az ENISA adott ki az elmúlt években az incidenskezelők számára. (Enisa 2017b, Kovács 2018a)

adatfeldolgozóhoz eljut. Ennek érdekében a korai előrejelző rendszerek alkalmazhatóságának jogszabályi kereteit is ki kell dolgozni.

Kiberelrettentés

Az elrettentés a hidegháborúban alapvetően a nukleáris elrettentő erőre épült. Ez filozófiáját tekintve meglehetősen egyszerű megoldás volt, hiszen a cél olyan nukleáris erő felmutatása volt, amely eltántorítja, elrettenti a szembenálló felet a támadástól, illetve az elsőként alkalmazott csapásméréstől. Ehhez az elrettentésre épülő stratégiához természetszerűleg a hagyományos fegyverekkel történő elrettentő erő is nagyban hozzájárult.

Az elrettentés, mint biztonságpolitikai módszer a 21. században ismét előkerült. Bár sokáig az a vélekedés uralkodott, hogy az elrettentés a kibertérre nem érvényesíthető, mégis ma már számos ország nemzeti biztonsági stratégiája és nemzeti kiberbiztonsági stratégiája is tartalmazza. Ezt az elrettentést a kibertérben megjelenő olyan erős védelem felépítésével, illetve olyan támadó képességek kialakításával kívánják elérni, amelyek eltántorítják a potenciális támadókat akcióiktól. Ehhez az elrettentéshez több filozófiai magyarázat társulhat. Egyrészt az elrettentés megnyilvánulhat abban, hogy olyan erős védelmet épít ki az egyik fél, amelyet csak nagyon magas anyagi és humán erő ráfordítással lehet sikeresen támadni, azaz a támadás költségei nem lesznek arányban az elérhető esetleges sikerrel, másrészt az elrettentés megnyilvánulhat abban is, hogy az egyik fél kinyilatkoztatja és megfelelően kommunikálja azt a szándékát, hogy egy esetleges kibertámadásra – akár a fizikai térben is – megfelelő válaszcsapásokkal fog reagálni. Ehhez kapcsolódhat az ilyen válaszcsapás-képességek felmutatása, akár a nemzeti biztonsági stratégiában, akár a nemzeti kiberbiztonsági stratégiában. (Burton 2018)

Az elrettentés az Egyesült Államok Védelmi Minisztériuma korábbi kiberstratégiájában így jelenik meg: *„[a] fokozódó fenyegetés, amellyel szembe nézünk, szükségessé teszi, hogy Védelmi Minisztérium hozzájáruljon egy átfogó kiberelrettentési stratégia kidolgozásához és végrehajtásához, annak érdekében, hogy megakadályozza a legfontosabb állami és nem állami szereplőket amerikai érdekek elleni kiber támadások elkövetésében."* (US DoD Cybersecurity Strategy 2015)

Lengyelország nemzeti biztonsági stratégiájába a kibertéri elrettentés a következőképpen került be: *„[a] kibertér a fegyveres küzdelem dimenziójává vált. Ezen a területen a Lengyel Köztársaság fegyveres erőinek rendelkezniük kell védelmi és támadó képességekkel annak érdekében, hogy a potenciális ellenfelek elrettentése megvalósítható legyen. Különösen*

készen kell állniuk – akár függetlenül, akár szövetségeseinkkel együttműködve – védelmi műveletek szélesebb körű megvalósítására kiberkonfliktus vagy kiberháború esetén." (Lengyelország 2014b)

Ezzel analóg módon a lengyel kiberbiztonsági stratégia a következőket tartalmazza: „*[a] hibrid természetű támadások mind gyakoribbá válása azt jelenti, hogy elengedhetetlen az elrettentés és a védelmi képességekbe való beruházás, amelybe beletartozik a kibertámadásokkal szembeni rugalmas, gyors és hatékony reagálási képességek kialakítása is."* (Lengyelország 2017b)

A kibertérre megfogalmazott elrettentés tehát több tényezőre épít. Egyrészt ez olyan kibervédelmi megoldások kialakítását jelenti az adott országban, amelyek áttörése nem, vagy csak komoly erőforrások mozgósításával lehetséges, másrészről olyan kibertámadó képességek kiépítését jelenti, amelyek egy adott ellenséges kibertámadás esetén a támadóval szembeni ellentámadást helyezik kilátásba. Önmagában a kiberbiztonsági stratégiában rögzített ilyen képességek nem elegendőek, mert azok akkor fognak csak valódi elrettentő erőt képviselni, ha azok valóban – bizonyítható módon – működnek is.

2. FEJEZET
A KIBERBIZTONSÁG STRATÉGIAI SZINTŰ MEGJELENÉSE

2.1. A nemzeti biztonság és a kiberbiztonság stratégiai összefüggései

A kiberbiztonság stratégiájának áttekintése előtt szükséges a stratégia jelentésének majd annak nemzeti biztonsággal való kontextusát és alkalmazását röviden felvázolni anélkül, hogy stratégiaelméleti kérdésekben állást foglalna jelen dolgozat.

A stratégia és a mögötte lévő a fogalom az ókori görög stratēgos kifejezésből származtatható, amely akkori jelentése a legfőbb katonai vezető volt. Ennek a jelentésnek megfelelően évszázadokig a katonai hadműveletek megtervezésének és a katonai csapatok tervszerű mozgatásának jellemzésére használták a stratégia kifejezést. (Kovács 2018b)

A katonai stratégia fejlődésével számos stratégiai elmélet született, amely közül Liddell Hart nagystratégia elméletét a következő idézettel tudjuk napjainkra is érvényesíteni: *„[a]míg a stratégia csupán a katonai győzelem kivívásának problémájával foglalkozik, a nagystratégiának kötelező messzebbre tekintenie: ennek problémája ugyanis a béke megnyerése."* (Liddell Hart 2002)

Azonban az idő előrehaladtával már nem csak a katonai terület, hanem a gazdaság, vagy a vállalatok vezetése és irányítása is felhasználta a stratégiát, illetve ezt a tevékenységet. Mindezt jól összefoglalja az államok közötti kapcsolatrendszerének, illetve az azok során feltárható biztonságpolitikai vonatkozások során kialakult elképzelések jellemzése: *„[m]odern értelmezésben a stratégia – már nem csupán a katonai szférához köthető, a katonai győzelem esélyének növelését célzó tevékenységek összességeként, hanem úgynevezett 'nagy stratégiaként' – az államok lehetőségeinek komplex alkalmazását jelenti a nemzetközi rendszerben."* (Csiki 2008, idézi: Kovács 2018b)

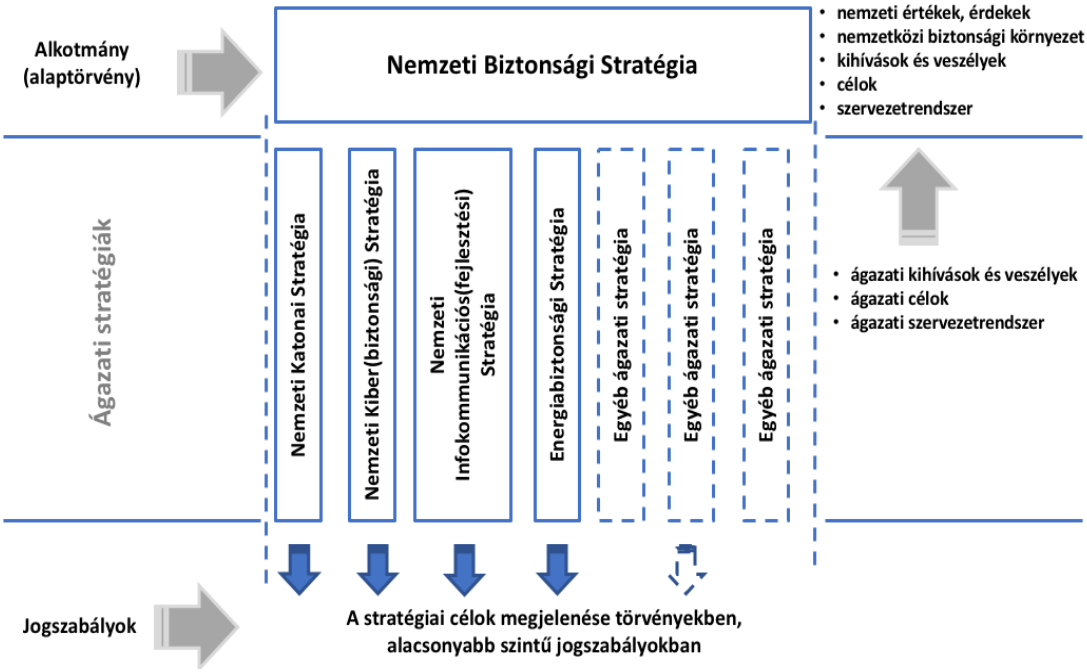
Ezt erősíti Yarger a 21. századi stratégiai elméletről írt „kis könyve"[48], amelyben a szerző a következőket állapítja meg a jó stratégiával kapcsolatban: *„[ez] megköveteli a stratégiát alkotó szakembertől, hogy lépjen ki a megszokott tervezési gondolkodásmódból, és alkalmazzon más megoldásokat is a stratégiai környezetre. Ez különösen igaz a nagy változások és a zűrzavar időszakában, amikor a sikeres katonai stratégiát harmonizálni kell a közigazgatási szervek más stratégiáihoz, hiszen ezek egymástól függenek."* (Yarger 2006)

[48] Utalás Yarger, az US War College professzora könyvének címére: *Stratégiai elmélet a 21. századra: egy kis könyv a nagy stratégiáról* (Strategic Theory for the 21st Century: The Little Book on Big Strategy).

Yarger a stratégiai környezetet olyan komplex rendszernek írja le, amely interaktív és adaptív, mert az államoknak és az egyéb szereplőknek megvannak azok a lehetőségeik, hogy egyénileg vagy közösen fellépjenek az új kihívásokkal szemben. (Yarger 2006)

Amennyiben napjaink stratégiai gondolkodást megvizsgáljuk, és ezt az állam biztonsággal való viszonyával kapcsolatban elemezzük, akkor a stratégiai dokumentumok mára viszonylagosan egységesen kialakult rendszerét találjuk meg. Ezeknek a dokumentumoknak az egymáshoz való viszonyában a legmagasabb szinten az adott állam érdekeinek és értékeinek a meghatározása jelenik meg. Ez leggyakrabban az adott ország alkotmányában (alaptörvényében) kerül rögzítésre, amely kiinduló pontját képezi az adott ország nemzeti biztonsági stratégiájának. Ebben rögzítésre kerülnek azok az elvek, amelyek alapján az adott ország érdekei és értékei, azok elérése, megvédése vagy biztosítása nemzetközi környezetben megvalósításra kell, hogy kerüljön.

Ennek megfelelően tehát a nemzeti biztonsági stratégiájában az adott ország megadja mindazon értékek és érdekek védelmének elérését biztosító elgondolásait, amelyeket az alkotmányban korábban meghatározásra kerültek. A stratégia erre építve tartalmazza az értékek és érdekek érvényesítését meghatározó biztonsági környezetet, felvázolva az abban meglévő és a jövőre előre jelezhető stratégiai szintű kihívásokat és veszélyeket. Ezeknek a veszélyeknek és kihívásoknak az elemzése és értékelése, majd az abból levonható következtetések alapján a stratégia megadja azokat a legfontosabb célokat, amelyek megfelelő válasz adnak a feltárt kihívásokra és veszélyekre. A stratégia ezekhez a célokhoz feladatokat és tevékenységeket rendel, valamint meghatározza a szükséges szervezeti, jogszabályi és anyagi erőforrásokat.



4. ábra
A stratégiai dokumentumok rendszere

Forrás: Kovács 2018b, szerkesztette*:* szerző

Nyilvánvalóan egy adott ország biztonsági stratégiai dokumentumai esetében *„az államközpontú nemzetközi rendszerben a politikai, gazdasági vagy katonai szövetségek szintén meghatároznak olyan – a biztonságukat kifejező – elveket, amelyek vizsgálata szükséges, hiszen sok esetben ezek a nemzetközi elvek visszahatnak és befolyásolják a nemzeti szintű dokumentumokat, illetve az abban foglaltakat."* (Kovács 2018b)

Az adott ország nemzeti biztonsági stratégiáját ágazati stratégiák[49] támogatják. Az ágazati stratégiákban az adott ágazatra vonatkoztatva jelennek meg a biztonság egyes elemei. Ennek megfelelően a nemzeti kiberbiztonsági stratégiában, mint az egyik ágazati stratégiában a kibertérre vetítve jelennek meg az adott ország kibertéri érdekei, valamint ezen érdekek védelméhez szükséges stratégiai célkitűzések. A nemzeti kiberbiztonsági stratégiának ennek megfelelően egyrészt vissza kell utalnia a nemzeti biztonsági stratégiában feltárt veszélyek és kihívások kezelésére, majd ezekkel párhuzamosan a kibertérben megjelenő kihívások kezelésére megfelelő válaszokat adva kell támogatnia a nemzeti biztonsági stratégiában megfogalmazott stratégiai célkitűzéseket.

[49] Ilyen ágazati stratégia például a nemzeti katonai stratégia, amely sok ország esetében már tartalmazza a kibertéri veszélyekre való katonai válaszokat, például az adott ország haderejének kiberműveleti felkészültségének emelésére tett célkitűzésekkel, de ilyen ágazati stratégia a nemzeti kiberbiztonsági stratégia, az energiabiztonsági stratégia, a gazdaságbiztonsági stratégia stb.

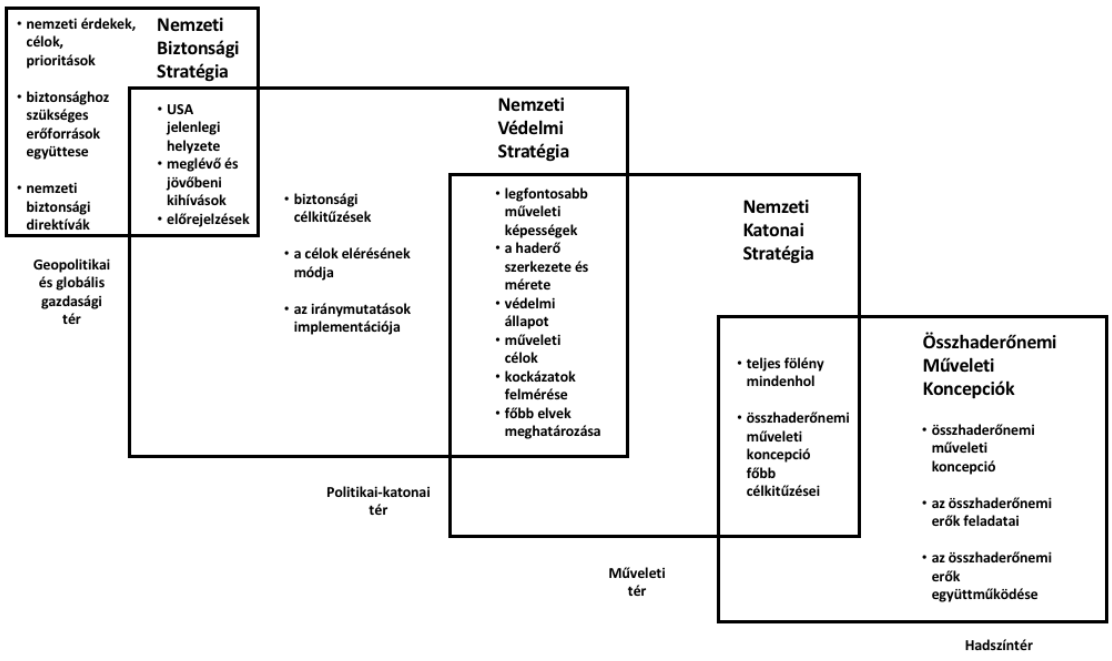
Az ágazati stratégiákban foglaltak végrehajtását – akár kötelező érvényűen elrendelő – különböző jogszabályokkal kell alátámasztani. Ennek érdekében törvényekben, vagy más, alacsonyabb szintű jogszabályokban, illetve egyes olyan esetekben, mint például a katonai terület, különböző doktrínákban kell rögzíteni a stratégiákban megfogalmazottak végrehajtásához szükséges folyamatokat, szervezeti hátteret, működési rendet.

2.2. Nagyhatalmak és a kibertér

2.2.1. Amerikai Egyesült Államok

Az Amerikai Egyesült Államok a világ egyik vezető hatalmaként a kiberteret érintő kérdésben is meghatározó szerepet tölt be. Az USA gazdasága nagyban támaszkodik a kibertérre, így ez a tényező meghatározza a kiberbiztonsággal kapcsolatos szabályozását és a különböző kibertéri tevékenységeit is.

Az USA stratégiai dokumentumainak rendszere kis mértékben eltér a korábban bemutatott stratégiai dokumentumok rendszerétől, amelyek összefüggéseit a következő ábra szemlélteti. Az ábrán látható, hogy az USA-ban a nemzeti biztonsági stratégia mellett megjelenik egy nemzeti védelmi stratégia is.



5. ábra
Az USA legfontosabb stratégiai dokumentumainak rendszere
Forrás: HSDL 2018, Kovács 2018b, szerkesztette: szerző

1997-ben az akkori elnök, Bill Clinton vezette adminisztráció átfogó módon vizsgálta meg az USA kritikus infrastruktúráinak helyzetét. Ez a vizsgálat számba vette az Egyesült Államok létfontosságú rendszereivel szemben megjelenő veszélyeket és kihívásokat. A vizsgálat kitért a kibertérre, kiemelve a kibertéri kapcsolatokkal rendelkező létfontosságú rendszerekre is. Már ekkor megjelent a köz- és magánszektor közötti együttműködés és információmegosztás, mint a védelem egyik elengedhetetlen eszköze. Az együttműködésben nagyon fontos tényező az információmegosztás, hiszen csak így biztosítható az érdekelt felek számára, hogy a sérülékenységeket felismerjék, és esetleges támadás során az infrastruktúrák egymásrautaltságából eredő kérdéseket kezelni tudják. A vizsgálat eredményeként született jelentés meghatározta a kritikus infrastruktúra egyes területein (szektoraiban) a védelem területén megvalósítandó legfontosabb teendőket. A jelentés külön kiemelte azokat a sérülékenységeket, illetve az azokat potenciálisan kihasználó fenyegetéseket és azok bekövetkezése esetén az esetleges következményeket, amelyek az infokommunikáció, a szállítás, az energia, a bank és pénzügy, valamint a közműszolgáltatások területén jelentkezhetnek. A jelentés ezen szektorok esetében külön javaslatokat is tett az adott szektor védelmének fokozására. (Critical Foundations 1997, Kovács 2018b)

Az említett 1997-es elnöki vizsgálat és 2012 között több, mint 10 stratégiai dokumentum és irányelv született az Egyesült Államok aktuális nemzeti biztonsági stratégiájának főbb célkitűzései kibertéri támogatására. (GAO 2013)

Ezekből a dokumentumokból önkényesen kiemelve a Barack Obama hivatalba lépése után elrendelt kiberbiztonsági felülvizsgálat eredményeit és megfogalmazott javaslatait, jól látszik, hogy a kibertér és annak fontossága exponenciálisan nőtt. A vizsgálat eredményeit és javaslatait összefoglaló jelentés többek között egy középtávú akciótervet is tartalmazott. Ebben olyan feladatok kerültek meghatározásra, mint egy erős, megfelelő kapacitásokkal és felhatalmazással bíró nemzeti kiberbiztonsági igazgatóság megalakítása. A javaslat alapján ez a szervezet a nemzeti kiberbiztonsági stratégia kidolgozását és végrehajtását volt hivatott koordinálni. A további akciótervek között szerepelt a kiberbiztonság elnöki prioritássá emelése, valamint egy kiberbiztonsági mérési rendszer kialakítása. Ezeken kívül az egyik leghangsúlyosabb feladat a köz- és magánszféra közötti együttműködés erősítése és a kiberbiztonság jogszabályi hátterének kialakítása, illetve az oktatás, képzés és ezeken keresztül a kiberbiztonsági tudatosság fejlesztése voltak. (DHS 2009, Kovács 2009b, Kovács 2018b)

Az USA nemzeti biztonsági stratégiája

Mielőtt az USA nemzeti kiberbiztonsága és annak stratégiai alapjai bemutatásra kerülnének szükséges az ország nemzeti biztonsági stratégiáját górcső alá venni, hiszen korábbi elemzéseimben bemutattam, hogy ez meghatározó jelentőségű egy adott ország kiberbiztonságának stratégiai alapjai vonatkozásában.

2017 decemberében jelent az az Egyesült Államok új nemzeti biztonsági stratégiája, amelyet Donald J. Trump jegyez. A stratégia négy fő fejezetben – a dokumentum szóhasználatával élve pillérekben – határozza meg az amerikai érdekek és értékek védelme miatt szükséges globális és/vagy regionálisan stratégiai célokat. A kibertér és annak védelme már az első pillérben *Az amerikai emberek, a szülőföld és az amerikai életmód* (*Pillar I.: Protect the American People, the Homeland, and the American Way of Life*) című részben megjelenik. Ebben a stratégia azokat a veszélyforrásokat veszi számba, amelyek közvetlenül vagy közvetett módon veszélyt jelentenek a megfogalmazott értékekre nézve. (White House 2017)

A kibertérben megjelenő általános veszélyek felsorolása mellett a stratégia meghatározza azokat a legfontosabb prioritásokat, amelyek szövetségi szinten feladatként is értelmezhetők:

- a kockázatok azonosítása és priorizálása, amelyen belül a kritikus infrastruktúrák területén történő kockázatok és veszélyek azonosítása során hat fő kritikus infrastruktúra területre kell koncentrálni: nemzetbiztonság, energiaszektor, banki és pénzügyi szektor, egészségügy, kommunikáció, valamint szállítás;
- védhető kormányzati hálózatok kiépítése: a szövetségi hálózatok fejlesztése és a modernizáció során a legújabb információtechnológiai megoldásokra, az elosztott szolgáltatásokra, a legjobb gyakorlatokra alapozott információtechnológia alkalmazások megvalósítására kell törekedni;
- a rosszindulatú kibertéri szereplők visszaszorítása: elsősorban a kritikus infrastruktúrák védelmére koncentrálva megfelelő hatósági jogkörökkel és megfelelő szaktudással, nemzetközi kapcsolatokkal rendelkező szervezetek létrehozása, amely mindezek alapján olyan elrettentéssel bír, hogy a potenciális támadókban kétséget ébresszen a kritikus infrastruktúrák támadhatósága;
- az információmegosztás erősítése: az információmegosztás sebességének növelése, és esetleg az abban lévő titkosítási szintek miatti információáramlás

nehézségeinek legyőzése a kritikus infrastruktúrák területén hozzá kell, hogy járuljon a kormányzati és magánszféra együttműködéséhez, így a védelemhez;

- réteges védelem kialakítása: a globálisan jelentkező fenyegetések, illetve azok a hálózatok minden rétegében való megjelenése miatt a védelmet is minden rétegben érvényesíteni kell, és ott kell kialakítani, ahol a veszélyek megjelennek, nem megengedve, hogy azok céljaikat elérjék. (White House 2017, Kovács 2018b)

A kibertéri veszélyeket bemutatva a stratégia az állami és nem állami szereplők által elkövetett rosszindulatú kibertámadások emelkedő számát és azok potenciális voltát emeli ki, amelyek ráadásul a világon bárhol, bárhonnan és bármely célpont ellen bekövetkezhetnek, és amelyek következményeként a kritikus infrastruktúrák működésükben sérülhetnek. Ez kihatással lehet a megtámadott ország gazdasági és politikai működésére, csakúgy, mint a globális demokratikus rendszerekbe vetett bizalomra is. Ezekkel a veszélyekkel kapcsolatban stratégia így fogalmaz: *„[s]zámos ország a kiberképességeket mások befolyásolására, míg néhányan az autokratikus rezsimek védelmére és azok kiterjesztésére használják. A számítógépes támadások a modern konfliktusok kulcsfontosságú elemévé váltak."* (White House 2017, idézi: Kovács 2018b)

A politikai és gazdasági befolyásolással[50] kapcsolatban a dokumentum utal arra, hogy néhány állam a hírszerzési információit mesterségesen gyártott és azokat többé-kevésbé valós információkkal vegyítve, információs fegyverként használja más országgal szemben: *„Amerika versenytársai az információt fegyverként használva értékeket és intézményeket támadnak úgy, hogy azok aláássák a szabad társadalmakat, miközben a támadók saját magukat a külső információk behatásai ellen felvértezik. A marketingtechnikákat kihasználva az egyéneket tevékenységük, érdekeik, véleményeik és értékeik alapján célozzák meg. Félretájékoztatást és propagandát terjesztenek."* (White House 2017, idézi: Kovács 2108b)

A stratégia nevesíti is ezeket az országokat: Kína és Oroszország. Kína esetében a kínai állampolgárok lojalitásának mérésére és az emberek totális ellenőrzésére, amíg Oroszország

[50] Ahogy korábban már utaltam rá a politikai befolyásolás a 2016-os amerikai elnökválasztási kampány során hatalmas visszhangot kapott. Az elemzések már a választási küzdelem alatt arra a következtetésre jutottak, hogy az orosz állam támogatásával különböző csoportok befolyásolták a választókat, és így a választások kimenetelét is. (Kovács–Krasznay 2017)

esetében az információs műveletek támadó eszközeként és módszereként utal a dokumentum a fentiekre. (White House 2017)

A kibertérben megjelenő kihívásokra és veszélyekre válaszul a kibervédelmi képességek fejlesztését határozza meg a stratégia, amely a következőket jelentheti:

- növelni kell annak a képességét, hogy a kibertámadások mögött álló személyek, csoportok vagy országok azonosíthatóak legyenek, hozzájárulva a gyors válaszreakciók kialakításához;
- növelni kell a kibervédelem eszközkészletét és szakmai hátterét: ezeket a konfliktusok széles területén javítani kell, azokat fel kell készíteni az Egyesült Államok kormányzati eszközeinek és az Egyesült Államok kritikus infrastruktúrájának védelmére, valamint meg kell teremteni az adatok és információk integritásának védelmét. Mindezen feladatokhoz szükséges olyan munkaerő alkalmazása, képzése, és nem utolsó sorban azok megtartása, akik képesek ezen feladatok teljes spektrumát ellátni;
- javítani kell a hatóságok és eljárások integrációját az Egyesült Államok kormányán belül, hogy a potenciális ellenfelekkel szembeni számítógépes műveleteket szükség szerint végre lehessen hajtani. Ez a kibertéri információszerzés és információmegosztás jogi hátterének átalakítását is igényli, amelyhez a Kongresszus támogatása szükséges. (White House 2017)

A stratégia világosan leszögezi, hogy az USA a nemzetközi jog keretein belül képzeli el a kibertérben megvalósuló folyamatokat, beleértve a védelem különböző akcióit is. Ezzel összefüggésben a dokumentum hangsúlyozza az ingyenes és a nyílt internet védelme megvalósításának fontosságát, amelyet az Egyesült Államok az olyan meghatározó nemzetközi szervezetekben való aktív részvétellel kíván elérni, mint például az ICANN (Internet Corporation for Assigned Names and Numbers), az IGF, vagy az ITU.

Az USA nemzeti védelmi stratégiája

Az Egyesült Államok legújabb nemzeti védelmi stratégiája 2018 év elején jelent meg. Az új stratégiát Jim Mattis[51] tábornok jegyzi, és talán részben ebből is következő módon a stratégia

[51] James (Jim) Mattis korábbi tengerészgyalogos tábornok volt az Obama adminisztráció idején a Központi Parancsnokság (Cantral Command) parancsnoka. Jelen stratégia készítése idején a Trump adminisztráció védelmi minisztere. Róla, illetve a stratégiáról nyilatkozta Joe Dunford tengerészgyalogos tábornok az Egyesített Vezérkari Főnökök Bizottságának főnöke: *„Biztosíthatom önöket, hogy az egyik olyan dolog, amely miatt teljesen biztos vagyok benne, hogy a Nemzeti Védelmi*

legfontosabb célja az USA versenyképes katonai előnyének helyreállítása annak felépítését, technikai eszközeit és alkalmazott eljárásait modernizálva. A legfontosabb cél mögött álló kiinduló kérdés *„megakadályozni Oroszországot és Kínát abban, hogy akár az Egyesült Államokat, akár szövetségeseit támadva megpróbálja felborítani a II. világháború óta fennálló nemzetközi rendet”* (Garamone 2018, idézi: Kovács 2018b), illetve ezzel az orosz és kínai haditechnikai potenciál olyan felülmúlása, amellyel kialakítható egy hatékony katonai elrettentés az irányukba. (Garamone 2018)

A stratégia elemzi a veszélyeket és kihívásokat, amely során a hagyományos négy hadviselési dimenzió mellé a kibertér is bekerül. (Department of Defense 2018a) Ennek megfelelően a veszélyforrások már a kibertérből jelentkező veszélyeket is tartalmazzák. Az egyik ilyen veszély, az az, hogy Egyesült Államok is célpontja lehet olyan támadásoknak, amelyek a dimenzió jellegéből adódóan bárhonnan bekövetkezhetnek. A 2019-2023 időszakra tervezett védelmi költségvetést a stratégia úgy határozza meg, hogy abban nagy szerepet kap a modernizáció.

A katonai vezetés információs rendszereinek (Command, Control, Communication, Computer, Intelligence, C4I) területén már korábban is fogalmaztak meg kritikákat – ezek közül például a Nemzeti Biztonsági Stratégia volt az egyik –, amelyek szerint azok korszerűsítése és kiberbiztonsági állóképességük fejlesztése nem várhat tovább[52]. (Department of Defense 2018a)

Mindezek alapján azt a következtetés lehet levonni az USA Nemzeti Védelmi Stratégiájából, hogy az abszolút módon előtérbe helyezi a hadsereg átalakítását, annak nagymértékű és gyors ütemű modernizációját. A stratégia az elrettentésre épül, és ebben hatalmas szerepet kap a technológiai fejlesztés, benne a kibertéri támadó és védelmi képességek kialakítása.

Stratégia pozitív hatással lesz tevékenységünkre, az az, hogy Mattis miniszter úr jegyzi azt, és ő ténylegesen elkötelezett abban, hogy az amerikai katonaságot egy olyan irányba vezesse, amely valóban támogatja ezt.” (Garamone 2018, idézi: Kovács 2018b)

52 Ezt támasztja alá az USA Elszámoltatási Hivatalának 2018 októberében publikált jelentése is. Ebben a dokumentumban összefoglaló módon kerül bemutatásra számos olyan probléma, amelyeket az USA 2012 és 2017 között gyártott különböző fegyverrendszereinek kibertámadásokkal szembeni védelmével kapcsolatban tapasztalt a hivatal. A célzott kibertámadásoknak kitett kiválasztott fegyverrendszerek közül volt olyan, amelyet néhány másodperc alatt sikerült kibertámadásokkal kompromittálni (azaz feltörni), és volt olyan is amelyből több száz gigabájt adatot sikerült ilyen módon kinyerni. (GAO 2018)

Az USA kiberbiztonsági stratégiája

Az Egyesült Államokban a 2000-es évek kezdete óta több mint 15 olyan stratégiai dokumentum – stratégia, elnöki rendelet, törvény, kezdeményezés stb. – látott napvilágot, amelyek a kiberbiztonsággal és/vagy a kritikus infrastruktúrák, illetve kritikus információs infrastruktúrák védelmével kapcsolatosak. Korábbi kutatásaim során ezeket a következő táblázatban foglaltam össze.

6. táblázat
Az Egyesült Államok kiberbiztonságra és kritikus infrastruktúrákra vonatkozó fontosabb stratégiái és törvényei 2000-2018[53]

Megjelenés éve	Eredeti cím	Cím
2000	National Plan for Information Systems	Nemzeti terv az információs rendszerekre
2003	The National Strategy to Secure Cyberspace	Nemzeti stratégia a kibertér biztonságának megteremtésére
2003	Homeland Security Presidential Directive-7	Elnöki rendelet a belbiztonságra
2008	Comprehensive National Cybersecurity Initiative	Átfogó kiberbiztonsági kezdeményezés
2009	National Infrastructure Protection Plan (update)	Nemzeti infrastruktúra védelmi terve (felülvizsgálat)
2009	Cyberspace Policy Review	Kibertéri politika felülvizsgálata
2011	International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World	Nemzetközi stratégia a kibertérhez. Jólét, biztonság és nyitottság egy hálózatos világban

[53] Az itt felsorolt stratégiai dokumentumokon és törvényeken kívül természetesen számos egyéb kiberbiztonságot erősítő rendelkezés született az Egyesült Államokban. Az egyik ilyen doktrinális szintű rendelkezés a hadseregé. A Kibertéri műveletek doktrínája (JP 3-12 Cyberspace Operations), amely átdolgozott és frissített kiadása 2018 júniusában jelent meg. (JP 3-12 2018) Egy másik fontos dokumentum az Egyesült Államok kibertéri incidenskezelését meghatározó elnöki politikai irányelv. Ez a PPD-41 direktíva 2016 júliusában jelent meg még Obama elnök aláírásával. Ebben a kiberincidenseket két kategóriára osztják fel: kiberincidensek és súlyos kiberincidensek. Ez utóbbiak kezelésére három szintű koordinációt határoz meg a direktíva: nemzeti politikai koordinációt (az elnök vezette Nemzetbiztonsági Tanács támogatásával); nemzeti műveleti koordináció, amely szövetségi ügynökségek koordinációját foglalja magába; valamint az operatív szintű koordináció. (PPD-41 2016)

2013	President's Executive Order on Drawing up a Strategy for Improving Critical Infrastructure Cybersecurity	Az elnöki rendelet a kritikus infrastruktúra kiberbiztonságának javítását célzó stratégia kidolgozásáról
2014	Draft Strategy for Improving Critical Infrastructure Cybersecurity	Stratégiai tervezet a kritikus infrastruktúra kiberbiztonságának fejlesztéséért
2014	Cybersecurity Enhancement Act of 2014	Kiberbiztonság növelése törvény
2014	National Cybersecurity Protection Act 2014	Nemzeti kiberbiztonsági törvény
2015	The Department of Defence Cyber Strategy	A Védelmi Minisztérium kiberstratégiája
2015	Cybersecurity Information Sharing Act of 2015	Törvény a kiberbiztonsági információmegosztásról
2015	Cybersecurity Act of 2015	Kiberbiztonsági törvény
2017	Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	Elnöki rendelet a szövetségi hálózatok és a kritikus infrastruktúrák kiberbiztonságának megerősítéséről
2018	The Department of Defence Cyber Strategy 2018	A Védelmi Minisztérium kiberstratégiája 2018
2018	National Cyber Strategy of the United States of America	Az Amerikai Egyesült Államok Nemzeti Kiberstratégiája

Forrás: Kovács 2018b, szerkesztette: szerző

Az Egyesült Államok kiberbiztonsági stratégiáinak sorában az egyik meghatározó dokumentum az USA Védelmi Minisztériumának (Department of Defense, DoD) kiberstratégiája (Department of Defense Cyber Strategy). Ennek legfrissebb kiadása 2018 szeptemberében jelent meg, de érdemes az előző – a 2015 áprilisában született – változatot

is megvizsgálni, hiszen az USA kiberbiztonságára és kibertéri tevékenységére meghatározó jelentőséggel bírt.

A stratégia arra a három – a DoD szempontjából – markáns területre épült, amelyek egyben a legfontosabb feladatokat is jelentették, nevezetesen a DoD hálózatainak, számítógépeinek és adatainak védelmét; az Egyesült Államok és annak érdekeinek védelmét a súlyos következményekkel járó kibertámadásokkal szemben; valamint a katonai műveletek kibertámogatását. (Department of Defense 2015)

A dokumentum öt stratégiai célkitűzést, valamint az ehhez szükséges akciókat határozott meg:

- a kibertéri műveletek végrehajtásához szükséges készenléti erők és képességek kialakítása, fenntartása: az ehhez szükséges humánerőforrás képzési, a technikai eszközök beszerzési és fejlesztési elképzeléseit a stratégia egy öt éves időintervallumban határozza meg;
- a védelmi minisztérium hálózatainak és adatainak védelme, valamint a műveletek során jelentkező kockázatok csökkentése: a stratégia kijelenti, hogy a védelmi minisztérium hálózatainak összessége túl nagy ahhoz, hogy azt teljes egészében és minden támadással szemben megvédjék, ezért priorizálni kell a legfontosabb védendő objektumokat és adatokat, valamint fel kell készülni az abban a helyzetben való folyamatos munkavégzésre és vezetésre, amikor egy-egy rendszert támadás ér és azok a támadások következményeként nem működnek;
- az Egyesült Államok legfontosabb érdekeinek védelme a kibertámadások és azok következményeivel szemben: olyan felderítő (hírszerzési), figyelmeztető, műveleti és együttműködési képességeket kell kiépíteni, amelyekkel még azelőtt lehetséges a potenciális támadásokról információkat szerezni, mielőtt azok az Egyesült Államokat vagy annak különböző érdekeltségeit elérnék;
- olyan kiberlehetőségek kiépítése és fenntartása, amelyekkel a különböző konfliktusok eszkalálódása megakadályozható, vagy azok bekövetkezése esetén a helyzet kezelhető: olyan kibertámadási képességeket kell kiépíteni, amelyekkel szükség esetén, a megfelelő elnöki felhatalmazás megléte esetén, az ellenséges szándékú támadók hálózataira, eszközeire és kibertéri képességeire hatás gyakorolható. Ezeket a saját oldali kibertámadásokat a kinetikus támadásokkal szinkronizált módon, a katonai műveletek teljes spektrumában kell tervezni;

- széles nemzetközi együttműködés és partnerség kialakítása, illetve fenntartása, amellyel megakadályozható a fenyegetések terjedése, és amelyek hozzájárulnak a nemzetközi biztonsághoz és stabilitáshoz: a stratégia hangsúlyozza, hogy azokon a területeken kell a partnerségre fókuszálni, ahol az Egyesült Államok nemzeti érdekei azt megkívánják. A dokumentumban meghatározott következő öt évben ezek az elsődleges területek a Közel-Kelet, Ázsia csendes-óceáni térsége, illetve a legfontosabb NATO szövetségesek. (Department of Defense 2015)

Fontos hangsúlyozni, hogy a dokumentum a stratégiai célok implementálására és azok végrehajtására konkrét és mérhető tevékenységeket határozott meg. Ezeket a stratégiai célokat támogató tevékenységeket korábban a következő publikált táblázatban foglaltam össze.

7. táblázat
Az Egyesült Államok Védelmi Minisztériumának kiberstratégiájának stratégiai céljai és az azokat támogató tevékenységek

Stratégiai cél	**A stratégiai célt támogató tevékenység**
I. A kibertéri készenléti erők/képességek kialakítása és fenntartása	• kibercsapatok felállítása: o képzés, felkészítés, oktatási infrastruktúra o karrierpálya kialakítása o Nemzeti Gárda bevonása o fokozott toborzás o csereprogram a magánszektorral o nemzeti kiberképzési program támogatása • a kiberműveletekhez szükséges technikai képességek kialakítása: o egységes platform kialakítása a kiberműveleti erők számára o gyorsabb kutatás-fejlesztés • pontosított vezetés a kiberműveletek során • kiberszimulációs és modellezési képességek növelése • a kiberműveleti erők értékelése
II. A védelmi minisztérium hálózatainak és adatainak védelme	• Egyesített Információs Környezet (Joint Information Environment, JIE) biztonságos architektúra létrehozása • az Egyesített Erők Központ Védelmi Minisztériumi információs hálózat védelme (Joint Force Headquarters for DoD Information Network, DoDIN) • az ismert sérülékenységek csökkentése

	• a Védelmi Minisztérium kibervédelmi erőinek értékelése • a Védelmi Minisztérium számítógép-hálózat védelmi szolgáltatója (DoD Computer Network Defense Service Provider, CNDSP) hatékonyságának növelése • terv a hálózatbiztonság és ellenállóképesség növelésére: o a kiber integrálása a műveleti biztonságba o a Kibervédelmi Csoport (Cyber Protection Team, CPT) képességeinek értékelése o a fegyverrendszerek kibervédelmének növelése • saját támadó erők (Red Team) hálózati védelmének növelése • a belső veszélyforrások csökkentése • a civil hatóságok támogatását célzó gyakorlatok levezetése • beszerzések során érvényesíthető kiberbiztonsági követelmények növelése • adatvesztések csökkentése a különböző katonai, hírszerzési szervezetekkel és civil hatóságokkal • elhárítás fejlesztése • a szellemi termékek eltulajdonítása elleni szabályozók kialakításának támogatása
III. Az Egyesült Államok legfontosabb érdekeinek védelme a kibertámadásokkal szemben	• a várható kibertámadásokkal kapcsolatos hírszerzési és figyelmeztetési képességek folyamatos fejlesztése • az USA kritikus infrastruktúráinak védelmében való közreműködés • automatikus információmegosztási eszközök kialakítása • a kiberelrettentés stratégiájának értékelése
IV. Kiberlehetőségek kiépítése és fenntartása a különböző konfliktusok kezelésére	• a kibertérben megjelenő lehetőségek beépítése a harctevékenységek műveleti tervezésébe
V. Széles nemzetközi együttműködés és partnerség kialakítása	• a legfontosabb régiókban partnerségi kapcsolatok kiépítése, erősítése • a rosszindulatú szoftverek és támadások megelőzésére szolgáló megoldások kidolgozása • a nemzetközi partnerekkel együtt történő kiberműveleti képzés és kiképzés • kiberegyüttműködési tárgyalások folytatása és erősítése Kínával

Forrás: Department of Defense 2015, Kovács 2018b, szerkesztette: szerző

A stratégia végrehajtását biztosító szervezetrendszerben kiemelt helyet kapott az Egyesült Államok Kiberparancsnoksága (United States Cyber Command, USCYCOM, vagy USCYBERCOM). A védelmi jellegű feladatok mellett a USCYBERCOM egyik legfontosabb feladata a szembenálló fél hálózati és egyéb kibertéri rendszerei elleni akciók végrehajtása akár a kibertéren kívül is: *„[a]z Egyesült Államok Cyber Command (USCYBERCOM) tevékenysége arra is irányulhat, hogy – adott esetben más amerikai kormányhivatalokkal együttműködve – kiberműveleteket hajtson végre más területeken fennálló stratégiai fenyegetések elrettentése vagy felszámolása érdekében."* (Department of Defense 2015, idézi: Kovács 2018b)

A kezdetben az Egyesült Államok Stratégiai Parancsnoksága (US Strategic Command, USSTRATCOM) alárendeltségében működő USCYBERCOM 2017 augusztus közepén önálló műveleti parancsnoksági státuszt kapott. A parancsnokság legfőbb küldetése önnön meghatározása szerint: *„[a] műveletek vezetése és a Védelmi Minisztérium hálózatainak védelme érdekében tervezi, koordinálja, integrálja és szinkronizálja és a különböző tevékenységeket, valamint előkészíti és elrendelés esetén vezeti a katonai kibertér teljes spektrumában a műveleteket annak érdekében, hogy azok minden területen megvalósulhassanak, és hogy biztosítsák az USA és a Szövetségesek cselekvési szabadságát a kibertérben, és megfosszák attól a szembenálló felet."* (Stratcom 2018, idézi: Kovács 2018b)

Az USCYBERCOM alárendeltségében találhatóak a haderőnemek kiberparancsnokságai, de a parancsokság mellett több, mint 130 kiberműveleti csoport (Cyber Mission Force, CMF) is működik. (Department of Defense 2015, Stratcom 2018)

Az USA kiberbiztonságának civil feladatainak ellátásában a Belbiztonsági Minisztérium (Department of Homeland Security, DHS) is részt vesz. Így részben a DHS felelős a kiberbűnözés elleni fellépésért, a kritikus infrastruktúrák védelméért, valamint a szövetségi hálózatok biztonságáért. (Department of Homeland Security 2018a)

Mindezek mellett a DHS alárendeltségében működik a Nemzeti Kiberbiztonsági és Kommunikáció Integrációs Központ (National Cybersecurity and Communications Integration Center, NCCIC). Ez a szervezet folyamatos működéssel, azaz napi 24 órában, heti 7 nap biztosítja szövetségi szinten az eseménykezelési és irányítási feladatokat, valamint kapcsolatot biztosít a szövetségi kormány, a hírszerző közösség és a kiberbűnözés elleni hatóságok között. Az NCCIC az állami- és magánszféra között információmegosztási feladatokat is betölt. Ennek során a sebezhetőségekre, incidensekre, biztonsági eseményekre, valamint azok elhárítására vagy bekövetkezésük esetén azok

következményeinek enyhítésére ad tanácsokat, információkat. Az NCCIC keretében kapott helyett az US-CERT (United States Computer Emergency Readiness Team, US-CERT) és az Ipari Irányító Rendszerek CERT-je (Industrial Control Systems Cyber Emergency Response Team, ICS-CERT), amely a kritikus infrastruktúra ágazatok és alágazatok kiberbiztonságáért felelős. (Department of Homeland Security 2018b, Kovács 2018b)

A Trump adminisztráció védelmi minisztériuma 2018 szeptemberében, közel három évvel a korábbi DoD kiberstratégia megjelenése után egy új stratégiával állt elő. A *Védelmi Minisztérium Kiberstratégia 2018* (Department of Defense Cyber Strategy 2018) című dokumentum teljes szövege nem, csak egy mindössze 10 oldalas összefoglaló érhető el nyílt forrásokból. (Department of Defense 2018b)

Az új stratégia rögtön a bevezetőjében hangsúlyozza, hogy Kína és Oroszország az USA stratégiai versenytársai a kibertérben. Mint ilyenek hosszútávú stratégiai veszélyt is jelentenek mind az Egyesült Államokra, mind szövetségesei számára. A dokumentum meg is nevezi ezeket a veszélyeket: Kína esetében ez az USA katonai erejének és gazdaságának gyengítése, amelyet Kína az amerikai közigazgatásból, illetve magánvállalatoktól ellopott adatokkal és információkkal igyekszik elérni. Oroszország esetében az olyan kiberalapú információs műveleteket sorolja ide a dokumentum, amelyek az amerikai demokratikus folyamatok befolyásolását célozzák. Ezek mellett a stratégia Észak-Koreát és Iránt is azok közé a stratégiai veszélyek közé sorolja, amelyekkel az országnak fenyegetésként számolnia kell. (Department of Defense 2018b)

A stratégia öt olyan célt sorol fel, amelyek stratégiai célokként is értelmezhetők. Ezek a következők:

- az amerikai hadsereg képességeinek fejlesztése a kibertérben zajló műveletek sikeres megvívásához;
- az amerikai hadsereg fejlesztése és megerősítése olyan kibertér-műveletek végrehajtásával, amelyek az USA katonai előnyéhez hozzájárulnak;
- az Egyesült Államok kritikus infrastruktúrájának védelme az olyan rosszindulatú kibertevékenységekkel szemben, amelyek önmagukban vagy egy támadássorozat részeként jelentős kibereseményt okoznának;
- a DoD információinak és rendszereinek védelme a rosszindulatú kibertevékenységek ellen, beleértve a DoD és a nem DoD tulajdonú hálózatokat is;

- a DoD kiberterületen történő együttműködésének kiterjesztése a közigazgatási szereplők, az ipari és nemzetközi partnerek felé. (Department of Defense 2018b)

Ezeket a célokat a korábbi kiberstratégiákban megfogalmazott célokkal összehasonlítva megállapíthatjuk, hogy kisebb súlypont eltolódásokat leszámítva igazi, generális változás nincs az új stratégiai irányban. Továbbra is az USA haderejének kibertérre is érvényes dominanciája a cél, amely kiterjed a civil, stratégiailag fontos infrastruktúrák védelmére, valamint az ehhez szükséges civil-katonai együttműködésekre. A nemzetközi biztonsági rendszerben az USA továbbra is Kínát és Oroszországot tekinti a legfontosabb olyan veszélyforrásoknak, amelyek az USA saját területén is képesek a kibertéren keresztüli támadások kivitelezésére, illetve komoly – akár politikai, akár gazdasági – károk okozására. Ugyanakkor a stratégiai célok közül az első kettő egyértelműen arra utal, hogy az USA az elrettentés politikáját kívánja a kibertérben is folytatni. Ez ebben az esetben azt jelenti, hogy a potenciális támadónak ne legyen érdeke kibertámadásokat végrehajtani az USA és annak információs rendszerei ellen, mert az egyrészt a védelem fejlettsége miatt nem lehet sikeres, másrészt akár a fizikai térben bekövetkező katonai válaszokat von maga után.

Az elrettentés politikájához járulhatnak hozzá közvetett módon Paul Nakasone tábornok, a USCYBERCOM 2018 májusában kinevezett új parancsokának[54] tanulmányában megfogalmazottak is, amely a *Kivívni és fenntartani a kibertéri fölényt* (Achieve and Maintain Cyberspace Superiority) címet kapta. Ebben az új parancsnok hangsúlyozza, hogy a kibertérben elérni kívánt fölénynek a katonai tevékenységek minden dimenziójában hozzá kell járulnia az ott elérendő sikerhez. A parancsoki szándék kifejezése során a tábornok a következőket jelenti ki: *„[a]z USCYBERCOM hozzájárul a nemzeti stratégiai elrettentéshez. Fel fogunk készülni, működtetjük* [erőinket] *és együttműködünk a harcoló parancsokokkal, szolgálatokkal, minisztériumokkal, szövetségeseinkkel, valamint az iparral, hogy az ellenséges kibertéri szereplőket tevékenységükben akadályozzunk és ellenük folyamatosan harcoljunk bárhol legyenek is."* (USCYBERCOM 2018)

A fenti DoD kiberstratégiával közel azonos időben jelent meg az USA nemzeti kiberstratégiája, amely az *Amerikai Egyesült Államok Nemzeti Kiberstratégiája* (National Cyber Strategy of the United States of America) címet viseli. A stratégia – hasonlóan a 2017 év végén megjelent nemzeti biztonsági stratégiához – úgynevezett pillérekre építve

[54] Az USCYBERCOM parancsnoka egyben a Nemzetbiztonsági Ügynökség (National Security Agency) vezetője is egyben.

határozza meg a legfontosabb stratégiai irányokat[55], természetesen a kibertérre vonatkoztatva. A stratégia első fejezete, amely címében is azonos az említett nemzeti biztonsági stratégia első fejezetének címével – *Az amerikai emberek, a szülőföld és az amerikai életmód* (*Pillar I.: Protect the American People, the Homeland, and the American Way of Life*) – a szövetségi hálózatok és információk védelmének fontosságát hangsúlyozza, amelyben a szövetségi kiberbiztonság centralizálása az egyik hangsúlyos elem. A fejezet a kiberbűnözés elleni fellépés mellett kitér a kritikus infrastruktúrák védelmére is, amelyben a feladatok és a felelősségi körök szövetségi szervezetek és ügynökségek közötti pontosabb meghatározásában, illetve ezek újraelosztásában nyilvánul meg. Nagyon előremutató feladatot is tartalmaz ez a rész, amelyben már jelen van a korábban nem teljes mértékben jellemző dinamizmus is. A stratégia kiemelt tevékenységként határozza meg, hogy az azonosított veszélyekhez alkalmazkodva kell megvalósítani a kritikus infrastruktúrák védelmét a magánszektorral történő együttműködés keretében. Ezek mellett olyan védelmi tevékenységeket kell végrehajtani, amelyek hét kulcsterületen – a nemzetbiztonság, az energiaszektor, a bankszektor, az egészségügy, az infokommunikációs szektor, valamint a közlekedés és szállítás – járulnak hozzá a kockázatok csökkentéséhez. (White House 2018)

A stratégia második fejezete – szintén a nemzeti biztonsági stratégia felépítése analógiáját követve, azonos fejezetcímmel –, amely *Az amerikai jólét növelése* (Promote American Prosperity) címet kapta a digitális gazdaság, az abba való befektetések ösztönzését és ezzel együtt az Egyesült Államok kiberbiztonsági területen megvalósuló humán és technikai képességeinek a fejlesztését tűzte ki célul. (White House 2018)

A dokumentum harmadik fejezete az állam erős fellépését tűzi ki fő célként az olyan küldő behatásokkal szemben, amelyek a kibertéren keresztül destabilizálni és gyengíteni kívánják az országot. Ennek érdekében a stratégia egyrészt a területre érvényes nemzetközi jogi szabályok és normák kialakításában, az azok betartásában, másrészt a kiberelrettentésben látja a megoldást. A stratégia az elrettentés érdekében egy nemzetközi kiberelrettentési kezdeményezést javasol, amelynek fő célja, hogy az USA a szövetségeseivel egy olyan nemzetközi koalíciót hozzon létre, amely részstratégiák kidolgozásával világosan jelzi a potenciális ellenségnek azt az erőt a kibertérben, amely annak rosszindulatú tevékenységtől való eltántorítását eredményezi. Ebben a kezdeményezésben, illetve az így létrejövő koalícióban az információmegosztás, a súlyos

[55] Ezeket az irányokat úgynevezett priorizált tevékenységekkel adja meg a stratégia.

kibertámadások elleni közös fellépés, valamint közös válasz intézkedések is helyet kaphatnak. (White House 2018)

A stratégia negyedik fejezete az amerikai befolyás és az amerikai vezető szerep növelését tűzte ki célul. Ennek érdekében a legfontosabbnak az internet szabadságának, nyitottságának, illetve annak biztonságos és megbízható működésének biztosítása, mert ezen keresztül biztosítható az amerikai befolyás és vezető szerep a világban. (White House 2018)

2.2.2. Kína

Zbigniew Brzezinski már az 1990-es évek közepén felhívta a figyelmet arra, hogy a világ egyik legnagyobb hatalma, és így az Egyesült Államok hatalmas vetélytársa az elkövetkező évezred küszöbére Kína lesz. (Brzezinski 1999, Kovács 2009a, Kovács 2018b)

Brzezinski előrejelzése a maga idejében nem váltott ki túl nagy visszhangot, de ma már Kína nem csak hogy elérte, de jócskán meg is haladta azt, amit a volt biztonságpolitikai főtanácsadó megjósolt. Kína a 21. század elejére politikai és gazdasági értelemben is globális nagyhatalommá vált. Mindezek mellett az ország katonai potenciálja is figyelemre méltó. (Heath–Gunness–Coope 2016) Olyan új kínai haditechnikai eszközök jelennek meg a hagyományos fegyverek területén is, amelyek alapvetően az információtechnológiára alapozva jöhettek létre. Kína a nagy ütemben fejleszti az információtechnológia iparát, amely a polgári felhasználás mellett annak egyre több katonai alkalmazásában is megfigyelhető. (Kovács 2018b)

Kína és a kibertér civil oldala

Az elmúlt két évtizedben a kínai gazdasági fejlődés egyik motorja az információtechnológia, és közvetett módon az internet volt. 2017-ben a kínai internetfelhasználók száma elérte a 740 millió fő, amely a világ teljes internethasználóinak közel a 20%-a, és a kínai információtechnológiai vállalatok világszintű technológiai fejlettsége sok esetben ezeket a cégeket a világ élmezőnyébe repítették.

Azonban ezek a tényezők számos kérdést is felvetettek Kínában. Az első kérdés az, hogy hogyan lehet akár valós időben ellenőrizni azt, hogy a kínai állampolgárok az internet segítségével milyen információkhoz jutnak hozzá (Raud 2016), a másik kérdés pedig Kína nemzetközi térben való stratégiai tevékenységének kérdése.

Az állampolgárok ellenőrzésének egyik megoldása a szabályozott internethozzáférés, amely többek között webes cenzúrát jelent. Ennek érdekében a kínai állampolgárok kínai

területről csak az úgynevezett Nagy Tűzfalon[56] keresztül érhetik el az internetet, illetve ezen keresztül használhatnak különböző alkalmazásokat. A rendszer számos technikai megoldással – például IP címek, HTTP, FTP, vagy POP3 protokollok blokkolásával –, valamint több ezer erre a célra kiképzett rendőr alkalmazásával felügyeli, hogy a kínai állampolgárok ne jussanak olyan politikailag[57], társadalmilag, vagy erkölcsileg káros tartalomhoz, mint például az 1989-es Tiananmen téri tüntetéssel kapcsolatos információk, a tajvani kormány hivatalos oldalaihoz, a Tibet függetlenségéhez kapcsolódó információkhoz vagy pornográf webes tartalmakhoz. (Kovács 2009a, Kovács 2018b)

Mindezek egyenes következménye, hogy a kínai társadalomban az internethasználók ma már csak a kínai központi hatalom által ellenőrzött infokommunikációs alkalmazásokat használják. Mivel Kínában nem elérhető a Facebook és ma már a Twitter sem, ezért a kínai emberek – beleértve a fiatalabb generációt is – nem ezeket a közösségi médiumokat, hanem ezek kínai alternatíváit használják. Így az egyik legnépszerűbb mobil alkalmazás a WeChat (pinjin: Wēixìn), amely egy azonnali üzenetküldő szolgáltatás, és amely egy közösségi média felületté nőtte ki magát az elmúlt években. A WeChat-hez hasonlóan hatalmas népszerűségnek örvend a Sina Weibo (pinjin: Hszinlang Vejpo), amely bár szintén komolyan cenzúrázott, de mégis a közel 300 millió felhasználója miatt nem csak a Twitter egyszerű kínai megfelelője, hanem a nagy tömegek számára történő felhívások és vélemények közzétételének egyik legalkalmasabb eszköze is egyben.

Ugyanakkor a cenzúrával, illetve magával a politikával kapcsolatban nagyon érdekes vélemények is napvilágot látnak, amelyek tükrözhetik az egyszerű kínai ember álláspontját. Ezekből kiderül, hogy a kínai állampolgárok jórészt még akkor sem használják a tiltott internetes alkalmazásokat, amikor azt megtehetnék – például amikor külföldön vannak –, vagy egyszerűen nem is érdekli őket a politika olyan szinten, amely a politikai tartalmakhoz, vagy a politikai hírekhez való hozzáférés szükségességét jelentené. (Yuan 2018)

---

[56] A Kínai Nagy Tűzfal, amely hivatalos nevén *Aranypajzs* (Jindun gongcheng) egy hardver és szoftver együttes, amelyet a kínai Közbiztonsági Minisztérium tart fent 2003 óta. Az Aranypajzs hivatalos kínai neve *Nemzeti Közbiztonsági Információs Technológia*. Emellett számos más biztonsági – „Arany" – rendszer is működik, mint például az *Aranyhíd*, amely gazdasági információs rendszer, az *Arany szokások*, amely a külföldi üzleteket felügyelő rendszer, vagy az *Aranyadó*, amely nevéből adódóan is az adózást felügyelő rendszer. (Kovács 2018b)

[57] Ilyen politikailag érzékeny terület az ujgur kisebbség aktivitása. 2009 nyarán Hszincsiang tartomány fővárosában, Urumcsiban kitört ujgur zavargások után az adott területen az internethozzáférés megszüntetése és a nemzetközi telefonvonalak lekapcsolása volt a kínai kormány egyik eszköze az információáramlás korlátozására és a további zavargások megakadályozására. Ez egyben válasz is volt arra, hogy a szeparatista Ujgur Világkongresszus vezetője Rebija Kadír az interneten szervezte és irányította a tüntetéseket. (Jacobs 2009, Kovács 2009, Kovács 2018b)

Ugyanakkor a fenti állampolgári magatartásnak az egyik oka lehet az is, hogy a Kína egy úgynevezett szociális kreditrendszer bevezetését tervezi. A 2014-ben napvilágot látott terv, amelynek egyes elemeit számos helyi közigazgatási egység már részben használja is, többek között az állampolgárok internetes tevékenységéről, mobil applikációiból gyűjtött és elemzett adatokra támaszkodva, számos más adatot – például banki és pénzügyi adatok, rendőrségi nyilvántartások, bírósági nyilvántartások – összehasonlítva egy állampolgári megbízhatósági listát, illetve rangsort készít. Ez alapján dönthető el, hogy az adott állampolgár kezdhet-e üzleti vállalkozást, vagy nyerhet-e felvételt állami munkakörbe, vagy egyáltalán jogosult-e utazni. (USCC 2017)

Kína kibertérrel kapcsolatos másik nagy dilemmája a nemzetközi térben való tevékenység, amely önmagában is két részre osztható. Az első része a kérdésnek, hogy az olyan nagy nemzetközi információtechnológiai vállalatokkal, mint például a Google, milyen legyen a kapcsolata, azaz milyen feltételekkel engedje kínai terültre ezeket a szolgáltatásokat. 2006-ban, a Google kínai változatának, a google.cn elindításakor[58] ez a keresőóriás részéről hatalmas kompromisszumokat jelentett, hiszen a cég arra a következtetésre jutott, hogy ha Kínában jelen akar lenni, akkor el kell fogadnia a kínai állam feltételeit. Andrew McLaughlin, a Google kormányzati kapcsolatokért felelős vezetője ezzel kapcsolatban akkor így nyilatkozott: „*[a] google.cn meg fog felelni a kínai törvényeknek és rendeleteknek. Abban a döntésben, hogy hogyan jelenünk meg a kínai, vagy bármely más piacon, szerepet kap annak az egyensúlynak a kialakítása, amely a kötelezettségvállalásaink, a felhasználók igényei, valamint a helyi követelményeknek való megfelelés területeit érintik.*" (Mills 2006, idézi: Kovács 2018b)

A másik nemzetközi teret érintő kérdés Kína részvétele az internet irányításában, valamint annak nemzetközi biztonsági szabályozása. Kína is támogatta 2013-ban az ENSZ egyik szakértői csoportjának jelentését, amely az államok kibertérben történő tevékenységének szabályozására az ENSZ Alapokmányát, valamint a hatályos nemzetközi jog alkalmazását szorgalmazta. (ENSZ 2013, Kovács 2018b)

Kína azonban először 2011-ben, majd kis kiegészítésekkel 2015-ben a Shanghaji Együttműködési Szervezeten (Shanghai Cooperation Organisation, SCO) keresztül,

[58] Természetesen nem meglepő, hogy ezek után nagyon erős kritikák érték a Google kínai tevékenységét, amely kritikák elsősorban az Egyesült Államokból érkeztek. Ezeknek is komoly hatása lehetett arra, hogy a keresőóriás 2010-ben felfüggesztette ezt a szolgáltatását Kínában. 2018-ban azonban a Google egy új Kínának szánt keresőmotor fejlesztésébe kezdett. A Dragonfly névre keresztelt projekt azonban szintén nagyon sok kritikát kapott a cégen belülről is, mert az már a projekt elején nyilvánvalóvá vált, hogy ez is egy komoly cenzúrát magába foglaló internetes felület lesz. (Gallagher 2018)

Oroszországgal,[59] valamint számos Közép-ázsiai országgal – például Kazahsztánnal, Kirgizisztánnal, Tádzsikisztánnal, Üzbegisztánnal – közösen az ENSZ közgyűléséhez egy saját információbiztonságra vonatkozó nemzetközi magatartási kódexet nyújtott be. (ENSZ 2015, idézi: Raud 2016) A benyújtott javaslatból két markáns következtetés vonható le:

- a kibertérben megjelenő felhasználók irányítását és ellenőrzését az államnak kell végeznie;
- a kibertér szuverenitása közvetlenül az adott ország, tehát ebben az esetben Kína szuverenitását is meghatározza. Így annak szabályozása nem lehetséges olyan külső szervezet, mint például az ICANN[60] (Internet Corporation for Assigned Names and Numbers), vagy külső jogrend alapján. (Kovács 2018b)

Ezeken kívül Kína szorgalmazza egy közös és integrált globális internetes irányítási rendszer kidolgozását, amely ellensúlyozná az USA jelenlegi dominanciáját a nemzetközi szervezetek vezetésében és a kibertér nemzetközi jogi meghatározásában. (Raud 2016)

Kína kibertéri tevékenységeit az Egyesül Államok Kongresszusa egyik bizottsága is folyamatosan figyelemmel kíséri. A bizottság 2017-es összefoglaló jelentésében az információ ellenőrzésével, a média befolyásolásával, valamint a kibertér egyéb tevékenységeivel kapcsolatban a következő megállapításra jutott: (USCC 2017)

- Kína jelenlegi információ ellenőrzési gyakorlata, valamint a kormány új média ellenőrzési terve jelentős (negatív) előrelépést jelentenek a hatósági cenzúra, az emberek megfigyelése, és a magánélet megsértése területeken;
- a kínai újságírók állami elnyomása ma már egyre inkább kiterjed a külföldi újságírókra és azok Kínában dolgozó munkatársaira. Ebből következően a politikailag érzékeny történések kivizsgálása egyre nehezebb minden újságíró számára. Mindezeken túl az amerikai médiavállalatokban történt kínai gazdasági befektetések hatására az addig független vállalatok esetében is jelentkezik az öncenzúra, amikor politikailag érzékeny kínai, vagy Kínával kapcsolatos ügyeket

[59] Ennek a magatartási kódexnek a betartása meglehetősen kérdéses Oroszország részéről, hiszen ahogy korábban utaltam rá Oroszország beavatkozott a 2016-as amerikai, illetve a 2017-es francia és német elnökválasztásokba. (Kovács–Krasznay 2017, Kovács 2018b)

[60] Az ICANN nonprofit közhasznú társaság, melynek tagjai a világ minden tájáról biztosítják az internet biztonságos, stabil és interoperábilis működését. A szervezet egyik legfontosabb feladata a fejleszteni az internet egyedi azonosítókkal kapcsolatos politikáját, valamint fenntartani a szabad versenyt az interneten. Az internet elnevezési rendszerének koordinációs szerepén keresztül fontos hatással van az internet bővítésére és fejlődésére, de mivel alapvetően amerikai dominancia uralkodik a szervezeten belül, ezért sok ország – köztük Kína és Oroszország is – kritikus a szervezettel kapcsolatban. (ICANN 2018, Kovács 2018b)

kellene bemutatni. Ezzel párhuzamosan a külföldi média irányába tett kínai befolyásoló műveletek miatt a nyugati média jelentős része már direkt kínai nyomásgyakorlás nélkül is öncenzúrát gyakorol a kínai ügyekben;

- Kína hivatalosan az *internet szuverenitás* fogalmát hangsúlyozza, ezzel igazolja, illetve gyakorlatilag legitimálja a szólásszabadság korlátozását az országban. Ugyanakkor kereskedelmi célok miatt Kína akadályozza az amerikai vállalatok a határokon átnyúló adatátvitelét, amely alapvető nézeteltérést okoz Washington és Peking között;
- a globális internetes kormányzásról, a kibertér normáiról és a kiberbiztonságról szóló nemzetközi tárgyalásokon való részvételében Peking arra törekszik, hogy biztosítsa a hálózatok és információk folyamatos ellenőrzését Kínában, valamint, hogy csökkentse más országok Kína számára kockázatokat jelentő megnyilvánulásait. Attól tartva, hogy a nemzetközi jogot más országok Kínával szemben felhasználják, Peking nem hajlandó megállapodni a nemzetközi jognak a kibertérrel kapcsolatos konkrét alkalmazásairól. (USCC 2017, Kovács 2018b)

Kína és a kibertér katonai oldala

Kínában a kibertér védelmével kapcsolatos publikációk a 2000-es évek legelején még majdhogynem kizárólag csak katonai folyóiratokban jelentek meg. A kibertér kifejezést sem használták a 2010-es évek közepéig olyan széles körben, mint a nyugati országok, ehelyett az információs jelző volt az általánosan elfogadott kifejezés a területre.

Sokan a modern kínai katonai gondolkodás és stratégia alapjának is tekintik azt az 1999 februárjában megjelent könyvet, amelynek angolra fordított címe *Unrestricted Warfare*[61] (magyarul: Korlátlan hadviselés). A Kínai Népi Felszabadítási Hadsereg kiadásában megjelent könyv szerzői Qiao Liang és Wang Xiangsui ezredesek.[62]

A könyv katona-szakmai alapossággal megírt hadtudományi átfogó elemzés a hadviselésről, amelyben az USA haderejének az elmúlt idők fegyveres küzdelmeiben és

[61] A könyv angol fordítását az amerikai FBIS (Foreign Broadcsat Information Service), a CIA külföldi információs szolgálata végezte el 2000 januárjában. A könyv több amerikai kiadást is megért, például Unrestricted Warfare: China's Masterplan to Destroy America, azaz Korlátlan hadviselés: Kína mesterterve Amerika elpusztítására címmel 2002-ben, amely már az Egyesült Államokat ért 2001. szeptember 11-i terrortámadások után született. (Kovács 2018b)

[62] Legalábbis az ő nevük került feltüntetésre a könyvön, de sok kutató ezt kétségbe vonja, és inkább azt feltételezi, hogy a hadsereg több tisztje – magasabb szintű politikai és katonai irányítás mellett – vett részt annak megírásában.

háborúiban alkalmazott stratégiája és a katonai vezetésének kritikai bemutatása kapja a fő hangsúlyt.

A kibertér (az angol fordításból eredően) az Öböl-háborúval kapcsolatban jelenik meg elsőként *A légi-szárazföldi csatán túl* című fejezetben: *„Douhet azon jóslata, hogy 'a levegőben lévő csatatér lesz a döntő', úgy tűnik, hogy elkésett megerősítést kapott. Mindazonáltal mindaz, ami a levegőben történt az Öböl felett, messze meghaladta ezt a gondolatot. Akár Kuvaitban, akár Irakban, a légi fölény kivívása érdekében egyetlen légi harc sem volt, hanem olyan integrált légi kampány jelent meg, amely összekapcsolta az összes harci műveletet, mint például a felderítést, a korai előrejelzést, a bombázásokat, a kommunikációt, az elektronikai támadásokat, a vezetés és irányítást stb., és magában foglalta a világűr és a kibertérben történő harcot, illetve azok megszállását is."* (Liang–Xiangsui 2002, idézi: Kovács 2018b)

A könyv még nem említi a konkrét kibertevékenységeket, de a kibertér fontossága és az ott folytatott műveletek sok helyen felmerülnek. Kína kibertérben folytatott műveletei pedig nem csak katonai céllal és nem csak katonai célpontok ellen irányuló műveleteket jelentettek már ebben az időben sem. Az is nagyon bizonytalan volt ekkor még, hogy ezeket a kibertéri műveleteket a kínai hadsereg hajtja-e végre. Azóta Kína esetében sokszor felmerül a gyanú, hogy: *„[a] Kínai Népköztársaság szándékosan, államilag támogatott projektet hajt végre a kutatás költségeinek megkerülésére, a kulturális hátrányok leküzdésére és így más nemzetek kreativitásának kihasználásával a történelem legnagyobb növekedésére tör."* (Hannas–Mulvenon–Puglisi, 2013, idézi: Munoz 2013)

Az Egyesült Államok Kongresszusa számára 2008 őszén készült jelentés azonban már utal arra, hogy már 2002-től kezdődően számos Kínának tulajdonítható informatikai behatolás sorozatot észleltek az USA-ban. Ezek az alapvetően kiberkémkedési akciók katonai, kormányzati és kormányközeli vállalatok hálózatait érintették[63]. (USCC 2008)

A Mandiant (ma már FireEye) információbiztonsági elemző cég 2006 és 2013 között közel 200 APT (Advanced Persistent Threat, azaz fejlett, folyamatosan fennálló) támadásra szakosodott csoportot azonosított, amelyek közül 20 volt Kínához köthető[64] valamilyen

[63] A legnagyobb kibertérben bekövetkezett, alapvetően kémkedési célú akció a Titan Rain (Titán Eső) nevet kapta. A 2000-ben kezdődött támadást, amely során kínai hackerek 20 tera bájtnyi adathoz fértek hozzá, csak 2003-ban fedezték fel. A támadás célpontjai között volt a NASA, a Lockheed Martin, és a Redstone Arsenal. Ugyanakkor még 2005-ben is voltak arra utaló nyomok, hogy kínai területről érkező hasonló hálózati behatolások történtek a SANS Institute, a Lockheed Martin, a Sandia National Laboratories vagy a Pentagon különböző rendszereibe. (Kovács 2009a)

[64] Ilyen Kínához köthető adatlopásre derült fény 2007 augusztusában Németországban. Ekkor több német kormányzati számítógépen is kínai kémprogramokat találtak. Az ügy azért is volt nagyon kínos, mert

formában, amelyek közül az egyik az APT1 nevet kapta[65]. (Fireeye 2017) A Mandiant megállapította, hogy az APT1 Sanghajhoz köthető a hivatalos kínai kormány által támogatott csoport. Elemzésükben cég azt az is kijelenti, hogy az APT1 mögött a Kínai Népi Felszabadítási Hadsereg (People's Liberation Army, PLA) Vezérkarának 2. Csoportfőnöksége alatt működő 61398 nevet viselő egysége áll. Erre a következtetésre az adott alapot, hogy megállapították: az APT1 és a 61398 egység Sanghajban ugyanabban a kerületben, ugyanabban az utcában, sőt ugyanabban az épületben találhatók. (Fireeye é.n.)

Ugyanakkor a kémkedési célú támadásoknál sokkal súlyosabb eset történt 2009-ben, amikor kínai (és vélhetően orosz) hackerek behatoltak az Egyesült Államok villamosenergia irányító rendszerébe. A támadók számos kritikus rendszerelemet elértek, de nem okoztak igazi kárt, azon kívül, hogy a rendszerek gyenge és sebezhető pontjait feltérképezték. Ezt követően 2013-ban, 2015-ben és 2017-ben is történtek ilyen, az egyik legfontosabb kritikus infrastruktúrát, illetve kritikus információs infrastruktúrát célzó támadások. Természetesen ezeknek a támadásoknak az esetében is igaz, hogy az elkövetők kilétének bizonyítása nagyon nehéz. A bizonyítás nehézségéhez még egy-egy belső munkatárs vagy egy, az adott rendszerben alkalmazott, de Kínában gyártott hardver és/vagy szoftver elem is hozzájárulhat. (Pagliery 2015, Kovács 2018b) Ugyanakkor az említett támadásokra közvetett bizonyíték lehet az Edward Snowden által kiszivárogtatott dokumentum. E szerint az NSA (National Security Agency, Nemzeti Biztonsági Ügynökség) már 2010-ben felfigyelt a kínai Kuangtun tartományban lévő, sencseni központú Huawei belső kommunikációjára. (Sanger–Perlroth 2014, idézi: Raud 2016) Az NSA megfigyelte a cég belső kommunikációját, hogy feltárja és bizonyítsa a Huawei és a Kínai Népi Felszabadítási Hadsereg közötti kapcsolatot. (Sanger–Perlroth 2014, idézi: Raud 2016)

A kínai probléma megoldása érdekében 2015 őszén Barack Obama amerikai és Hszi Csing-ping (pinjin: Xi Jinping) kínai elnök tárgyalásai eredményeként a kínai és az amerikai

az közvetlenül a német kancellár hivatalos kínai útja előtt került napvilágra. A Német Szövetségi Alkotmányvédelmi Hivatal egyik korábbi jelentésében ugyanakkor már utalt arra, hogy Németország kiemelt célpontja a kínai – elsősorban gazdasági – kémkedésnek. (Spiegel 2007, Kovács 2009a) A kormányzati rendszerekben felfedezett kémprogramok azonban újszerűek voltak, hiszen azt megelőzően elsősorban az ipari kémkedés és a szellemi tulajdon ellopása volt az elsődleges cél (amelyek csak Németország esetében több milliárd dollár kárt okoztak évente) nem pedig politikai információk megszerzése. (Spiegel 2013)

65 Az APT1 egyidejűleg több tucat szervezettől is képes volt adatokat lopni, ráadásul úgy, hogy miután az APT1 hozzáférést biztosított a megtámadott rendszerhez, ezt a hozzáférést több hónapon, vagy akár több évig is fenntartották. A Mandiant elemzése olyan célpontokat is feltárt, amelyek esetében majdnem 4 évig volt hozzáférése a támadóknak. (Fireeye é.n.)

fél is kötelezettséget vállalt arra, hogy nem támogatják a kibertérben elkövetett – a szellemi tulajdonra, a kereskedelmi titkokra vagy a bizalmas üzleti információkra – vonatkozó lopásokat. (Raud 2016, Kovács 2018b) Ezt követően számos elemzés rámutatott, hogy valóban csökkent az amerikai cégek elleni kibertámadások száma, bár ennek oka az is lehet, hogy elkövetések szofisztikáltabb, azaz nehezebben felderíthetővé váltak, vagy akár harmadik országon keresztül történnek. (Harold 2016, idézi: Raud 2016; Fireeye 2016, Kovács 2018b)

Kína és a kiberbiztonsági stratégia

Kína kiberbiztonsági stratégiája nem egy kézzelfogható, jól körülhatárolható és világos célokat megfogalmazó dokumentumra épül. Ahogy korábban bemutatásra került, a kiber, mint jelző is sokkal ritkábban használatos, mint azt az európai vagy az amerikai terminológiában megszokhattuk. Ennek oka abban keresendő, hogy Kína az információs tér és az információs társadalom kialakítása oldaláról közelíti meg a kérdést. Ennek megfelelően sem a kiber, sem a kibertér kifejezést nem használják olyan sűrűn és olyan széles körben, mint a nyugati országok, hiszen a kiberteret csak az információs tér egyik szegmensének tartják. (Raud 2016) A kibertér, mint kifejezés csak a 2017. június 1-el életbe lépett kínai kiberbiztonsági törvénnyel jelenik meg szélesebb körben.

Ebből következően korábban a kiberbiztonság is sok esetben az információs tér biztonságával kapcsolódott össze. Ráadásul, ahogy a kínai katonai kibertevékenységek esetében utaltam rá, nagyon nehéz élesen szétválasztani a közigazgatás (kormányzati) és a katonai tevékenységet[66] ezen a területen.

Mindezek alapján szükséges megvizsgálni, hogy mely jogszabályok, illetve stratégiák azok, amelyek a kiberbiztonságra hatással vannak Kínában.

Az első ilyen jogszabály Kína nemzetbiztonsági törvénye, hivatalos címén a *Kínai Népköztársaság Nemzetbiztonsági Törvénye*[67], amelyet 2015. július 1-jén fogadtak el. Ez

[66] Mindez annak tükrében válik könnyen érthetővé, ha megvizsgáljuk a Kínai Népi Felszabadítási Hadsereg Kínán belüli szerepét. A kínai hadsereg vezetése a Kínai Kommunista Párt Központi Katonai Bizottsága alá tartozik. Ennek elnöke a Kínai Kommunista Párt főtitkára (jelenleg Hszi Csing-ping), aki egyben a Kínai Népköztársaság elnöke és a KKP Politikai Bizottsága Állandó Bizottságának elnöke is. Rajta kívül a Katonai Bizottság két alelnökből és négy tagból áll. (MoD PRC 2018, Lindsay–Ming–Reveron 2015, Kovács 2018b)

[67] Ez a jogszabály másik két törvénnyel együtt meghatározó szerepet játszik Kína biztonságról alkotott elképzeléseiben. A másik két törvénnyel – a külföldi nem-kormányzati szervezetekről szóló törvény, valamint a terrorizmus elleni törvény – együtt ez a három törvény az elnök közvetlen irányítása alá tartozó Központi Biztonsági Ügynökség hatáskörét nagymértékben kiterjesztette, amely hatáskör a hadseregre is kiterjed. (Wong 2015, Kovács 2018b)

még a kibertérről nem rendelkezik ugyan, de törvény a 25. cikkelye[68] egy olyan hálózati és információbiztonsági rendszer kialakítását irányozza elő, amely célja: „ ... *a hálózat- és információbiztonság védelmét szolgáló kapacitás növelése; a hálózati és információs technológiák innovatív kutatásának, fejlesztésének és felhasználásának növelése; a biztonság alapvető technikáinak és kulcsfontosságú infrastruktúrájának kialakítása a hálózatokra és az információkra, az információs rendszerek fontos területeire, valamint az adatokra; a hálózatok kezelésének növelése, a jogellenes és bűncselekmények megakadályozása, megállítása és jogszerű megbüntetése olyan esetekben, mint a hálózati támadások, a számítógépes támadás és a jogellenes és káros információk terjesztése; a kibertér szuverenitása, a biztonság és a fejlesztési érdekek fenntartása.*" (MoD PRC 2015, China Law Translate 2015, Kovács 2018b)

Ebből két következtetést is le tudunk vonni. Az első: legfelsőbb politikai szinten is megtörtént annak felismerése, hogy a kínai gazdaság és társadalmi-politikai élet nagyban függ az információtechnológiától, a második: Kína mind a külső, mind a belső információáramlást az eddiginél is erőteljesebb módon az ellenőrzése alatt akarja tartani.

Hivatalos kiberbiztonsági stratégia hiányában számos elemző Kína kiberteret érintő stratégiai gondolkodásának hátterében az úgynevezett 27-es Dokumentumot látja meghatározónak. Ennek a dokumentumnak az előzményei 2001-ig nyúlnak vissza, amikor az akkori Állami Információs-fejlesztési Vezető Csoport[69] Kína nemzeti információtechnológiai tervét kidolgozta.

Az Állami Információs-fejlesztési Vezető Csoport[70] egyik munkacsoportja az Állami Hálózati és Információbiztonsági Koordinációs Munkacsoport adta ki 2003-ban az úgynevezett 27-es Dokumentumot. Ez a dokumentum az információtechnológiai terület

---

68 A törvény kínai Védelmi Minisztérium hivatalos honlapján elérhető angol nyelvű változata csak az első 24 cikkelyt tartalmazza, de a nem hivatalos fordítást nyújtó China Law Translate elérhetővé tette a törvény teljes szövegét. Természetesen ennek megbízhatósága bizalmi elven alapul. (China Law Translate 2015)

69 Az erős centralizált vezetést Kínában a Kínai Kommunista Párt (KKP) gyakorolja, amelyen belül is központosított a hatalom. A KKP központi szervezetei közül az egyik legfontosabb plénum a pártkongresszus. Ez alatt található a Központi Bizottság (KB), de a valódi hatalmat a KB Politikai Bizottságának 4-7 főből álló úgynevezett Állandó Bizottsága gyakorolja. (Lindsay–Ming–Reveron 2015, Kovács 2018b) Mindezeken túl a különböző vezetési szinteken úgynevezett vezető csoportok találhatók, amelyek kislétszámú, szakértői csoportok szakmai támogatói munkát végezve. (Miller é.n., Kovács 2018b)

70 2014-ben Hszi Csing-ping elnök újjászervezte a vezető csoportokat, így a kiberbiztonság területére, illetve az azzal kapcsolatos kidolgozó munkára is egy új vezető csoport jött létre. Ugyanakkor 2014 előtt az Állami Információs-fejlesztési Vezető csoport és az Államtanács Információs Irodája voltak a terület fő felelősei. (Lindsay–Ming–Reveron 2015)

biztonságának meghatározó irányelveit tartalmazta. A dokumentumban meghatározott irányelvek között számos előremutató is volt, többek között egy többszintű védelmi séma kialakítására, a kriptográfiára, az információbiztonság monitoring rendszerére, a kritikus infrastruktúrák védelmére, a terület terminológiájára, illetve a kutatás-fejlesztésre vonatkozó konkrét feladatokkal együttese jelent meg. (Lindsay–Ming–Reveron 2015, Kovács 2018b)

Ezt követően a 27-es Dokumentum főbb irányelvei 2007 és 2010 között részletesen is kidolgozásra kerültek, de már az eredeti munkacsoport kevesebbet szerepelt ebben a munkában. Az egyes területek kidolgozásában a kínai hadsereg is meghatározó szerepet kapott, hiszen a kínai hadsereg a rádióelektronikai felderítés (Signals Intelligence – SIGINT) és az elektronikai hadviselés mellett a korábban bemutatott akciókkal és tevékenységekkel hangsúlyosan jelen van a kibertérben[71]. (Lindsay–Ming–Reveron 2015)

Hszi Csing-ping megjelenése és hatalomra kerülése azonban egy újfajta politikát is jelentett Kína számára, amely új irány a kibertérrel kapcsolatban is igaz. Ezzel kapcsolatban olyan nagyratörő tervet tartamaz az új politika, amely a technológiai fölény kivívásától – amelyben például helyet kap az a nagyon ambiciózus terv, miszerint 2030-ra Kína váljon a mesterséges intelligencia kutatások és alkalmazások vezető hatalmává – egészen az állampolgárok teljes digitális kontrolljáig terjed.[72] (Larson 2018)

Ebben a politikában fontos szerepet kap a már említett szociális kreditrendszer, valamint a 2016-ban megjelent kínai információbiztonsági törvény. A törvény 2017-es hatálybalépése számos területen kihatással van a kibertérre és annak biztonságára:

- személyes adatok védelme: meghatározza – az említett szociális kreditrendszernek megfelelően –, hogy milyen adatok gyűjthetők az állampolgárokról, illetve azok tevékenységeiről;

---

71 A kínai hadsereg vezérkara 3. csoportfőnöksége a felderítésért, a 4. az elektronikai hadviselésért felelős. Mindezek túl a kínai hadsereg felépítése katonai körzetekre osztott (alapvetően területi alapon, de az alól például néhány katonai felsőoktatási intézmény kivétel, amelyek szintén katonai kerületi szintű besorolásúak) és körzetenként vannak felderítő főnökségek. Emellett a kínai hadsereg számos egyetemet, illetve az ott folyó kutatás-fejlesztési tevékenységeket is támogat. Mivel az egyetemek feltételezhetően szoros kapcsolatokat ápolnak az úgynevezett, önkéntes alapon szerveződő kibermilíciákkal, amelyek civil hackerekből álló szervezetek, így azt a következtetést is levonhatjuk, hogy akár külföldi célpontok ellen is lehetőség van ezeknek a szervezeteknek a tudását és képességeit felhasználni. (Kovács 2018b)

72 Ezt támasztják alá azok a már korábban említett hírek is, amelyek a Google és a kínai hatóságok közös fejlesztésű – alapvetően Kínának szánt – keresőmotorjáról érkeznek. A Dragonfly munkanévre keresztelt internetes kereső folyamatosan frissülő adatbázisban rögzíti azokat a kulcsszavakat és azokat az URL vagy webcímeket, amelyeket a kínai hatóságok cenzúra alá vettek és amelyek a Weibo, azaz a legnépszerűbb kínai keresőóriás esetében már eleve blokkoltak. E mellett a szolgáltatás használatához telefonszámos regisztrációt írna elő a kormány, amely szintén az állampolgárok ellenőrizhetőségét szolgálná. (Gallagher 2018)

- kritikus információs infrastruktúrák védelmére;
- a szolgáltatók feladataira és felelősségére;
- az érzékeny adatok megőrzésére: a kritikus infrastruktúrák adatait hazai (kínai) területen kell tárolni, amennyiben például üzleti vagy üzemeltetési okok miatt más országokban keletkezik ilyen adat, azt a kínai hatóságoknak át kell adni;
- a törvény előírásainak be nem tartása miatt büntetéseket – például az adott vállalkozás megszüntetését – explicit módon tartalmazza. (Cheng 2016, KPMG 2017)

A törvény a kínai kritikus infrastruktúrákat érő esetleges külföldi támadásokkal kapcsolatban egy nagyon érdekes kitételt tartalmaz: *„[ha] a külföldi intézmények, szervezetek vagy magánszemélyek a Kínai Népköztársaság kritikus információs infrastruktúráját veszélyeztető támadásokat hajtanak végre, vagy azokba károkat okozó beavatkozásokat, vagy azok ellen egyéb olyan tevékenységeket folytatnak, amelyek súlyos következményekkel járnak, akkor ellenük a törvényeknek megfelelően kell eljárni; a Közbiztonsági Minisztérium az Államtanács és az illetékes szervezeti egységek úgy is dönthetnek, hogy befagyasztják azok eszközeit, vagy más szükséges büntető intézkedéseket hoznak ellenük."* [Kína kiberbiztonsági törvénye 75. cikk] Bár a törvény nem nevesíti, hogy egy ilyen támadás, vagy károkozás milyen egyéb büntető intézkedést is jelent, de a fentiekből nem nehéz arra a következtetésre jutnunk, hogy ezek akár ellentámadást is jelenthetnek.

2.2.3. Oroszország

Oroszország kibertérhez való viszonya sokban hasonlít Kínáéhoz. Az orosz terminológiában is sokkal inkább információs, semmint kibertéri műveleteknek tekintik azokat az akciókat, amelyek többek között a médiaeszközökkel történő befolyásolást, vagy az elektromágneses spektrum katonai célú felhasználását jelentik. Ezt támasztja alá az amerikai Haditengerészeti Elemzési Központ (Center for Naval Analyses, CNA) egyik tanulmánya[73] is: *„[a]z orosz katonai teoretikusok általában nem használják a kiber vagy kiberhadviselés kifejezést.*

[73] Meg kell jegyezni, hogy az idézett amerikai tanulmány fogalmi meghatározása is eltér a NATO hivatalos terminológiai és fogalmi meghatározásától. Az információs műveletek NATO szerinti értelmezése alapján abba beletartozik a számítógép-hálózati műveletek, az elektronikai hadviselés és a pszichológiai műveletek is. Ez azonban mégis nagyon jól rávilágít arra, hogy az orosz gondolkodás magának az információnak eszközként, akár fegyverként való alkalmazását helyezi előtérbe, és nem a kibertér és annak folyamatainak meghatározását. (Kovács 2018b)

Ehelyett a kiberműveletek fogalmát az információs hadviselés szélesebb keretén belül, egy holisztikus koncepcióval fogalmazzák meg, amely magába foglalja a számítógép-hálózati műveleteket, az elektronikai hadviselést, a pszichológiai műveleteket és az információs műveleteket." (Connell–Vogler 2017, idézi: Kovács 2018b)

A fenti idézetben foglaltakra az egyik legjobb példa az, hogy Oroszország az elektronikai hadviselési képességei fejlesztése terén hatalmasat lépett előre a közelmúltban. Az így megvalósított eszközök és rendszerek az ukrajnai, majd a szíriai háborúban alkalmazásra is kerültek. Az ezekben a konfliktusokban alkalmazott új haditechnikai eszközökből, valamint az ezekkel vívott fegyveres küzdelmet jellemző eljárásmódokból számos, akár hosszútávra is érvényes következtetést tudunk levonni: „*...az orosz fél komoly fejlesztéseket hajtott végre a fegyveres erejének modernizációja terén, amely során az elektronikai hadviselési képességek is hatalmas fejlődést mutatnak. Az orosz hadsereg megtartotta, sőt fejlesztette a hagyományos elektronikai hadviselési erőit, ezen belül kiemelt figyelmet fordítottak a rádiózavaró, navigációs zavaró, illetve egyéb szárazföldi elektronikai eszközök, valamint rádiólokációs zavaró képességeik fejlesztésére*." (Kovács 2017)

Ebből levonható az a következtetés, hogy a rövidtávú célok vezérelte K+F tevékenység helyett a hosszútávú, a politikai, a stratégiai, és a katonai irányokat is szem előtt tartó képességek kialakítása lehet csak a sikeres a jövőben. A kibertérre kivetítve ez pedig a kiberhadviselés korábban már röviden elemzett elméletéhez, az abban alkalmazható kiberfegyverek kifejlesztéséhez, valamint a kiberelrettentéshez vezet. (Kovács 2018b)

Oroszország tevékenysége a kibertérben

Oroszország kibertérben lévő akcióit és azok mozgatórugóit jól jellemzi James R. Clapper az USA volt nemzeti hírszerzési igazgatójának egyik szenátusi meghallgatásán tett nyilatkozata 2016-ban: „*Oroszország esetében egyre inkább növekvő kibertéri jelenlét feltételezhető abból kiindulva, hogy készek a kritikus infrastruktúrákat támadni, illetve kiberkémkedési műveleteket folytatni, még akkor is, ha észlelték őket, vagy ha nagyobb nyilvános ellenőrzés alatt állnak. Az orosz kiberműveletek valószínűleg az USA érdekeltségeit célozzák a stratégiai céljaik elérésének támogatására. Információgyűjtést folytatnak az orosz döntéshozatal támogatása érdekében az ukrán és a szíriai válságok során, a katonai és politikai célkitűzések támogatására pedig befolyásolást végeznek, valamint a kiberkörnyezetet folyamatosan készítik elő a jövőbeni tevékenységekre.*" (Clapper 2016, idézi: Connell–Vogler 2017 és Kovács 2018b)

Az idézet megállapításait számos elemzés is alátámasztja. Az egyik ilyen, amely 2014-ben készült, a már többször hivatkozott FireEye nevű kiberbiztonsági cég vizsgálata, amely során egy Oroszországhoz köthető, célzott támadásokra szakosodott csoportot azonosítottak be,[74] amely később több nevet is – például APT28, vagy Fancy Bear – kapott. (Fireeye 2014)

A FireEye említett jelentésének címe *APT28: egy ablak Oroszország kiberkémkedési műveleteire?* egyben utal annak céljára is: „*[a]kárcsak az APT1-ről szóló jelentésben, itt is fel kellett ismernünk, hogy egyetlen entitás sok év alatt sem értette meg teljesen a kiberkémkedés teljes és összetett képét. Ezért ezen jelentés közreadásával célunk az, hogy értékelést nyújtsunk, tájékoztassuk és felhívjuk a közösség figyelmét az Oroszországból származó támadásokra*." (Fireeye 2014, idézi: Kovács 2018b)

A Fireeye elemzései azt is jól mutatják, hogy az APT28 geopolitikai alapon három nagy csoportra osztotta fel célpontjait: a Kaukázus, ezen belül is elsősorban Grúzia; Kelet-Európa, amely térségen belül a kelet-európai kormányzatok, kormányzati szervezetek és hadseregek, valamint az olyan biztonsági vagy katonai szervezetek, mint az EBESZ és a NATO voltak a célpontok. Ugyanakkor a csoport más régiókban is hajtott végre akciókat. Így 2016-ban az Egyesült Államokban az amerikai elnökválasztás során, de Norvégia, Irak vagy éppen Jordánia is ezek között szerepelt. (Fireeye 2014, idézi: Kovács 2018b)

Az APT28 2016-os amerikai elnökválasztással kapcsolatos akcióit elemezve korábban azt a megállapítást tettünk, hogy a csoport valószínűleg az Oroszországi Föderáció Fegyveres Erői Vezérkarának Felderítő Főcsoportfőnökségéhez (röviden: Glavnoje Razvedivatyelnoje Upravlenyije, GRU), azaz az orosz katonai titkosszolgálathoz kapcsolható. Erre szintén több, bár csak közvetett bizonyíték szolgált, nevezetesen, hogy hogy a csoport célpontjai sok esetben katonai célpontok, illetve katonai célok támogatásával voltak kapcsolatosak. (Kovács–Krasznay 2017) A következtetésünk a következő volt: „*[a] 2016-os amerikai elnökválasztás eseményeiben komoly szerepet játszottak az internetes támadások. Ezek a hackerek által elkövetett internetes akciók azonban számos esetben nem vagy csak részben bizonyíthatók. Ugyanakkor az akciók volumene mindenképpen átlépte azt a küszöböt, amikor érdemes megvizsgálni azt, hogy az internetes támadások hogyan és milyen mértékben tudnak befolyásolni egy olyan eseményt, amely elviekben a világ egyik*

[74] Az Egyesült Államok hivatalosan is megnevezte Oroszországot, mint az APT28 csoport állami támogatóját miután a 2016-os amerikai elnökválasztással kapcsolatos kibertámadások során erre számos közvetett bizonyítékot találtak. (US DHS–FBI 2016)

legjobban szervezett és legjobban felügyelt választásához kapcsolódik." (Kovács–Krasznay 2017)

Ugyanakkor elemzésünkben az APT28-on kívül egy másik hasonló csoportot az APT 29-et, más néven Cozy Bear-t is nevesítettük amerikai jelentések alapján: *„[a] Cozy Bear-t az orosz titkosszolgálatok közül vagy a Szövetségi Biztonsági Szolgálathoz (Fegyeralnaja Szluzsba Bezopasznosztyi Rosszijszkoj Fegyeracii – FSZB) vagy az Külső Hírszerző Szolgálathoz (Szluzsba Vnyesnyej Razvedki – SZVR) kapcsolják, tehát feltehetően polgári kötődésük van. Jellemzően hosszabb időt, akár éveket hagynak egy-egy adatlopási kampányra. Ezt azt jelenti, hogy a leginkább rejtve maradnak, lassú ütemben „szívják le" az információt. Első feltűnésük 2008-ra datálódik, ekkor kötötték őket a miniDuke kártékony kódhoz, mely diplomáciai szervezeteket támadott, többek között magyar külképviseleteket is. Felderítésében óriási szerepe volt a Budapesti Műszaki és Gazdaságtudományi Egyetemen működő CrySys Labornak."* (Kovács–Krasznay 2017, idézi: Kovács 2018b)

Oroszország nemzeti biztonsági stratégiája

Oroszország mind politikai, mind katonai erejét tekintve a világ egyik vezető hatalma, hiszen meglévő katonai ereje[75] és annak erőkivetítő képessége (például a szíriai válság esetében bizonyítottan) erre enged következtetni és ez meghatározza a nemzeti biztonsági stratégiájának legfontosabb elemeit is.

Vlagyimir Putyin elnök aláírásával az Orosz Föderáció új Nemzeti Biztonsági Stratégiája 2015 év végén került kiadásra. Az új dokumentum a 2009-es korábbi nemzeti biztonsági stratégiát váltotta fel.

Ahogy már többször utaltam rá Oroszország sem használja a kiber kifejezést és a mögötte lévő tartalmat olyan széles körben, mint a nyugati országok. Helyette az információs tér kifejezéssel él, amely meg is jelenik az új nemzeti biztonsági stratégia önnön magáról alkotott megfogalmazásában, miszerint a stratégia: „*magába foglalja az ország biztonságát és védelmét, amelyet az Orosz Föderáció Alkotmánya és az Orosz Föderáció jogszabályai által megfogalmazott – állami, köz-, információs, környezetvédelmi, gazdasági, közlekedési és energia – területeken valósulnak meg."* (Orosz Föderáció 2015, idézi: Kovács 2018b)

A stratégia számba veszi mindazokat a veszélyeket, amelyekkel az országnak szembe kell néznie. Ebben a többközpontú világrendből adódó instabilitás, a támadó fegyverek

[75] A Military Ballance adatai alapján az orosz fegyveres erők létszáma több, mint 1 millió fő. A CIA országértékelésének adatai alapján az orosz katonai kiadások 2016-ban elérték a GDP 5,4%-át, bár ez alaposan – mintegy 10-15%-al – csökkent 2018-ban. (Military Ballance 2018, CIA 2018)

korszerűsítésére való törekvés, az Afrikából és a Közel-Keletről érkező migrációs nyomás, illetve az erre adott európai elégtelen válasz mellett megjelenik a korszerű információtechnológiában rejlő kihívás is: *„[j]ogellenes tevékenységek olyan új formái jelennek meg, amelyek felhasználják az információs, kommunikációs és legkorszerűbb technológiákat. Ezeknek a veszélyeknek az ellenőrizetlen és illegális migrációhoz, az emberkereskedelemhez, a kábítószer-kereskedelemhez és a transznacionális szervezett bűnözés egyéb megnyilvánulásaihoz való kapcsolódása fokozódik."* (Orosz Föderáció 2015, idézi: Kovács 2018b)

A stratégia természetesen felsorolja mindazokat az érdekeket és célokat, illetve ahogy a dokumentum fogalmaz *prioritásokat*, amelyek Oroszország számára a legfontosabbak. Ebben azonban a stratégia felépítése nem egységes, mert amíg az állam és a közbiztonság területén számos közvetlen és közvetett veszélyforrást sorol fel (például az állam biztonságával szemben megjelenő külföldi hírszerző szolgálatok információszerző tevékenységét, a terror és egyéb extrémista szervezetek jelenléte és akciói, a korrupció, a szervezett bűnözés is kiemeli), addig a nemzeti védelem területén csak általános értelemben vett veszélyeket sorol fel. (Kovács 2018b)

Az állampolgárok életszínvonalának emelése érdekében prioritásként jelenik meg információtechnológia széleskörű elterjedésének támogatása: *„többek között az információs infrastruktúra fejlesztésével támogatni kell, hogy a társadalom szociálpolitikai, gazdasági és szellemi életével kapcsolatos különböző kérdésekkel kapcsolatos információk, valamint az állami szolgáltatások egyenlő módon hozzáférhetőek legyen az Orosz Föderáció területén;"* (Orosz Föderáció 2015, idézi: Kovács 2018b)

Nagyon érdekes következtetéseket von le a stratégia a nemzetközi közösség Oroszországgal szemben bevezetett szankciói miatt kialakult helyzettel kapcsolatban. A stratégia veszélyforrásként jelöli meg a nemzetközi szankciók miatt import tilalommal sújtott tudományos berendezések, elektronikai alkatrészek, számítógépes hardver és szoftver összetevők hiányából fakadó helyzetet. Ezeknek a szankcióknak a következményeként nem megfelelő módon fejlődő tudományos-technológiai kutatásoknak egyrészt közvetlen negatív hatásai vannak a tudomány, az innováció és a technológiai kutatások területeire, másrészt közvetett hatásuk az, hogy így a tanári és a mérnöki szakma presztízse csökken, amely a műszaki és tudományos, illetve az általános és középfokú szakképzés és a felsőoktatás minőségében is csökkenést fog eredményezni. (Orosz Föderáció 2015, Kovács 2018) Így nem meglepő módon a stratégia kitér a technológiai biztonságra is, mint arra a területre, amely a nemzeti biztonság növelésének egyik legfőbb szegmensére, és amelybe az

információs tér is beletartozik: „*[a] tudomány, a technológia és az oktatás területén a nemzeti biztonság fenntartásának egyik fő területe a technológiai biztonság szintjének emelése, beleértve az információs térséget is.*" (Orosz Föderáció 2015, idézi: Kovács 2018b)

Oroszország katonai stratégiája

Oroszország jelenlegi katonai stratégiája 2014 év végén jelent meg az *Orosz Föderáció Katonai Doktrínája* hivatalos címmel. A stratégiaként értelmezhető doktrína a modern katonai konfliktusok jellemzőjeként utal arra, hogy az ellenséggel szemben a hagyományos hadviselési dimenziók, azaz a szárazföld, levegő, tenger mellett a globális információs térben is végrehajthatók akciók. (Orosz Föderáció 2014, Kovács 2018b)

A doktrína a külső veszélyforrások felsorolása és értékelése során már utal a kibertérben megjelenő fenyegetésekre (bár ahogy korábban említettem, Oroszország nem a kiber, hanem ehelyett az információs jelzőt alkalmazza). A doktrína az *Orosz Föderáció katonai veszélyei és katonai fenyegetettségei* című részben fő külső katonai veszélyként megállapítja, hogy: *„az információs és kommunikációs technológiák katonai és politikai célokra történő felhasználása a nemzetközi joggal ellentétesen, a, szuverenitással, a politikai függetlenséggel, az államok területi integritásával és a nemzetközi békét, biztonságot, globális és regionális stabilitást veszélyeztetve."* (Orosz Föderáció 2014, idézi: Kovács 2018b)

Ezen kívül a doktrína az információs infrastruktúrák veszélyeztetettségére külön is utal, amikor a belső katonai fenyegetéseket veszi számba: *„az Orosz Föderáció alkotmányos rendjének erőszakos megváltoztatását célzó tevékenységek, destabilizálva az országban tapasztalható hazai politikai és társadalmi helyzetet, megzavarva az állami hatóságok működését, fontos állami és katonai létesítményeket, vagy az Orosz Föderáció információs infrastruktúráját."* (Orosz Föderáció 2014, idézi: Kovács 2018b)

A doktrína nagyon egyértelműen leszögezi a hadsereg alkalmazásának eseteit és lehetőségeit. Ennek során a dokumentum megfogalmazza, hogy ha az országot vagy szövetségeseit támadás vagy agresszió éri, akkor a fegyveres erőket ezen támadások visszaszorítására, illetve a törvényes rend helyreállítására bevetheti. Ugyanilyen egyértelmű megfogalmazással él a doktrína az infrastruktúrák kettős rendeltetésű felhasználásával kapcsolatban is, amely alapján a fegyveres erők védelmi feladataik ellátására igénybe vehetik a szükséges polgári infrastrukturális elemeket. (Orosz Föderáció 2014)

A doktrína meghatározza a fegyveres erők információbiztonságának hatékony fenntartását is, de nem ad részletes utasításokat ehhez. (Orosz Föderáció 2014, idézi: Kovács–Krasznay 2017)

Oroszország kiberbiztonsági stratégiája

A 2016 decemberében jelent meg az *Orosz föderáció információbiztonsági doktrínája,* amely az ország kiberbiztonsági stratégiájaként értelmezhető.

A doktrína egyik legfontosabb céljául a nemzeti biztonsághoz való hozzájárulásban határozza meg. A dokumentum bevezetőjében meghatározza a legfontosabb definíciós készletet, amelyben az információs tér, illetve a doktrína hivatalos meghatározása szerint *információs szféra* (oroszul *информационная сфера)* a következő: *„információk, informatikai célú objektumok, információs rendszerek, az internet informatikai és telekommunikációs hálózatain belüli weboldalak összessége, valamint a kommunikációs hálózatok, az információs technológiák, az információ előállításában és feldolgozásában érintett egységek, a fenti technológiák kifejlesztése és felhasználása, csakúgy, mint az információbiztonság megteremtése, valamint a tömegkommunikáció szabályozása a szférában."* (Orosz Föderáció 2016, idézi: Kovács 2018b)

A doktrína az orosz nemzeti biztonsági stratégia felépítéshez hasonló szerkezetű[76]. Elsőként a nemzeti érdekeket információs térben való meghatározását adja meg, amelyben a legfontosabb annak a deklarálása, hogy az információtechnológia az állam és a társadalom integráns részét képezik, így ezek alkalmazása nem csak hogy az információs társadalom alapját képezi, de a gazdaság növekedéséhez is elengedhetetlen. A doktrína egyik legfontosabb eleme az információs tér nemzeti stratégiai célok és prioritások elérésében játszott szerepének hangsúlyozása. A doktrína alapján Oroszország nemzeti érdekei az információs térben a következők:

- az alkotmányos emberi és polgári jogok, valamint szabadság biztosítása és azok védelme az információk felhasználása tekintetében;
- az információs infrastruktúra fenntartható és zavartalan működésének biztosítása, elsősorban az Orosz Föderáció kritikus információs infrastruktúrájának vonatkozásában;

[76] Itt érdemes megjegyezni, hogy az USA 2018-ban megjelent nemzeti kiberstratégiája ugyanígy a nemzeti biztonsági stratégia szerkezetének megfelelő módon épül fel.

- az információtechnológiai és elektronikai szektor fejlesztése, beleértve a kutatás-fejlesztés ösztönzését is;
- mind a belső mind a nemzetközi közvélemény megbízható információkkal való támogatása az Orosz Föderáció állami politikájáról és működéséről;
- elősegíteni a nemzetközi információbiztonsági rendszerek fejlesztését. (Orosz Föderáció 2016, Kovács 2018b)

Természetesen a stratégia felsorolja és röviden elemzi a legfontosabb információs veszélyforrásokat és fenyegetéseket is, amelyek lényegi elemei a következők:

- az információtechnológia széleskörű alkalmazása, amely során annak határokon átnyúló jellege a nemzetközi biztonságot negatívan befolyásoló geopolitikai és katona-politikai célokra történő alkalmazását segíti elő;
- az információs infrastruktúra katonai célokra történő alkalmazása és felhasználása, valamint a műszaki-technikai alapú hírszerzés az orosz kormányszervek, kutató intézetek és a védelmi-ipari komplexumok vállalkozásai irányában fokozott tevékenységet mutatnak;
- egyes államok pszichológiai befolyásolásra használják a hírszerzésük által megszerzett információkat különböző régiók destabilizálása érdekében. Ennek során a külföldi média az Orosz Föderációval szemben elfogult híreket tesz közzé, megakadályozzák az orosz újságírók külföldi munkáját, valamint információs nyomást gyakorolnak elsősorban az orosz ifjúságon keresztül a lakosságra;
- a különböző terrorista és szélsőséges szervezetek széles körben használják az információs eszközöket a közvélemény befolyásolására, illetve aktívan fejlesztenek támadó eszközöket a kritikus információs infrastruktúrák rombolására;
- emelkedik a kiberbűnözés, amely elsősorban a pénzügyi szférát érinti, de a személyes adatok elleni bűncselekmények is egyre gyakoribbá és egyre szofisztikáltabbá válnak;
- a gazdasági szféra nem megfelelő információbiztonsági rendszerekkel és mechanizmusokkal rendelkezik;
- többször is visszatérő veszélyforrásként értékeli a stratégia más országok azon igyekezetét, hogy a kibertérben technikai fölénybe és stratégiai vezető és

domináns szerepet játsszanak, és amely alól sok esetben a stratégiai partnerek sem kivételek;

- mindezeken túl a nemzetközi jogi normák hiányát, az internet erőforrásainak jelenleg nem tisztességes elosztását, azok alkalmazási mechanizmusát (valószínűleg itt az ICANN és az internet konkrét, jórészt amerikai szabályozására utal a stratégia) nevezik meg a valódi stratégiai partnerség kialakítása ellen ható tényezőkként. (Orosz Föderáció 2016. Kovács 2018b)

A doktrína megadja az információbiztonság területén elérendő legfontosabb stratégiai célokat. A célokat kulcsfontosságú területekhez kapcsolja a dokumentum, amely területek között megjelenik a katonai terület is. Ezen belül olyan fontos területek kerülnek felsorolásra, amelyek az információbiztonság megteremtésével és növelésével járulnak hozzá a nemzeti biztonsághoz. Ennek megfelelően az Orosz Föderáció katonai politikáját úgy kell kialakítani, hogy az biztosítsa:

- a stratégiai elrettentést és megakadályozza a katonai konfliktusokat, amelyek az információs technológiák alkalmazásával járhatnak;
- a fegyveres erők információbiztonsági rendszereiknek és az információs ellentevékenységi eszközeiknek korszerűsítését;
- az információs fenyegetések előrejelzését és azonosítását, amelybe beletartozik a fegyveres erők ilyen jellegű fenyegetettsége is;
- az Orosz Föderáció szövetségesei érdekeinek érvényesítését az információs térségben;
- a pszichológiai tevékenységek elleni védelmet. (Orosz Föderáció 2016, Kovács 2018b)

Az állam és a közbiztonság területén legfontosabb információbiztonsági feladatok a következők:

- az alkotmányos rend megdöntése és szélsőséges ideológiák terjesztése érdekében használt információtechnológia megakadályozása;
- külföldi nemzetbiztonsági szervezetekkel szembeni védelem növelése;
- kritikus információs infrastruktúrák védelmének növelése;
- a kormányzati szervek közötti kommunikáció biztosítása a terület információs infrastruktúrái működésének folyamatos biztosításával;
- az automatizált irányítási rendszerek működésének biztosítása;

- a kiberbűncselekmények megelőzésének, illetve a kiberbűncselekmények elleni tevékenység fokozása;
- a titkosítást biztosító rendszerek fejlesztése;
- a korszerű információbiztonsági elveknek és követelményeknek megfelelő eszközök, rendszerek és szolgáltatások gyártása és azok üzemeltetése;
- az állami politika számára információtámogatási tevékenység nyújtása;
- azoknak az információs tevékenységek hatásainak kivédése, amelyek célja az ország lakosságának erkölcsi és morális állapotának gyengítése, aláásása. (Orosz Föderáció 2016, Kovács 2018b)

A gazdaság területén megfogalmazott stratégiai célok az információtechnológiai és az elektronikai szektorok nem megfelelő fejlődéséből következő negatív tényezők hatásainak ellensúlyozására hivatott versenyképes információbiztonsági eszközök kifejlesztésére és előállítására irányulnak. Hasonló célokat találunk a tudomány, a technológia és az oktatás területeken is, amelyeken szintén fontos prioritás a korszerű és versenyképes technológia megteremtése, az ahhoz szükséges kutatás-fejlesztési tevékenység biztosításával együtt. Ennek ki kell terjednie oktatásra is, mert csak megfelelő mérnöki, műszaki humánerőforrás képzésével biztosítható a magasszintű információtechnológia előállítása. Ez egyben az információs rendszerek biztonságtudatosabb használatához is hozzájárul. (Orosz Föderáció 2016, Kovács 2018b)

A doktrína a kijelölt célok eléréséhez szükséges szervezeti hátteret is meghatározza. Az ehhez szükséges információbiztonsági szervezeti rendszert az Orosz Föderáció nemzeti biztonsági rendszerének szerves részeként határozza meg a következő tényező figyelembe vételével: *„[a]z információbiztonságot az önkormányzatokkal, szervezetekkel és állampolgárokkal együttműködésben dolgozó kormányzati szervek jogalkotási, bűnüldözési, igazságügyi, felügyeleti és egyéb tevékenységeinek kombinációja biztosítja.”* (Orosz Föderáció 2016, Kovács 2018b)

A meghatározott információbiztonsági intézményi keretben a következő szereplőket azonosítja a doktrína:

- a kritikus információs objektumok tulajdonosai és üzemeltetői;
- tömegtájékoztatást és tömegkommunikációt végző szervezetek;
- monetáris, deviza, banki és egyéb pénzügyi intézmények;
- távközlési szolgáltatók;

- információs rendszereket üzemeltetők;
- információs és kommunikációs rendszereket gyártó és működtető szervezetek;
- az információbiztonsági eszközöket fejlesztő, gyártó és üzemeltető szervezetek;
- információbiztonsági szolgáltatásokat nyújtó szervezetek;
- információbiztonsági oktatási szolgáltatásokat nyújtó szervezetek. (Orosz Föderáció 2016, Kovács 2018b)

2.3. Az Európai Unió és a NATO kibertérhez kapcsolódó stratégiái

2.3.1. Az Európai Unió stratégiai szintű kiberbiztonsági törekvései

Az Európai Unió stratégiájának egyik legfontosabb pillére a digitális gazdaság. Ugyanakkor maga a gazdaság és benne a gazdasági folyamatok folyamatosan fennálló magas kitettséggel rendelkeznek a nemzetközi gazdasági és politikai változásokkal szemben. Az Európai Bizottság, de a tagállamok is már a 2010-es évek elején felismerték, hogy Európa versenyképessége nagymértékben a stabilitáson, ezen belül is a biztonságon múlik. Az Európai Bizottság 2010-ben meghirdetett Európa 2020 stratégiájának célja az EU versenyképességének növelése mellett a sérülékenységek csökkentését jelentette. Ennek a stratégiának az egyik fontos pilléreként hirdették meg az Európai Digitális Menetrendet. Ez az EU olyan, a digitális területen meglévő kihívásaira kíván – a tagállamok által egységesen kialakított keretben – választ adni, amelyek a digitális piac megosztottságában, a meglévő interoperabilitási problémákban, a kiberbűnözésben, az alacsony szintű kutatás-fejlesztési tevékenységekben vagy éppen a digitális írástudás alacsony szintjében jelentkeznek. (Európai Bizottság 2017c, Kovács 2018b)

Ezeknek a kihívásoknak a kezelése azonban a kibertér biztonságának megteremtése és emelése nélkül nem valósíthatók meg. Ennek megfelelően a kibertér biztonságának megteremtése kiberbiztonsági stratégiát igényelt. A stratégia kialakítása azonban nem volt vitáktól mentes, amely azt eredményezte, hogy a 2010-ben elfogadott Európa 2020 menterendet követően csak három évvel – 2013 februárjában – született javaslat az EU kiberbiztonsági stratégiájára. A javaslat két részből állt, amely első része maga a kiberbiztonsági stratégia – hivatalos formában az Európai Bizottság és a külügyi és biztonságpolitikai főképviselő közleményeként kiadva –, a második rész pedig az úgynevezett NIS irányelvre tett javaslat volt.

Bár nem egyidőben, de mindkét javaslatot elfogadta az Európai Parlament és az Európai Tanács is. Így a stratégia *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és*

biztonságos kibertér címmel 2013-ban kiadásra is került. (Európai Unió Kiberbiztonsági Stratégiája 2013)

Az új kiberbiztonsági stratégia egy olyan holisztikus megközelítést alkalmaz, amely nem csak a kibertéren, de az olyan kapcsolódó területek esetében is, mint a kritikus infrastruktúrák területe megfogalmazza a biztonságot növelő legfontosabb célkitűzéseket. (Kovács 2018b)

A stratégia lefekteti azokat a kiberbiztonsági alapelveket, amelyeket az Unió a kibertérben magáénak vall:

- az Európai Unió alapértékei ugyanolyan mértékben vonatkoznak a digitális, mint a fizikai világra;
- az alapvető jogok, a szólásszabadság, a személyes adatok és a magánélet védelme;
- mindenki számára biztosított hozzáférés;
- demokratikus és hatékony, számos érdekelt fél bevonásával történő irányítás;
- a biztonság közös felelősség. (Európai Unió Kiberbiztonsági Stratégiája 2013, Kovács 2018b)

Maga a stratégia öt alapelvre épül, amelyeket az EU egyben prioritáskén is kezel:

- a kibertámadásokkal szembeni ellenállóképesség megteremtése;
- a kiberbűnözés (a stratégiában használatos kifejezéssel élve számítástechnikai bűnözés) nagymértékű visszaszorítása;
- kibervédelmi politika kidolgozása úgy, hogy az a közös biztonság- és védelempolitikára épüljön[77];
- a kiberbiztonsághoz szükséges ipari és technológia fejlesztése;
- a kibertérre vonatkozó olyan nemzetközi szakpolitika meghatározása, amely a tagállamok mindegyike számára érvényes, és amely támogatja az alapvető uniós értékeket. (Európai Unió Kiberbiztonsági Stratégiája 2013, Kovács 2018b)

[77] Ennek elérése érdekében született meg 2014 novemberében az *EU kibervédelmi politika keretrendszer* (EU Cyber Defence Policy Framework), amely többek között az Európai Unió Védelmi Ügynöksége (European Defence Agency) számára határoz meg feladatokat a kibervédelem területén. (Európai Tanács 2014) Ennek kiegészítése és frissítése 2018-ban történt meg.

Ezekhez a prioritásokhoz intézkedéseket is hozzárendeltek, amelyek három nagy területen jelennek meg a kibertámadásokkal szembeni ellenállóképesség megteremtése és növelése érdekében:

- nemzeti szint: ezen a területen az állami és a magánszektor összefogása, a kapacitások, erőforrások és a hatékonyság fejlesztése az elsődleges feladat;
- az uniós szintű koordináció: ezen a területen a stratégia kiemelt szerepet szán az ENISA-nak, mivel a határokon átnyúló incidenskezelés – ide értve a kiberbűnözés elleni hatékony fellépést is – fejlesztésre szorul;
- jogalkotás területe: ennek ki kell terjednie a nemzeti stratégia és nemzeti együttműködési terv elkészítésére, valamint azoknak a minimum követelményeknek a megfogalmazására, amelyek alapján többek között a nemzeti kiberhatóságok kijelölésre kerülhetnek, valamint megalakíthatók a nemzeti CERT-ek. (Európai Unió Kiberbiztonsági Stratégiája 2013, Kovács 2018b)

A stratégia egyik nagyon előremutató meglátása, hogy a köz- és a magánszektor összefogásának hiánya alapvetően befolyásolhatja a stratégiában foglaltak végrehajtását: *„ha a kiberbiztonsági események megelőzése, feltárása és kezelése érdekében nem teszünk jelentős erőfeszítéseket az állami és privát kapacitások, erőforrások és eljárások javítására, Európa továbbra is sebezhető marad."* (Európai Unió Kiberbiztonsági Stratégiája 2013, idézi: Kovács 2018b)

A stratégia az ENISA számára is megfogalmaz feladatokat. Ezek közül az egyik legfontosabb a nemzeti képességek kialakításának támogatása: *„[a] tagállamok támogatása az erős nemzeti képességek kialakításában a kibertámadásokkal szembeni ellenálló képesség területén, főleg az ipari vezérlőrendszerek, a szállítás és az energiaipari infrastruktúra biztonságával és ellenálló képességével kapcsolatos ismeretek összegyűjtése révén."* (Európai Unió Kiberbiztonsági Stratégiája 2013, idézi: Kovács 2018b)

A stratégia kiemelt célként kezeli a kiberbiztonsági tudatosság fejlesztését, amelyben a felhasználók internetes tevékenységeinek minél nagyobb biztonsága kapja az egyik fő hangsúlyt. Ennek megvalósítása érdekében a stratégia az ENISA-t, az Europol-t és az Eurojust-ot is megnevezi. Az ENISA esetében már olyan előremutató kezdeményezést is

bemutat a stratégia, mint amely például az Európai kiberbiztonsági hónap[78] rendezvénysorozat. (Európai Unió Kiberbiztonsági Stratégiája 2013, Kovács 2018b)

A stratégia kitér az egyik legfontosabb veszélyforrás, a kiberbűnözés kezelésére is. Ennek drasztikus csökkentése érdekében olyan jogszabályok meghozatalát és azok betartását kéri a tagországoktól, amelyek mentén a kiberbűnözés elleni tevékenység szigorúbb és hatékonyabb lesz. A stratégia kiemeli a Budapest Konvenciót[79], illetve azt a nemzetközi jogszabályi keretet, amelyet ez nyújthat a tagországok számára. A jogszabályi keret kidolgozása mellett a kiberbűnözés elleni hatékonyabb uniós szintű fellépés érdekében a stratégia támogatta az EUROPOL-on belül a Számítástechnikai Bűnözés Elleni Európai Központ (European Cyber Crime Center, EC3)[80] kialakítását. A stratégiában megfogalmazottak alapján az EC3 lehet kiberbűnözés elleni hírszerzés, elemzés és operatív beavatkozás közös EU-s szervezete. (Európai Unió Kiberbiztonsági Stratégiája 2013, Kovács 2018b)

A stratégia kiemelt céljai közé tartozik egy olyan nemzetközi szakpolitika létrehozása, amely a már meglévő nemzetközi szabályozásokra építve járul hozzá az uniós alapértékek biztosításához. A kiberbiztonság nemzetközi területen történő, az együttműködésre és a partnerségre építő feladatokkal kapcsolatban a stratégia a következőket tartalmazza:

- a kibertér biztonsága be kell, hogy kerüljön az Unió külkapcsolataiba és a közös kül- és biztonságpolitikába;
- harmadik, azaz nem EU-s országokban is szükséges támogatni az információs infrastruktúrák fejlesztését és a kiberbiztonsághoz nélkülözhetetlen képességeket. (Európai Unió Kiberbiztonsági Stratégiája 2013, Kovács 2018b)

78 Ehhez a rendezvénysorozathoz Magyarország is csatlakozott 2013-ban és azóta minden év októberében több tucat kiberbiztonsági, illetve információbiztonsági tudatosság növelését célzó rendezvényt szervez.

79 A 2001-ben született Budapest Konvenció fő célja a kiberbűnözés és a kiberbűncselekmények elleni tevékenység nemzeti jogszabályokban rögzített harmonizációja. (Európa Tanács 2001) Hazánk a megállapodást 2004-ben iktatta törvénybe a 2004. évi LXXIX. törvénnyel, amelynek hivatalos címe *az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről*. (2004. évi LXXIX. törvény). Bár a megállapodást máig közel 60 ország ratifikálta, azonban néhány állam, mint például Oroszország vagy India számos kifogást emelve ezt nem tette meg. (Európa Tanács 2017)

80 Az EC3 az EUROPOL új szervezeteként 2013 januárjában került megalakításra. Az EC3-nak három kiemelt feladata van a kiberbűnözés elleni tevékenységgel kapcsolatban. Kriminalisztikai vizsgálatokat végez, közreműködik a kiberbűnözés elleni stratégiaalkotásban és operatív nyomozásokat végez a kiberbűncselekmények felderítése érdekében. (Europol 2017a, Europol 2017b, Kovács 2018b)

A stratégia – többek között a fentieken megfogalmazottak alapján – a kiberbiztonságot a közös európai biztonság- és védelempolitika (Common Security and Defence Policy, CSDP) részének tekinti. Ennek megfelelően a kibertér biztonságának megteremtése érdekében szükség van az Unió és a NATO szoros együttműködésére a kormányzati hálózatok és védelmi információs rendszerek biztonságának növelése érdekében. A stratégiában megfogalmazottak szerint ez a következőt jelenti: *„[h]atékony védelmi képességek biztosítása, együttműködési területek meghatározása és a felesleges erőfeszítések elkerülése érdekében párbeszéd biztosítása nemzetközi partnerekkel, ideértve a NATO-t, más nemzetközi szervezeteket és a többnemzeti kiválósági központokat."* (Európai Unió Kiberbiztonsági Stratégiája 2013, idézi: Kovács 2018b)

A kiberbiztonság nem képzelhető el az ipari és technológiai erőforrások fejlesztése nélkül. Ennek érdekében a stratégia a már meglévő és a jövőben megjelenő termékek számára egységes piacot kíván teremteni úgy, hogy emellett ösztönzi a K+F célú beruházásokat és az innovációt. (Európai Unió Kiberbiztonsági Stratégiája 2013, Kovács 2018b)

Az EU 2013-ban elfogadott kiberbiztonsági stratégiája ma már azonban felülvizsgálatra szorul, mert egyrészt azóta számos technikai, politikai és gazdasági változás következett be, másrészt a stratégia végrehajtása nem minden területen és nem minden tagországban ment zökkenőmentesen. A stratégia felülvizsgálatának másik oka a 2016-ben megjelent új európai uniós kül- és biztonságpolitikai stratégia[81], amely a kiberbiztonságot kiemelt helyen kezeli. Az Unió szorgalmazza, hogy a tagállamok a nyílt kibertér megtartása mellett olyan kiberbiztonsági technikai fejlesztéseket és innovatív IKT eszközöket és rendszereket fejlesszenek, illetve alkalmazzanak, amelyek hozzájárulnak a kiberbiztonsági ellenállóképesség és a kritikus információs infrastruktúrák támogatásához. Fontos kiemelni, hogy ehhez a munkához az EU támogatást is nyújt. (Európai Unió 2016)

A fentieknek megfelelően az Európai Bizottság elnöke 2017 szeptemberében bejelentette, hogy bár történtek előrelépések a kiberbiztonság uniós megvalósítása terén, de még sok teendő van hátra: *„[a]z elmúlt három évben előrelépéseket tettünk az európaiak online biztonságának garantálása terén. Ám Európa még mindig nem rendelkezik elég eszközzel a kibertámadások elhárítására. A Bizottság ezért ma új eszközöket javasol az ilyen*

[81] Ennek címe: *Közös jövőkép, közös fellépés: erősebb Európa - Globális stratégia az Európai Unió kül- és biztonságpolitikájához* (Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy) (Európai Unió 2016)

támadásokkal szembeni védelem megerősítésére, többek között egy európai kiberbiztonsági ügynökség létrehozását." (Európai Bizottság 2017a, idézi: Kovács 2018b)

Ezt követően az Európai Bizottság egy új javaslatcsomaggal, a gyakran a Cybersecurity Act, azaz Kiberbiztonsági Törvénynek nevezett javaslattal állt elő. Ez a csomag az európai kiberbiztonság teljes reformját irányozza elő. A javaslatcsomag többek között tartalmazza egy új *Európai Uniós Kiberbiztonsági Ügynökség* felállítását is, amely ügynökség az ENISA-ra épülve a tagállamok számára nyújtana a kibertámadások megelőzéséhez és az azokra való reagáláshoz segítséget. Az új ügynökség feladatai közé tartozik majd az európai kiberbiztonsági gyakorlatok megszervezése és levezetése. Mindezeken túl a javaslatcsomag a digitális termékek és szolgáltatások biztonságos használatát lehetővé tevő és az azokat garantáló új európai tanúsítási rendszer kidolgozását is magába foglalja. (Európai Bizottság 2017b, Kovács 2018b)

Visszatérve az EU 2013-as javaslatcsomagjára, annak is második részére, amely az említett a NIS irányelv javaslat volt, ki kell jelenteni, hogy ez az egyik legfontosabb kiberbiztonsági direktíva az EU működésében. Ennek elfogadására azonban a kiberbiztonsági stratégia után még közel 3 évet kellett várni. Végül a NIS irányelvként ismertté vált – a tagországok számára – kötelező érvényű direktíva 2016 év közepén került elfogadásra, de hatályba csak 2018 májusában lépett.

Az elfogadott irányelvet szakmai körökben is nagyon gyakran csak NIS direktívaként említik. Ez az angol *Network and Information Systems Directive*, azaz hálózati és információs rendszerek kifejezésekből ered. A direktíva hivatalos címe *az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.*[82] (NIS Direktíva 2016)

A NIS direktíva a tagállamok nemzeti hálózati és információs rendszereire vonatkozólag egyik legfontosabb előírása egy nemzeti kiberbiztonsági stratégia kidolgozására és elfogadására vonatkozik: *„[v]alamennyi 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*

[82] A NIS irányelv hivatalos angol címe: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

intézkedéseket, legalább a II. mellékletben említett ágazatokra és a III. mellékletben említett szolgáltatásokra vonatkozóan." (NIS Direktíva 2016, Kovács 2018b)

A NIS fentiekben megfogalmazott utasításai alapján egyrészt a tagországoknak létre kell hozniuk egy nemzeti kiberbiztonsági stratégiát, másrészt az idézetben is szereplő NIS mellékletek tartalmazzák azokat a hálózati és információs rendszereket, amelyeket az EU nemzeti és uniós szinten is kritikus infrastruktúra ágazatoknak tart. Ennek megfelelően a nemzeti kiberstratégiának ezekre is ki kell térnie. (Kovács 2018b)

A nemzeti biztonsági stratégiák konkrét felépítéséhez is megfogalmaz ajánlásokat a direktíva. A NIS a következő elemeket (területeket) várja el a nemzeti biztonsági stratégia esetében kidolgozandónak:

- a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia céljai és prioritásai;
- a stratégia céljainak és prioritásainak végrehajtását szolgáló irányítási keretrendszer, amely meghatározza a kormányzati szervek és egyéb érintett szereplők szerepkörét és felelősségét is;
- azokat az intézkedések, amelyek felkészültségre, a reagálásra és a helyreállításra vonatkoznak;
- a köz- és a magánszféra közötti együttműködés keretei;
- a stratégiához kapcsolódó oktatási, tájékoztató és képzési programokra vonatkozó elképzelések;
- a stratégiához kapcsolódó kutatási és fejlesztési tervek;
- a kockázatok feltárására szolgáló kockázatértékelési terv;
- a stratégiában megfogalmazottak végrehajtásába bevont szervezetek és szereplők jegyzéke. (NIS Direktíva 2016, Kovács 2018b)

Mindezeken túl a direktíva a tagországok közötti együttműködés biztosítása érdekében egy olyan együttműködési csoport felállítását is elrendeli, amely *„a stratégiai együttműködés, a hatékony kommunikáció és a bizalom kialakításával támogatja a NIS fő célkitűzését, azaz a hálózati és információs rendszerek egységesen magas szintű biztonságának Unión belüli megvalósítását."* (Kovács 2018b)

A nemzeti kiberbiztonsági stratégia mellett a NIS még egy nagyon fontos elemet meghatároz a tagországok számára. Ez egy nemzeti illetékes hatóság (vagy hatóságok) kialakítását, valamint ezek közül egy nemzeti kapcsolattartó pont kijelölését jelenti. A

hatóság fő feladata az említett – külön meghatározott kritikus infrastruktúra – ágazatok hálózati és információs rendszerei biztonságának megteremtése. A hatóság mellett létre kell hozni egy nemzeti eseménykezelő csoportot, amely mellett ágazati szinten is számítógép-biztonsági események kezelésére alkalmas csoportoknak (CSIRT vagy CERT) kell működnie. E csoportokhoz megfelelő erőforrásokat, biztonságos kommunikációs és információmegosztási megoldásokat kell biztosítani. A nemzeti kapcsolattartó pontnak olyan központi szervezetet kell kijelölni, amely hatékonyan tudja koordinálni az ágazati CSIRT-ek közötti tevékenységeket és a képes a tagországok felé információcserét lehetővé tevő kommunikációt biztosítani. (NIS Direktíva 2016, Kovács 2018b)

A NIS ezeken kívül a hálózati és információs szolgáltatásokat nyújtó szervezetek számára is megfogalmazza azokat a legfontosabb követelményeket, amelyek minden tagországban egységesek kellenek, hogy legyenek. Így a direktíva külön kitér az alapvető szolgáltatásokat nyújtó szereplők feladataira. (NIS Direktíva 2016, Kovács 2018b)

2.3.2. A NATO kiberbiztonsági stratégiája

A NATO életében a kiberbiztonság, illetve kibervédelem[83] területén a közelmúlt legfontosabb eseménye minden bizonnyal 2016 júniusa volt. Az ekkor megrendezett Varsói Csúcstalálkozó és az ott hozott fontos döntések újabb, jelentős lökést adtak ahhoz, hogy a Szövetség megfelelő válaszokat tudjon adni a kibertéri kihívásoknak.

Ugyanakkor közel tíz évvel korábban – 2007-ben – a NATO több évtizedes fennállása során először szembesült azzal, hogy a kibertérben is érheti támadás magát a Szövetséget, vagy annak egyik tagországát. A nem fizikai dimenzióban bekövetkező támadásra azonban a NATO nem volt felkészülve. 2007 áprilisában és májusában az akkor már NATO tagország Észtországot közel három héten át erős kibertámadások érték. A támadások technikáját tekintve alapvetően DDoS támadások voltak, amelyek a már akkor is igen fejlett észt közigazgatási, banki és egyén információs rendszereket támadták. A támadások az anyagi károkon kívül nagy társadalmi károkat is okoztak, hiszen a kormányzatba vetett bizalom alaposan megrendült azzal, hogy sem a kormány, sem a Szövetség nem képes megvédeni még az alapvető információs rendszereket és szolgáltatásokat sem. (Kovács 2014)

Az észt incidens gyökeres biztonságpolitikai percepció változást is okozott, hiszen a támadások mögött sejtett Oroszország miatt a NATO nehéz politikai és stratégiai

[83] A NATO terminológiában a kibervédelem (Cyber Defence) használatos széles körben a területre.

dilemmával találta szembe magát, hiszen a NATO fennállása alatt nem volt még példa egy szövetséges tagállam elleni ilyen mértékű kibertámadásra.

Természetesen már az észt események előtt is történtek lépések a NATO kibervédelmi politikájának stratégiai szintű kidolgozása érdekében, hiszen a 2002-es Prágai NATO Csúcsértekezletet zárónyilatkozatába már bekerült a veszélyek meghatározásánál a kibertámadások növekvő száma és az azokkal szembeni védelem fontossága. Ennek ellenére az észt incidens utáni felismerés vezetett a Szövetségben arra, hogy a 2010-es lisszaboni NATO csúcstalálkozó után a szervezet Stratégiai Koncepciójában markánsabban kell megjeleníteni a kérdést. (NATO 2002, NATO 2010, Kovács 2018b)

A lisszaboni csúcstalálkozó után kiadott stratégiai koncepció ennek megfelelően már a következőket tartalmazta: *„[a] kibertámadások egyre gyakoribbá, szervezettebbé és a kormányok, vállalkozások, gazdaságok és potenciálisan a közlekedési és ellátási hálózatok valamint más kritikus infrastruktúrák számára is egyre nagyobb károkat okozóvá válnak. Elérhetik azt a küszöböt, ami már a nemzeti és euro-atlanti prosperitást, biztonságot és stabilitást veszélyezteti. Külföldi haderők és titkosszolgálatok, szervezett bűnözők, terrorista és/vagy szélsőséges csoportok egyaránt lehetnek egy ilyen támadás végrehajtói."* (Biztonságpolitikai Szakkollégium 2010, idézi: Kovács 2018b)

Időközben szervezeti szinten is komoly előrelépés történt, mert többek között a kibervédelem felkészülési kérdései támogatására – oktatás, képzés, kutatás-fejlesztés, stratégiai tanácsadás stb. – 2008-ban felállításra került a NATO Kibervédelmi Kiválósági Központ Tallinnban, amelynek Magyarország is tagja 2010-óta. (CCDCOE 2018, Kovács 2018a)

Ezt követően az egyik legmarkánsabb lépés 2011-ben történt a Szövetségben. 2011. június 8-án írták alá a NATO tagországok védelmi miniszterei a Szövetség új kibervédelmi politikáját. Ez nem csak a kibervédelem stratégiai céljait, hanem egy kibervédelmi cselekvési terv kidolgozását is előirányozta. A 2011 októberében elfogadott cselekvési terv alapján kezdődött meg 2012 februárjában a NATO kiberincidens kezelési képességének (NATO Cyber Incident Response Capability, NCIRC)[84] a teljes kiépítése, amellyel párhuzamosan egy kiberfenyegetés előrejelző központ (Cyber Threat Awareness Cell) kialakítása is megkezdődött. (NATO 2018a, Kovács 2014, Kovács 2018b)

[84] Az NCIRC technikai központja a koordinációért felelős szervezettel együtt a NATO SHAPE (Supreme Headquarters Allied Powers Europe, azaz Szövetséges Erők Európai Főparancsnoksága) kötelékében Mons-ban, Belgiumban van. Az NCIRC egyik legfontosabb feladata a NATO saját információs rendszereinek és számítógép-hálózatainak a védelme. (NATO 2018a)

A NATO kibervédelmi tevékenységéhez újabb lökést adott a 2012-es Chicagói Csúcstalálkozó, amely döntött a képességfejlesztés felgyorsításáról. A csúcstalálkozó zárónyilatkozatában ez így jelent meg: *„[é]pítve a NATO meglévő képességeire, a NATO Számítógép Vészhelyzeti Incidenskezelő Képesség (NATO Computer Incident Response Capability, CIRC) Teljes Műveleti Képessége (Full Operational Capability, FOC) kialakításra kerül 2012 végéig, beleértve a legtöbb helyszínt és a felhasználót. Vállaljuk, hogy biztosítjuk a forrásokat és véghez visszük a szükséges reformokat ahhoz, hogy minden NATO alá tartozó szerv központosított számítógépes védelemben részesüljön, annak érdekében, hogy a fokozott számítógépes védelmi képességekkel megvédjük a kollektív NATO értékeket."* (NATO 2012)

Ugyanakkor az eltérő technikai fejlettségű tagországok eltérő kiberbiztonsági és kibervédelmi gyakorlattal, és így nagyon heterogén képességekkel rendelkeznek, amelyek hatalmas kockázatot jelentenek a Szövetség számára. Ennek megfelelően az azonos, vagy közel azonos képességek kialakítása prioritást kell, hogy élvezzen szövetségi szinten. Ennek deklarálása, illetve feladatként történő meghatározása a Chicagói Csúcstalálkozó zárónyilatkozatába is bekerült: *„[t]ovább integráljuk a számítógépes védelmi intézkedéseket a Szövetség struktúrájában és folyamataiban, valamint minden egyes tagországában, és továbbra is elkötelezettek vagyunk mindazon nemzeti kibervédelmi képességek ügyében, amelyek erősítik az együttműködést és a kölcsönös átjárhatóságot a Szövetségen belül, többek között a NATO védelmi tervezési folyamatokban."* (NATO 2012)

A NATO elkötelezett a kibervédelem nemzetközi együttműködése iránt, amely érdekében folyamatos az együttműködése az ENSZ-el, az EU-val, az Európai Tanáccsal, illetve az EBESZ-el.

A nemzetközi térben történő együttműködéshez, illetve a tudományos kutatásokhoz nagyban hozzájárul a NATO említett kiber kiválósági központja. A Kibervédelmi Kiválósági Központ keretében történt többek között annak a tanulmánykötetnek is a létrejötte, amely a kiberhadviselés nemzetközi jogi szabályozását vizsgálta. A több európai és amerikai egyetem szakértői által összeállított Tallinn Manual, magyarul Tallinni Kézikönyv címet viselő kötet első kiadása 2013-ban történt meg. A könyv egyik legfontosabb célja annak a kérdésnek a megválaszolása, hogy a kiberhadviselés területén mennyiben alkalmazható a meglévő nemzetközi jog illetve hadijog. A Tallinn Manual két nagy részre osztva – *A nemzetközi kiberbiztonsági jog* (International Cyber Security Law), illetve a *Kiberhadijog* (The Law of Cyber Armed Conflict) –, 7 fejezetben mutatta be a kérdésre adandó válaszokat. A tanulmány készítői összesen 95 úgynevezett szabályt

azonosítottak a nemzetközi jog területén. (Schmitt 2013) Ezek megítélése, azaz, hogy valójában a nemzetközi hadijog mennyire is alkalmazható a kiberhadviselésben ekkor még meglehetősen vegyes fogadtatásra talált a szakértők részéről. A tanulmánykötet nagyon előremutató módon megvizsgálta a kiberhadviselés területén alkalmazható nemzetközi jogi normákat, ugyanakkor számos nyitott kérdés is maradt. Kutatóként és egyetemi oktatóként személy szerint én sem voltam meggyőződve, hogy ezek a szabályok teljes egészében és valóban alkalmazhatóak egy esetleges kiberkonfliktus esetén.

A tallinni kézikönyv első kiadását követően 2016-ban jelent meg a Tallinn Manual 2.0. Az új tanulmánykötet tartalmazza az első részben bemutatott és megvizsgált kérdéseket (szabályokat), de ezek mellett, azokat jelentősen kibővítve már 154 olyan szabály elemzése történik meg, amelyek a kiberműveletekben[85] a nemzetközi jogból levezetve alkalmazhatóak. (Schmitt 2016)

A 2014-es Walesi Csúcstalálkozó után a Szövetség kibervédelmi politikája felülvizsgálatra került, majd ezt 2017-ben egy új akcióterv követette. Az új kibervédelmi politika rögzíti, hogy a kibervédelem a NATO legfontosabb kollektív védelmi feladatainak része. (NATO 2018a) Ebből következően minden tagállam számára nem csak önkéntes, hanem kötelező érvényű feladatokat jelentenek, amelyek ki kell, hogy terjedjenek a képességek kialakítására, valamint egy esetleges konfliktus esetében a kollektív – kiberműveleti – feladatok ellátására.

Ahogy az alfejezet elején utaltam rá 2016 gyökeres változást hozott a NATO kibervédelmi politikájában. Az áttörést a 2016-os Varsói Csúcstalálkozón deklarált azon kitétel hozta meg, amely szerint a kibertér műveleti dimenziónak tekinthető, tehát a kibertér hadviselési dimenzióvá vált. A csúcstalálkozó hivatalos zárónyilatkozata a következőképpen fogalmazott ezzel kapcsolatban: „*[a] számítógépes támadások egyértelműen kihívást jelentenek a Szövetség biztonsága szempontjából, és ugyanolyan károsak lehetnek a modern társadalmak számára, mint a hagyományos támadások. Walesben megállapodtunk abban, hogy a számítógépes védelem része a NATO kollektív védelmi feladatainak. Most Varsóban megerősítjük a NATO védelmi mandátumát, és elismerjük a kiberteret olyan műveleti területnek, amelyben a NATO-nak olyan hatékonyan kell megvédenie magát, mint a levegőben, a szárazföldön és a tengeren.*” (NATO 2016a, idézi: Kovács 2018b)

[85] A kiberhadviselés terminológiai alkalmazása is megváltozott és már kiberműveletek szóhasználattal találkozhatunk a tanulmánykötet címében is.

A Varsói Csúcstalálkozónak volt még egy nagyon fontos hozadéka a kibervédelem területén, ugyanis tagországok elfogadtak egy úgynevezett NATO kibervédelmi felajánlás csomagot (NATO Cyber Defence Pledge) is. Ebben a tagországok a következő képességek és feladatok kialakítását vállalták:

- a nemzeti információs infrastruktúrák és számítógép-hálózatok védelmének teljeskörű fejlesztése;
- a megfelelő nemzeti szintű erőforrások megteremtése, amelyek így a szövetség kibervédelmi képességeihez is hozzájárulnak;
- növelik a kibervédelemben érdekelt felek közötti együttműködést és a legjobb gyakorlatok cseréjét nemzeti szinten is;
- növelik a kiberfenyegetésekkel kapcsolatos ismereteket, amelyekbe beletartozik az információmegosztás és a fenyegetések értékelése is;
- növelik a kiberbiztonsági tudatosságot és a kiberhigiéniát, amelyek a legfejlettebb és legbiztonságosabb kibervédelmen keresztül valósulnak meg;
- növelik a csapatok és erők kiberképzését, kiképzését és gyakorlatait, fejlesztik a képzés intézményi hátterét, amely hozzájárul a bizalom és a tudás magasabb szintjének eléréséhez;
- felgyorsítják a kötelezettségvállalások végrehajtását, beleértve azoknak a nemzeti rendszerek körét is, amelyekre a NATO is támaszkodik;
- a felajánláscsomagban foglaltak végrehajtásának nyomon követésére mutatókon alapuló étékelést készítenek, amelyet a következő csúcsértekezleten megvizsgálnak. (NATO 2016b, Kovács 2018b)

Ugyanakkor nagyon fontos azt látni, hogy csakúgy, mint a katonai képességek jelentős részére a kibervédelem kérdésére a Szövetség alapvetően, mint a tagországok kötelezettségére tekint. A kiberbiztonság, illetve a kibervédelem területén azonban – ahogy azt többször is hangsúlyoztam – egy-egy ország nemzetközi együttműködés nélkül nem képes hatékony eredményeket elérni (ez még akár a képességei kiépítésére is igaz lehet), ezért a tagországok összefogása és folyamatos párbeszéde elengedhetetlenül fontos. *„[e]nnek a párbeszédnek ki kell terjednie az olyan információcserére is, amely a veszélyek és a fenyegetések időbeni felismerésére, vagy az ezek elleni technikai védekezés megoldásaira vonatkoznak.”* (Kovács 2018b)

2017 decemberében még magasabb szintre lépett a NATO kibervédelme, mert a tagországok védelmi miniszterei megállapodtak abban, hogy létrehoznak egy kibervédelmi műveleti központot. Ez a központ a NATO parancsnoki struktúra részét képezve járul hozzá a NATO kiberképességeihez. A NATO főtitkárának bejelentése ezzel kapcsolatban a következőket fogalmazta meg: *„ma a miniszterek megállapodtak egy új Kiberműveleti Központ létrehozásáról, amely a már felvázolt adaptált NATO-parancsnoki struktúra része lesz. Ez erősíteni fogja a kibervédelmünket, és segít integrálni a kiberkérdéseket a NATO tervezésébe és működésébe minden szinten. Egyetértettünk abban is, hogy képesek vagyunk integrálni a tagállamok nemzeti kiberképességeit a NATO missziókba és műveletekbe."* (NATO 2017)

A kiberműveleti központtal a NATO kiberteret érintő történtében egy új korszak is kezdődik. Már nem csak nemzeti, de szövetségi szinten is rendelkezésre áll az a képesség, amely képes a Szövetség érdekei és értékei védelme érdekében kibertevékenységeket folytatni. (Kovács 2018b)

A NATO 2018-as brüsszeli csúcstalálkozója egyrészt megerősítette, hogy a NATO műveleti térnek tekinti a kiberteret, a tagországok teljes mértékben megvalósítják a varsói csúcs után tett – kiberképességekre vonatkozó – vállalásaikat (Cyber Pledge), másrészt megerősítette a kiberműveleti központ[86] létrehozását Belgiumban. (NATO 2018b)

A brüsszeli csúcs zárónyilatkozata a kibertér fenyegetései felsoroláskor több alkalommal is megemlíti és nevesíti is Oroszországot, mint azt a hatalmat, amely a különböző rosszindulatú és befolyásolási célú kibertámadások mögött áll. A nyilatkozat a kibertámadásokat és a különböző rosszindulatú kibertéri műveleteket, mint a hibrid hadviselés része azonosítja. A befolyásolással és a hibrid műveletekkel kapcsolatos orosz támogatást, mint a nemzetközi biztonságot veszélyeztető egyik legfontosabb tényezőt a következőképpen fogalmazza meg a dokumentum: *„Oroszország az euró-atlanti biztonságot és a stabilitást is olyan hibrid akciókkal támadja, mint a széles körben elterjedt dezinformációs kampányok és rosszindulatú internetes tevékenységek, amelyekkel választási folyamatokba és a nemzetek szuverenitásába való beavatkozást kísérelnek meg, ahogy az Montenegróban is történt."* (NATO 2018b)

[86] Fontos annak hangsúlyozása, hogy a tervezett NATO kiberműveleti központnak az egyik legfontosabb feladata – ahogy az a zárónyilatkozatban is szerepel –, hogy a kibertérben történő tevékenységekről információkkal lássa el (helyzetképet biztosítson), valamint hozzájáruljon a NATO műveleti képességeihez. Ez a műveleti képesség minden hadviselési dimenzióra igaz, tehát a kiberműveleti képességek beépülnek a hagyományos dimenziókban folyó katonai műveletekbe.

2.4. Egyes európai országok nemzeti kiberbiztonsági stratégiái

A korábban bemutatott és elemzett nagyhatalmak kibertér vonatkozásában megfogalmazott stratégiái sok elemében eltérő, ugyanakkor sok elemében hasonlóságot mutató módon közelítik meg a kibertér folyamatait és ennem megfelelően alakítják tevékenységüket is.

Ez a fajta – részben eltérő megközelítés – még az olyan országok esetében is igaz, mint a következőkben bemutatni kívánt európai uniós és/vagy NATO tagországok. Korábbi kutatásaim alapján az eltérő megközelítések okaira a következő választ találtam: *„[a] különböző megközelítésékben tapasztalható eltéréseknek okait kutatva arra a következtetésre juthatunk, hogy ezek elsősorban abban fedezhetők fel, hogy az adott ország a technikai és technológia, az információs társadalom és annak fejlődését és zavartalan működését, illetve a kritikus információs infrastruktúrák védelmét tekintette-e korábban kiinduló pontnak."* (Kovács 2018b)

Természetesen sok olyan tényező is megtalálható a vizsgált európai országok kiberbiztonsági stratégiáiban, amelyek nagyban hasonlítanak egymásra. Ezek az azonos elemek vagy a szövetségi tagságból és az abban lévő – sok esetben kötelező érvényű szabályozásból (például az EU esetében ilyen a NIS direktíva) – vagy abból ered, hogy nagyon hasonló kibertéri kihívásokat azonosított az adott ország. Az egyik azonos elem a kiberbiztonság beemelése a nemzeti biztonsági stratégiába, majd ebből következően a nemzeti kiberbiztonsági stratégia legfontosabb céljainak olyan alakítása, amelyek a nemzeti biztonsági stratégia legfőbb céljai megvalósításának irányába hatnak. Tehát a nemzeti kiberbiztonsági stratégia ezekben az országokban nagyban épít a nemzeti biztonsági stratégiában megfogalmazott legfontosabb elvekre és a kiberbiztonsági célokkal támogatja az adott ország nemzeti biztonsági stratégiáját. (Kovács 2018b)

Mindezeknek megfelelően a következőkben megvizsgálni kívánt európai uniós és – Ausztria kivételével – NATO tagországok esetében szükséges a nemzeti biztonsági stratégia, és számos esetben az ezzel szorosan összefüggő katonai stratégia vizsgálata, mert ezek határozzák meg azokat a legfontosabb stratégiai célokat, amelyeket az adott országban az ágazati stratégiák – így a kiberbiztonsági stratégia – segítségével meg kell valósítani a biztonság érdekében.

A következőkben az Európai Unió tagországai közül 10 ország nemzeti biztonsági- és nemzeti biztonsági stratégiáit, valamint az ezekre épülő kiberbiztonsági stratégiáit mutatom be. Ezek alapján kívánok általános érvényű következtetéseket levonni arra vonatkozóan, hogy melyek azok a stratégiai szinten azonosítható elemek, amelyek segítségével hatékony

nemzeti kiberbiztonság alakítható ki. Az elemzéseket a következő országok stratégiái és a következő vázlatos indokok alapján kívánom elvégezni:

- Ausztria: bár gazdaságát tekintve lényegesen fejlettebb, mint hazánk, de szomszédos országként hasonló geopolitikai kihívásokkal néz szembe;
- Cseh Köztársaság: Visegrádi országként hazánk egyik fontos partnere, régiós szerepéből adódóan pedig hasonló kibertéri fenyegetettségek van kitéve, mint Magyarország;
- Egyesült Királyság: Európa és a világ egyik legnagyobb gazdaságaként nagyban kitett a kibertéri folyamatoknak. (Az értekezés írása idején még ez Európai Unió tagja);
- Észtország: balti országként speciális geopolitikai helyzetben van, valamint a 2007-es, az országot ért kiberincidensek után a világ első olyan országa, amely önálló nemzeti kiberbiztonsági stratégiát dolgozott ki;
- Franciaország: Európa egyik legnagyobb gazdasága, szerepe így a gazdaság mellett az európai politikában is meghatározó;
- Hollandia: fejlett gazdasága és fejlett információs társadalma példaértékű lehet a nemzeti kiberbiztonsági stratégia vonatkozásában is;
- Magyarország: hazánk már a 2000-es évek óta rendelkezik az információs társadalom kialakítását, majd annak fejlesztését célzó stratégiákkal, de a digitális gazdaság és társadalom területén, illetve ezek egyes szegmenseiben nagy az elmaradás az EU-s átlaghoz képest. Ezért vizsgálat tárgyát kell, hogy képezze az a kérdés, hogy a kiberbiztonság mennyiben befolyásolja az információs társadalom – mai szóhasználattal élve: digitális társadalom – fejlődését. A kiberbiztonság 2013-ban nemzeti stratégiában is megjelenik, de annak ismételt felülvizsgálata szükséges. Meg kell jegyezni, hogy a hazai nemzeti kiberbiztonsági stratégia jelen értekezés írásakor felülvizsgálat alatt áll. Azonban az új stratégia szövege még nem nyilvános, így annak felhasználása nem lehetséges a dolgozatban;
- Lengyelország: Kelet-Közép Európa egyik legnagyobb országaként, valamint a Visegrádi országok tagjaként stratégiai elképzelései a kiberbiztonságról meghatározóak lehetnek;
- Németország: Európa, és a világ egyik legfontosabb és egyik legnagyobb gazdasága. Ugyanakkor ennek a gazdaságnak a kibertérrel való számtalan

kapcsolódási pontja függőséget is jelent nem csak Németország, hanem közvetett módon a világgazdaság számára is. Ennek megfelelően célszerű megvizsgálni, hogy a világ egyik vezető gazdaságával rendelkező ország hogyan kezeli a kibertér kihívásait és veszélyeit;

- Szlovák Köztársaság: hazánkhoz hasonló méretű és gazdasági teljesítőképességű ország, valamint a Visegrádi országok tagja, ennek megfelelően ebben az esetben is célszerű megvizsgálni a kibertér biztonságáról alkotott stratégiai elképzeléseit.

2.4.1. Ausztria

Ausztria nemzeti biztonsági stratégiája

Ausztria nemzeti biztonsági stratégiája *Biztonság az új évtizedben, a biztonság megteremtése* (német eredeti címen: Österreichische Sicherheitsstrategie Sicherheit in einer neuen Dekade – Sicherheit gestalten, angolul Austrian Security Strategy Security in a new decade— Shaping security) címmel 2013-ban jelent meg. A stratégia rögtön annak legelején a kihívások, kockázatok és veszélyek számbavételekor tartalmaz utalásokat a kibertérre. Az infokommunikációs rendszerekkel szembeni legfontosabb veszélyként a kibertámadásokat nevezi meg a stratégia. (Ausztria 2013a, Ausztria 2013b, Kovács 2018b)

A dokumentum Ausztria belső biztonsága szempontjából kiemelt fontosságúnak tartja a kiberteret: *„[a] kiberbűnözés, a kibertámadások, az internet szélsőséges célokra való alkalmazása és a hálózat biztonsága komoly új kihívások jelent az összes érdekelt fél számára, így széles körű és átfogó együttműködésre van szükség."* (Ausztria 2013b, idézi: Kovács 2018b)

Ausztria nemzeti biztonsági stratégiája markánsan tartalmazza az ország védelmi politikáját is, így az kitér a hadsereg feladataira is. Az osztrák haderő számára előírja a kiberképességek kiépítését, azok fejlesztését, valamint a kibertámadások kezelésére való felkészülést. Mindezeket a következő formában adja meg a stratégia: *„[a] szubkonvencionális fenyegetések vagy a kibertámadásokból eredő új kockázatok kezelése új katonai tevékenységeket is jelenthetnek.* (Ausztria 2013b, idézi: Kovács 2018b)

Ebbe a meghatározott katonai tevékenységi körbe azonban sok minden belefér, de a stratégia alapvetően védelmi jellegű filozófiája miatt ez nyilvánvalóan a hadsereg kibervédelmi képességeinek emelését jelenti. Ezt támasztja alá az is, hogy a stratégia a katonai rendszerek kibervédelme érdekében akár az azok üzemeltetésében szerepet vállaló civil szereplők bevonását határozza meg, illetve elrendeli hadsereg és az osztrák Kiber Krízis

Menedzsment, amely legfontosabb szereplői a belügyi, illetve civil intézmények, szorosabb együttműködését. Nagyon érdekes, és Európában meglehetősen szokatlan módon a stratégia a hadsereg feladataként megjelöli a kritikus infrastruktúrák és a szélesebb értelemben vett kibertéri védelemben való közreműködést is. (Ausztria 2013b, Kovács 2018b)

A biztonsági stratégia a feltárt veszélyek kezelése érdekében ajánlásokat fogalmaz meg. Közvetett módon az egyik legfontosabb ilyen ajánlás a stratégia rendszeres felülvizsgálatára vonatkozik. Ez az ajánlás már az egyik fontos eleme lehet annak az eszközkészletnek, amely alapján biztosítható, hogy ne csak egy statikus dokumentum legyen a stratégia, hanem a folyamatosan változó és átalakuló környezethez dinamikusan alkalmazkodó valódi stratégia alakulhasson ki.

A stratégia egy másik fontos eleme egy a kiberbűnözésre szakosodott kiválósági központ létrehozására tett javaslat, amellyel párhuzamosan az európai uniós kiberbiztonsági politikák kialakításához való osztrák hozzájárulás is szükséges az állampolgárok és a vállalkozások kibertérben való hatékonyabb védelme érdekében. (Ausztria 2013b, Kovács 2018b)

Ausztria nemzeti kiberbiztonsági stratégiája

A fentiekben ismertetett osztrák nemzeti biztonsági stratégia meghatározta egy nemzeti kiberbiztonsági stratégia elkészítését. Ez 2013 tavaszán kiadásra is került, amely német címe *Österreichische Strategie für Cyber Sicherheit*, angol címe *Austrian Cyber Security Strategy*[87]. (Ausztria 2013c)

Ausztria nemzeti kiberbiztonsági stratégiája modell értékű abban a tekintetben, hogy az nagyban épít a nemzeti biztonsági stratégiában megfogalmazott alapelvekre és stratégiai célokra. A dokumentum a bevezető után felsorolja a kibertérben jelentkező lehetőségeket és az ott megjelenő veszélyeket. Mindezt úgy teszi meg, hogy kibertér, illetve az infokommunikációs technikában rejlő lehetőségek bemutatása lényegesen nagyobb hangsúlyt kap, mint a veszélyek. A stratégia nagy lehetőségként értékeli az információs és kommunikációs teret, mint olyan társadalmi interakciók megvalósítására alkalmas új teret, amelyben a gazdaság és kereskedelem, a politika, de akár a különböző fizikai folyamatok irányítása (például az IoT eszközök és azok infrastruktúrákban történő alkalmazása) az

[87] Nagyon előremutató és több célt szolgáló tényező, hogy az adott ország nemzeti biztonsági stratégiája, és ahogy ebben az az esetben látható nemzeti kiberbiztonsági stratégiája nem csak az adott ország hivatalos nyelvén, hanem angolul is kiadásra kerül. Ez hozzájárul, hogy valóban széles, nemzetközi körben is elérhetővé és érthetővé váljon az adott ország biztonsági felfogása, annak stratégiai alapjai. Ugyanakkor emellett ez üzenet értékű is lehet, mert az abban foglaltak világosan láthatóak, és akár – ahogy a későbbiekben utalni fogok rá – az elrettentés célját is szolgálhatja. (Kovács 2018b)

eddiginél hatékonyabban megvalósulhassanak. Mindezek a lehetőségek részletesen is elemzésre kerülnek, amíg a kockázatok és veszélyek egyetlen bekezdésbe sűrítve jelennek csak meg. (Kovács 2018b)

Ugyanakkor a stratégia a mellékletében bemutat egy kiberkockázati mátrixot, amely a veszélyek bekövetkezési valószínűsége függvényében adja meg azok lehetséges következményeinek nagyságát. Ehhez számos kockázati tényezőt mutat be, bár mindezek a stratégia megjelenését megelőzően két évvel korábban készültek. (Ausztria 2013d, Kovács 2018b)

A stratégiában megfogalmazott legfontosabb stratégiai célitűzések a következők:

- biztonságos kibertér megteremtése, amelynek a kockázatok és veszélyek kezelése miatt megfelelően redundásnak kell lennie;
- Ausztria biztosítja a biztonságos kiberteret, amely során a köz- és a magánszektor együttműködése elengedhetetlen;
- a kiberbiztonság jogi kereteinek megteremtése, illetve annak megvalósítása a különböző osztrák hatóságok, illetve azok magánszektorral történő együttműködése révén valósítható meg;
- Ausztria kiberbiztonsági kultúra építésébe kezd;
- a kiberbiztonság területén meglévő magán és közszféra közötti párbeszéd, valamint az új kezdeményezések a digitális társadalom területén olyan pozitív hatással vannak, amelyek többek között az üzleti befektetéseket is ösztönzi, így ezeket folytatni szükséges;
- Ausztria folytatja a kiberbiztonság területén lévő nemzetközi párbeszédre és együttműködés ösztönzésre irányuló tevékenységét;
- folytatni kell az e-kormányzati megoldások kiberbiztonságának növelését a szövetségi szinttől kezdődően a közigazgatás minden szintjéig;
- együttműködés szükséges az osztrák vállalatok kiberbiztonsági tevékenységeinek támogatásában;
- az állampolgárok kiberbiztonság tudatosságának növelése szükséges. (Ausztria 2013d, Kovács 2018b)

A stratégia a legfontosabb célok elérése érdekében úgynevezett akcióterületeket ad meg:

- a kiberbiztonság szerkezeti hátterének és folyamatainak kialakítása: ezen belül szükséges egy Kiberbiztonsági Irányító Csoport felállítása, amely alapvetően

koordináló szerepet tölt be, és amely a Nemzeti Biztonsági Tanács felé összekötőkkel rendelkezik. Ez a csoport lesz majd az egyik legfontosabb szereplője a stratégiában megfogalmazottak implementálásának is. E mellett műveleti szintű koordináló szervezetek felállítása is szükséges, például GovCERT (Government Computer Emergency Response Team, Kormányzati eseménykezelő csoport, MiLCERT (Military Cyber Emergency Readiness Team, Katonai kibervészhelyzeti készenléti csoport), C4 (Cyber Crime Competence Center, Kiberbűnözés kompetencia központ). Az állami szereplők mellett szükséges a kritikus infrastruktúra területen is a koordináló szervezetek kialakítása. Fel kell állítani egy krízis menedzsmentet, valamint erősíteni kell a már meglévő kiberbiztonsági struktúrát;

- a kormányzat feladatai: korszerű szabályozási környezetet kell kialakítani, meg kell határozni a minimum követelményeket, valamint éves jelentéseket kell előkészíteni a kiberbiztonságról;
- a kormányzat, a gazdaság és a társadalom közötti együttműködés: egy kiberbiztonsági platformot kell létrehozni, amely a kiberbiztonság szereplői között a PPP együttműködéseket tudja ösztönözni. Erősíteni kell a kis- és közepes vállalatok kiberbiztonsági támogatását, valamint elő kell készíteni egy kiberbiztonsági kommunikációs stratégiát;
- kritikus infrastruktúra védelem: a kritikus infrastruktúra szektorokban lévő kiberbiztonság erősítése és hozzájárulás a már meglévő osztrák kritikus infrastruktúra védelmi tervhez (Programm zum Schutz kritischer Infrastrukturen, APCIP);
- tudatosság növelése és képzés: a kiberbiztonsági kultúra növelése érdekében minden oktatási szinten be kell építeni a kiberbiztonságra vonatkozó ismereteket;
- kutatás és fejlesztés: nemzeti és EU-s kiberbiztonsági kutatás-fejlesztési programok ösztönzése és támogatása;
- nemzetközi együttműködés: az EU, az ENSZ, az EBESZ, az Európa Tanács, az OECD, illetve a NATO partnerségből adódó nemzetközi kapcsolatokat fel kell használni az európai, illetve a világméretű kiberbiztonság erősítésére. (Ausztria 2013d, Kovács 2018b)

2.4.2. Cseh Köztársaság

A Cseh Köztársaság nemzeti biztonsági stratégiája

2015-ben került kiadásra a Cseh Köztársaság jelenleg érvényes új nemzeti biztonsági stratégiája. A dokumentum a biztonsági stratégiák klasszikus és már említett felépítését követve elsőként leírja az ország biztonsági alapelveit, majd meghatározza azokat az értékeket, amelyek Csehország számára a biztonság területén a legfontosabbak. A stratégia már eben a felsorolásban utal a kibertérre, és kinyilvánítja, hogy a kibertér biztonságának megőrzése az egyik legfontosabb érdeke az országnak. (Cseh Köztársaság 2015b)

A stratégia az ország biztonsági környezetének bemutatása során értékeli és röviden elemzi a legfontosabb tényezőket és trendeket. A dokumentum itt megállapítja: *„[a]zok a szereplők, akik egyre növekvő ambícióik miatt érdekeik elérése érdekében hajlandóak katonai erőiket használni vagy azzal fenyegetni, nagymértékben befolyásolják a biztonsági környezet stabilitását. Ezeknek a szereplőknek a törekvései katonai képességeik jelentős növelésével járnak együtt, beleértve a támadó kiberképességeket, a tömegpusztító fegyvereket és azok szállítási eszközeit, valamint a kulcsfontosságú nyersanyagok iránti növekvő igényüket, a pénzügyi piacokon folytatott tevékenységüket, a stratégiai területeken való befolyásoló tevékenységüket és a politikai ambícióik fokozódó agresszív előmozdítását nemzetközi fórumokon. Egyes államok azon próbálkozása, hogy politikai, gazdasági és katonai nyomással, valamint hírszerző tevékenységük kombinációján keresztül kiterjesszék befolyásukat, fenyegetést jelentenek; ezek a befolyásolások és tevékenységek a kibertérben is előfordulnak."* (Cseh Köztársaság 2015b, idézi: Kovács 2018b)

A stratégia egyik legfontosabb nem katonai típusú veszélyforrásként értékeli – számos más veszéllyel együtt – a kibertámadások jelentette fenyegetést. A stratégia kibertámadásokkal kapcsolatban a kitér a kibertér néhány olyan jellegzetességére, amelyek az abban rejlő veszélyeket hatványozottabbá teszik. Ilyen jellemzők a kibertérre vonatkoztatva: annak határok nélkülisége vagy a fenyegetések forrása és a fenyegetések célpontjai közötti távolság relatívvá válása. A dokumentum utal arra, hogy a kibertámadások aszimmetrikus jellegűek, ennélfogva nem csak az állami szereplők, de államnál kisebb entitások is kivitelezhetnek kibertámadásokat, amelyek célpontjai a cseh infrastruktúra, illetve maga az állam digitális rendszerei lehetnek. A stratégia nevesíti a legfontosabb kritikus szektorokat, úgymint: kommunikáció, energia, közlekedés, pénzügy, ipar hálózatai. Ezeket a szektorokat, illetve az ezekben lévő információs rendszereket tekinti Csehország a

legfontosabb olyan infrastruktúráknak, amelyek kitettsége a legnagyobb a kibertámadásokkal szemben.

A stratégia kitér a kibertérben folyó politikai és gazdasági kémkedés veszélyessége mellett a katonai információs rendszerek elleni kibertámadásokra is. A katonai rendszerek ilyen támadások hatására bekövetkező működésképtelensége az állam védelmének egyik legfontosabb pillérében okoznak fennakadásokat. (Cseh Köztársaság 2015b, Kovács 2018b)

A stratégia meghatározza azokat a szükséges védelmi intézkedéseket, amelyek a feltárt veszélyforrások kezelésére, illetve azok csökkentésére kell, hogy irányuljanak. Ennek során a dokumentum kitér a kibertámadásokkal szemben szükséges intézkedésekre, valamint a kritikus információs infrastruktúrák védelmére is.

A védelem megvalósítása érdekében a stratégia elrendeli egy, a 2015-2020 évekre vonatkozó nemzeti kiberbiztonsági stratégia elkészítését, valamint a kibertámadások elleni fellépéshez szükséges szervezeti háttér kialakítását. Ebben a szervezeti rendszerben kiemelt szerepet szán a kormányzati CERT-nek. A CERT mellé, annak operatív feladatai ellátásának támogatására hatósági jogkörökkel felruházva, a nemzeti szintű kiberbiztonsági kérdések koordinációjára a stratégia a Nemzeti Biztonsági Hatóságot jelöli ki. E hatóságon belül elrendeli egy Nemzeti Kiberbiztonsági Központ kialakítását. E szervezeti elem egyik feladatául a nemzeti és a nemzetközi kiberbiztonsági korai előrejelző rendszerben való részvételt és a nemzetközi koordinációban Csehország képviseletét rendeli el. (Cseh Köztársaság 2015b, Kovács 2018b)

A Cseh Köztársaság nemzeti kiberbiztonsági stratégiája

A Cseh Köztársaságban 2008-ban jelent meg a Nemzeti Biztonsági Kutatási Stratégia, amely a biztonság fejlesztésére irányult, de közvetett módon már tartalmazott utalásokat például a kritikus infrastruktúrákra (beleértve az energia-, víz-, élelmiszer-, a közlekedés, banki és pénzügyi, az IKT szektorokat stb). (Kovács 2012)

Az első olyan stratégia, amely az információs rendszereket érintette 2011 év elején került kiadásra. Ez a Digitális Cseh Köztársaság stratégia volt, amely még fejlesztési irányok meghatározását, például a nagy sebességű hálózati hozzáférés kialakítását és elterjesztését tűzte ki célul. (Kovács 2012)

A Cseh Köztársaság első kiberbiztonsági stratégiája szintén 2011-ben jelent meg. Ez a 2011-2015 közötti időszakra határozta meg az akkori nemzeti biztonsági stratégiára alapozva azokat a legfontosabb elveket és feladatokat, amelyeket Csehországnak a

kiberbiztonság területén el kell látnia. A stratégia fő célja Csehország számítógépes biztonságának megszilárdítása, valamint egy megfelelő jogi háttérrel rendelkező információs társadalom kialakítása. Az információs társadalom kialakításával kapcsolatban a stratégia a biztonságos és szabad információtovábbítás és -feldolgozás fontosságát hangsúlyozta. A stratégiában megfogalmazott főbb célok a következők voltak:

- a kiberbiztonság jogszabályi hátterének kidolgozása;
- a közigazgatás és a kritikus infrastruktúrák kiberbiztonságának erősítése;
- nemzeti CERT megalapítása;
- nemzetközi együttműködés fokozása;
- együttműködés erősítése az állam, a magánszektor és az akadémiai szektor között;
- a kiberbiztonság tudatosságának növelése. (Kovács 2012, Kovács 2018b)

A 2011-es nemzeti kiberbiztonsági stratégiát 2015-ben egy új stratégia követte, amely címe Nemzeti Kiberbiztonsági Stratégia 2015-2020. Ennek kidolgozója a korábbi nemzeti biztonsági stratégiában előrevetített szervezet a Nemzeti Kiberbiztonsági Központ volt.

A stratégia meghatározza azokat az alapelveket, amelyek a nemzeti kiberbiztonság területén a legfontosabbak Csehország esetében. Ezek az alapelvek: az alapvető emberi jogok és a demokratikus szabályok védelme; az átfogó megközelítés, a szubszidiaritás és együttműködés elve; a köz- és magánszféra közötti együttműködés erősítése; a kiberbiztonsági képességek növelése. (Cseh Köztársaság 2015d, Kovács 2018b)

A stratégia által megfogalmazott célkitűzések között szerepel a legújabb kiberfenyegetettségeknek ellenálló kiberképességek kiépítése, valamint a nemzetközi együttműködésben való aktív és hatékony együttműködés, amely a NATO-n és az Európai Unió-n belüli, de bilaterális együttműködési keretek közötti együttműködéseket is előirányozza.

A dokumentum külön kitér a kritikus információs infrastruktúrák védelmére is, amely során hangsúlyozza: *„nem elegendő az egyes elemek védelmére koncentrálni, hanem szükséges a hálózatok egységes, az egész kibertérre – ebbe beleértve a teljes lakosságot is – kiterjedő komplex biztonságának megteremtése.”* (Kovács 2018b)

A kiberbiztonság megteremtése érdekében a stratégia a kormányzati CERT-nek (GovCERT.CZ) szánja a legfontosabb feladatot, amelybe az ágazati CERT-ek és/vagy CSIRT-ek koordinációja is beletartozik[88]. (Cseh Köztársaság 2015d, Kovács 2018b)

A stratégia több mint egy tucat, a kiberbiztonságra negatív hatással lévő veszélyt és kihívást azonosít. Ezek a veszélyek és kihívások a következők:

- Csehország, mint tesztalany: a csehországihoz hasonló fejlett infrastruktúrával és hálózati kiépítéssel rendelkező, de stratégiailag fontosabb országok támadásához szükséges felkészüléshez a cseh infrastruktúrákon való kibertámadások kipróbálása és tesztelése;
- bizalom megrendülése az államban: a kiberbiztonság állam által való szavatolásában, illetve az ezt biztosítani hivatott szervezetekben a bizalom megrendült, így mind az állampolgárok, mind a magánszektor önkéntes együttműködése az állammal kérdéses;
- az internethasználók számának és a kritikus technológiai hibáknak a növekedése;
- a mobil eszközöket használók számának, illetve ezzel párhuzamosan a mobil eszközökön megjelenő kártékony kódoknak a növekvő száma;
- a hardveres hátsóajtókon keresztüli információszivárgások növekedése;
- Internet of Things: a hálózatba kötött eszközök számának exponenciális növekedésével nem nőtt arányosan a kiberhigiénia;
- az IPv4 és IPv6 átállás biztonsági problémái;
- az e-kormányzat biztonsági kihívásai;
- a kis- és közepes vállalkozások nem kielégítő biztonsága;
- big data és az új adattárolási módszerek kihívásai;
- az ipari irányító rendszerek védelme és az egészségügy információs rendszerei;
- okos hálózatok: az alapvetően a jövő energiaellátásában kulcsszerepet játszó olyan eszközök biztonsága, amelyek a hatékony energiatermelésben és -elosztásban működnek;
- a védelmi szektor növekvő függősége az infokommunikációs eszközökkel és rendszerekkel szemben;
- a fejlett rosszindulatú szoftverek számának növekedése;

[88] A nemzeti kiberbiztonsági stratégia céljainak elérése érdekében Csehország egy akciótervet határozott meg a 2015-2020-as évekre, amelyben a célok mellé feladatokat, azok felelős szervezeteit (például minisztériumok, hivatalok, ügynökségek) és határidőket rendelt. (Cseh Köztársaság 2015e)

- botnetek, DoS (Denial of Servic, azaz túlterheléses támadás) és DDoS támadások;
- növekvő kiberbűnözés;
- a közösségi médiumok biztonsági kihívásai;
- a felhasználók alacsony szintű digitális tudása;
- kiberbiztonsági szakértők alacsony száma, valamint a képzésük reformjának szükségessége. (Cseh Köztársaság 2015d, Kovács 2018b)

A stratégia ezeknek a veszélyeknek az elhárítása, valamint a kihívásoknak való megfelelés érdekében nyolc fő feladatcsoportot határoz meg:

- a kiberbiztonsághoz szükséges minden szervezet, folyamat és együttműködés hatékonyságának növelése: a CERT-ek, CSIRT-ek és a kritikus információs infrastruktúrák védelmét biztosító szervezetek együttműködésének javítása, a nemzeti incidenskezelési képesség növelése, valamint a folyamatosan növekvő és fejlődő kihívásokra adandó válaszul a nemzeti biztonsági és a nemzeti kiberbiztonsági stratégia felülvizsgálata;
- aktív nemzetközi együttműködés: az EU, NATO, ENSZ és EBESZ különböző programjaiban való részvétel, valamint a közép-európai térségben a kiberbiztonság területén szükséges országok közötti párbeszéd elősegítése[89], nemzetközi kibergyakorlatok és képzések szervezése, valamint a nemzetközi jogi szabályozás és jogi keretek kialakításának felgyorsítása;
- a nemzeti kritikus információs infrastruktúrák és kiemelt információs rendszerek[90] védelme: világos eljárásrend kialakítása a kritikus infrastruktúrákat fenyegető veszélyek folyamatos elemzése, az infrastruktúrák ellenállóképessége és megbízhatósága növelése érdekében, valamint a Nemzeti Kiberbiztonsági Központ és a GovCERT.CZ technikai képességeinek, illetve humánerőforrásának fejlesztése, képzése és oktatása;
- együttműködés a magánszektorral: a magánszektor számára egy megbízható és biztonságos kibertér megteremtése, amely növeli a bizalmat, a kutatás-fejlesztési kedvet, valamint növelni kell a magánszektor biztonságtudatosságát képzésekkel,

[89] Erre az együttműködésre jó példa a cseh és osztrák kezdeményezésre létrejött Közép-Európai Kiberbiztonsági Platform. Ebben a két említett országon kívül hazánk, Lengyelország és Szlovákia is részt vesz. (Kovács 2018b)

[90] A stratégia kiemelt információs rendszereket (Important Information Systems, IIS) is meghatározott.

felvilágosító kampányokkal, illetve olyan megbízható információmegosztási platformot kell kialakítani, amely mindehhez hozzájárulhat;

- kutatás-fejlesztés és vásárlói bizalom: részt kell venni az európai kiberbiztonságot érintő kutatásokban, a Nemzeti Biztonsági Hatóság, mint kapcsolattartó kijelölése, együttműködés a magán- és az akadémiai szférával, valamint a kutatás-fejlesztést nemzeti prioritássá kell tenni;
- oktatás, biztonságtudatosság növelése, és az információs társadalom fejlesztése: az általános- és középiskolákban növelni kell a kiberbiztonságra való nevelést, valamint olyan biztonságtudatosító kampányokat kell szervezni, amelyek széles hallgatósághoz jutnak el, növelni kell a közigazgatásban dolgozók kiberbiztonsági oktatását, amelyben többek között meg kell, hogy jelenjen a kiberbűnözés veszélyeire történő figyelemfelhívás is;
- a cseh rendőrség kiberbűnözés elleni képességeinek fejlesztése: humán és technológiai erőforrás fejlesztés szükséges, valamint szükséges a nemzetközi együttműködés fokozása a területen;
- kiberbiztonság jogszabályi háttere: a meglévő jogszabályi környezetet figyelembe véve ki kell alakítani, illetve korszerűsíteni kell azokat a jogszabályokat, amelyek a kiberbiztonsághoz szükségesek, a megfelelő jogi oktatási háttér kialakításával együtt, mindezeket úgy kell megtenni, hogy a folyamatosan változó technikai kihívások, illetve a gyorsan fejlődő információs társadalom követelményeinek megfeleljenek. (Cseh Köztársaság 2015d, Kovács 2018b)

2.4.3. Egyesült Királyság

Az Egyesült Királyság nemzeti biztonsági stratégiája

Az Egyesült Királyságban 2010-ben került kiadásra a már címében is sokat sejtető nemzeti biztonsági stratégia. Az *Erős Nagy-Britannia a bizonytalanság korában: a Nemzeti Biztonsági Stratégia* (A Strong Britain in an Age of Uncertainty: The National Security Strategy) címmel megjelent dokumentum a hidegháború vége óta már a második nemzeti biztonsági stratégia az országban. A stratégia több módosításon esett át, először 2012-ben, majd 2015 novemberében. Ezekből a 2015-ös módosítás számos elemre kiterjedő

felülvizsgálat eredményeként született, és szerkezetében is új dokumentumot eredményezett. (Egyesült Királyság 2015, Kovács 2018b)

Ugyanakkor a stratégia 2010-es eredeti verziójában a kibertámadások, mint veszélyforrások már a dokumentum előszavában megjelennek. Rendhagyó módon a stratégia bevezetője felsorolja a brit Nemzeti Biztonsági Tanács által megfogalmazott kiemelt veszélyforrásokat:

- a nemzetközi terrorizmus, benne a vegyi fegyverek esetleges alkalmazása, valamint az Észak-Írországhoz kapcsolódó terrorizmus;
- a kibertámadások, amelyek mögött más államok, a szervezett bűnözés, vagy terrorszervezetek állhatnak;
- a nemzetközi katonai válságok;
- nagy ipari, vagy természeti katasztrófák. (Egyesült Királyság 2010, Kovács 2018b)

Ezeknek a veszélyeknek az Egyesült Királyságra gyakorolt hatásait elemezve a kibertérre vonatkozóan a következőket állapítja meg a stratégia: *„[a]z ellenfelek, akikkel szembe nézünk, változni fognak és diverzifikálódnak, mivel ellenségeink olyan fenyegető vagy támadási eszközöket keresnek, amelyek olcsóbbak, könnyebben elérhetők és kevésbé hasonlítanak a hagyományos hadviselésre. Ezek közé tartozik az ellenséges hírszerzés, a kibertámadás, a kritikus szolgáltatások megzavarása és az állampolgárok vagy kormányok rosszindulatú befolyásának gyakorlása."* (Egyesült Királyság 2010, idézi: Kovács 2018b)

A 2015-ös biztonsági felülvizsgálat során létrejött új dokumentumban, amely új címet is kapott: *Biztonságos és prosperáló Egyesült Királyság* (National Security Strategy and Strategic Defence and Security Review 2015 A Secure and Prosperous United Kingdom), azonban ennél már lényegesen markánsabban jelenik meg a kibertér és annak szerepe, valamint a kibertéri veszélyek. A kibertámadások, mint veszélyforrások a stratégiai célkitűzésekre is hatással vannak. Ennek megfelelően a kiberbiztonság területén – a dokumentum címében megfogalmazott prosperáló Egyesült Királyság eléréséhez hozzá járulva – nagyon kemény és innovatív intézkedések meghozatala és azok bevezetése szükséges. Ezek csak úgy képzelhetők el, ha az Egyesült Királyság a világ vezető hatalmai közé emelkedik ezen a téren. (Egyesült Királyság 2015, Kovács 2018b)

A stratégia egy külön fejezetet szentel a technológia szerepének, amelyben a kiberteret alkotó hálózati és információtechnológia szerepére is kitér, nem titkolva az abban rejlő veszélyeket: *„[a]z Egyesült Királyságot fenyegető kiberszereplők köre folyamatosan nő. A*

fenyegetés egyre inkább aszimmetrikus és globális. A megbízható, következetes kibervédelem tipikusan fejlett készségeket és jelentős befektetéseket igényel. Ám egyre nő azoknak az országoknak a száma, akik állami szintű erőforrásokkal, olyan fejlett kiberképességeket fejlesztenek ki, amelyek konfliktusokban potenciálisan alkalmazhatók, többek között a nemzeti kritikus infrastruktúra és a kormányzati intézmények ellen. A nem állami szereplők, ideértve a terroristákat és a kiberbűnözőket is, könnyen elérhető számítógépes eszközöket és technológiát használhatnak fel destruktív célokra." (Egyesült Királyság 2015, idézi: Kovács 2018b)

A stratégia a hadsereg számára is fogalmaz meg stratégiai alapelveket. Ilyen alapelv az *Egyesített Fegyveres Erő 2025* (Joint Force 2025) koncepcionális alapjainak meghatározása is. Ebben markáns szerepet kap a kiberképességek fejlesztése, amely stratégiai vezetési szinten kibercsoport felállítását is előirányozza.

Maga a stratégia az elrettentésre épül, amely többször is hangsúlyosan megjelenik a dokumentumban. Ennek során a dokumentum kijelenti, hogy *„a polgárok védelme érdekében az elrettentés fenntartása érdekében a képességeinek teljes spektrumát használni fogjuk, beleértve a katonai erőt és a kibertámadásokat is."* (Kovács 2018b)

A dokumentum leszögezi, hogy az Egyesült Királyság kibernagyhatalom, amelynek kialakításához mind az üzleti, mind a kormányzati szektor, beleértve a nemzetbiztonsági szolgálatokat és a védelmi szférát is nagyban hozzájárult. Ehhez a kibernagyhatalmi státusz eléréséhez szükséges volt a 2011-ben elkészült nemzeti kiberbiztonsági stratégia, amely mellé a kormány anyagi erőforrásokat is rendelt, valamint az ebben meghatározott szervezeti rendszer kialakítása is, hiszen így állt fel a Kiber Értékelési Központ (Centre for Cyber Assessment), illetve az Egyesült Királyság CERT-je (UK's Computer Emergency Response Team, CERT-UK). (Egyesült Királyság 2015)

A stratégia a nemzeti biztonsági stratégiák esetében szokatlanul nagyon részletesen elemzi a kiberteret, annak egyes elemeit, és ugyanígy szokatlan azoknak a tevékenységeknek a részletezése is, amelyek a kiberbiztonság megteremtése érdekében szükségesek. A stratégia ezekben a részletes bemutatásokban kitér a kibertámadások detektálására, az ellenük való védekezésre, valamint a válaszreakciók igényelte feladatokra is. Hasonló részletességgel kerül meghatározásra a kiberbűnözés elleni tevékenység, azon belül is például a Nemzeti Kiberbűnözés Elleni Egység (National Cyber Crime Unit, NCU) felállítása és képességeinek fejlesztése, de a nemzetközi téren szükséges kiberbiztonsági teendők meghatározása is. (Egyesült Királyság 2015, Kovács 2018b)

A stratégia tárgyalja a kritikus infrastruktúrák védelmét, benne a kiberbiztonság meghatározó szerepével. Ezen a területen többek között a kritikus infrastruktúra tulajdonosok és üzemeltetők számára szükséges kiberbiztonsági képzések kialakítását irányozza elő, mindamellett, hogy a terület szabályozásához el kell készíteni a megfelelő kibervédelmi ajánlásokat is. (Egyesült Királyság 2015, Kovács 2018b)

A stratégia az átfogó megközelítés elvét alkalmazva a gazdasággal kapcsolatosan külön kiemeli a kiberbiztonsági szektor növekedésének ösztönzését: *„[ö]sztönözni fogjuk az élénk kiberbiztonsági ágazat létrehozását és növekedését, beleértve két innovációs központ létrehozását; a legkorszerűbb kiber KKV-k támogatását; és hozzá kívánunk járulni az egyetemeken folyó kutatások eredményeinek kereskedelmi forgalomba hozatalához."* (Egyesült Királyság 2015, idézi: Kovács 2018b)

Az Egyesült Királyság nemzeti kiberbiztonsági stratégiája

Az Egyesült Királyság első kiberbiztonsági stratégiája 2011-ben jelent meg *Az Egyesült Királyság védelme és támogatása a digitális világban* (The UK Cyber Security Strategy Protecting and promoting the UK in a digital world) címmel. Az ebben megfogalmazott stratégiai célok a következők:

- a kiberbűnözés elleni küzdelem;
- a kibertámadásokkal szembeni ellenállóképesség növelése;
- biztonságos kibertér kialakítása a társadalom számára;
- kiberképességek, készségek és lehetőségek kiépítése, amelyek segítségével a biztonsági célkitűzések elérhetőek. (Egyesült Királyság 2011, Kovács 2018b)

Az öt éves időszakra tervezett stratégiát 2016-ban egy új nemzeti kiberbiztonsági stratégia követte, amely címe *Nemzeti Kiberbiztonsági Stratégia 2016-2021* (National Cyber Security Strategy 2016-2021). A stratégia legfontosabb elvi alapja a védelem-elrettentés-fejlesztés (defend-deter-develop) hármasban érhető tetten.

Az új stratégia bemutatja az Egyesült Királyságot fenyegető veszélyforrásokat, amelyek bár átfedésben vannak a 2011-ben megfogalmazott veszélyforrásokkal, de nyilvánvalóan azóta meg is változtak. Ezek a következők:

- kiberbűnözés;
- állami és állami támogatású kiberveszélyek, benne a kiberkémkedés és a kritikus infrastruktúrákat fenyegető kibertámadások;

- terrorizmus;
- hacktivizmus;
- script kiddies.[91] (Egyesült Királyság 2016, Kovács 2018b)

A stratégia felvázolja a legfontosabb kibertéri sérülékenységet is:

- az (IKT) eszközök számának nagyarányú növekedése;
- alacsony kiberhigiénia és -tudatosság;
- régi és sérülékeny rendszerek;
- nem megfelelő képzések és készségek;
- a támadó eszközök nyílt elérhetősége. (Egyesült Királyság 2016, Kovács 2018b)

A stratégia a kiberbiztonsági feladatokat és felelősségi köröket szétosztja a kibertér szereplői között. Így külön meghatározza az egyéni felhasználók, a gazdasági élet szereplőinek, valamint a kormányzat szereplőinek feladatát és felelősségét.

A stratégia meghatározza a kormányzat olyan általános érvényű feladatait, mint az állampolgárok kibertámadásokkal szembeni védelme, az információs rendszerek és az adatvagyon védelme, a kibertéri szereplők közötti együttműködés kialakítása és az érdekelt felek közötti koordináció biztosítása, de elrendeli egy Nemzeti Kiberbiztonsági Központ (National Cyber Security Centre, NCSC) felállítását is. (Egyesült Királyság 2016, Kovács 2018b)

Az NCSC 2016 őszén kezdte meg működését. Legfontosabb feladata a hatékony koordináció a kormányzat, a közigazgatás különböző szereplői, az ipar, illetve a társadalom között. A központ ezenkívül kormányzati kiberbiztonsági tanácsadói szerepet is betölt, de emellett nagyon fontos, hogy a társadalom számára egy olyan látható szervezet, amelyben egyrészt szakértelme révén garancia a kiberbiztonságra, másrészt hatékony védelmet nyújt az Egyesült Királyság szervezetei és állampolgárai számára a kibertámadásokkal szemben. A stratégia meghatározta az NCSC legfontosabb feladatait is:

- olyan világszínvonalú eseménykezelő képesség létrehozása, amely a szervezetek széles skálája – azaz a legkisebb szervezettől a nemzeti szintű vállalatig – esetén biztosítja az incidensekre adott hatékony válaszokat, valamint csökkenti azok következményeit;

[91] A script kiddies, azaz szkript kölykök csekély informatikai tudással rendelkező, de a különböző támadó eszközök felhasználásával károkat okozó fiatalok gyűjtőfogalma.

- olyan kommunikációs megoldások biztosítása, amelyekkel a magán- és a közszféra képes a kiberbiztonsági kockázatokra felkészülni;
- a kiberbiztonsági fenyegetésekkel kapcsolatos tanácsadás a kormányzat számára az olyan kritikus szektorokban, mint az energia, a telekommunikáció, vagy a pénzügyi szféra. (Egyesült Királyság 2016, Kovács 2018b)

A stratégia tartalmaz egy implementációs tervet is, amely a már említett védelem, elrettentés, fejlesztés filozófiai hármas mellett mutatja be az Egyesült Királyság számára a kiberbiztonság eléréséhez szükségesek tevékenységeket. Ez a következőket tartalmazza:

- a védelem területén:
  - aktív kibervédelmi megoldások;
  - biztonságos internet kialakítása;
  - a kormányzat és a közigazgatás, a kritikus infrastruktúrák védelme;
  - hatékony incidenskezelés;
  - a biztonságtudatosság alapvető átalakítása és fejlesztése;
- az elrettentés területén (a fizikai térben megvalósuló elrettentéshez hasonlóan):
  - a kiberbűnözés elleni fellépés, annak radikális csökkentése;
  - ellenséges külföldi szereplők elleni tevékenység;
  - terrorizmus elleni védelem;
  - támadó kiberképességek kiépítése;
  - erősebb titkosítási eljárások kidolgozása.
- a támadó képességek területén:
  - Nemzeti Kibertámadási Program (National Offensive Cyber Programme, NOCP) meghatározása.

A támadó képességek kialakításának legfontosabb célja: *„[b]iztosítani kell, hogy rendelkezésünkre álljanak a megfelelő támadó kiberképességek, amelyeket mind elrettentési, mind operatív célokra, a nemzeti és a nemzetközi jognak megfelelően, adott helyzetben döntésünknek megfelelően fogunk alkalmazni."* (Egyesült Királyság 2016, Kovács 2018b)

A kibertámadóképességek kialakítását, beleértve a technikai és humánképeségeket is a stratégia a hadsereghez rendeli hozzá. Elrendeli, hogy a Védelmi Minisztérium az NOCP-

ban meghatározottak szerint, együttműködve a Nemzeti Kommunikációs Központtal[92] (Government Communications Hedquarters, GCHQ) építse ki a támadó képességeket és eszközöket. Ehhez a fegyveres erőknél olyan képességeket kell kialakítani, amelyek alapján azok a katonai műveletekbe integrálhatók, valamint a kiberműveletek a katonai műveletekkel együtt alkalmazhatók. (Egyesült Királyság 2016, Kovács 2018b)

A stratégia meghatározza a kiberbiztonság fejlesztési feladatait is, amelyek a következők:

- a kiberbiztonsági jártasságok erősítése, növelése;
- a kiberbiztonsági szektor növekedésének elősegítése;
- a kiberbiztonság tudományos és technológiai háttere fejlesztésének támogatása;
- a kiberbiztonsággal kapcsolatos technológiai, biztonsági és politikai változások folyamatos monitorozása. (Egyesült Királyság 2016, Kovács 2018b)

A stratégia hangsúlyozza a nemzetközi együttműködés fontosságát. Ennek megfelelően külön fejezetben mutatja be a nemzetközi együttműködés feladatait hangsúlyozva az ENSZ, a G20, az EU, a NATO, az EBESZ, illetve a Brit Nemzetközösség szerepét, de kitér a kevésbé fejlett országok felzárkóztatásának feladatára is. (Egyesült Királyság 2016, Kovács 2018b)

A stratégia a 2021 utáni évekre vonatkozó vízióval zárul. Ebben nagyon előremutató módon megállapítja, hogy a rendkívül gyors technológiai változás megfelelő kiberbiztonsági stratégiát igényel. Ennek megfelelően a cél a kihívásokra és veszélyekre gyors, megfelelő és hatékony válasz lehetőségét magába foglaló stratégia kialakítása. Ez annál is inkább fontos, mert a következő évtizedre a technológiai robbanással párhuzamosan a kibertéri veszélyek is robbanásszerű fejlődésen fognak keresztül menni. A technológia mellett azonban fontos, hogy a mindennapi biztonság és a biztonságról való gondolkodás részévé tegyük a kiberbiztonságot. Ha ez megvalósul, akkor a társadalmi és a piaci szereplők, illetve a szolgáltatók fognak hatékonyan fellépni a kibertérben megjelenő kihívásokkal szemben. Ez pedig azzal a pozitív hozadékkal járhat, hogy az állami szerepvállalás kisebb mértékű, így olcsóbb, de a kibertér biztonságát tekintve hatékonyabb lehet. (Egyesült Királyság 2016, Kovács 2018b)

[92] Ennek részét képezi a kormányzati rádióelektronikai felderítő- és a kibertér technikai felderítő szervezet is.

2.4.4. Észtország

Észtország nemzeti biztonsági stratégiája

Észtország nemzeti biztonsági stratégiája az ország nemzeti biztonsági koncepciójában azonosítható, amely 2010-ben került kiadásra. Ugyanakkor az ország nemzeti biztonságát egy másik, az úgynevezett *nemzeti védelmi stratégia* is meghatározza. Ennek első kiadása 2005-ben, majd frissített és átdolgozott változata 2011-ben jelent meg. (Kovács 2018b)

Észtország geopolitikai helyzete rendkívül speciális, amelyhez hozzájárul a már említett 2007-es tavaszi kiberkrízis, illetve az akkori események társadalom egészére gyakorolt hatása is.

Az említett észt nemzeti biztonsági koncepció céljaiban nem különbözik egy nemzeti biztonsági stratégiában megfogalmazott céloktól, hiszen az ország függetlenségének, területi integritásának és az állampolgárok védelmének biztosítása és garantálása jelennek meg legfontosabb elemekként. A koncepció ezeknek a céloknak az elérése érdekében általános érvényű alapelveket fogalmaz meg mind hazai, mind nemzetközi – elsősorban a NATO keretei között – téren. (Észtország 2010, Kovács 2018b)

A koncepció értékeli a biztonsági környezetet, amely során megállapítja: *„[a]z országok ellenállóképessége egyre inkább függ a kibertér használatának növekedésétől. Az összehangolt számítógépes támadások, amelyek forrásait nehéz azonosítani, jelentős kárt okozhatnak a társadalomnak. A kibertérrel való visszaélés, beleértve a terrorista csoportokat és a szervezett bűnözést egyre növekszik."* (Észtország 2010, idézi: Kovács 2018b)

A fenti idézet is rávilágít arra gondolkodásra, amely mentén a koncepció kihívásként értékeli a kibertérben az infokommunikációs rendszerek egymásra való hatását, az azokban rejlő társadalmi és gazdasági függőséget, valamint az eddigi veszélyekre adott elégtelen válaszokat. A dokumentum hangsúlyozza a kiberbűnözés elleni tevékenység fokozásának szükségességét, kiemelve, hogy az információs rendszerek működőképességének biztosítása elengedhetetlen. A kiberbűnözés elleni tevékenységben az együttműködés és a jogszabályi háttér kidolgozását és megteremtését sürgeti a dokumentum. Az ehhez a feladathoz szükséges technikai- és humánerőforrásokkal kapcsolatban a következőket fogalmazza meg a stratégia: *„[a] kiberbűnözés megelőzésében és leküzdésében a nemzeti és nemzetközi szintű ügynökségek közötti fokozott együttműködésre kell törekedni, ugyanúgy, mint a jogszabályok fejlesztése és a közvélemény tudatosítása terén. Az állam garantálja a kiberbűnözés elleni*

küzdelemhez a szükséges technikai eszközöket és a know-how rendelkezésre állásának biztosítását." (Észtország 2010, idézi: Kovács 2018b)

A koncepció rendkívül előremutató módon a fenti feladatok végrehajtása érdekében részletes kiberbiztonsági akciótervet irányoz elő. (Észtország 2010, Kovács 2018b)

2011-ben került kiadásra Észtország nemzeti védelmi stratégiája, amely a gyorsan változó biztonságpolitikai helyzet, az újonnan megjelenő veszélyek és kihívások szaporodása és egyre hangsúlyosabbá válása miatt vált szükségessé, hiszen ez a 2005-ös első ilyen stratégia átdolgozott verziója. A stratégia leszögezi, hogy a nemzet védelme átfogó megközelítést igényel, így a katonai erőt és a katonai megoldásokat ötvözni kell más, nem katonai eszközökkel. (Észtország 2011, Kovács 2018b)

A stratégia elvégzi a biztonsági környezet elemzését is. Ezzel kapcsolatban a dokumentum megállapítja, hogy az ország biztonsága a NATO és európai uniós tagságából eredően magas szinten van, de a Balti-tenger térségének biztonsága, valamint a balti országok biztonsága és azok ezzel kapcsolatos tevékenysége alapvető kihatással vannak Észtországra. A stratégia veszélyként azonosítja az alacsony szintű konfliktusok időbeni gyors eszkalálódásának a lehetőségét is. Ez nyilvánvalóan utalás az Oroszország által jelentett, és a mindennapokban a befolyásolásban megnyilvánuló, de gyorsan magasabb szintre eljutható fenyegetésre.

A stratégia egyik fontos megállapítása, hogy az országgal szemben a közvetlen katonai támadás valószínűsége kicsi, de az nem zárható ki teljesen. Ezzel szemben az ország NATO tagsága bizonyos garanciákat nyújt. Ugyanakkor az olyan nem katonai támadásoknak, amelyek az energia és/vagy más kritikus infrastruktúra rendszereket céloznak veszélye lényegesen nagyobb. (Észtország 2011, Kovács 2018b)

A veszélyekkel kapcsolatban a stratégia nevesíti Oroszországot, mert annak belpolitikai és külpolitikai tevékenysége egyaránt hatással van Észtországra: *„[a]z észt biztonsági környezetet is befolyásolja az Orosz Föderáció bel- és a külpolitikája. Az Orosz Föderáció fokozott érdeklődést mutat a befolyásának visszaállításához, valamint az európai biztonsági környezetre gyakorolt hatásának megerősítéséhez. Az Orosz Föderáció katonai erőinek jelenléte az észt határ közelében növekedett."* (Észtország 2011, idézi: Kovács 2018b)

A stratégia részletesen tárgyalja Észtország védelmi politikáját is. Ebből megállapítható, hogy *„az észt védelmi politika a katonai erő és katonai védelem hangsúlyozása mellett a NATO tagságból eredő szövetségesi struktúrában, a katonai szektor civil támogatásában, a belső biztonság megteremtésében, a közszolgáltatások biztosításában és a pszichológiai –*

alapvetően a külső és belső befolyásolás elleni – védelemben látja a védelem stratégiai pontjait." (Kovács 2018b)

A védelmi politika mellett a katonai erő és annak fejlesztése is része a stratégiának. Nagyon előremutató módon a stratégia a védelmi minisztérium feladatai közé sorolja a kibervédelem koordinálását is. A dokumentum a védelmi minisztérium és a hadsereg kibervédelmi feladat mellett az észt Nemzeti Védelmi Liga, amely a hadsereg támogatására hivatott önkéntes civil szerveződés, esetében is meghatározza a kibervédelmi képességek fejlesztését.[93]

Észtország nemzeti kiberbiztonsági stratégiája

Észtország volt az első olyan ország, amely önálló nemzeti kiberbiztonsági stratégiát adott ki. A 2008-ban megjelent észt nemzeti kiberbiztonsági stratégiát a Védelmi Minisztérium dolgozta ki a 2008-2013-as időszakra.

A stratégia kidolgozására a 2007-es – korábban többször említett Észtországot ért kibertámadások és azok következményei – nagy hatással voltak. Mindezek következménye, hogy az átfogó megközelítés elvét magáénak valló stratégia olyan kérdésekre is koncentrált, amelyek korábban nem jelentek meg hangsúlyos elemként az észt biztonságfelfogásban. Ilyen kérdések az információbiztonsági tudatosság nemzeti szintű emelése, megfelelő jogszabályi környezet kidolgozása a kibertérre és a kapcsolódó területekre, illetve a nemzetközi együttműködés sokkal nagyobb arányú megjelenésének szükségessége a kiberbiztonság területén is. (Osula 2015, Kovács 2018b)

A 2008-as, világviszonylatban is első nemzeti kiberbiztonsági stratégiát 2014-ben egy új stratégia követte. Ennek címe *Nemzeti Kiberbiztonsági Stratégia 2014-2017* (Küberjulgeoleku strateegia 2014-2017) volt. (Észtország 2014a, Kovács 2018b) Az új stratégia az előző stratégia kiadása óta eltelt időben megjelent veszélyeket és kihívásokat elemzi, majd bemutatja azokat a lépéseket, amelyeket Észtország a kiberbiztonság területén tett. Ezeknek a fontos lépéseknek az egyike, hogy 2009-ben a Kormány Biztonsági Bizottságának részeként felállításra került a Kiberbiztonsági Tanács. Emellett megerősítésre került a korábbi észt informatikai központ, amely nem csak erősebb szervezetet, hanem új

[93] Ezzel kapcsolatban meg kell jegyezni azt a magyar kezdeményezést, amely filozófiájában nagyban hasonlít a fenti észt elgondolásra. Ez a Magyarországon az Önkéntes Kibervédelmi Összefogás (KIBEV) néven létrejött szerveződés. Ennek lényege, hogy tagjai felajánlják informatikai, illetve kibervédelmi tudásukat és szakértelmüket az állam és annak különböző szervezetei és hatóságai – például a Magyar Honvédség, államigazgatási szervek, nemzetbiztonsági szolgálatok – számára. (KIBEV 2018)

nevet is kapott: Észt Információs Rendszer Hatóság (Riigi Infosüsteemi Amet, RIA). A hatóság új feladatként megkapta a kritikus infrastruktúrák védelmét, illetve az azokon belül lévő információs rendszerek biztonságának megteremtését is. Ennek a feladatnak a hatékony ellátása érdekében a RIA egy Kritikus Információs Infrastruktúra Védelmi Osztállyal került megerősítésre. (Észtország 2014b, Kovács 2018b)

A stratégia a legfőbb kihívásként az IKT eszközök, rendszerek és szolgáltatások gyors fejlődési üteméből adódó veszélyeket jelölte meg. Ennek megfelelően a következő területeken van szükség beavatkozásra:

- alapvető közműszolgáltatások: a határokon átnyúló technológiai függőség azt eredményezi, hogy már nem csak Észtország belső problémájával kell szembenézni. Ezért szükséges minden szolgáltatás és az azok jelentette interdependencia feltérképezése;
- kiberbűnözés: a gazdasági károk mellett a bizalomvesztés is súlyos kihívás, ezért a korszerű IKT eszközök és rendszerek alkalmazása a kiberbűnözés elleni tevékenység – nyomozás, nemzetközi információcsere – során elengedhetetlen;
- nemzeti védelem: ezen a területen integrált katonai és civil összefogás szükséges (ez visszautalás a nemzeti védelmi stratégiában megfogalmazott átfogó megközelítés elvére);
- a jövő biztonsága: folyamatos technikai fejlesztés és innováció, valamint folyamatos emberi erőforrás fejlesztés is szükséges a jövőben várhatóan megjelenő veszélyek hatékony kezelése érdekében. (Észtország 2014b, Kovács 2018b)

A dokumentumban megfogalmazott stratégiai cél nagyon egyértelmű: *„[a] kiberbiztonsági stratégia négyéves célja a kiberbiztonsági képességek és a lakosság tudatosságának növelése a kiberfenyegetésekkel szemben, ezáltal a kibertérben való folyamatos bizalom megteremtése."* (Észtország 2014b, idézi: Kovács 2018b)

Ennek a legfőbb célnak az elérése érdekében a következő részcélokat adta meg a stratégia: (Észtország 2014b)

- a fontos szolgáltatások alapját képező információs rendszerek védelme:
    - alternatív megoldások biztosítása fontos szolgáltatások számára;
    - a fontos szolgáltatások közötti függőség kezelése;
    - az IKT infrastruktúra és -szolgáltatások biztonságának növelése;
    - az állami és a magánszektorban megjelenő kiberfenyegetések kezelése;

    - nemzeti kiberbiztonsági rendszer bevezetése;
    - az állam digitális üzletmenetfolytonosságának biztosítása;
    - a nemzetközi együttműködés előmozdítása a kritikus információk infrastruktúrájának védelmében;
- a kiberbűnözés elleni tevékenység fokozása:
    - a kiberbűncselekmények felderítésének fokozása;
    - a kiberveszélyekkel szembeni tudatosság növelése;
    - nemzetközi együttműködés fokozása a kiberbűnözés ellen;
- a nemzeti kibervédelmi képességek fejlesztése:
    - a katonai tervezés és a civil hatóságok felkészülésének összehangolása;
    - kollektív kibervédelem és nemzetközi együttműködés fejlesztése;
    - a katonai kibervédelmi képességek fejlesztése;
    - az új kiberfenyegetések kezelése;
    - fel kell építeni a kibervédelmi szakemberek új generációját;
    - támogatni és koordinálni kell az előremutató kiberbiztonsági kutatás-fejlesztési programokat;
    - a magánszektor vállalatait be kell vonni a nemzeti kibervédelmi megoldásokba;
- nemzetközi együttműködés fokozása:
    - nemzetközi kiberbiztonsági politika kialakítása;
    - szorosabb együttműködés a partnerekkel és a szövetségesekkel;
    - az Európai Unió kiberbiztonsági képességeinek növelése. (Észtország 2014b, Kovács 2018b)

2.4.5. Franciaország

Franciaország nemzeti biztonsági stratégiája

Emmanuel Macron elnöksége alatt 2017-ben került felülvizsgálatra Franciaország 2013-ban kiadott nemzeti biztonsági stratégiája. A felülvizsgálat eredménye egy új stratégia, amely azonban nagyon sok mindenben épít a 2013-as stratégiára. (Nádudvari 2018, Kovács 2018b)

A 2013-ban megjelent korábbi stratégia, amely címe *Fehér Könyv: Védelmi és Nemzeti Biztonság 2013* (Livre Blanc: Défense et Sécurité Nationale 2013). (Franciaország 2013a) Ez a meglehetősen hosszú, minegy 160 oldal terjedelmű dokumentum három prioritásra épül: védelem, elrettentés, intervenció. Ez a három tényező jelenti a stratégiában

megfogalmazott célkitűzések hátterét is. A kibertér, illetve a kibertéri veszélyek, valamint azok kezelésének lehetséges módjai mindhárom prioritás esetében markánsan megjelennek. (Kovács 2018b)

A stratégia a megszokott módon megadja a Franciaország értékeit és érdekeit, majd ezeknek megfelelően elemzi a biztonsági környezetet. A kibertérrel kapcsolatban kiemeli a nem állami szereplők által indított kibertámadások egyre gyakoribbá válását. Az ázsiai térség elemzése során a dokumentum meg is nevezi a kibertérben az egyik ilyen állami szereplőt: *„Kína a védelmi korszerűsítése esetén haladt előre rendkívül gyors ütemben, különösen a nukleáris arzenálja fejlesztése, korszerűsítése, valamint annak erő kivetítése, és a kibertámadások képességének terén."* (Franciaország 2013b, idézi: Kovács 2018b)

Mindezeken túl a stratégia veszélyként azonosítja, hogy az internet és az információtechnológia segítségével nagyon könnyen elérhetővé váltak az olyan információk, amelyek például a robbanóanyagokhoz való hozzáférést és azok gyártását mutatják be. Ugyanakkor hangsúlyozza, hogy az információs rendszerek olyan szinten épültek be a társadalomba, hogy az azokban esetlegesen bekövetkező rendszerkiesések magára a társadalomra is negatívan hatnának. A stratégia azt is megjegyzi, hogy a digitális technológia fejlődése nem szükségszerűen járt együtt azok biztonságának megteremtésével. Az információs rendszerekkel, illetve a kibertérrel kapcsolatban konkrét veszélyeket azonosít a stratégia, amelyeket eltérő szintekre sorol be:

- legalacsonyabb szintű veszélyek:
    - kiberbűnözés (például személyiséglopások, zsarolások, személyes adatok eltulajdonítása);
- legmagasabb szintű veszélyek:
    - a kritikus információs infrastruktúrák vagy a stratégiai katonai információs rendszerek elleni kibertámadások. (Franciaország 2013b, Kovács 2018b)

Ezeknek a veszélyeknek az elemzése után a stratégia megfogalmazza a kiberhadviselés bekövetkeztének lehetőségét is: *„[a] kibertér így konfrontáció terévé vált. Ahogy azt a korábbi Fehér Könyv már előre jelezte, a nemzeti információs rendszerek elleni jelentős kibertámadások lehetősége egy kiberhadviselési forgatókönyvben rendkívül súlyos fenyegetést jelentenek Franciaország és európai partnerei számára."* (Franciaország 2013b, idézi: Kovács 2018b)

A védelem, mint stratégiai prioritással kapcsolatban a dokumentum a következő fő veszélyforrásokat azonosítja:

- az ország területével szembeni, másik ország által elkövetett agresszió;
- terrorista támadások;
- kibertámadások;
- a tudományos és technikai potenciál sérülése;
- a szervezett bűnözés súlyos megnyilvánulásai;
- a természeti-, egészségügyi-, technológiai-, ipari katasztrófák;
- francia állampolgárok és érdekeltségek támadása külföldön. (Franciaország 2013b, Kovács 2018b)

Mivel ezek között a legfontosabb veszélyforrások között ott van a kibertámadások jelentette veszély is, ezért az azok elleni fellépés érdekében a stratégia meghatározza a hírszerzési tevékenység fokozását, valamint elrendeli a szükséges technikai és humánerőforrás fejlesztését. Mindezek mellett a stratégia hangsúlyozza, hogy ki kell építeni azokat a kibertámadó képességeket, amelyekkel hatékony válasz adható a kibertéri veszélyekre. (Franciaország 2013b, Kovács 2018b)

Az általános feladatokon túl a stratégia egy külön alfejezetben részletesen meghatározza a kibertér védelme érdekében megvalósítandó tevékenységeket. Ezek valóban stratégiai szintű tevékenységeket jelentenek:

- nagyarányú humánerőforrás fejlesztést kell végrehajtani, amelyben példa Németország és az Egyesült Királyság;
- fokozni kell a kibertéri veszélyek azonosítását és felismerését (ez a nemzeti szuverenitás alapjává kell, hogy váljon);
- elkülönített éves költségvetési keretet kell biztosítani a kibervédelemre;
- meg kell őrizni a nemzeti és európai információtechnológiai ipart;
- ki kell alakítani a megfelelő jogalkotási és szabályozási eljárásokat, valamint a kiberfenyegetésekkel szemben támasztott biztonsági követelményeket;
- az állami- és magánszereplők jogainak és kötelezettségeinek világos szabályozását meg kell tenni, beleértve az ellenőrzések, a kiberbiztonsági incidensek és események bejelentésének szabályozását is;
- növelni kell a Nemzeti Információbiztonsági Ügynökség (Agence nationale de la sécurité des systèmes d'information, ANSSI)[94] incidenskezelő, koordináló és együttműködési kapacitásait. (Franciaország 2013b, Kovács 2018b)

[94] Az ANSSI 2009-ben a Védelmi Minisztérium (Secrétaire général de la défense et de la sécurité nationale, SGDSN) alárendeltségében kezdte meg működését. A szervezet a kiberbiztonságért és a

A súlyos kibertámadások kezelését a következő két alapelv megadásával határozza meg a stratégia:

- az állami információs rendszerek, a stratégiai iparágak és az alapvető infrastruktúra-üzemeltetők számára megfelelően kialakított, erős és rugalmas védelmet kell kialakítani, amely egy, a miniszterelnöki hivatal által koordinált, az e rendszerek védelmét szolgáló operatív szervezethez kapcsolódik, és amelyet a különböző állami ügynökségek szoros együttműködéssel támogatnak a kiberfenyegetések lehető legkorábbi azonosításában és minősítésében;
- a különböző kibertámadásokat elsőként a diplomáciai, igazságügyi vagy rendőri erőforrásra támaszkodva kell kezelni, anélkül, hogy ezek a megoldások kizárnák a védelmi minisztérium erőforrásainak fokozatos bevonását abban az esetben, ha a nemzeti stratégiai érdekek veszélybe kerülnének. (Franciaország 2013b, Kovács 2018b)

A stratégia több helyen is hangsúlyozza a nemzetközi együttműködés fontosságát, amelyben kiemelt szerepet szán a Németországgal és az Egyesült Királysággal való szoros együttműködés mellett az európai kritikus infrastruktúrák és az infokommunikációs rendszerek védelmének. (Franciaország 2013b, Kovács 2018b)

A dokumentum meghatározza a francia haderő stratégiai feladatait is. Ezen a területen az egyik prioritásnak a katonai kibervédelmi képességek fejlesztését tűzi ki. Nagyon előremutató, hogy ezeket a katonai kibervédelmi képességeket, illetve a kibervédelmi feladatokat ellátó szervezeteket integrálni kell a hadsereg alakulataiba. A korábban említett kibertámadó képességek kiépítését szintén a hadsereg számára dedikálja a stratégia. (Franciaország 2013b, Kovács 2018b)

Ahogy a fentiekben utaltam rá 2017 őszére elkészült a 2013-as Fehér Könyv felülvizsgálata, amely új stratégiát is jelent egyben.

Ez az új stratégia, csakúgy, mint a 2013-as előző verzió kiemelten kezeli a kiberteret és az abban jelentkező veszélyeket. A stratégiai környezet elemzésekor dokumentum nagyon markáns megállapítást tesz a kibertéri támadásokkal kapcsolatban: „*[a] kibertérben bizonyos támadások fegyveres agressziónak tekinthetők nagyságuk és súlyosságuk okán.*

hálózatbiztonságért felelős francia nemzeti hatóság. Technikai és szakértői támogatást ad a kormányzati és a gazdasági szféra egyes szereplőinek, de emellett tanúsítási feladatokat is ellát az informatikai eszközök és szolgáltatások területén. Mindezeken túl az ANSSI képviseli Franciaországot a nemzetközi CERT-ek hálózatában. (ANSSI 2018, Kovács 2018b)

Nagyobb kibertámadások az általuk okozott esetleges károkra tekintettel az ENSZ Alapokmánya 51. cikke szerinti jogos védelmi intézkedéseket is életre hívhatnak." (Franciaország 2017, idézi: Kovács 2018b)

Ennek fényében nem meglepő, hogy a kibertámadó képességekkel kapcsolatban ez a stratégia is szorgalmazza azok fejlesztését és műveleti képességekbe való beépítését. (Franciaország 2017, Kovács 2018b)

Érdemes megjegyezni, hogy ez a stratégia Oroszországot még a legnagyobb regionális veszélyként és fenyegetésként határozza meg, de Kína esetében a fenyegetés helyett a *globális ambíció* kifejezést használja. Ugyanakkor a stratégia felhívja a figyelmet, hogy ezeket az ambíciókat Kína a kibertérben és az információtechnológiai fejlesztésekben is felmutatja. (Nádudvari 2018, Kovács 2018b)

Franciaország nemzeti kiberbiztonsági stratégiája

2015-ben került kiadásra Franciaország jelenlegi nemzeti kiberbiztonsági stratégiája, amely címe *Francia Nemzeti Digitális Biztonság Stratégia* (Stratégie nationale pour la sécurité du numérique).

A dokumentum öt stratégiai célkitűzést fogalmaz meg. Ezeket kulcsszavakkal jelölt területekként adja meg, amely területek a következők:

- alapvető érdekek, az állami információs rendszerek biztonsága és védelme; súlyos kiberbiztonsági válságok;
- digitális bizalom, adatvédelem, személyes adatok, kiberrosszindulat;
- tudatosság növelés, alapvető felkészítés, folyamatos képzés;
- a digitális technológia üzleti környezete, iparpolitika, export és nemzetköziesítés;
- Európa, digitális stratégiai autonómia, kibertér stabilitása. (Franciaország 2015b, Kovács 2018b)

Ehhez az öt stratégiai célkitűzéshez a stratégia megadja az adott területen meglévő jelenlegi helyzetet, részletezi magát a célkitűzést, amelyek végrehajtásához meghatározza a legfontosabb feladatokat is.

Az első stratégiai céllal kapcsolatban a stratégia rögzíti Franciaország kibertérben érvényesítendő érdekei, a digitális biztonság megerősítése, valamint a kritikus infrastruktúrák védelme érdekében történő elkötelezettségét. Mindezek a következő feladatokat jelentik:

- meg kell teremteni a szükséges tudományos, technikai és ipari képességeket, amelyek a kiberbiztonságot és a megbízható digitális gazdaságot támogatják: ennek érdekében többek között egy szakértői panel is felállításra kerül, valamint az információbiztonságért felelős hatóság mellett számos minisztérium, civil szervezet, ipari és tudományos testület kerül bevonásra;
- meg kell teremteni a biztonsági technológiák alkalmazásának helyzetét az állam, a vállalkozások és az állampolgárok részéről is: ebben a feladatban kiemelt szerep hárul az ANSSI-ra, amely ezt a monitorozást folyamatosan kell, hogy végezze, és veszély esetén a különböző minisztériumokat információkkal kell ellátnia;
- fel kell gyorsítani az állami információs rendszerek kiberbiztonságára vonatkozó fejlesztéseit[95];
- Franciaország és a hozzá kapcsolódó multilaterális egyezmények alapján működő szervezetek felkészítése egy esetleges súlyos kiberkonfliktusra: a 2013-as nemzeti biztonsági stratégiában azok a szereplők már felszólításra kerültek, akik a francia létfontosságú rendszereket üzemeltetik, és ők már ezt a fajta felkészülési munkát meg is kezdték. Ugyanakkor ezt fel kell gyorsítani és a felkészülés során figyelembe kell venni az EU NIS irányelvében meghatározott feladatokat is. Ebben a munkában az egyik legfontosabb koordináló szervezet a Védelmi Minisztérium és az ANSSI. Európai szinten Franciaország együttműködik és támogatja az ENISA, valamint az CERT-EU munkáját ebben a feladatban. Katonai oldalról ugyanezt a NATO NCIRC esetében is hangsúlyozza a dokumentum. (Franciaország 2015b, Kovács 2018b)

A második stratégiai cél a francia állampolgárok és azok jogainak védelme a kibertérben, valamint a kiberbűnözéssel szembeni hatékony fellépés. Ennek érdekében végrehajtandó feladatok:

- a francia értékeket meg kell védeni az elektronikus kommunikációs hálózatokban és az ezekhez kapcsolódó nemzetközi eljárásokban: ebben az állam az egyik legfontosabb szereplő, mert az ő kötelessége informálni és felhívni az

[95] 2010 óta már számos fejlesztés megvalósult. Ennek érdekében például 2014-ben kiadásra került a *Nemzeti Információs Rendszerek Biztonsági Politikája* (Politique de sécurité des systèmes d'information, PSSIE), de a technikai fejlődés miatt szükséges a kiberbiztonsági megoldások folyamatos fejlesztése. (Franciaország 2014, Kovács 2018b)

állampolgárok figyelmét a kibertéri veszélyekre, az információval történő befolyásolásra és rosszindulatú propaganda tevékenységekre[96];

- a kiberbűncselekmények, illetve az ártó szándékú kibertevékenységek áldozatainak helyben kell segítséget nyújtani: ebben a feladatban többek között a Belügyminisztérium az ANSSI együttműködésével, számos más hivatal és szervezet bevonásával a kiberbűnözés áldozatai számára nemzeti segítségnyújtási rendszer kiépítését kezdte meg 2016-ban;
- a kiberbűnözéssel szembeni hatékony fellépés: ezen a téren az egyik legfontosabb feladat egy megbízható nyilvántartási rendszer felállítása, amely mindez idáig hiányzott ezen a területen. Ennek kialakítására a Belügyminisztérium és az ANSSI kapott feladatot;
- a francia emberek digitális életének és személyes adatainak védelme: ennek a feladatnak a végrehajtására a kormánynak ütemtervet kell kidolgoznia, amely a digitális azonosítás EU-s szabályait is figyelembe véve a Digitális Technológia és Államreform terv részét fogja képezni;
- olyan műszaki megoldások ajánlása az állampolgárok és a vállalkozások számára, amelyek célja a digitális élet biztonságának megteremtése;
- a nemzetközi kölcsönös jogi segítségnyújtás működési mechanizmusainak megerősítése és a számítógépes bűnözésről szóló Budapest Konvenció elveinek egyetemessé tétele. (Franciaország 2015b, Kovács 2018b)

A harmadik stratégiai cél a kiberbiztonsági tudatosság növelésére, az alapvető kiberbiztonsági felkészítésre és a folyamatos képzésre irányul, amelyekkel kapcsolatosan a következő feladatokat kell végrehajtani:

- a kiberbiztonság tudatosságának növelése a francia emberekben;
- a kiberbiztonság tudatosságának oktatását integrálni kell minden felső és továbbképzési oktatási programba;
- a kiberbiztonsági képzéseket – benne technológiai ismeretekkel – integrálni kell a felsőoktatásba és ilyen szakokat kell létrehozni;

[96] A 2015-ös terrortámadások után egy információmegosztó portált hozott létre a kormány, amelynek URL címe is sokatmondó és árulkodó annak célját tekintve: Stop-djihadisme.gouv.fr (Franciaország 2015, Kovács 2018b)

- fel kell mérni és előre kell jelezni a továbbképzési igényeket. (Franciaország 2015b, Kovács 2018b)

A negyedik stratégiai cél a digitális versenyképesség javítása a kiberbiztonság területén kutatás-fejlesztéssel foglalkozó francia vállalatok számára. Ezen a területen meglévő feladatok:

- támogatni kell a (digitális) biztonsági termékeket és szolgáltatásokat gyártók nemzeti és európai tevékenységét, amelyhez egy új francia kiberipari fejlesztési tervet is előirányoz a stratégia;
- a magánszektor számára biztosítani kell és át kell adni mindazt a felgyülemlett tudást és információt, amellyel a kiberbiztonságot kezelni képesek: ez hozzájárul ahhoz, hogy megbízható és biztonságos termékeket és szolgáltatásokat gyártsanak mind a magánszektor, mind a közigazgatás számára;
- a felhasználók magasabb szintű felkészítésével, valamint a kiberbiztonságban az érintett szereplők információkkal történő támogatásával növelhető a megelőzés;
- a kiberbiztonsági követelmények beépítése a közbeszerzésekbe;
- a kiberbiztonság üzleti szférájának nemzetköziesítése, amely ki kell, hogy terjedjen a kis- és közepes vállalkozások támogatására. (Franciaország 2015b, Kovács 2018b)

Az utolsó stratégiai cél a digitális stratégiai autonómia és a kibertér stabilitásának megteremtését irányozza elő. A stratégia ezzel kapcsolatban kifejti, hogy az Európai Unió tagországai stratégiai önállóságát biztosítani kell ahhoz, hogy a kibertér biztonságos, stabil és nyílt maradjon. Ennek kialakításában Franciaország vezető szerepre törekszik a következő stratégiai feladatok támogatásával:

- az önkéntes tagországok között egy stratégiai ütemtervet kell készíteni, amelyben meghatározhatóak mindazok a kulcs területek, amelyek rövid távon is biztosítják a stratégiai autonómia kialakítását úgy, hogy a résztvevő országok függetlensége nem sérül;
- a francia jelentét és befolyás megerősítése a nemzetközi kiberbiztonsági tárgyalásokban;
- a globális kiberbiztonság megteremtése érdekében Franciaország kész tapasztalatait és tanácsait más országokkal megosztani, és kész segítséget nyújtani ezen országok kiberbiztonsági képességeinek fejlesztéséhez. (Franciaország 2015b, Kovács 2018b)

2.4.6. Hollandia

Hollandia nemzeti biztonsági stratégiája

Hollandia jelenleg érvényes nemzeti biztonsági stratégiája *Hollandia biztonságáért világszerte végzett munka Integrált nemzetközi biztonsági stratégia 2018-2022* (Wereldwijd voor een veilig Nederland Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022) címmel 2018 tavaszán jelent meg.

A stratégia filozófiája a megelőzés, védelem, megerősítés szavakkal jellemezhető. A dokumentum a stratégia biztonsági környezet és biztonsági viszonyok bemutatásakor az Európában, illetve a Holland Királyság karibi érdekeltségei vonatkozásában jelentkező instabiltást és veszélyt okozó tényezőket mutatja be. A stratégia kiemelt figyelmet szentel a technológia gyors ütemű fejlődéséből – például az önvezető járművek, a robotizáció, a szintetikus biológia vagy a mesterséges intelligencia – eredő pozitív gazdasági és a társadalmi hatásokra. Ugyanakkor azok könnyű hozzáférhetősége és megvalósíthatósága miatt az abban rejlő veszélyekre is figyelmeztet: *„[a]z önvezető járművek, a robotizálás, a szintetikus biológia és a mesterséges intelligencia mind lehetőségeket jelentenek a társadalom számára, de ezek rossz kezekben gyorsan biztonsági kockázatokká válnak."* (Hollandia 2018a, idézi: Kovács 2018b)

A stratégia szintén kiemelt figyelmet szentel a hibrid konfliktusok megjelenésére, és megállapítja, hogy *„vannak olyan államok, amely a hagyományos katonai, politikai, diplomáciai és gazdasági eszközökkel kombinálják az új technológia által elérhetővé vált különböző megoldásokat, amelyekkel céljuk a befolyásolás, valamint a stratégiai céljaik elérésére."* (Kovács 2018b) Így a hibrid konfliktusokat a stratégia az egyik olyan legmarkánsabb veszélyforrásként értékeli, amely megoldása a legsürgetőbb feladat is egyben. (Hollandia 2018a, Kovács 2018b)

A stratégia a fentiek mellett a legfontosabb veszélyeket a következőkben azonosítja:

- terrorista támadások;
- kiberveszélyek[97];
- nemkívánatos külföldi beavatkozások és zavarkeltések;
- katonai veszélyek;

[97] 2017-ben készült egy, a holland nemzeti kiberbiztonságot bemutató elemzés, amely egyik legfontosabb megállapítása, hogy Hollandia kiberfenyegetésekre való felkészültsége nagy lemaradásban van a gyors ütemben fejlődő veszélyekkel szemben. (Hollandia 2018a)

- gazdasági folyamatokra negatív hatást gyakorló veszélyek;
- a vegyi, biológiai, radiológiai és nukleáris fegyverek jelentette veszélyek. (Hollandia 2018a, Kovács 2018b)

A stratégia szerkezeti felépítését tekintve harmadik legnagyobb fejezete a korábban már említett megelőzés, védelem és megerősítés három pillérre építve mutatja be azokat a legfontosabb feladatokat, amelyeket az országnak a kihívásokra válaszul meg kell tennie.

A kihívások kezelése érdekében a stratégia meghatározza a kiberveszélyek elleni hatékony fellépést, valamint a kritikus infrastruktúrák, az energia, és egyéb fontos erőforrás védelmét. Ezt a védelmet nemzetközi együttműködésben, a következő stratégiai területeken és a következő feladatok elvégzésével látja kivitelezhetőnek a dokumentum:

- a fegyveres erők fejlesztése és modernizációja (ezt a terület Fehér Könyvében rögzítették is);
- a külkereskedelemre és a fejlesztési együttműködésekre vonatkozó politika kidolgozása;
- a diplomácia fejlesztése;
- integrált migrációkezelési terv;
- tematikus regionális és bilaterális kerettervek;
- a gazdasági biztonság növelésének akcióterve;
- nemzeti politika a nemzetbiztonsági szolgálatoka;
- Nemzeti Kiberbiztonsági Stratégia;
- Digitalizációs Program;
- nemzetközi politikai stratégia;
- Nemzeti Terrorizmus-elleni Stratégia. (Hollandia 2018a, Kovács 2018b)

A megelőzés, mint stratégiai pillér érdekében a dokumentum kiemeli a kibertevékenységekre vonatkozó világos nemzetközi normák meghatározásának szükségességét. Ehhez hatékony kiberdiplomáciára van szükség, amelyben Hollandia kész szerepet vállalni. A kibertérre vonatkozó nemzetközi jogi szabályozás kiinduló pontja Hollandia felfogása szerint a jelenlegi nemzetközi humanitárius jog, amelyet a kibertérre is érvényesíteni kell. Ezzel párhuzamosan a stratégia a kiberfegyverek exportjának[98]

[98] Itt nem csak a kiberfegyverek, hanem a kibertéri megfigyelő és ellenőrző rendszerek exportjának szabályozása is felmerül a stratégia alapján, mert Hollandia szerint az autokratikus államok gyakran

szabályozási kérdéseit is felveti: *„[a]z exportszabályozás hasznos és szükséges ahhoz, hogy megakadályozza az olyan katonai és egyéb kiberképességek elterjedését, amelyek kiberfegyverkezési versenyhez vezetnének."* (Hollandia 2018a, idézi: Kovács 2018b)

A második stratégiai pillér, azaz a védelem vonatkozásában a következő célkitűzéseket teszi a stratégia:

- modern, kollektív önvédelem Hollandia és a NATO országok területének védelme érdekében;
- erős kiberelrettentés;
- terrorelhárítás;
- társadalmi ellenállóképesség a külföldi befolyásolással szemben;
- gazdasági biztonság megteremtése;
- a nemzetközi bűnözés kezelése. (Hollandia 2018a, Kovács 2018b)

A felsorolt célkitűzések között szerepel a kiberelrettentés kialakítása is, de a stratégia ezt nem részletezi. A védelem egyik alapja lehet a már kialakult terrorizmus elleni diplomáciai hálózat, amely segítségével egyensúly teremthető a preventív és a represszív akciók között. Ebben a feladatban a magán- és a civil szféra bevonása is szükséges. (Hollandia 2018a, Kovács 2018b)

A megerősítés stratégiai pillér a következő feladatokat jelenti:

- a jelenlegi nemzetközi jogrend támogatása;
- a nemzetközi biztonsági együttműködések támogatása és erősítése;
- integrált és megbízható határellenőrzés. (Hollandia 2018a, Kovács 2018b)

Hollandia nemzeti kiberbiztonsági stratégiája

Hollandia jelenlegi kiberbiztonsági stratégiája 2018 áprilisában jelent meg *Hollandia Kiberbiztonsági Menetrendje: Hollandia digitálisan biztonságos* (Nederlandse Cybersecurity Agenda Nederland digitaal veilig) címmel. A dokumentum korábbi, 2011-ben, majd 2013-ban kiadott Nemzeti Kiberbiztonsági Stratégia legfontosabb megállapításaira épít, így azok felvillantása is célszerű ezen a helyen.

ezeknek a rendszereknek a használatával korlátozzák saját állampolgáraik személyiségi jogait. (Hollandia 2018a, Kovács 2018b)

A 2011-ben megjelent holland Nemzeti Kiberbiztonsági Stratégia számos olyan intézkedést tartalmazott, amelynek máig tartó szervezeti kihatásai is vannak a holland kiberbiztonság megvalósításában. A korábbi stratégia legfontosabb célja a biztonságos és megbízható IKT rendszerekre épülő digitális holland társadalom kiépítése. Többek között ennek érdekében került megalakításra a stratégiában felvázolt módon a Nemzeti Kiberbiztonsági Tanács,[99] valamint a Nemzeti Kiberbiztonsági Központot[100]. (Hollandia 2011, Kovács 2018b)

A stratégia a 2013-ban történt Nemzeti Kiberbiztonsági Értékelésre alapozva határozza meg a legfontosabb kibertéri kihívásokat és veszélyeket:

- a dolgok internete és az összekapcsoltság növekedése;
- a digitális formában elérhető adatok mennyiségének növekedése;
- a kibertér meghatározottsága nem csak a kormányokon, hanem a magánszférán is múlik;
- a kibertérben a polgári és katonai terület egyre inkább összefonódik, mivel a hasonló IKT rendszereket és alkalmazásokat használ mindkét terület, és jelentős a kölcsönös függőség is a rendszerek komplexitása miatt;
- egyre több és egyre felkészültebb szakembert igényel a terület. (Hollandia 2013b, Kovács 2018b)

Ez a stratégia a korábbi kiberbiztonsági stratégiához képest új megközelítést alkalmaz. A korábbi szervezeti struktúra központú stratégiával szemben az új stratégia a hálózatokra és a stratégiai együttműködésre helyezi a hangsúlyt, és emellett egy kockázat alapú megközelítést alkalmaz. Ezzel a fajta megközelítéssel a védelem és a különböző – például gazdasági, hatalmi stb. – érdekek között egyensúly teremthető. Ebben a fajta megközelítésben a szociális-gazdasági előnyök játszanak főszerepet úgy, hogy a kormányzat koordináló és irányító szerepet tölt be ebben. Így, bár a kormány felelős a kiberbiztonság megteremtéséért, de ez csak a személyiségi jogok védelmének figyelembe vételével,

[99] A Nemzeti Kiberbiztonsági Tanács a kormány független tanácsadó testülete. Feladata a kiberbiztonsággal kapcsolatos stratégiai tanácsadás és megoldási javaslatok kialakítása. A Tanács tagjai állami- és magánszervezetek, valamint a tudomány magas szintű képviselői. (Hollandia 2018b, Kovács 2018b)

[100] A nemzeti Kiberbiztonsági Központ az Igazságügyi Minisztérium alatt a kiberbiztonság nemzeti szintű koordinációjáért, a kiberbiztonsággal kapcsolatos információmegosztásért és a 24 órás incidenskezelésért felelős. (Hollandia 2018c, Kovács 2018b)

átlátható módon valósulhat meg. Ebben a munkában az állampolgárok, de a vállalkozások közreműködése, személyes felelősségvállalása, valamint elszámoltathatósága elengedhetetlen. (Kovács 2018b)

A stratégia által megfogalmazott legfontosabb célkitűzések (ambíciók):

- Hollandia ellenáll a kibertámadásoknak és megvédi létfontosságú érdekeit a kibertérben;
- Hollandia hatékonyan fellép a kiberbűnözéssel szemben;
- Hollandia olyan biztonságos IKT termékekbe és szolgáltatásokba invesztál, amelyek a magánélet védelmét biztosítják;
- Hollandia a kibertérben koalíciót hoz létre a szabadságért, a biztonság és a béke megvalósításáért;
- Hollandia kialakítja a kiberbiztonsághoz szükséges tudást és készségeket, valamint megteremti a kiberbiztonság megvalósításához szükséges IKT rendszerek innovációját. (Hollandia 2013b, Kovács 2018b)

Ezekhez a stratégiai célokhoz évente felülvizsgálandó akcióterv elkészítését is elrendeli stratégia, amely a 2014-2016 évekre a stratégia mellékleteként el is készült. (Hollandia 2013b, Kovács 2018b)

A stratégia hangsúlyozza, hogy a kiberbiztonsági célok elérése nemzetközi feladatokat is jelent, hiszen csak az integrált és más országokkal közös együttműködés révén lehet eredményre jutni. A nemzetközi együttműködésben az EU szintű gyakorlatok és a hatékony kiberbűnözés elleni nyomozati tevékenységek kiemelt szerepet játszanak. A nemzetközi munkában Hollandia meghatározó szerepet kíván játszani egyrészt egy nemzetközi együttműködési koalíció létrehozásával, másrészt nemzetközileg elfogadható kiberbiztonsági szabályozás kialakításával. A jogi szabályozás területén Hollandia is támogatja a Budapest Konvenció szélesebb körű, még több országra kiterjedő ratifikációját. (Hollandia 2013b, Kovács 2018b)

A stratégia a hadsereg kibertérben játszott szerepére és a hadsereg kibervédelmi képességeinek növelésére is kitér. Ugyanakkor a fentiekben megfogalmazottak alapján a dokumentum hangsúlyozza a polgári és katonai együttműködés szükségességét is. A kibertér komplex környezetében a polgári hírszerző, rendőrségi, vagy kiberbiztonsági szervezetek információi és kiberbiztonsági képességei szükségesek a hadsereg feladatainak ellátásához.

A 2013-ban megjelent Nemzeti Kiberbiztonsági Stratégia után 2018 áprilisában a Holland Kormány elfogadta *Hollandia Kiberbiztonsági Menetrendje: Hollandia digitálisan biztonságos* című dokumentumot. Ebben az egyik legmarkánsabb elem annak kijelentése, hogy a kiberbiztonság a nemzeti biztonság része. A dokumentum utal arra, hogy Hollandia korábbi kiberbiztonsági stratégiái (2011, 2013) megfelelő alapot nyújtottak a nemzeti kiberbiztonság megteremtéséhez, ugyanakkor az újabb kiberveszélyek és fenyegetések ezek áttekintését és részben módosítását igénylik.

A stratégia a kormányzat és a magánszektor közötti szoros összefogást tűzi ki célul. Ezzel kapcsolatban Ferd Grapperhau holland Igazságügyi és Védelmi Miniszter, aki a stratégia előszavát is jegyzi, így nyilatkozott: *„[a] kiberbiztonság elválaszthatatlanul kapcsolódik a nemzetbiztonsághoz és társadalmunk zavartalan működéséhez. Most, hogy látjuk a kibertámadások fenyegetése tovább növekszik, a biztonság alapvető szintjét is emelni kell. Ugyanakkor ezt a Kormány egyedül nem tudja elvégezni. A holland kiberbiztonsági menetrend csak akkor lehet sikeres, ha a kormány és az üzleti szféra együttesen lép fel annak érdekében."* (Hollandia 2018d, idézi: Kovács 2018b)

Az új stratégiában megfogalmazott stratégiai célkitűzések hasonlóak a korábbi stratégiák által megadottakhoz:

- Hollandiának megvan a saját digitális ereje;
- Hollandia hozzájárul a nemzetközi béke és biztonság megteremtéséhez a digitális területen;
- Hollandia élen jár a biztonságos hardverek és szoftverek népszerűsítésében és azok fejlesztésének ösztönzésében;
- Hollandia rendelkezik a biztonságos digitális technológiákkal és kritikus infrastruktúrákkal;
- Hollandia a megfelelő kiberbiztonsággal harcol a kiberbűnözés ellen;
- Hollandia vezető szerepet tölt be a kiberbiztonsághoz szükséges tudásfejlesztés terén;
- Hollandia az integrált, magán- és közszféra együttműködésére épülő megközelítést képviseli a kiberbiztonság terén. (HSD Foundation 2018, Hollandia 2018d, Kovács 2018b)

Természetesen a stratégia ezekhez a célokhoz feladatokat is hozzárendel. Az egyik ilyen feladat például a kiberbűnözés elleni törvény elkészítése és annak 2020-ban történő hatálybaléptetése. További feladatok:

- az ágazati CERT-ek (például az egészségügyi, vagy a biztosítási szektorban) felállítása;
- nemzeti kibertámadás detektáló hálózat felállítása;
- NCSC és a Digitális Megbízhatósági Központ (Digital Trust Center, DTC) képességeinek fejlesztése;
- a Globális Bizottság a Kibertér Stabilitásáért (Global Commission on the Stability of Cyberspace, GCSC)[101] munkájának támogatása. (Hollandia 2018d, Kovács 2018b)

2.4.7. Magyarország

Magyarország nemzeti biztonsági stratégiája

Magyarország nemzeti biztonsági stratégiája jelenleg felülvizsgálat alatt áll. A felülvizsgálat oka az elmúlt hat évben bekövetkezett biztonságpolitikai változások, valamint az időközben megjelent új biztonsági kihívások és veszélyek.

Ennek megfelelően jelenleg csak a 2012-ben megjelent Nemzeti Biztonsági Startégiát és az abban a kibertérre vonatkozó kitételeket lehet elemezni, illetve bemutatni. A stratégia, amely hivatalosan a *Kormány 1035/2012. számú határozata Magyarország Nemzeti Biztonsági Stratégiájáról* címet viseli alapvető változásokat hozott a kibertér biztonságáról való kormányzati gondolkodásban. Erre az egyik legjobb bizonyíték a stratégia Magyarország biztonságát meghatározó tényezők, illetve veszélyforrások meghatározása, amelyek közé markánsan bekerült a kiberbiztonság és a kibertérben jelentkező veszélyek együttese: „*Kiberbiztonság. Az állam és a társadalom működése – a gazdaság, a közigazgatás vagy a védelmi szféra mellett számos más területen is – mind meghatározóbb módon a számítástechnikára épül. Egyre sürgetőbb és összetettebb kihívásokkal kell számolnunk az informatikai- és telekommunikációs hálózatok, valamint a kapcsolódó kritikus infrastruktúra fizikai és virtuális terében. Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem-állami – akár terrorista – csoportok arra használhatják, hogy*

[101] A Globális Bizottság a Kibertér Stabilitásáért nevű szervezetet a Hágai Stratégiai Tanulmányok Központja (The Hague Centre for Strategic Studies, HCSS) a Kelet-Nyugat Intézettel (EastWest Institute, EWI) közösen hozta létre. A bizottság támogatói között van a holland és azt észt kormány, valamint a francia külügyminisztérium is. A szervezet legfontosabb feladata, hogy a kibertér biztonságának fokozása érdekében szükséges nemzetközi együttműködéseket elősegítse. (GCSC 2018, Kovács 2018b)

megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését. E támadások eredetét és motivációját gyakran nehéz felderíteni. A kibertérben világszerte növekvő mértékben jelentkező nemzetbiztonsági, honvédelmi, bűnüldözési és katasztrófavédelmi vonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelem feladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására Magyarországnak is készen kell állnia. [A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról]

A stratégia a holisztikus megközelítés elvét alkalmazza, amely érvényes a kiberbiztonság esetében is. Ez a következőkben érhető tetten: *„[...] egyszerre jelenik meg a kibertértől való függőség, annak minden lényeges és – a társadalom egésze számára – fontos jellemzője, az olyan veszélyforrások, mint a szabad információáramlás és az ezt esetlegesen kihasználó, így a támadások megszervezéséhez meglehetősen könnyen információkhoz hozzáférő terrorizmus, valamint a kritikus infrastruktúra védelme is."* (Kovács 2018b)

A Nemzeti Biztonsági Stratégia alapján a kibertérben jelentkező fenyegetések és veszélyek kezelése állami tevékenység kell, hogy legyen. (A stratégiából adódóan ezek nyilvánvalóan a stratégiai szintű veszélyek kezelésére vonatkoznak, amely alapján az üzemeltetők, tulajdonosok, valamint felhasználók a saját szintjükön kell, hogy megtegyék a tőlük elvárható védelmi megoldásokat). A stratégia a kiberbiztonság állami feladatait is megnevezi: „*a) Elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális fenyegetések és kockázatok rendszeres felmérése és priorizálása, a kormányzati koordináció erősítése, a társadalmi tudatosság fokozása, valamint a nemzetközi együttműködési lehetőségek kiaknázása. b) A nemzeti kritikus információs infrastruktúra védelmének erősítése mellett szövetségeseinkkel és EU-partnereinkkel együtt arra törekszünk, hogy az információs rendszerek biztonsága erősödjön, valamint részt vegyünk a megfelelő szintű kibervédelem kialakításában."* [A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról]

Magyarország nemzeti katonai stratégiája

Eltérően néhány európai ország – például Ausztria, Szlovákia, Franciaország – stratégiai dokumentumaitól, amelyek úgynevezett fehér könyvben rögzítik az adott ország védelempolitikai alapelveit és a hadsereg stratégiai feladatait, hazánk külön nemzeti katonai stratégiában határozza meg a hadsereg és a hadügy stratégiai kérdéseit.

Magyarország Nemzeti Katonai Stratégiája a nemzeti biztonsági stratégiához hasonlóan 2012-ben jelent meg. A dokumentum előremutató módon már számos kiberbiztonsággal kapcsolatos kitételt tartalmaz. Ilyen, a kiberbiztonsággal kapcsolatos megállapítás a biztonság és stabilitás ellen ható folyamatok bemutatása során is megjelenik: *„[ú]j kihívást és potenciális veszélyforrást jelent a globális közjavak – a nyílt tenger, a nemzetközi légtér, a világűr és a kibertér – hozzáférhetősége, használata. Ezek közül kiemelkedik a számítógépes hálózatok elleni támadások növekvő száma és károkozási potenciálja. A kiberfenyegetésnek a hagyományos fenyegetésektől eltérő jellemzői szükségessé teszik a háborúval kapcsolatos fogalmaink átfogó felülvizsgálatát és adott esetben módosítását."* [A Kormány 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról 33. pont]

A fenti idézet utolsó mondata – *„[a] kiberfenyegetésnek a hagyományos fenyegetésektől eltérő jellemzői szükségessé teszik a háborúval kapcsolatos fogalmaink átfogó felülvizsgálatát és adott esetben módosítását"* – sokkal többet engedtek sejtetni, mint ami például a nemzeti biztonsági stratégia kibertérrel kapcsolatos meghatározásaiból következne. Ez alapján ugyanis lehetőség lett volna a kiberhadviselés hazai definíciós készletbe való átültetésére, illetve annak kidolgozására. Ez azonban nem történt meg doktrínális szinten, csak a tudományos kutatók körében voltak erre kísérletek. Ugyanakkor ez annál is inkább előremutató lett volna, mert a NATO csak ezt követően, mintegy négy évvel később, a 2016-os a varsói csúcsértekezleten deklarálta a kiberteret, mint hadviselési dimenziót.

A stratégia utal az aszimmetrikus kihívások miatt átalakuló biztonsági kihívások során a haderő várható alkalmazásának jellemzőire, ahol már meg is jelenik a kiberhadviselés, mint kifejezés: *„[a] nem fegyverrel elkövetett, halálos áldozatot közvetlenül nem követelő, de hatalmas anyagi károkat és káoszt előidézni képes újfajta, aszimmetrikus kihívások miatt bővült a háború és a támadás fogalmainak jelentése. A károkozás mértékétől függően egy nem fegyveres támadás – megítélését tekintve – akár egy fegyveres támadással is egyenértékű lehet. Ilyen fenyegetést jelent elsősorban a kiberhadviselés, amely anyagi kár okozásában és a közrend megzavarásában potenciálját tekintve egyre kevésbé marad el a hagyományos fegyverektől."* [A Kormány 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról 52. pont]

A stratégia kitér a Magyar Honvédség kibertérrel kapcsolatos feladataira is: *„[a] Magyar Honvédség egyik célja a hálózatalapú hadviselés feltételeinek megteremtése. Ennek részeként erősíteni kell a Magyar Honvédség kibervédelmét, amihez koncepcionálisan*

megalapozott rendszabályok kidolgozása, modern eszközök beszerzése, valamint az állomány megfelelő felkészítése és kiképzése szükséges." [A Kormány 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról 82. pont]

A fentiekben a kiberhadviseléssel kapcsolatosan megfogalmazott kritikám itt is igaz, hiszen a Magyar Honvédség kibervédelmi képességeinek fejlesztése megkezdődött, az ehhez szükséges jogszabályi és szervezeti keretrendszer kialakításával, de magának a kiberhadviselésnek sem a jogszabályi, sem a szervezeti keretei egyelőre nem kerültek felállításra és kidolgozásra. Az első fejezetben bemutatott kiberhadviselés fogalmi háttere is nagyon jól szemlélteti, hogy a kiberhadviselési képességek összetett, komplex rendszerben jöhetnek csak létre, amelyben a kibertéri felderítés, a kibervédelem, a kibertámadás, és a rendszerszintű nemzetközi együttműködés egyaránt helyet kell, hogy kapjon.

Magyarország nemzeti kiberbiztonsági stratégiája

Magyarország jelenleg érvényben lévő nemzeti kiberbiztonsági stratégiája 2013-ban jelent meg. Maga a stratégia épít a nemzeti biztonsági stratégia a kibertérrel kapcsolatos elveire, és túlzás nélkül kijelenthető: történelmi dokumentumról van szó, hiszen ez hazánk első olyan stratégiai dokumentuma, amely kimondottan a kiberbiztonságot célozza meg, és mint ilyen nyugodtan nevezhető mérföldkőnek is, hiszen meghatározó jelentőséggel bír a hazai kiberbiztonság területén[102]. (Kovács 2018b)

A stratégia összesen 6 oldalnyi terjedelmű dokumentum, amely azonban ebben a rövid terjedelemben is iránymutatást adott és feladatokat szabott a kiberbiztonság hazai megvalósítása érdekében. Ugyanakkor nyilvánvalóan ebbe a terjedelembe nem fért bele a kibertéri kihívások és veszélyek részletese elemzése, azok összefüggéseinek bemutatása. Ennek megfelelően a stratégia csak utal a nemzeti biztonsági stratégia legfontosabb célkitűzéseinek kiberbiztonsággal való támogatására, de a hatásokat nem fejti ki részletesen.

A stratégia célja, építve Magyarország Alaptörvényére, illetve a már említett nemzeti biztonsági stratégiában meghatározott célkitűzésekre a következőkben foglalható össze:

[102] A nemzeti kiberbiztonsági stratégiát megelőzően számos hazai stratégia született az információs társadalom fejlesztése oldaláról, például 2001-ben és 2003-ban. (NITS 2001, MITS 2003, Kovács 2018b) Ugyanakkor ezen a téren az első olyan stratégia, amely a biztonságot is érintette a *Digitális megújulás cselekvési terv 2010-2014* volt. (DMCST 2010, Kovács 2018b) Nem sokkal a nemzeti kiberbiztonsági stratégiát követően jelent meg a *Nemzeti Infokommunikációs Stratégia 2014-2020*, amely a kiberbiztonsággal kapcsolatban szintén számos stratégiai elemet tartalmazott például a kritikus információs infrastruktúrák, a közigazgatás rendszereinek, vagy a felhasználói adatok védelmének területén. Ez a stratégia mindezek mellett a felhasználóknak a kibertéri kockázatokkal és azok kezelésével kapcsolatos folyamatos tájékoztatására is kitért. (Nemzeti Infokommunikációs Stratégia 2014, Kovács 2018b)

„[j]elen stratégia célja, hogy az Alaptörvény elveivel összhangban, az értékek és érdekek számbavétele, valamint a kibertér biztonsági környezetének elemzése alapján meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is." [1139/2013. (III. 21.) Korm. határozat 1. pont]

A stratégia egy új fogalmat is bevezetett, amely a magyar kibertér. Ezt a következőkkel magyarázza a dokumentum: *„Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.*" [1139/2013. (III. 21.) Korm. határozat 3. pont]

A stratégia igyekszik bemutatni Magyarország kiberbiztonsági környezetét (benne a már említett magyar kibertérrel) és komplex módon értelmezi a kibertérben lévő veszélyeket és kihívásokat. Azok egymásra gyakorolt hatását ugyanakkor csak megemlíti. Magára a kiberbiztonságra azonban egy jól alkalmazható meghatározást ad: *„[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."* [1139/2013. (III. 21.) Korm. határozat 5. pont]

A dokumentum megadja azokat a stratégiai célokat, amelyeket hazai kiberbiztonság kialakítása és fenntartása érdekében szükségesek. A célok logikusan épülnek egymásra és azok kiterjednek a felhasználókra (állampolgárokra) és a szervezetekre egyaránt. A stratégiai célok a következők:

- a meglévő és potenciálisan jelentkező kihívásokkal szemben ki kell alakítani egy hatékony megelőző, észlelési, reagálási képességet, amelybe a kibertámadások esetleges bekövetkezése esetén a helyreállítási képességek is bele kell, hogy tartozzanak;
- a nemzeti adatvagyon védelmét kiemelten kell kezelni;
- az információs rendszerek és szolgáltatások színvonalát a lehető legmagasabban kell tartani, és biztosítani kell azok nemzetközi biztonsági tanúsítványoknak való megfelelését;

- az oktatás és képzés, valamint a kutatás-fejlesztés területeken biztosítani kell a legmagasabb színvonalat;
- biztosítani kell a kibertérben a gyermekek védelmét. [1139/2013. (III. 21.) Korm. határozat]

Ezekhez a sok esetben csak általánosságban megfogalmazott célokhoz a stratégia feladatokat hozzárendel. Ezek részletesebb tárgyalásban jelennek meg a dokumentumban. Összefoglalva ezek főbb elemeit a következő feladatok kerültek a hazai kiberbiztonság érdekében stratégiai szinten meghatározásra:

- olyan kormányzati koordinációt kell megvalósítani, amely során a Miniszterelnökség vezetésével az összkormányzati koordináció erősödik, valamint a kormányzati és ágazati erőforrásokat koordináltan és lehetőleg koncentráltan kerülnek felhasználásra és alkalmazásra;
- erősíteni kell az együttműködést, amelyhez olyan operatív együttműködési fórumok működtetése szükséges, amelyeken keresztül a köz- és a magánszféra, valamint a tudományos területek hozzá tudnak járulni a megfelelő kormányzati döntések előkészítéséhez;
- megfelelő szakintézmények kialakítása szükséges, amelyek a szakértelem mellett megfelelő hatáskörrel is rendelkeznek, és amelyek képesek együttműködni a hatósági feladatokat ellátó más szervezetekkel is. Ezeknek a szakintézményeknek, nevezetesen a kormányzati eseménykezelő központnak és az ágazati eseménykezelő központoknak az európai kormányzati incidenskezelő csoport (European Governmental CERT Group) által kell akkreditációt szerezniük;
- megfelelő szabályozási környezetet kell kialakítani, amely alapján a magán-, a köz- és az akadémiai szféra között is olyan együttműködési megállapodások jöhetnek létre, amelyek a kiberbiztonság területén megvalósuló közös felelősségvállalást teszik lehetővé;
- folytatni és erősíteni kell a nemzetközi együttműködést, amely az EU és a NATO keretein belül már kialakult a kiberbiztonság területén, valamint az ENSZ és az EBESZ kiberbiztonsági együttműködési tevékenységében is aktívan részt kell venni;

- erősíteni kell mind az egyéni felhasználók, mind a kis- és középvállalkozások kiberbiztonsági tudatosságát, amelyhez fel kell használni egyrészt a szakintézményeket, valamint a civil, a gazdasági és a tudományos terület szereplőivel kialakított már meglévő együttműködéseket is;
- tovább kell növelni az oktatás, valamint a kutatás-fejlesztés területén a kiberbiztonsággal kapcsolatos tevékenységeket, amely egyrészt a kiberbiztonság oktatásba való integrációját, másrészt a kiberbiztonsági kutatás-fejlesztésben kiemelkedő és nemzetközileg is jegyzett, ott eredményeket elérő egyetemi és tudományos kutatóhelyekkel történő együttműködést jelenti;
- erősíteni kell a kibertérben megvalósuló gyermekvédelmet, amely az ennek a korosztálynak szánt minőségi online tartalmak előállítására, a tudatosságnövelő és felkészítő intézkedések kialakítására és bevezetésére, valamint a gyermekek online zaklatása és kizsákmányolása elleni küzdelemre kell, hogy kiterjedjen;
- erősíteni kell a gazdasági szereplők motivációját, amely az infokommunikációs eszközöket, rendszereket és szolgáltatásokat gyártók számára a nemzetközi biztonsági tanúsítási szabványoknak való megfelelést irányozza elő, másrészt a gazdasági élet szereplőivel közösen kidolgozandó a kiberbiztonság fokozását célzó intézkedéseket jelent. [1139/2013. (III. 21.) Korm. határozat] (Kovács 2018b)

A stratégia ezeknek a feladatoknak a sikeres elvégzését széles társadalmi összefogásban látja. Ennek megfelelően a szükséges a kormányzati szervezetek, a magánszektor szervezetei és az akadémiai szféra (Magyar Tudományos Akadémia, egyetemek, kutatóintézetek) szoros és világos elvi alapokon nyugvó együttműködése.

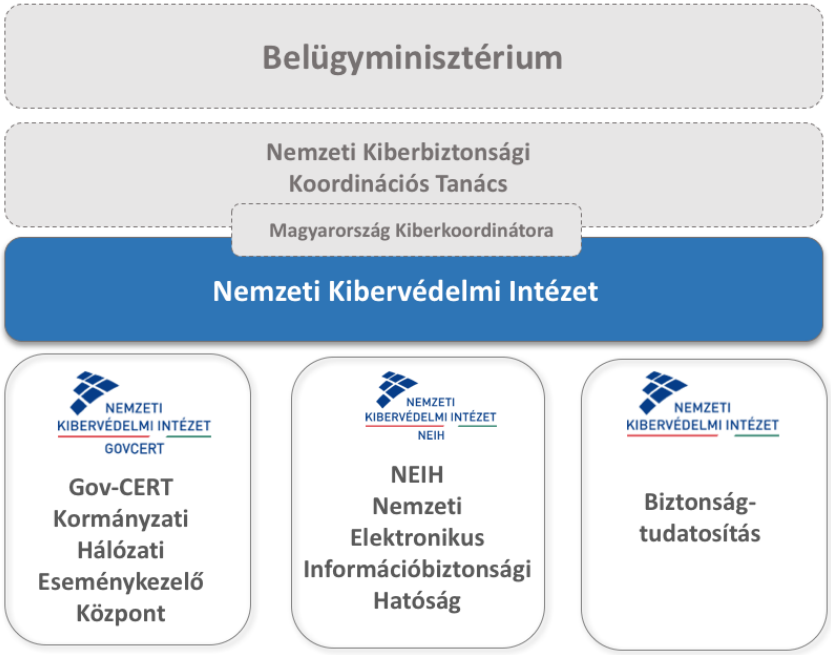
A feladatok végrehajtására hivatott kormányzati szervezetrendszer már korábban is működött egyfajta kiépítésben, de ennek átalakítása és fejlesztése szükséges volt. Az eseménykezelés területén ekkor már működtek hazai CERT-ek, például a 2002-ben megalakított CERT-Hungary,[103] vagy a SZTAKI CERT. Ugyanakkor a koordináció és az

[103] A CERT-Hungary 2002 alakult meg a Puskás Tivadar Közalapítvány égisze alatt. 2010. január 1-étől *Az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendelet* alapján a Nemzeti Hálózatbiztonsági Központ nevet kapta kiterjesztett feladatokkal. (Kormányzati Eseménykezelő Központ 2009, Kovács 2018b) Ezt követően a 2013. évi L törvény alapján létrejött a Kormányzati Eseménykezelő Központ (GovCERT-Hungary) 2013 júliusában. Ennek megfelelően a CERT-Hungary (Nemzeti Hálózatbiztonsági Központ) megszűnt. (Kovács 2018b)

együttműködés javítása elengedhetetlen volt. Erre a feladatra hozta létre a stratégia a Nemzeti Kiberbiztonsági Koordinációs Tanácsot. (Kovács–Szentgáli 2015, Kovács 2018b)

A nemzeti kiberbiztonsági stratégia teremtette meg a keretet ahhoz, hogy a hazai kiberbiztonság, illetve információbiztonság törvényi szabályozása megtörténjen. 2013-ban fogadta el az Országgyűlés az úgynevezett információbiztonsági törvényt, amely a *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról* hivatalos címet kapta. E törvény – és nyilvánvalóan a stratégia – hatására átalakult a hazai kiberbiztonsági szervezetrendszer. Ez azonban az első két évben heterogén volt, *„a szervezeti elemek gyakran egymás feladatait is jelentős mértékben átfedték.”* (Kovács 2018b)

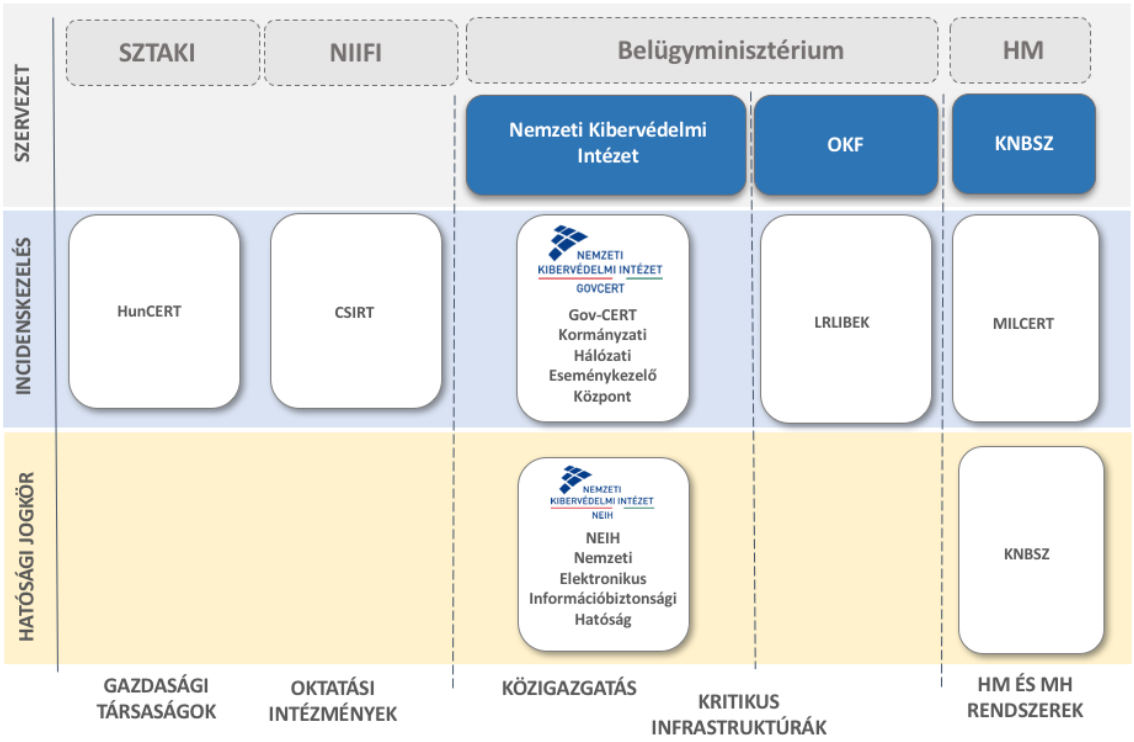
Az információbiztonsági törvény módosításra kerül, és 2015. október 1-gyel új szervezeti rendszer kialakítása történt meg hazánkban. Létrejött a Nemzeti Kibervédelmi Intézet (NKI), amelyet a Belügyminisztérium égisze alatt lévő Nemzetbiztonsági Szakszolgálat (NBSZ) működtet. Az NKI egyik lényeges eleme a GovCERT-Hungary, azaz Kormányzati Hálózati Eseménykezelő Központ. Az NKI másik fontos pillére a Nemzeti Elektronikus Információbiztonsági Hivatal (NEIH). Az NKI mindezen feladatok mellett információbiztonsági tudatosítási, valamint az állami- és önkormányzati szervezetek munkatársainak felkészítési tevékenységeit is ellátja. (Kormányzati Eseménykezelő Központ 2017, Kovács 2018b)



6. ábra
A Nemzeti Kibervédelmi Intézet pillérei és kapcsolódásai

Forrás: Bencsik 2015, Kovács 2018b, szerkesztette: szerző

Az információbiztonsági törvény említett módosítása és az időközben bekövetkezett változások bár új szervezeti keretrendszert jelentenek a hazai kibervédelemben, az mégsem homogén. Ennek oka sokrétű, hiszen számos szervezet, mint például a már említett Nemzeti Kibervédelmi Intézet, amely fő feladataként az állami és önkormányzati szervezetek rendszerei védelmében vesz részt, vagy a kritikus infrastruktúrák védelméért is felelős Országos Katasztrófavédelmi Főigazgatóság (OKF) alárendeltségében működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (LRLIBEK), és később a Honvédelmi Minisztérium (HM) alatt a Katonai Nemzetbiztonsági Szolgálatnál (KNBSZ) létrejött katonai CERT (HÁEIEK, azaz Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ) is felelős a hazai kibertér egy-egy szegmenséért.



7. ábra
A 2015-óta működő hazai állami kibervédelmi szervezetek

Forrás: Bencsik 2015, szerkesztette: szerző

Az inhomogenitás másik oka pedig a szervezetek eltérő képességeiben, valamint a már stratégiai szinten sem teljesen jól szabályozott feladatokban keresendők. Ilyen, a feladatban megjelenő szabályozási hiányosság a stratégiai szinten hatékony koordinációt biztosító szervezet hiánya. Másik stratégiai hiányosság a már szintén említett kibertámadó képességek és ennek megfelelő szervezethez (például hadsereg) való kötésének hiánya.

A nemzeti kiberbiztonsági stratégia említett felülvizsgálata eredményeként létrejövő új stratégia ezekre a kérdésekre is választ kell, hogy adjon.

2.4.8. Lengyelország

Lengyelország nemzeti biztonsági stratégiája

2014-ben született meg Lengyelország jelenleg érvényben lévő nemzeti biztonsági stratégiája. A stratégia felsorolja Lengyelország értékeit és érdekeit, majd globális, regionális és nemzeti szinten is megvizsgálja az ország biztonsági környezetét, stratégiai tevékenységekként mutatja be a nemzeti biztonsági célokat, illetve az ezekhez a célokhoz szükséges feladatokat és szervezeti keretrendszert. (Lengyelország 2014b, Kovács 2018b)

A kibertér markánsan jelenik meg a nemzeti érdekek és az ezekkel összefüggő stratégiai célok meghatározásánál. A stratégia kiemeli, hogy Lengyelország biztonságos működésének egyik alapfeltétele a kibertér biztonsága. Ennek megfelelően a nemzeti biztonság garantálása érdekében megfogalmazott védelmi képességek sorában a kibervédelmi kapacitásoknak is rendelkezésre kell állniuk.

A stratégia értékeli azokat a globális kihívásokat és veszélyeket, amelyekkel Lengyelországnak szembe kell néznie. Ebben a kibertér a következő módon jelenik meg: *„[a]z új információs és kommunikációs technológiák (IKT) megjelenésével és az internet fejlődésével új fenyegetések jelentek meg, mint például a számítógépes bűnözés, a kiberterrorizmus, a kiberkémkedés és a kiberkonfliktusok nem állami szervezetek támogatásával, valamint megjelent a kiberháború, mint az országok közötti kibertéri konfrontáció. A virtuális térben bekövetkező fenyegetések alakulásának jelenlegi tendenciái egyértelműen azt mutatják, hogy a kibertér biztonsága egyre növekvő befolyást gyakorol az ország általános biztonságára. Figyelembe véve, hogy növekszik az IKT-tól való függés, a kibertéri konfliktusok súlyosan megzavarhatják a társadalom és az államok működését."* (Lengyelország 2014b, idézi: Kovács 2018b)

A regionális biztonsági környezet értékelése során szintén megjelenik a kibertér védelme. Ezzel kapcsolatban a bilaterális alapon, vagy a NATO és EU szövetséges keretek között megvalósuló nemzetközi együttműködés fontosságát emeli ki a stratégia. A nemzeti szintű biztonsági környezet értékelése során a kibertér vonatkozásában a nemzeti infokommunikációs rendszerek zavartalan működésének biztosítása az egyik kiemelt cél, de a felhasználók kiberbiztonsági tudatosságának alacsony fokában jelentkező kihívások kezelése is bekerült a stratégiába. (Lengyelország 2014b)

A stratégia a hadsereg kibertéri tevékenységei és az ehhez szükséges képességek kialakítása vonatkozásában is eligazítást ad: *„[a] kibertér a fegyveres küzdelem*

dimenziójává vált. Ezen a területen a Lengyel Köztársaság fegyveres erőinek rendelkezniük kell védelmi és támadó képességekkel annak érdekében, hogy a potenciális ellenfelek elrettentése megvalósítható legyen. Különösen készen kell állniuk – akár függetlenül, akár szövetségeseikkel együttműködve – védelmi műveletek szélesebb körű megvalósítására kiberkonfliktus vagy kiberháború esetén." (Lengyelország 2014b, idézi: Kovács 2018b)

A stratégia meghatározza egy Nemzeti Kiber Incidens Kezelési Rendszer kiépítését és egy nemzeti kiberkoordinációs központ felállítását is. A kiberbiztonsági szervezeti rendszernek támogatnia kell a köz- és magánszféra együttműködését, ezen belül a PPP konstrukciók megvalósítását, és hozzá kell járulnia a kiberbiztonság tudatosság emeléséhez Lengyelországban. A szervezetet úgy kell kialakítani, hogy az együtt tudjon működni más országok hasonló rendszereivel. (Lengyelország 2014b, Kovács 2018b)

Lengyelország nemzeti kiberbiztonsági stratégiája

Lengyelországban 2010-ben jelent meg a *Kormányzati kiberbiztonság 2011-2016 cselekvési terv* (Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011-2016, RPOC) című dokumentum, amely első volt a kiberbiztonságot meghatározó stratégiai dokumentumok között. Többek között az ebben a dokumentumban meghatározottak alapján állt fel a lengyel CERT közösség, benne a CERT GOV.PL is. (CertGov.PL 2017) Ez a kormányzati CERT adott keretet a Belső Biztonsági Ügynökségnek (ABW), amely aktív szerepet töltött be a kormányzati CERT feladatainak megvalósulása során. Ebben az időszakban együttműködésben a legrégebbi nemzeti incidenskezelővel, a CERT CERT Polskával, olyan előremutató fejlesztéseket hajtottak végre, mint az ARAKIS-GOV nevű korai kiberfenyegetés előrejelző rendszer kiépítése. (Kovács 2012, Kovács 2018b)

2017-ben azonban új kiberbiztonsági stratégia született *Lengyelország Kiberbiztonsági Politikájának Keretrendszere 2017-2020* címmel. Az ebben megfogalmazott stratégiai cél a köz- és magánszektor biztonságának garantálása az alapvető digitális szolgáltatások használata során. Ennek a legfőbb célnak az elérése érdekében a következő részcélokat és az azokhoz kapcsolódó feladatokat határozza meg a stratégia:

- megnövelt nemzeti kiberbiztonsági képességek létrehozása az IKT rendszerek hatékony védelme érdekében: olyan jogszabályi keretrendszer kidolgozása szükséges, amely megfelel a kibertér kihívásainak; erősíteni kell a kibervédelmi szervezetek rendszerét; erősíteni kell az érdekelt felek együttműködését; növelni kell az IKT eszközök és rendszerek biztonságát a kritikus infrastruktúrákban;

fejleszteni kell azokat a szabályzókat, ajánlásokat, valamint törekedni kell azoknak a legjobb gyakorlatok bevezetésére, amelyek a hálózati és információs rendszerek biztonságához hozzájárulnak; növelni kell a kockázatmenedzsment hatékonyságát; növelni kell a beszállítói lánc biztonságát;

- a kiberfenyegetések elleni hatékony fellépés növelése: ennek magába kell foglalnia a kiberbűnözés, a kiberkémkedés és kibertéri terrorista akciók elleni fellépés hatékonyságának növelését; el kell érni azokat a katonai képességeket, amelyek lehetővé teszik, hogy a hadsereg a műveletek teljes spektrumában képes legyen a kibertérben[104] tevékenykedni; nemzeti szintű kiberfenyegetettség értékelő képességet kell kiépíteni; a nemzetbiztonság számára biztonságos kommunikációs rendszert kell felállítani; biztonságos audit és teszt képességekkel kell rendelkezni;
- nemzeti potenciál és kompetencia növelése a kibertér biztonsága érdekében: a kiberbiztonsági célú ipari és technológiai erőforrások fejlesztését ösztönözni kell; együttműködési mechanizmusokat kell kialakítani a köz- és magánszektor között; motiválni kell a kiberbiztonsági kutatás és fejlesztési tevékenységeket; növelni kell az IKT rendszereket használók digitális kompetenciáit és képességeit, amelynek ki kell terjednie az állampolgárok ilyen képességeire is;
- erős nemzetközi pozíció kiépítése Lengyelország számára a kiberbiztonság területén mind stratégiai, mind politikai szinten. (Lengyelország 2017b, Kovács 2018b)

Ezeknek a céloknak az elérése érdekében egy olyan akcióterv (Action Plan for implementetion of the National Framework of Cybersecurity Policy) elkészítését is elrendeli a stratégia, amelynek többek között a megvalósítandó feladatok anyagi hátterének biztosítására is ki kell terjednie. (Lengyelország 2017b, Kovács 2018b)

[104] A stratégia itt utal arra, hogy a NATO a 2016-os Varsói Csúcstalálkozón a kiberteret hadviselési dimenzióként elismerte. (NATO 2016a, Lengyelország 2017b, Kovács 2018b)

2.4.9. Németország

Németország nemzeti biztonsági stratégiája

2016 nyarán jelent meg Németország jelenlegi nemzeti biztonsági stratégiája, amely címe *Fehér könyv 2016 Biztonságpolitika és a Bundeswehr jövője* (Weissbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr).

A dokumentum előszavában Angela Merkel kancellár már utal a kibertérre, és ezzel kapcsolatban rámutat, hogy a kibertér ma már nem csak előnyöket hordoz magában, hanem a gyűlölet és az erőszak ideológiáinak terjesztésére is felhasználható eszköz. (Németország 2016a, Kovács 2018b)

A stratégia a német biztonságpolitika legfontosabb tényezőinek számba vételével kezdődik, amelyben Németország nemzetközi biztonsági rendszerben betöltött szerepe kerül bemutatásra és elemzésre. Ezt követően a stratégia felsorolja az ország értékeit és érdekeit. (Németország 2016a, Kovács 2018b)

Németország biztonsági környezetének értékelése során a stratégia feltárja a legfontosabb biztonsági kihívásokat. Ezekben már helyet kapnak a kibertéri kihívások is:

- nemzetközi terrorizmus;
- a kiber- és az információs tér kihívásai;
- nemzetek közötti konfliktusok;
- labilis államok és gyenge kormányzás;
- globális fegyvergyártás és kereskedelem, valamint a tömegpusztító fegyverek proliferációja;
- az információs és kommunikációs rendszereket, az ellátási láncokat, és szállítást, a nyersanyagok biztosítását és az energia szektort fenyegető veszélyek;
- a klímaváltozás;
- az ellenőrizetlen migráció;
- epidémia és pandémia. (Németország 2016a, Kovács 2018b)

A kihívások felsorolásakor látható, hogy a kiber- és információs térben jelentkező, valamint az információs és kommunikációs rendszereket fenyegető veszélyek külön kategóriát jelentenek. Ugyanakkor a kibertéri veszélyek esetében nagyon markánsan fogalmaz a stratégia, hiszen megállapítja, hogy a kibertérben bekövetkező konfliktusok hatásaik tekintve egyenlőek lehetnek a fizikai térben bekövetkező fegyveres

konfliktusokkal: *„[a] kibertámadások hatásai megegyezhetnek a fegyveres konfliktusok hatásaival, és a fizikai dimenzióra is kiterjedhetnek."* (Németország 2016a, idézi: Kovács 2018b)

Bár a kihívások felsorolásánál látható módon az információs és kommunikációs rendszereket fenyegető veszélyek külön szerepelnek, de azokat a stratégia nem különíti el teljes mértékben a kibertértől. A stratégia ezzel kapcsolatban arra a függőséget kívánja a figyelmet felhívni, amelyek az információ, az energia, a szállítás, nyersanyagok, mint erőforrásokkal szemben alakultak ki. Ezt a következőképpen fogalmazza meg a stratégia: *„[a] jövőben hazánk fellendülése és állampolgáraink jóléte jelentősen függ a globális információs és kommunikációs rendszerek, az ellátási láncok, a szállítási útvonalak, valamint a nyersanyagok és az energia biztonságos ellátásának akadálytalan felhasználásától. Az ilyen globális közjavakhoz való földi, légi, tengeri, kiber és információs térben, valamint az űrben való hozzáférés megszakadása jelentős kockázatot jelent államunk működésére és polgáraink jólétére nézve."* (Németország 2016a, idézi: Kovács 2018b)

A fentiekben ismertetett kihívások után a stratégia megadja azokat a legfontosabb célokat, amelyek Németország biztonsággal összefüggő stratégiai céljaiként értelmezhetők:

- a mindenre kiterjedő biztonság kormányzati szintű biztosítása;
- a NATO és az EU kohéziójának és képességeinek erősítése;
- az információs és kommunikációs rendszerek, az ellátási láncok, a szállítás, valamint a nyersanyagok és az energia biztonságos ellátásának akadálytalan használata;
- a válságok és konfliktusok korai felismerésének, megakadályozásának és megoldásának biztosítása;
- a kialakult világrend fenntartásához való hozzájárulás. (Németország 2016a, Kovács 2018b)

Itt ismét megjelenik a kibertér, mert a fenti stratégiai céloknak, illetve ahogy a stratégia fogalmaz: prioritásoknak az eléréséhez szükséges feladatok meghatározása során hangsúlyozza, hogy Németország biztonságpolitikája globális és ez a biztonsági gondolkodás az űrre és a kibertérre is kiterjed. (Kovács 2018b)

A stratégiában megfogalmazott elvek szerint a biztonság megteremtése érdekében az állam mellett az iparnak, a tudományos közösségeknek és a társadalomnak is meghatározó szerepet kell vállalnia. Ez igaz a kiberbiztonság területére is, ahol szintén szükséges a

nemzeti, és emellett a nemzetközi szintű együttműködés is. A nemzetközi együttműködéshez szükséges szervezeti keretet a stratégia a NATO-ban és az EU-ban azonosítja. Ennek megfelelően ezt a készülő új Nemzeti Kiberbiztonsági Stratégiában is érvényesíteni kell. (Kovács 2018b)

A stratégia kitér a német haderő, a Bundeswehr fejlesztésére, valamint annak jövőbeni szerepére és feladataira is. A Bundeswehr legfontosabb feladatai között a stratégia az első között meghatározza a kiberfenyegetések elleni tevékenységekre való felkészülést, de ebben a kérdésben – nyilvánvalóan a német alkotmányból következően – csak védelmi képességek kiépítését rendeli el, a kibertámadó képességek fejlesztése nem szerepel a stratégiában. A stratégiában megfogalmazottak alapján a Bundeswehrnek fel kell készülnie a saját rendszerei kibervédelmére, de emellett az ország kibervédelmében is szerepet kell játszania. Ezeknek a feladatoknak a megvalósításához szükséges feladatok a hadsereg technológiai fejlesztése és a megfelelő humánerőforrás kiválasztása, azok képzésével és folyamatos tréningjével együtt. (Németország 2016a, Kovács 2018b)

Németország nemzeti kiberbiztonsági stratégiája

2011-ben került kiadásra Németország első kiberbiztonsági stratégiája, amely a *Kiberbiztonsági Stratégia Németország számára* (Cyber-Sicherheitsstrategie für Deutschland) címet viselte. Az ebben meghatározott legfontosabb stratégiai célok a következőek voltak:

- kritikus információs infrastruktúrák védelme;
- biztonságos IKT rendszerek alkalmazása az állampolgárok és a KKV részéről;
- a közigazgatás információbiztonságának erősítése[105];

[105] A közigazgatás információbiztonságának erősítése stratégiai céllal kapcsolatban meg kell jegyezni, hogy Németországban már 2010-ben létezett stratégia az elektronikus kormányzattal kapcsolatos feladatok végrehajtására. Ennek a 2010-es, e-Kormányzat Stratégiája (Nationalen E-Government-Strategie, NEGS) című dokumentumnak 2015-ben történt meg a felülvizsgálata. Ennek eredményei e-*Kormányzat Stratégiai Felülvizsgálat 2015* (Nationale E-Government-Strategie Fortschreibung 2015) címmel publikálásra is kerültek 2015 őszén. Az e-kormányzattal kapcsolatosan az egyik legfontosabb stratégiai célkitűzés a szövetségi szinten megvalósítandó magasszintű, elektronikus közigazgatási szolgáltatások kialakítása, melynek során az információbiztonság és az adatok védelme magas szinten teljesül. Ez nyilvánvalóan hozzájárul az állampolgárok e-közigazgatási szolgáltatásokkal szembeni bizalmának építéséhez. (Ezt tovább gondolva, az állampolgári bizalom megléte esetén nőhet az e-közigazgatási rendszerek használata, amely az egyik kiemelt indikátor az EU DESI indexében, és amely alacsony volta miatt éri nagyon sok kritika hazánkat). Az e-közigazgatás, illetve az abban megvalósuló információbiztonság garantálása érdekében a stratégia a közigazgatási dolgozók rendszeres információbiztonsági képzését és továbbképzését rendeli el. (Németország 2015, Kovács 2018b) Ez a képzést elrendelő stratégiai irány nagyban összecseng a hazai 2013. évi L-es törvényben megfogalmazott elvekkel, miszerint a hazai közigazgatási dolgozóknak hasonló képzéseken kell részt venniük.

- nemzeti kiberreagáló központ létrehozása és működtetése;
- nemzeti kiberbiztonsági tanács létrehozása és fenntartása;
- a kiberbűnözés elleni hatékony fellépés;
- hatékony és koordinált európai és nemzetközi tevékenységek a kiberbiztonság növelése érdekében;
- megbízható információtechnológia használata;
- a szövetségi hatóságok munkatársainak kiberbiztonsági fejlesztése;
- a kibertámadások kezelésére alkalmas hatékony eszközök fejlesztése és alkalmazása. (Németország 2011, Kovács 2018b)

A 2011-es stratégiát 2016-ban egy új nemzeti kiberbiztonsági stratégia követte *Kiberbiztonsági Stratégia Németország számára 2016* (Cyber-Sicherheitsstrategie für Deutschland 2016) címmel.

Az új stratégia terjedelmében hasonló a korábbi stratégiához, de szerkezetében némileg eltér attól. Az új dokumentum négy nagy tevékenységi körben – a stratégia szóhasználatával élve akcióterületen – határoz meg különböző kiberbiztonsági feladatokat. Az említett négy tevékenységi kör:

- biztonságos és önálló tevékenység a digitális környezetben;
- az állam és az üzleti élet közös erőfeszítései és kiberbiztonságra irányuló tevékenységei;
- hatékony és fenntartható állami kiberinfrastruktúra;
- Németország aktív pozicionálása az európai és nemzetközi kiberbiztonság politikájának alakításában. (Németország 2016b)

Az első, azaz a biztonságos és önálló tevékenység a digitális környezetben akcióterületen megfogalmazott feladatok a stratégia legfontosabb célkitűzéseinek elérését szolgálják az olyan feladatokkal, mint a digitális írástudás fejlesztése, amely során a kiberbiztonsági tudatosság is fejleszthető; a biztonságos elektronikus kommunikáció és internetes szolgáltatások feltételeinek a kialakítása; az állampolgárok biztonságos elektronikus azonosítása, amely magába foglalja egy elektronikus személyi igazolvány bevezetését is; információbiztonsági tanúsítványok iránti igény növelése, amely egy információbiztonsági

tanúsítvány bevezetésével együtt valósulhat meg; vagy a kiberbiztonsági kutatások támogatása. (Németország 2016b, Rothenpieler 2016, Kovács 2018b)

Az állam és az üzleti élet közös erőfeszítései és kiberbiztonságra irányuló tevékenységei című második akcióterület alapvetően a kritikus infrastruktúrák védelmét,[106] a németországi vállalatok és vállalkozások védelmének biztosítását, a hazai informatikai ipari ágazatok megerősítését, a szolgáltatókkal történő szoros együttműködést, illetve ezeknek a szolgáltatóknak a kiberbiztonság megteremtésébe és fenntartásába való bevonását jelenti. Ezeken kívül az akcióterület egy olyan platform létrehozását is előirányozza, amely segítségével megvalósulhat a gyors és hatékony információcsere a sérülékenységek, veszélyek, kibertámadások, és a védelem terén. (Németország 2016b, Rothenpieler 2016, Kovács 2018b)

A stratégia harmadik akcióterülete, azaz a hatékony és fenntartható állami kiberinfrastruktúra létrehozása a következő feladatokat jelenti:

- a Nemzeti Kiber Reagáló Központ további fejlesztése;
- a helyszíni kiberelemzési és reagálási képességek/lehetőségek növelése[107];
- a kiberbűnözés elleni tevékenységhez szükséges képességek növelése, a szükséges szervezeti háttér fejlesztése;
- hatékony fellépés a kiberkémkedés és a kiberszabotázs tevékenységekkel szemben;
- a külföldről érkező kibertámadások korai előrejelző rendszerének kialakítása;
- egy informatikai biztonsági központi szervezet[108] létrehozása;
- a német CERT-ek szervezeti rendszerének megerősítése;

---

106 Németország első nemzeti kritikus infrastruktúra védelmi stratégiája 2009-ben született. Ez meghatározta a kritikus infrastruktúra fogalmát, és fel is osztotta azokat technikai alapú infrastruktúrákra és társadalmi-gazdasági szolgáltató infrastruktúrákra. (Németország 2009, Kovács 2018b) Ezt követően az Információbiztonsági törvény 2015-ben számos kiegészítést tett a kritikus infrastruktúra védelemmel kapcsolatban is. Ezek alapján a kritikus ágazatok és alágazatok, illetve az abban megvalósítandó kibervédelem hatékonysága többek között az incidensjelentés, a kommunikáció és az együttműködés területén megalkotott új szabályok hatására növekedhet. (BMI 2018, Kovács 2018b)

107 A helyszíni kiberelemzések érdekében mobil incidenskezelő csoportok (Mobile Incident Response Team, MIRT) kerültek létrehozásra. (Kovács 2018b)

108 Ez a központi szervezet a ZITiS (Zentral Stelle für Informationstechnik im Sicherheitsbereich, azaz a biztonsági szektor információtechnológiai központja) néven jött létre, amely feladata: *„A ZITiS a számítógépes technikai megoldások kutatási és fejlesztési testülete. Németország biztonsági hatóságainak nyújtunk szolgáltatásokat, és technikai know-how egyesítésével támogatjuk őket. Szakértelmünk révén olyan eszközöket és megoldásokat hozunk létre, amelyek elengedhetetlenek a biztonsági hatóságok tevékenységeihez."* (ZITiS 2018, idézi: Kovács 2018b)

- a szövetségi kormány védelme;
- a tartományi és az állami szintek közötti szorosabb együttműködés kialakítása;
- olyan pénzügyi források biztosítása, amelyek a kiberbiztonság növelése érdekében felhasználhatóak;
- szakemberek képzése, továbbképzése. (Németország 2016b, Rothenpieler 2016, Kovács 2018b)

A negyedik akcióterület, azaz európai és nemzetközi kiberbiztonság politikájának alakításában való aktív német részvétellel kapcsolatosan a stratégia csak általános feladatokat határoz meg. Ezek közé tartozik a hatékony európai kiberbiztonsági politika kialakítása, a NATO kibervédelmi politikájának megerősítése, illetve az ezekben való német részvétel. Ezen kívül a stratégia szorgalmazza a kétoldalú és regionális együttműködések kialakítását és a kiberbűnözés elleni közös nemzetközi fellépés erősítését. (Németország 2016b, Rothenpieler 2016, Kovács 2018b)

Németországban a kiberbiztonság, illetve az információbiztonság szervezeti rendszerének egyik legfontosabb szereplője a Szövetségi Információs Biztonsági Hivatal (Bundesamt für Sicherheit in der Informationstechnik, BSI)[109]. A BSI 1991-ben került megalapításra és azóta nyújt különböző célcsoportok számára információbiztonsági tanácsadást és elemzéseket. Az alapítása óta a szervezet Németország információbiztonságának legmagasabb szintű szervezeti felelősévé vált. A BSI szervezete öt osztályt foglal magában, egy központi és négy szakosodott szervezeti egységgel. A központi osztály, azaz „Z" osztály a központi feladatok ellátásért (például a humán és gazdasági ügyek), míg a négy szakosodott osztály közül az úgynevezett „CK" osztály a kiberbiztonságért valamint a kritikus infrastruktúrák védelméért, a „B" osztály a kormányzat és a magánszektor közötti együttműködésért, a „KT" osztály a kriptotechnológiáért és a kiemelt biztonsági követelményekért, a „D" osztály pedig a kiberbiztonság tanúsításához és szabványosításához szükséges feladatok ellátásáért felelős. (BSI 2018a, BSI 2018b, Kovács 2018b)

[109] A BSI megalapításáról 1991-ben törvény rendelkezett. Ezt a törvényt a 2009-ben kiadott új BSI törvény (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik [BSI-Gesetz – BSIG], azaz törvény a Szövetségi Információs Biztonsági Hivatalról) váltotta fel. (BSI-Gesetz 2009, Kovács 2018b) Ugyanakkor a BSIG mellett a már említett 2015-ös információbiztonsági törvény is számos jogkört és feladatot, köztük a kritikus infrastruktúra védelem nemzeti koordináló feladatait rendelte a BSI hatáskörébe. (Kovács 2018b)

2.4.10. Szlovák Köztársaság

A Szlovák Köztársaság nemzeti biztonsági stratégiája

Szlovákia nemzeti biztonsági stratégiájaként a *Fehér Könyv Szlovákia nemzeti védelméről*[110] című dokumentum értékelhető, amely először 2013-ban, majd erősen átdolgozott formában 2016-ban jelent meg. Az új fehér könyv kiadását az olyan – az előző stratégia óta megjelent – biztonsági kihívások indukálták, mint például Oroszország Krím-félszigetet érintő annektálása. (Kovács 2018b)

A dokumentum értékeli az ország külső biztonsági környezetét, amelyben utal a kibertérre is. Ennek során a dokumentum kiemeli, hogy a katonai tevékenységek súlypontja egyre inkább a nem-konvencionális területekre helyeződik át, amelyek tartalmazzák az információs-, elektromágneses-, és kiberteret, valamint az űrt is. Így az ezeken a területeken megvalósuló technológiai fejlődés gyors üteme alapjaiban változtatják meg a biztonságról alkotott elképzeléseket. (Szlovákia 2016b, Kovács 2018b)

A kibertér és a hadügy vonatkozásában a dokumentum a következőket állapítja meg: *„[a] kibertér a harctevékenységek új dimenziójává vált. A kibertérben végrehajtott támadás az Észak-atlanti Szerződés 5. cikkének életbe léptetését eredményezheti és a kollektív védelemhez vezethet, vagy akár a NATO tagországok koordinált válaszát eredményezheti."* (Szlovákia 2016b, idézi: Kovács 2018b)

A kibertér veszélyei, nevezetesen a kibertámadások megjelennek a Szlovák Köztársaságot fenyegető legfontosabb globális katonai és nem-katonai, szimmetrikus és aszimmetrikus biztonsági fenyegetések, illetve veszélyforrások felsorolásakor is, mégpedig a terrorizmus, illetve a szervezett terrorcsoportok után a második helyen. (Szlovákia 2016b, Kovács 2018b)

A Szlovák Köztársaság nemzeti kiberbiztonsági stratégiája

Szlovákiában már a 2000-es évek elején, egészen pontosan 2004-ben született stratégia az információs társadalom fejlesztése érdekében, amely egy cselekvési tervet is tartalmazott. 2009-ben a *Szlovákia Információs Társadalom Stratégia 2009–2013* című dokumentummal azonban egy komplex, az információs technológia és a digitális társadalom fejlesztésére elgondolás született. Ez a stratégia számos olyan fejlesztendő területet megjelölt, amelyek

[110] A fehér könyv alapvetően a katonai terület és a hadsereg fejlesztését célozza, de ezekkel párhuzamosan a nemzeti biztonság alapelvei is megjelennek benne.

közvetlenül vagy közvetve Szlovákia információs társadalmának építése során elengedhetetlenek:

- szélessávú hozzáférés növelése;
- információbiztonsági szabványok kidolgozása;
- e-kormányzat és e-egészségügy fejlesztése;
- digitális írástudás fejlesztése, e-oktatás kialakítása;
- az energia fogyasztás csökkentése és az energia hatékonyság növelése. (Kovács 2012, Kovács 2018b)

A kiberbiztonságra, illetve annak egyes elemeire azonban csak 2008-ban született stratégia: Szlovákia Nemzeti Informatikai Biztonsági stratégiája formájában. A stratégia három szintű feladatstruktúrát irányozott elő:

- első szint: a hosszú távú információbiztonsági stratégiai célok meghatározása;
- második szint: a stratégiai prioritások lefektetése;
- harmadik szint: a legfontosabb problémák és az ezek kezelésével kapcsolatos feladatok meghatározása. (Kovács 2012, Kovács 2018b)

A dokumentum ehhez a három szintű feladatlistához világos hatásköröket rendelt hozzá és meghatározta ezek között a prioritásokat, valamint a legfontosabb intézkedéseket. (Kovács 2012, Kovács 2018b)

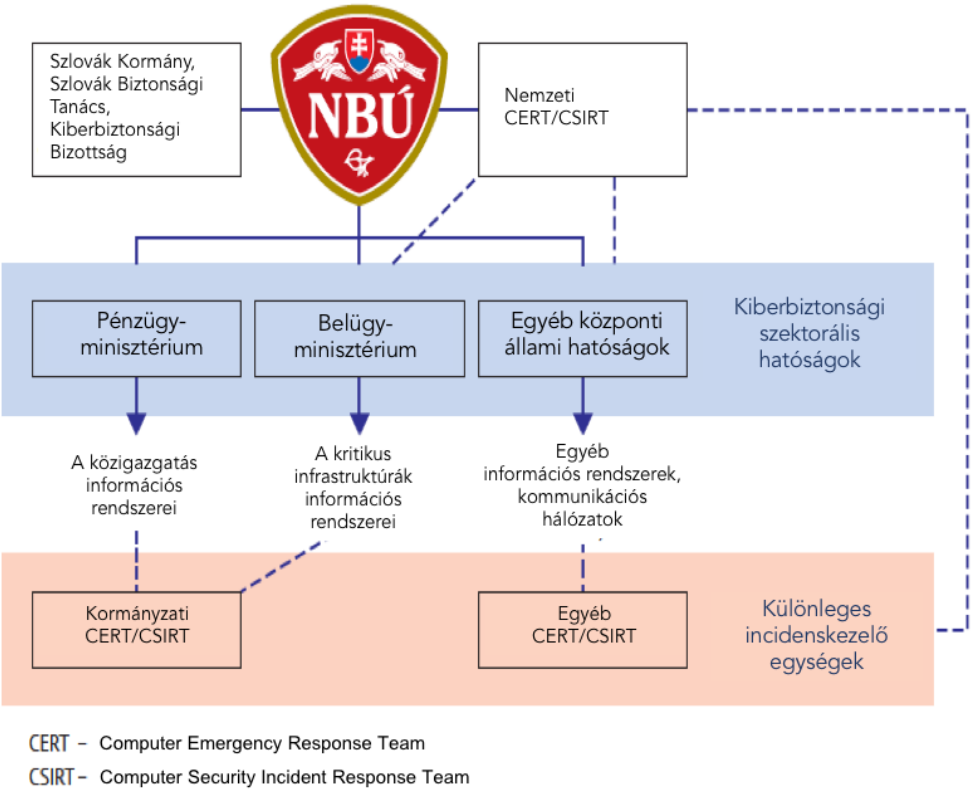
A kiberbiztonságra vonatkozó átfogó stratégia 2015 jelent meg a *Szlovák Köztársaság kiberbiztonsági koncepciója 2015-2020* címmel. Ebben az egyik legfontosabb feladat a kiberbiztonság szervezeti keretrendszerének a kiépítése Szlovákiában. Előremutató módon a stratégia az Európai Unió kiberbiztonsági stratégiájára és a NATO kibervédelmi politikájára épül, valamint az akkor csak tervezett EU NIS irányelv céljait és prioritásait is figyelembe véve készült. (Szlovákia 2015b, Kovács 2018b)

A kiberbiztonsági koncepció alapelvei között szerepel a nemzetközi együttműködés erősítése, a kibertérben megjelenő kihívások rendszerszintű problémakezelése, a magán és az állami szféra együttműködésének erősítése. Ezen alapelvekre épülve jelenik meg a stratégia legfontosabb – bár meglehetősen általános – célkitűzése: a kibertérből érkező kockázatokat úgy kell csökkenteni, hogy a magának a kibertérnek a használatát ne korlátozzák és amely során az állampolgárok személyiségi jogai sem sérülnek. Ehhez a következő feladatokat tűzi a stratégia:

- a kiberbiztonság irányítási rendszerének és annak jogi hátterének a megteremtése (intézményi-, szabályozási- és módszertani keretrendszer), beleértve ebbe a szakosított intézményeket és a terminológiát is;
- a magán- és az állami szektor közötti információcsere növelése és hatékonyabbá tétele, amely együtt kell, hogy járjon a kiberbiztonsági szereplők tudásának növelésével, valamint magasabb szintű kockázatok kezelési kultúrával;
- a kiberbiztonság különböző területeit érintő oktatási, valamint tájékoztatási rendszer kiépítése;
- a nemzeti és nemzetközi együttműködés fokozása, amelybe a magán- és az állami szféra közötti együttműködésének fokozása is bele kell, hogy tartozzon;
- a kiberbiztonság területén megvalósuló kutatás-fejlesztés-innováció támogatása, amelyhez biztosítani kell a nemzeti és az EU-s források kihasználását. (Szlovákia 2015b, Kovács 2018b)

Ahhoz, hogy ezek a feladatok végrehajthatóak legyenek a stratégia úgynevezett kulcs intézkedéseket fogalmaz meg:

- a kiberbiztonsági igazgatás intézményi kereteinek kiépítése, amelyhez felelősségi köröket, illetve a szükséges kompetenciákat is meghatározza a dokumentum;
- a kiberbiztonság jogi kereteinek létrehozása és elfogadása, amelyhez a szükséges legfontosabb törvényeket és jogszabályokat meg is nevezi a koncepció (például a kiberbiztonsági törvény);
- a kibertér adminisztrációja biztonságához szükséges alapvető mechanizmusok meghatározása és bevezetése;
- a kiberbiztonság területén szükséges oktatási rendszer előkészítése és bevezetése, amely során a legalapvetőbb kiberbiztonsági tudást az általános- és a középiskolai, majd a szükséges speciális tudást az egyetemi oktatásba kell beépíteni;
- a szükséges kockázatkezelési kultúra kialakítása, valamint az érintett felek között az ehhez szükséges kommunikáció biztosítása, amelynek során elő kell készíteni a szükséges módszertant, valamint azokat a szabványokat, amelyek alapján a kockázatok kezelése hatékonyabbá tehető;
- aktív nemzetközi együttműködés;
- a kiberbiztonság területén szükséges tudomány és kutatás támogatása. (Szlovákia 2015b, Kovács 2018b)



8. ábra
A szlovák kiberbiztonsági szerezetek kapcsolatai
Forrás: Szlovákia 2015b, Kovács 2018b; szerkesztette: szerző

A stratégiában rögzített módon azt egy cselekvési terv kiadása követte 2016-ban. Ez a cselekvési terv tartalmazza *„azokat a feladatokat, amelyek célja a kibertér megfelelő védelmének biztosítása az olyan potenciális kiberveszélyekkel szemben, amelyek helyrehozhatatlan károkat okozhatnak a Szlovák Köztársaságnak, és ezáltal károsíthatják az állam, illetve az állami szervezetek megbízhatóságát."* (Szlovákia 2016c, Kovács 2018b)

A cselekvési terv a 2016 és 2020 közötti időszakra meghatározott kiberbiztonság területén megvalósítandó feladatait határozza meg. A feladatok kiterjednek a jogalkotásra, a szabványokra és szabályzókra, a különböző kiberbiztonsági módszertanokra, valamint a biztonsági politikák kialakításra. Ezeken kívül abban nagy hangsúlyt kap a nemzetközi együttműködés erősítése, a tudatosság növelése, valamint a kiberbiztonsági képességek és kapacitások növelésére is. (Szlovákia 2016c, Kovács 2018b)

A kiberbiztonsági koncepcióban (stratégiában) megfogalmazott hét legfontosabb feladat mentén a cselekvési terv hét területen határoz meg részletesen kifejtett feladatokat. Ezekhez a területekhez, illetve az azokon végrehajtandó feladategyüttesekhez felelős szervezetet és a feladatok végrehajtásához egy időintervallumokat is hozzárendel a dokumentum. (Szlovákia 2016c, Kovács 2018b)

2.5. A dolgozatban bemutatott országok egyes kibertéri jellemzői és kiberbiztonsági stratégiai céljai[111]

Amerikai Egyesült Államok			
Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*	*GCI (index/hely az összehasonlításban)*
326,4	286,9	87,9%	0,919 / 2.
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Department of Defense Cyber Strategy 2018[112]		
Kiadás ideje:	2018		
Kiberbiztonsági stratégiai célok:	• az amerikai hadsereg képességeinek fejlesztése a kibertérben zajló műveletek sikeres megvívásához; • az amerikai hadsereg fejlesztése és megerősítése olyan kibertér-műveletek végrehajtásával, amelyek az USA katonai előnyéhez hozzájárulnak; • az Egyesült Államok kritikus infrastruktúrájának védelme az olyan rosszindulatú kibertevékenységekkel szemben, amelyek önmagukban vagy egy támadás sorozat részeként jelentős kibereseményt okoznának; • a DoD információinak és rendszereinek védelme a rosszindulatú kibertevékenységek ellen, beleértve a DoD és a nem DoD tulajdonú hálózatokat is; • a DoD kiberterületen történő együttműködésének kiterjesztése a közigazgatási szereplők, az ipari és nemzetközi partnerek felé.		
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen		

[111] Az adatok 2017-re vonatkoztatva kerültek megadásra. A teljes népesség, az internethasználók száma, valamint az internetpenetráció forrása az adott országra vetítve: http://www.internetworldstats.com. A GCI pontok és világ országai között elfoglalt helyezés forrása 2017-re megadva, forrásuk: ITU 2017b. Az alfejezetben szereplő táblázatok szerkesztője a szerző.

[112] Az USA Nemzeti Kiberstratégiája 2018 szeptemberében, néhány nappal a DoD kiberstratégiája után jelent meg. Ugyanakkor annak általános érvényű megállapításai nagyban hasonlítanak a DoD stratégiában foglaltakhoz. A DoD kiberstratégia bővebb, szélesebb látókört tartalmaz, így ez került ezen a helyen bemutatásra.

Kibertámadó képesség meghatározásra kerül-e:	Igen

Kína			
Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*	*GCI (index/hely az összehasonlításban)*
1388	738,5	53,2%	0,624 / 32.
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Feltételezhetően a 27-es dokumentum		
Kiadás ideje:	2010		
Kiberbiztonsági stratégiai célok:	Mivel nincs egyetlen jól körülhatárolható és világos célokat megfogalmazó dokumentum ezért csak a kibertéri tevékenységből lehet következtetni a stratégiai célokra: • kínai érdekek védelme; • belső információmegosztás ellenőrzése; • hírszerzés (politikai és gazdasági egyaránt); • katonai kiberképességek támogatása.		
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen		
Kibertámadó képesség meghatározásra kerül-e:	Igen		

<table>
<tr><th colspan="4">Oroszország</th></tr>
<tr><td>Teljes népesség
(millió fő)</td><td>Internethasználók száma
(millió fő)</td><td>Internetpenetráció
(a teljes lakosság százalékos arányában)</td><td>GCI
(index/hely az összehasonlításban)</td></tr>
<tr><td>143,4</td><td>109,5</td><td>76,4%</td><td>0,788 / 10.</td></tr>
<tr><td>Jelenlegi nemzeti kiberbiztonsági stratégia címe:</td><td colspan="3">Orosz Föderáció információbiztonsági doktrínája</td></tr>
<tr><td>Kiadás ideje:</td><td colspan="3">2016</td></tr>
<tr><td>Kiberbiztonsági stratégiai célok:</td><td colspan="3">Katonai terület:
stratégiai elrettentés;
a fegyveres erők információbiztonsági rendszereiknek és az információs ellentevékenységi eszközeiknek korszerűsítése;
az információs fenyegetések előrejelzése és azonosítása;
az Orosz Föderáció és szövetségesei érdekeinek érvényesítése;
pszichológiai tevékenységek elleni védelem.
Az állam és a közbiztonság területeken:
az alkotmányos rend megdöntése és szélsőséges ideológiák terjesztése érdekében használt információtechnológia megakadályozása;
külföldi nemzetbiztonsági szervezetekkel szembeni védelem növelése;
kritikus információs infrastruktúrák védelmének növelése;
a kormányzati szervek közötti kommunikáció biztosítása;
az automatizált irányítási rendszerek működésének biztosítása;
a kiberbűncselekmények elleni tevékenység fokozása;
a titkosítást biztosító rendszerek fejlesztése;
a korszerű információbiztonsági elveknek és követelményeknek megfelelő eszközök, rendszerek és szolgáltatások gyártása és azok üzemeltetése;
az állami politika számára információtámogatási tevékenység nyújtása;
ország lakosságának erkölcsi és morális állapotának gyengítésére és aláásására irányuló információs tevékenységek hatásainak kivédése.
Gazdasági terület:</td></tr>
</table>

	• az információtechnológiai és az elektronikai szektorok nem megfelelő fejlődéséből következő negatív tényezők hatásainak ellensúlyozása; • versenyképes információtechnológiai eszközök fejlesztése. Tudomány, technológia, oktatás terület: • versenyképes technológia támogatása; • K+F támogatása; • oktatás korszerűsítése.
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen
Kibertámadó képesség meghatározásra kerül-e:	Igen

Ausztria			
Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*	*GCI (index/hely az összehasonlításban)*
8,6	7,2	84,6%	0,639 / 30.
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Osztrák kiberbiztonsági stratégia		
Kiadás ideje:	2013		
Kiberbiztonsági stratégiai célok:	• biztonságos kibertér megteremtése, amelynek a kockázatok és veszélyek kezelése miatt megfelelően redundásnak kell lennie; • Ausztria biztosítja a biztonságos kiberteret, amely során a köz- és a magánszektor együttműködése elengedhetetlen; • a kiberbiztonság jogi kereteinek megteremtése, illetve annak megvalósítása a különböző osztrák hatóságok, illetve azok magánszektorral történő együttműködése révén valósítható meg; • Ausztria kiberbiztonsági kultúra építésébe kezd; • a kiberbiztonság területén meglévő magán és közszféra közötti párbeszéd, valamint az új kezdeményezések a digitális társadalom területén olyan pozitív hatással vannak, amelyek többek között az üzleti befektetéseket is ösztönzi, így ezeket folytatni szükséges; • Ausztria folytatja a kiberbiztonság területén lévő nemzetközi párbeszédre és együttműködés ösztönzésre irányuló tevékenységét; • az e-kormányzati megoldások kiberbiztonságának növelését a szövetségi szinttől kezdődően a közigazgatás minden szintjén folytatni kell; • az osztrák vállalatok kiberbiztonsági tevékenységeinek támogatásában együttműködés szükséges; • a kiberbiztonság tudatosságának állampolgári szinten történő emelése szükséges.		
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen		

Kibertámadó képesség meghatározásra kerül-e:	Nem

Cseh Köztársaság			
Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*	*GCI (index/hely az összehasonlításban)*
10,5	9,3	88,4%	0,609 / 35.
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	A Cseh Köztársaság Nemzeti Kiberbiztonsági Stratégiája 2015-2020		
Kiadás ideje:	2015		
Kiberbiztonsági stratégiai célok:	• a kiberbiztonsághoz szükséges minden szervezet, folyamat és együttműködés hatékonyságának növelése: a CERT-ek, CSIRT-ek és a kritikus információs infrastruktúrák védelmét biztosító szervezetek együttműködésének javítása, a nemzeti incidenskezelési képesség növelése; • aktív nemzetközi együttműködés: az EU, NATO, ENSZ és EBESZ különböző programjaiban való részvétel; • a nemzeti kritikus információs infrastruktúrák és kiemelt információs rendszerek védelme; • együttműködés a magánszektorral; • kutatás-fejlesztés és vásárlói bizalom; • oktatás, biztonságtudatosság növelése; • a cseh rendőrség kiberbűnözés elleni képességeinek fejlesztése; • kiberbiztonság jogszabályi háttere: a meglévő jogszabályi környezetet figyelembe véve ki kell alakítani, illetve korszerűsíteni kell azokat a jogszabályokat, amelyek a kiberbiztonsághoz szükségesek.		
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen		
Kibertámadó képesség meghatározásra kerül-e:	Nem		

Egyesült Királyság			
Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*	*GCI (index/hely az összehasonlításban)*
65,5	62,1	94,8%	0,783/ 12.
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Nemzeti Kiberbiztonsági Stratégia 2016-2021		
Kiadás ideje:	2016		
Kiberbiztonsági stratégiai célok:	Nincsenek egyértelműen és általánosságban megfogalmazott stratégiai célok, de a következő hármas elv mentén építi fel a dokumentum a célrendszert: • védelem; • elrettentés; • fejlesztés. Ezek elérése érdekében elveket fogalmaz meg a stratégia, amely szerint a kormány: • megvédi az embereket és a fejlődést; • kezelik a kibertámadásokat és a hagyományos támadásokkal egyenértékűként kezeli; • a nemzetközi egyezményeket és szerződéseket betartja; • az ország alap értékeit – demokrácia, a jogrend, a szabadság, az emberi jogok és a szabadság – támogatja és terjeszti; • az állampolgárok személyiségi jogait a kibertérben is betartja; • együttműködésben végzi a munkáját az országon belül és kívül is (más országokkal való együttműködés; • nem engedi meg azoknak a veszélyeknek a terjedését, amelyek az állampolgárokat, az államot fenyegetik, még akkor sem, ha üzleti érdekek állnak ezek mögött.		
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen		

Kibertámadó képesség meghatározásra kerül-e:	Igen

Észtország			
Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*	*GCI (index/hely az összehasonlításban)*
1,3	1,27	97,7%	0,846 / 5.
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Nemzeti Kiberbiztonsági Stratégia 2014-2017		
Kiadás ideje:	2014		
Kiberbiztonsági stratégiai célok:	Stratégiai cél: a kiberfenyegetésekkel szembeni kiberbiztonsági képességek és a lakosság tudatosságának növelése, ezáltal a kibertérben való folyamatos bizalom biztosítása. Részcélok: • a fontos szolgáltatások alapját képező információs rendszerek védelme; • a kiberbűnözés elleni tevékenység fokozása; • a nemzeti kibervédelmi képességek fejlesztése; • az új kiberfenyegetések kezelése; • nemzetközi együttműködés fokozása.		
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen		
Kibertámadó képesség meghatározásra kerül-e:	Nem		

Franciaország			
Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*	*GCI (index/hely az összehasonlításban)*
64,9	56,4	86,8%	0,819 / 8.
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Francia Nemzeti Digitális Biztonság Stratégia		
Kiadás ideje:	2015		
Kiberbiztonsági stratégiai célok:	• alapvető érdekek az állami információs rendszerek biztonsága és védelme és a súlyos kiberbiztonsági válságok elkerülése; • a digitális bizalom, az adatvédelem, a személyes adatok védelmének növelése, a rosszindulatú kibertevékenységek csökkentése; • a tudatosság növelése, alapvető felkészítés, és folyamatos képzés; • a digitális technológia üzleti környezetének, az ehhez szükségese iparpolitika támogatása, az export és nemzetköziesítés ösztönzése; • Európa támogatása, a digitális stratégiai autonómia és a kibertér stabilitásának megtartása mellett.		
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen		
Kibertámadó képesség meghatározásra kerül-e:	Igen		

Hollandia			
Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*	*GCI (index/hely az összehasonlításban)*
17,0	16,1	94,8%	0,760 / 15.
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Hollandia Kiberbiztonsági Menetrendje: Hollandia digitálisan biztonságos		
Kiadás ideje:	2018		
Kiberbiztonsági stratégiai célok:	A stratégia ambíciókat fogalmaz meg, amely célokként is értelmezhetők: • Hollandiának megvan a saját digitális ereje; • Hollandia hozzájárul a nemzetközi béke és biztonság megteremtéséhez a digitális területen; • Hollandia élen jár a biztonságos hardverek és szoftverek népszerűsítésében és azok fejlesztésének ösztönzésében; • Hollandia rendelkezik a biztonságos digitális technológiákkal és kritikus infrastruktúrákkal; • Hollandia a megfelelő kiberbiztonsággal harcol a kiberbűnözés ellen; • Hollandia vezető szerepet tölt be a kiberbiztonsághoz szükséges tudásfejlesztés terén; • Hollandia az integrált, magán- és közszféra együttműködésére épülő megközelítést képviseli a kiberbiztonság terén.		
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen		
Kibertámadó képesség meghatározásra kerül-e:	Nem		

Magyarország			
Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*	*GCI (index/hely az összehasonlításban)*
9,8	7,9	80,2%	0,534 / 51.
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Nemzeti Kiberbiztonsági Stratégia		
Kiadás ideje:	2013		
Kiberbiztonsági stratégiai célok:	• a meglévő és potenciálisan jelentkező kihívásokkal szemben ki kell alakítani egy hatékony megelőző, észlelési, reagálási képességet, amelybe a kibertámadások esetleges bekövetkezése esetén a helyreállítási képességek is bele kell, hogy tartozzanak; • a nemzeti adatvagyon védelmét kiemelten kell kezelni; • az információs rendszerek és szolgáltatások színvonalát a lehető legmagasabban kell tartani, és biztosítani kell azok nemzetközi biztonsági tanúsítványoknak való megfelelését; • az oktatás és képzés, valamint a kutatás-fejlesztés területeken biztosítani kell a legmagasabb színvonalat; • biztosítani kell a kibertérben a gyermekek védelmét.		
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen		
Kibertámadó képesség meghatározásra kerül-e:	Nem		

Lengyelország			
Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*	*GCI (index/hely az összehasonlításban)*
38,6	28,3	73,3%	0,622 / 33.
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Lengyelország Kiberbiztonsági Politikájának Keretrendszere 2017-2020		
Kiadás ideje:	2017		
Kiberbiztonsági stratégiai célok:	A stratégia legfontosabb célja a köz- és magánszektor biztonságának garantálása az alapvető digitális szolgáltatások használata során. Ezen belül részcélokat határoz meg: • megnövelt nemzeti kiberbiztonsági képességek létrehozása az IKT rendszerek hatékony védelme érdekében, amelyen belül szükséges olyan jogszabályi keretrendszer kidolgozása, amely megfelel a kibertér kihívásainak; erősíteni kell a kibervédelmi szervezetek rendszerét; erősíteni kell az érdekelt felek együttműködését; növelni kell az IKT eszközök és rendszerek biztonságát a kritikus infrastruktúrákban; fejleszteni kell azokat a szabályzókat, ajánlásokat, valamint törekedni kell azoknak a legjobb gyakorlatok bevezetésére, amelyek a hálózati és információs rendszerek biztonságához hozzájárulnak; növelni kell a kockázatmenedzsment hatékonyságát; növelni kell a beszállítói lánc biztonságát; • a kiberfenyegetések elleni hatékony fellépés növelése, amely a kiberbűnözés, a kiberkémkedés és kibertéri terrorista akciók elleni fellépés hatékonyságának növelését is jelenti; el kell érni azokat a katonai képességeket, amelyek lehetővé teszik, hogy a hadsereg a műveletek teljes spektrumában képes legyen a kibertérben tevékenykedni; nemzeti szintű kiberfenyegetettség értékelő képességet kell kiépíteni; a nemzetbiztonság számára biztonságos kommunikációs rendszert kell kiépíteni; biztonságos audit és teszt képességekkel kell rendelkezni; • nemzeti potenciál és kompetencia növelése a kibertér biztonsága érdekében, amely magába kell, hogy foglalja a kiberbiztonsági célú ipari és technológiai erőforrások fejlesztését; együttműködési mechanizmusokat kell kialakítani a köz- és magánszektor között; motiválni kell a kiberbiztonsági kutatás és fejlesztési tevékenységeket; növelni kell az IKT rendszereket használók digitális kompetenciáit és képességeit, amelynek ki kell terjednie az állampolgárok ilyen képességeire is; • erős nemzetközi pozíció kiépítése Lengyelország számára a kiberbiztonság területén, amely mind stratégiai, mind politikai szinten meg kell, hogy történjen.		

Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen
Kibertámadó képesség meghatározásra kerül-e:	Igen

Németország			
Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*	*GCI (index/hely az összehasonlításban)*
80,7	72,2	89,6%	0,679/ 24.
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Kiberbiztonsági Stratégia Németország számára 2016		
Kiadás ideje:	2016		
Kiberbiztonsági stratégiai célok:	A stratégia négy tevékenységi kört (stratégiai akcióterületet), és ezeken belül feladatokat határoz meg: • biztonságos és önálló tevékenység a digitális környezetben: digitális írástudás fejlesztése, amely során a kiberbiztonság tudatosság is fejleszthető; biztonságos elektronikus kommunikáció és internetes szolgáltatások feltételeinek a kialakítása; biztonságos elektronikus azonosítás az állampolgárok részére, amely magába foglalja egy elektronikus személyi igazolvány bevezetését is; információbiztonsági tanúsítványok iránti igény növelése; a kiberbiztonsági kutatások támogatását; • az állam és az üzleti élet közös erőfeszítései és kiberbiztonságra irányuló tevékenységei: a kritikus infrastruktúrák védelme; a németországi vállalatok védelmének biztosítása; a hazai informatikai ipari ágazatok megerősítése; a szolgáltatókkal történő szoros együttműködést és ezen szolgáltatók bevonását a kiberbiztonság megteremtésébe; platform létrehozása a hatékony információcsere, sérülékenységek, veszélyek, kibertámadások, és a védelem gyors biztosítására; • hatékony és fenntartható állami kiberinfrastruktúra: a Nemzeti Kiber Reagáló Központ további fejlesztése; a helyszíni kiberelemzés és reagálási képességek és lehetőségek növelése; a kiberbűnözés elleni tevékenységhez szükséges képességek növelése, a szükséges szervezeti háttér fejlesztése; hatékony fellépés a kiberkémkedés és a kiberszabotázs tevékenységekkel szemben; a külföldről érkező kibertámadások korai előrejelző rendszerének kialakítása; egy informatikai biztonsági központi szervezet létrehozása; a német CERT-ek szervezeti rendszerének megerősítése; a szövetségi kormány védelme; a tartományi és az állami szintek közötti szorosabb együttműködés kialakítása; olyan pénzügyi források biztosítása, amelyek a kiberbiztonság növelése érdekében felhasználhatóak; szakemberek képzése, továbbképzése; • Németország aktív pozicionálása az európai és nemzetközi kiberbiztonság politikájának alakításában: a NATO kibervédelmi politikájának megerősítésében való részvétel; a kétoldalú és regionális együttműködés erősítése; a nemzetközi (kiber) bűnüldözés megerősítése		

Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen
Kibertámadó képesség meghatározásra kerül-e:	Nem

Szlovák Köztársaság			
Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*	*GCI (index/hely az összehasonlításban)*
5,4	4,5	82,5%	0,362/ 81.
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Szlovák Köztársaság kiberbiztonsági koncepciója 2015-2020		
Kiadás ideje:	2015		
Kiberbiztonsági stratégiai célok:	A legfontosabb célkitűzés mindazoknak a kockázatoknak a csökkentése, amelyek a kibertérből érkeznek, anélkül, hogy a kibertérnek a használatát csökkentenék. Ennek a célnak az elérése érdekében a következő feladatokat tűzi ki a stratégia: • a kiberbiztonság irányítási rendszerének és annak jogi hátterének a megteremtése beleértve ebbe a szakosított intézményeket és a terminológiát is; • a magán- és az állami szektor közötti információcsere növelése és hatékonyabbá tétele, a kiberbiztonsági szereplők tudásának növelésével, valamint magasabb szintű kockázatok kezelési kultúrával együtt; • a kiberbiztonság különböző területeit érintő oktatási, valamint tájékoztatási rendszer kiépítése; • a nemzeti és nemzetközi együttműködés fokozása, amelybe a magán- és az állami szféra közötti együttműködés fokozása is bele kell, hogy tartozzon; • a kiberbiztonság területén megvalósuló kutatás-fejlesztés-innováció támogatása.		
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen		
Kibertámadó képesség meghatározásra kerül-e:	Nem		

3. FEJEZET
A NEMZETI KIBERBIZTONSÁGI STRATÉGIA MODELLJE

3.1. Eddigi stratégiai modellalkotási példák

Eddigi kutatásai során megvizsgáltam azokat az elérhető, a nemzeti kiberbiztonsági stratégia kialakítására és felépítésére vonatkozó tanulmányokat, amelyek kiindulási alapot nyújthatnak egy egységes kiberbiztonsági stratégia modelljének elkészítéséhez.

Ezek közül három tanulmányt emelek ki és mutatok be legfőbb elemeik vonatkozásában:

- az ENISA 2012-ben készített, majd 2016-ban felülvizsgált javaslatgyűjteményét, amelyek címe *National Cyber Security Strategies Practical Guide on Development and Execution*, azaz magyarul Nemzeti kiberbiztonsági stratégiák gyakorlati útmutató a fejlesztésről és végrehajtásról, illetve *NCSS Good Practice Guide. Designing and Implementing National Cyber Security Strategies,* azaz Nemzeti kiberbiztonsági stratégiák jó gyakorlat útmutató. A nemzeti kiberbiztonsági stratégiák tervezése és végrehajtása;
- az ITU 2011-ben kiadott *The ITU National Cybersecurity Strategy Guide,* azaz Az ITU nemzeti kiberbiztonsági stratégiai útmutatója;
- a NATO CCDCOE *National Cyber Security Framework Manual*, azaz magyarul Nemzeti kiberbiztonsági keretrendszer kézikönyv, amely 2012-ben jelent meg.

Az ENISA ajánlásgyűjteményében megfogalmazott nemzeti kiberbiztonsági stratégia felépítésére vonatkozó javaslatok összefoglalása

Az ENISA ajánlásgyűjteménye alapján a kiberbiztonsági stratégia két fázisból áll, amelyek a stratégia vonatkozásában életciklusként is értelmezhetők. Az első fázis a stratégia megalkotása és bevezetése, a második fázis a stratégia felülvizsgálata, fejlesztése, majd a közben levont következtetések és tapasztalatok alapján a stratégia szükségszerű átalakítása. (ENISA 2012, ENISA 2014, Kovács 2018b)

A 2012-ben született ENISA ajánlás a nemzeti kiberbiztonsági stratégia ajánlott felépítésére, illetve kialakítására a következő elemeket javasolta:

- a stratégia hatókörének, céljainak és prioritásainak meghatározása;
- nemzeti szintű kockázatértékelési módszertan kialakítása és meghatározása;
- a meglévő szakpolitikák, szabályzók és képességek felmérése;
- világos irányítási struktúra kialakítása;

- az érintettek azonosítása és bevonása;
- a megbízható információmegosztási mechanizmusok létrehozása;
- kiberbiztonsági vészhelyzetkezelési tervek kidolgozása;
- kiberbiztonsági gyakorlatok megtervezése és megszervezése;
- az alapszintű biztonsági követelmények megállapítása;
- kiberincidensek jelentési mechanizmusainak kialakítása;
- az állampolgárok információbiztonsági tudatosságának növelése;
- K+F tevékenység ösztönzése a kiberbiztonság különböző területein;
- kiberbiztonsági képzési és oktatási programok bevezetése és ösztönzése;
- incidenskezelési képességek kialakítása, fejlesztése;
- a kiberbűnözés elleni hatékony fellépés és tevékenység kialakítása;
- a kiberbiztonság területén nemzetközi együttműködésekben való aktív részvétel;
- a köz- és magánszféra közötti partnerség kialakítása;
- az állampolgárok jogainak tiszteletben tartása és a biztonsági intézkedések közötti egyensúly megteremtése;
- a kiberbiztonságra vonatkozó értékelési séma (rendszer) kidolgozása, bevezetése és alkalmazása;
- a nemzeti kiberbiztonsági stratégia finomhangolása. (ENISA 2012, Kovács 2018b)

2016 novemberében az ENISA felülvizsgálta a fenti nemzeti kiberbiztonsági stratégiákra vonatkozó ajánlásgyűjteményét. A felülvizsgálat során az új ajánlásgyűjteménybe bekerült 17 ország olyan tapasztalata, amelyeket a meglévő nemzeti kiberbiztonsági stratégiái készítésekor, vagy azok frissítése, illetve módosítása során szereztek. Ennek megfelelően az új útmutató a 2012-es tanulmány eredményeire nagyban épít, de az annak készítése óta eltelt időszak tapasztalatait figyelembe véve mutatja be a nemzeti kiberbiztonsági stratégiák célszerű felépítését és ez alapján a nemzeti kiberbiztonsági rendszer stratégiai szintű működtetését. (ENISA 2016, Kovács 2018b)

A 2012-es ajánlás még a fentiekben bemutatott lépéseket tartalmazta a kiberbiztonsági stratégia kialakításához, annak bevezetéséhez és fenntartásához. Ugyanakkor mindezt csak két életciklus szakaszra osztotta. Ezzel szemben a 2016-os ajánlásgyűjtemény már négy fázisra osztotta ezt az életciklust. Az első fázis a stratégia kialakításának lépése, a második a stratégia bevezetése és működtetése, a harmadik az értékelési szakasz, majd ezt követi a

negyedik, azaz a fenntartási fázis. Az ajánlásgyűjtemény mind a négy fázishoz visszacsatolásokat is hozzárendel, amelyek az adott fázis fejlesztéséhez, de összességében a nemzeti kiberbiztonsági stratégia folyamatos fejlesztéséhez is támpontokat adnak. A visszacsatolások alapján időközönként felül kell vizsgálni és frissíteni kell a stratégiát, valamint az ahhoz tartozó akcióterveket is. (ENISA 2016, Kovács 2018b)

Az ITU ajánlásgyűjteményének összefoglalása

2011 szeptemberében jelent meg az ITU nemzeti kiberbiztonsági stratégiára vonatkozó útmutatója. Bár a kiadványt egy szerző – Frederick Wamala – jegyzi, az mégis az ITU már említett Globális Kiberbiztonsági Programjához (GCA) szorosan illeszkedik, és mint ilyen az ITU hivatalos kiadványa. A javalatgyűjtemény célja: *„[ez] a dokumentum a nemzeti kiberbiztonsági stratégia kidolgozásának referenciamodellje. Elemzi, hogy milyen alkotóelemei vannak a nemzeti kiberbiztonsági stratégiának, valamint bemutatja a végső célokat és a végrehajtást befolyásoló környezetet."* (Wamala 2011, idézi: Kovács 2018b)

Ennek megfelelően az ajánlásgyűjtemény referenciamodellként is funkcionálhat, amely a kiberbiztonság globális helyzetelemzésével kezdődik. Ebben elemzésre kerül a kibertér szerepe a globális gazdaságban, amely természetszerűleg a nemzetek gazdaságára is hatással van. Ugyanakkor ez az elemzés az ENSZ információs társadalom és kiberbiztonság fejlesztése során megvalósuló tevékenységeket mutatja csak be. A gazdaság globalitása és abban a kibertér szerepe csak nagy vonalakban kerül ismertetésre. (Kovács 2018b) A referencia modell a nemzeti kiberbiztonsági helyzet elemzésekor rámutat a kritikus infrastruktúrák és kritikus információs infrastruktúrák szerepére és fontosságára, illetve azokra a tényezőkre, amelyek kihívásként és veszélyként értékelhetőek egy nemzet esetében a különböző szektorokban. A referenciamodell holisztikus megközelítést alkalmaz a nemzeti kiberbiztonság stratégiájának felépítéséhez, amelyben fontos szerepet kap az említett veszélyek és kihívások felmérése, az azokra adott – sok esetben nemzetközi együttműködést igénylő, így a nemzetközi szerződésekben és egyezményekben rögzített – válaszok kialakítása, de az adott ország nemzeti érdekei megtartása és az ezek mentén kialakított stratégiai célok megfogalmazása is. (Wamala 2011, Kovács 2018b)

Az ITU referencia modellje a nemzeti kiberbiztonsági stratégia kialakítását célzó nemzeti kiberbiztonsági program elemeit mutatja, amelyeket a következő táblázatban foglaltam össze. Az ebben szereplő pontok sok esetben átfedést mutatnak a korábban bemutatott és elemzett ENISA-ajánlásban szereplő stratégiai elemekkel.

8. táblázat

Az ITU nemzeti kiberbiztonsági program elemeire vonatkozó ajánlásának összefoglalása

	A nemzeti kiberbiztonsági program elemei
1.	A legfontosabb kormányzati szereplők kiberbiztonsági szempontból történő elszámoltathatósága: • a legfelsőbb kormányzati vezetők felelősek a nemzeti stratégia kidolgozásáért, valamint a helyi, nemzeti és globális ágazatok közötti együttműködés előmozdításáért.
2.	Nemzeti kiberbiztonsági koordinátor: • egy iroda vagy magánszemély felügyeli a kiberbiztonsági tevékenységeket az egész országban.
3.	Nemzeti kiberbiztonsági pont: • egy központi elemként funkcionáló szervezet, amely minden típusú kiberfenyegetés elleni tevékenységre felkészült.
4.	Jogi intézkedések: • az ország kibertérrel kapcsolatos jogszabályi hátterének felülvizsgálata és szükség esetén új jogszabályok kidolgozása, például a kiberbűnözés visszaszorítására.
5.	Nemzeti kiberbiztonsági keretrendszer: • olyan keretrendszer kialakítása, amely meghatározza a minimum- vagy kötelező érvényű kiberbiztonsági követelményeket.
6.	Számítógép-vészhelyzeti reagálócsoport: • a stratégiának nemzeti szintű incidenskezelési képességeket és az erre alkalmas szervezetre vonatkozó elképzelést is tartalmaznia kell.
7.	Kiberbiztonsági tudatosság és oktatás: • a kiberfenyegetésekkel kapcsolatos figyelemfelkeltés érdekében nemzeti programot kell létrehozni.
8.	A köz- és a magánszektor kiberbiztonság területén meglévő partnersége: • a kormányoknak partnerséget kell kialakítaniuk a magánszektor szereplőivel.
9.	Kiberbiztonsági készségek és képzési programok: • olyan programokat kell kidolgozni, amelyek segítik a kiberbiztonsági szakemberek képzését.
10.	Nemzetközi együttműködés: • a globális együttműködés létfontosságú a kiberfenyegetések határok nélkülisége miatt.

Forrás: Wamala 2011, Kovács 2018b, a szerző szerkesztése

A NATO CCDCOE ajánlásgyűjteményének összefoglalása

2012-ben jelent meg a NATO Kiberbiztonsági Kiválósági Központ kiadásában a *Nemzeti kiberbiztonsági keretrendszer kézikönyv* (National Cyber Security Framework Manual), amely tanulmányaival sokkal inkább filozófiai alapokat nyújt a nemzeti kiberbiztonsági stratégiák megalapozásához, semmint kézzelfogható olyan referenciamodellt, mint ahogy azt például a fentiekben ismertettet ENISA vagy ITU ajánlás tette.

Ugyanakkor a nemzeti kiberbiztonsági stratégia egyes elemei kidolgozásához nagyon sok támpontot nyújt ez a tanulmánykötet is. A nemzeti kiberbiztonsági stratégia legfontosabb céljai vonatkozásában például a következőket állapítja meg:

- a kibertér, illetve az ott megjelenő biztonság hozzá kell, hogy járuljon a nemzeti biztonsági stratégia célkitűzéseihez;
- a támadó kiberképességek meghatározása vitatható (mint ahogy ezt a képességet a korábban említett módon sok ország nem is határozza meg), ugyanakkor ez a képesség, mint cél hozzájárulhat ahhoz, hogy a szembenálló fél ne tudjon hozzáférni, vagy ne tudja használni az érzékeny adatokat, illetve az azok elérését biztosító rendszereket;
- nemzeti kiberbiztonsági stratégiák kialakításakor gyakran tapasztalható, hogy a különböző megközelítések – például a katonai és a sokszor ezzel szembenálló vagy az ezzel nem teljesen harmonizáló civil vagy akár a kiberbűnözés elleni szervezetek által követett eltérő irányok – feszültségekhez vezetnek. Hasonló feszültséget okozhat az is, ha a nemzeti kiberbiztonsági stratégia fő filozófiai háttere a rugalmasság, vagy ha az az elrettentés elvét jelenti, hiszen e két megközelítés egymással sokszor ellentétes értelmet ad a stratégiának;
- a nemzeti kiberbiztonsági stratégia megalkotása és az abban foglaltak végrehajtása során számos nemzeti sajátosságot kell figyelembe venni, amelyek az előfeltételekben, a különböző folyamatokban, illetve az együttműködés rendszerében jelentkeznek;
- a nemzeti kiberbiztonsági stratégiához erőforrásokat kell hozzárendelni, valamint meg kell határozni számszerűsíthető és mérhető célokat is;
- a kiberbiztonság megteremtéséhez szükséges humán erőforrás kialakítása gyakran nehezebb, mint ahogy az előre becsülhető. Ennek oka elsősorban az, hogy a biztonság megteremtése nagyszámú érdekelt fél bevonását igényli. (Klimburg 2012, Kovács 2018b)

A stratégiai célok megfogalmazása mellett a tanulmánykötetet a kiberbiztonság nemzeti szintű szervezeti rendszerének kialakításával kapcsolatban is megfogalmaz sok olyan kérdést, amelyek már a stratégia kialakításkor, de méginkább annak végrehajtása során lesznek fontos tényezők:

- a nemzeti kiberbiztonsági stratégia öt különálló területre osztható: katonai terület, kiberbűnözés, kritikusinfrastruktúra-védelem és válságkezelés, kiberhírszerzés és -elhárítás, valamint kiberdiplomácia és internetkormányzás;
- ezeket a területeket fel kell térképezni mind az incidenskezelés, mind a kormányzás vonatkozásában, legyen szó akár politikai, stratégiai vagy műveleti szintekről;
- az említett területek azonban átfedésben és kapcsolatban vannak egymással a koordináció (például információcsere), a kutatás és fejlesztés, valamint az oktatás területein;
- a koordináció a különböző területeken csakúgy, mint azok között, kiemelten fontos;
- a szervezetrendszer kialakításakor fontos figyelemmel lenni arra a korábban már szintén említett tényre, hogy a szervezetek széles köre vesz részt a nemzetközi kiberbiztonsági tevékenységekben. Ezek közül a szervezetek közül a legfontosabbak gyakran nem állami csoportok;
- ugyanakkor, amennyiben a területeket nem sikerül szétválasztani és jól lehatárolni, akkor egymással ellentétes jogi követelmények és nem megfelelően működő kiberbiztonsági szervezetek nem megfelelő feladatokkal, funkciókkal és képességekkel jönnek létre;
- az erőforrások nélküli kiberbiztonsági stratégia ugyanolyan komoly veszélyforrásokat rejt magában (például a hamis biztonságtudat miatt), mintha nem is lenne a területre érvényes stratégia megfogalmazva. (Klimburg 2012, Kovács 2018b)

A korábban általam bemutatott és elemezett nemzeti biztonsági stratégiák többsége tartalmazott utalásokat a kiberbiztonság nemzetközi jogi szabályozásának szükségességére. Ezzel kapcsolatban a NATO CCDCOE tanulmánykötet a következőket állapítja meg:

- a meglévő és vonatkozó nemzetközi jogi környezet, illetve az ezekben foglalt meglévő kötelezettségvállalások korlátozhatják a nemzeti szintű döntéshozatal

szabadságát (ez természetesen igaz a már meglévő nemzeti szintű olyan jogi szabályozásra is, amely kihatással van a kiberbiztonság területére);

- nemzetközi szinten egyre inkább elfogadottá válik, hogy a nemzetközi humanitárius jog alkalmazható a kiberkonfliktusokra is. Ennek következtében az is nyilvánvaló, hogy e megközelítés alapján egy adott kibertámadás akár a fegyveres támadás szintjét és nemzetközi jogi besorolását is elérheti;
- a kiberbűnözésről szóló egyezmény[113] jelenleg az egyik legfontosabb nemzetközi keret. Az egyezmény 23–34. cikke a nemzetközi együttműködés szintjével és típusával kapcsolatban (például 24 órás elérhetőség) komoly elvárásokat fogalmaz meg, amelyeket a nemzeti kiberbiztonsági stratégia megalkotása során is figyelembe kell venni;
- a kiberbiztonság területén meglévő valamennyi nemzeti szintű szabályozással összhangban kell kialakítani a kiberbiztonság nemzeti szintű szervezeti hátterét;
- a NATO fokozta a kiberbiztonság területén megvalósuló együttműködését a nem NATO-nemzetekkel, az EU-val és egyéb nemzetközi szervezetekkel. Ez további tervezési keretet biztosít mind a nemzeti kiberbiztonsági stratégia, mind az ennek végrehajtására létrehozott szervezetrendszer hatékonyabbá tétele során. (Klimburg 2012, Kovács 2018b)

3.2. A megvizsgált kiberbiztonsági stratégiák elemzéséből levonható szintetizált következtetéseim

A kiberbiztonság vonatkozásában megvizsgált nagyhatalmak – Kína, Oroszország, Egyesült Államok –, a NATO és az Európai Unió, valamint az EU egyes tagországainak nemzeti biztonsági és nemzeti kiberbiztonsági stratégiái alapján olyan szintetizált következtetések levonása lehetséges, amelyek alapjául szolgálhatnak a kutatási céljaim között szereplő általános érvényű nemzeti kiberbiztonsági stratégia modelljének felállításához. Mielőtt ezeket az általános érvényű következtetéseket bemutatnám, szükséges a megvizsgált stratégiákból levonható következtetések ismertetése.

[113] A tanulmánykötet szövegéből nem derül ki explicit módon, de feltételezhetően ez utalás a Budapest Konvencióra. (Kovács 2018b)

A megvizsgált nemzetközi szervezetek és a különböző országok stratégiái legfontosabb elemei és az azokból levonható következtetéseim

Az Európai Unió kiberbiztonsággal kapcsolatos stratégiájából és irányelveiből levonható következtetéseim a következők:

- az EU kiberbiztonsági stratégiája a kibertámadásokkal szembeni tagállami és Uniós szintű ellenállóképesség fokozását célozza meg;
- a stratégia meghatározza a kibervédelmi politika közös biztonság- és védelempolitikai alapjait;
- a NIS irányelv 2018 májusától a tagországok számára meghatározza a nemzeti kiberbiztonsági stratégia elkészítésének feladatát;
- a NIS alapján a nemzeti kiberbiztonsági stratégiának tartalmaznia kell a kritikus infrastruktúra védelmével kapcsolatos feladatokat is;
- a kiberbiztonság nemzeti szervezeti rendszerének egyes elemeit – többek között az uniós kapcsolattartás érdekében – szintén meghatározza a NIS.

A NATO kiberbiztonsággal kapcsolatos stratégiájából és irányelveiből levonható következtetéseim:

- a kibertér, mint hadszíntér értelmezés számos következménnyel járhat a tagországok számára is (például szélesebb körű kibervédelmi feladatok delegálása a hadsereg számára, kibertámadó képességek kialakítása, kiberparancsnokságok felállítása);
- a NATO kibervédelmi felajánlás csomag egyik célja a tagországok jelenleg eltérő szintű kibervédelmi képességeinek egymáshoz való közelítése;
- a NATO kibervédelmi műveleti központja nem csak a katonai, de a civil infrastruktúra védelmében is fontos szerepet játszhat;
- a Szövetség elősegíti a nemzetközi együttműködés erősítését mind a tagországok, mind a nem NATO országok között.

Az Amerikai Egyesült Államok stratégiáinak legfontosabb elemei és a stratégiákból levonható következtetéseim a következők:

- jól szabályozott, de heterogén szervezeti háttér jellemzi az Egyesült Államok kiberbiztonságát;
- a nemzeti biztonsági stratégia és a nemzeti védelmi stratégia fontos része a kibertér védelme;

- új elem az USA nemzeti kiberstratégiája az eddigi DoD kiberstratégia mellett;
- az egyik legfontosabb jellemző a katonai orientáltság, ennek megfelelően a hadsereg kibervédelmi és kibertámadó képességei fontos szerepet játszanak az USA kibervédelmében;
- a biztonság az elrettentésre épül;
- alapvető fontosságú a kritikus infrastruktúrák és kritikus információs infrastruktúrák védelme;
- a köz- és magánszféra együttműködésének fontosságát minden stratégiai dokumentum kiemelten kezeli;
- a nemzetközi együttműködés fontossága szintén hangsúlyos elemként jelenik meg a biztonsági dokumentumokban.

Kína kibertéri tevékenységéből és stratégiai elképzeléseiből levonható összegzett következtetéseim:

- nincs egyértelmű kiberstratégia;
- teljes állami ellenőrzés az állampolgárok (például a cenzúra és a társadalmi kreditrendszer alkalmazásával), valamint a gazdasági társaságok kínai tevékenysége felett;
- Kína politikai szinten is felismerte a gazdaság információtechnológiától való függőségét, így annak védelme és fejlesztése a biztonsági dokumentumokba is stratégiai célként került be;
- a kibertér szuverenitása meghatározza Kína szuverenitását is;
- Kína jelentős információszerző tevékenységet folytat a kibertérben, amelyben a hadsereg is részt vesz;
- a 2016-ban megjelent kiberbiztonsági törvény mind a kínai állampolgárok, mind a nemzetközi kibertér szereplői Kínában történő tevékenysége számára szabályokat fogalmaz meg, kínai érdekek megsértése esetén esetleges – konkrétan nem definiált – szankciókat is kilátásba helyez;
- a kiberbiztonsági törvény rendelkezik a kritikus infrastruktúrákról és a kritikus információs infrastruktúrák védelméről is.

Oroszország kibertéri tevékenységéből és stratégiai elképzeléseiből levonható összegzett következtetéseim:

- a kiber kifejezés helyett információs fogalmi háttér a jellemző;
- Oroszország információbiztonsági doktrínával rendelkezik;
- az információbiztonsági doktrína épít a nemzeti biztonsági stratégiára, illetve az abban megfogalmazott célkitűzésekre;
- az információbiztonsági doktrína tartalmaz utalásokat a kritikus infrastruktúra védelmére is;
- stratégiai cél az elektronika és információtechnológia területeken a nemzeti K+F tevékenység ösztönzése;
- aktív jelenlét a kibertérben, amely elsősorban az információszerzésre irányul, valamint a politikai és gazdasági érdekből történő befolyásolást jelenti;
- a nemzeti biztonsági stratégia az Oroszországgal szembeni legfontosabb kibertéri veszélyeket a külföldi hatalmak által folytatott információszerzésben és befolyásolásban jeleníti meg;
- a stratégiai az elrettentésre épít;
- hivatalosan Oroszország a kibertér nemzetközi jogi normáinak (újra)kialakítása mellett érvel;
- nem fogadja el az internet erőforrásainak jelenlegi elosztási mechanizmusát.

Ausztria stratégiáiból levonható következtetéseim:

- a nemzeti biztonsági stratégia fontos szerepet lát a kiberbiztonságban;
- a kiberbűnözés visszaszorítás és az ehhez szükséges szervezeti háttér kialakítása fontos cél a biztonsági stratégiában;
- a nemzeti biztonsági stratégia a hadsereg kiberképességeinek növelését is meghatározza;
- a nemzeti biztonsági stratégia elrendeli a nemzeti kiberbiztonsági stratégia elkészítését;
- a nemzeti kiberbiztonsági stratégia a technikai veszélyforrásokat is tárgyalja;
- kiberkockázati mátrix készült a kiberbiztonsági stratégia részeként;
- a kiberbiztonsági stratégia meghatározza a szervezeti háttér legfontosabb elemeit;
- a kiberbiztonság területén ösztönzi a K+F tevékenységet, valamint a nemzetközi együttműködést;

- stratégiai cél a PPP növelése a kiberbiztonság területén.

Csehország stratégiáiból levonható következtetéseim:

- előremutató nemzeti biztonsági stratégia (2015):
  - tartalmaz előírásokat a kritikus infrastruktúrák és a hadsereg információs rendszerei védelmére is;
  - meghatározza a nemzeti kiberbiztonsági stratégia elkészítését;
  - a kiberbiztonság szervezeti rendszerét nagy vonalakban leírja;
- nemzeti kiberbiztonsági stratégia második kiadása van életben, amely mellé akcióterv is készült;
- szervezeti háttér hatékonyabb működését határozza meg;
- a kritikus infrastruktúra védelem területére is meghatároz feladatokat;
- magán- és közszféra együttműködésének fokozása szükséges;
- K+F ösztönzése;
- kiberbűnözés elleni tevékenység növelése a hatékony jogszabályi környezet kialakításával együtt;
- hangsúlyozza a nemzetközi együttműködés fontosságát.

Az Egyesült Királyság stratégiáiból levonható következtetéseim:

- a nemzeti biztonsági stratégia a kiberteret stratégiai fontosságúnak tartja, amelyen belül:
  - több frissítésen átesett, de mindegyik számol az információtechnológia jelentőségével, és az Egyesült Királyságot kibernagyhatalomként jelöli meg;
  - számol a kibertéri veszélyekkel, amelyek kezelése a stratégiai célok között is megjelenik;
  - a hadsereg számára is megfogalmaz feladatokat a kibertérrel kapcsolatosan;
  - stratégiai eszköz az elrettentés, amely a kibertéri támadások vonatkozásában is nagy hangsúlyt kap;
  - előremutató módon a kritikus infrastruktúrák védelmének fontossága bekerült a stratégiai célok közé;
- a nemzeti kiberbiztonsági stratégia második kiadása van jelenleg érvényben;

- a kiberbiztonság megteremtése érdekében a társadalom számos szereplője számára meghatároz feladatokat és felelősségi köröket;
- a stratégia szervezeti hátteret rendel a feladatok koordinációjához;
- a stratégia tartalmaz implementációs tervet is a különböző feladatok végrehajtása érdekében;
- a stratégia kibertámadóképességek kialakítását is meghatározza;
- a kiberbiztonság fejlesztése feladatrendszerben integrálja a kiberbiztonsági tudatosság emelését, az ipari támogató háttér fejlesztését, valamint a technológiai és politikai változások folyamatos figyelemmel kísérését és azok megállapításainak kiberbiztonság terültére való beépítését;
- hangsúlyosan jelenik meg a nemzetközi együttműködés fontossága;
- a stratégia dinamizmusát annak időbeni hatókörén (2016-2020) túlnyúló elképzelések tárgyalása jól mutatja, amelyben a 2021 utáni időszak – elsősorban – technikai fejlődésből eredő kihívásait vázolja fel.

Észtország stratégiáiból levonható következtetéseim:

- az ország nemzeti biztonsági koncepcióval rendelkezik, amelyben:
  - hangsúlyos a kibertér és annak biztonsága;
  - megjelenik a speciális geopolitikai helyzetből adódó veszélyek felmérése, például az orosz fenyegetés a kibertérben;
  - részletes kiberbiztonsági akcióterv elkészítését rendeli el;
  - a védelmi minisztérium feladatául rendeli a kiberbiztonság koordinálását;
- a világ első országa, amely önálló nemzeti kiberbiztonsági stratégiával rendelkezett (2008), amely nyilvánvaló legfontosabb oka a 2007-es súlyos kiberincidens volt;
- jelenleg a második nemzeti kiberbiztonsági stratégia van életben (2014);
- a stratégia meghatározott időintervallumra érvényes (jelenleg 2014-2017), így annak felülvizsgálata szükséges;
- katonai és civil összefogás a kibervédelem területén;
- kiberbűnözés elleni tevékenység fokozása;
- nemzeti szintű kibervédelmi képességek fejlesztése, amelyben a katonai és civil tervezés koordináltan történik, és amelyben a kollektív védelem alapoz a nemzetközi együttműködésre is;

- a nemzetközi kiberbiztonsági együttműködés fokozása érdekében szükséges a nemzetközi kiberbiztonság politikájának és jogi hátterének a kialakítása.

Franciaország stratégiáiból levonható következtetéseim:

- harmadik nemzetbiztonsági stratégia (fehér könyv) van életben, amelyben:
  - a stratégiai célkitűzések között markánsan megjelenik a kibertér és annak biztonsága;
  - a veszélyek között azonosítja a kiberbűnözést, valamint a kritikus infrastruktúrákat, illetve a stratégiai katonai információs rendszereket célzó kibertámadásokat;
  - számol a kiberhadviselés megjelenésével;
  - a katonai kibervédelmi és kiberműveleti – beleértve a kibertámadó – képességeket fejleszteni kell, az ezeket a feladatokat ellátó egységeket integrálni kell a hadsereg szervezeteibe;
  - Oroszországot és Kínát is fenyegetésként (kihívásként) értékeli a területen;
  - a kibervédelem területén is fontos tényezőként említi a nemzetközi együttműködést, kiemelten Németországgal és az Egyesült Királysággal;
- a nemzeti kiberbiztonsági stratégia épít a nemzeti biztonsági stratégiában megfogalmazottakra;
- a stratégiai célok között szerepel a kritikus infrastruktúrák védelme, a kiberbűnözéssel szembeni fellépés, a kiberbiztonsági tudatosság növelése, a digitális versenyképesség növelése, valamint a kibertéri autonómia megőrzése.

Hollandia stratégiáiból levonható következtetéseim:

- a jelenleg érvényben lévő nemzeti biztonsági stratégia (2018):
  - a kibertéri veszélyek technika és társadalmi oldalát is elemzi;
  - számol a hibrid konfliktusokkal, bennne a kibertéri támadásokkal;
  - a kiberelrettentésre, mint stratégiai célra utal, de nem részletezi annak kialakítását és az azzal kapcsolatos feladatokat sem;
  - meghatározza a nemzeti kiberbiztonsági stratégia megalkotását;
- a korábbi (2013-as) nemzeti kiberbiztonsági szervezeti megközelítése helyett az új stratégia az együttműködésre helyezi a hangsúlyt;

- harmadik nemzeti kiberbiztonsági stratégia (2018) van életben;
- a kiberbiztonságot a nemzeti biztonság részének tekinti;
- a kiberbiztonság sikeressége érdekében a köz- és magánszféra közötti szoros együttműködést határozza meg;
- új kiberbiztonsági szervezetrendszert határoz meg.

Magyarország stratégiáiból levonható következtetéseim:

- a nemzeti biztonsági stratégia fontos utalásokat tartalmaz a kiberbiztonságra, illetve a kibertér fontosságára. A stratégia jelenleg felülvizsgálat alatt van többek között a megváltozott biztonságpolitikai helyzet és az újonnan megjelent biztonsági kihívások miatt;
- a nemzeti katonai stratégia szintén számol a kibertérben megjelenő veszélyekkel, meghatározza a Magyar Honvédség kibervédelmének fokozását, és utal a kiberhadviselésre is. Ugyanakkor a kiberhadviselés területén sem stratégiai, sem szervezeti szinten nem történt előrelépés hazánkban. Ez a stratégia is felülvizsgálat alatt van jelenleg;
- a nemzeti kiberbiztonsági stratégia több mint öt évvel ezelőtt készült;
- a nemzeti kiberbiztonsági stratégia nagyon vázlatosan ugyan, de megfelelő feladatrendszert és ehhez stratégiai szintű szervezeti hátteret is rendelt a kiberbiztonság megteremtése, illetve növelése érdekében;
- a stratégia megfelelő alapot nyújtott a kibertéri szabályozás kialakításához (például az Ibtv. elfogadásához) valamint a társadalmi egyeztetések és együttműködések megkezdéséhez;
- a kiadásakor előremutató stratégia jelenleg felülvizsgálat alatt van.

Lengyelország stratégiáiból levonható következtetéseim:

- a jelenleg érvényes nemzeti biztonsági stratégia (2014) a következő fontos elemeket tartalmazza a kibertérrel kapcsolatosan:
    - a kibertér biztonsága stratégiai érdek;
    - kihívás a kiberteret fenyegető veszélyek együttese, amelyben nevesíti a kiberhárború veszélyét is;
    - a nemzetközi együttműködés regionális szinten is hangsúlyos kell, hogy legyen a kibertér biztonsága érdekében;

    - a hadsereg kiberképességeit növelni kell, beleértve a támadó képességeket is;
    - meghatározza a kiberbiztonság szervezeti hátterének alapjait;
- jelenlegi kiberbiztonsági stratégia (2017) már a második nemzeti szintű kiberstratégia;
- a nemzeti szintű kiberbiztonság érdekében a kialakult szervezeti rendszer együttműködési képességeit erősíteni kell;
- kiberbűnözés és kiberkémkedés elleni hatékony fellépést kell kialakítani;
- növelni kell a kiberbiztonság területén megvalósuló K+F tevékenységeket, amellyel párhuzamosan az állampolgárok digitális készségeit és kompetenciáit is emelni kell;
- a nemzetközi együttműködés hangsúlyozása mellett Lengyelország számára erős stratégiai és politikai pozíciót kell kiépíteni nemzetközi téren;
- a stratégiában meghatározott feladatokhoz egy akcióterv elkészítését is elrendeli.

Németország stratégiáiból levonható következtetéseim:

- a nemzeti biztonsági stratégia (2016):
    - kihívásként azonosítja a kibertéri veszélyeket;
    - a kibertéri veszélyeket a fizikai térben jelentkező veszélyekkel egyenértékűnek tekinti;
    - a kiberbiztonság területén a nemzeti és a nemzetközi együttműködés növelését hangsúlyozza;
    - a hadsereg kibervédelmi képességeinek növelését határozza meg;
    - a hadseregnek a saját rendszerei kibervédelme mellett az ország kibervédelmében is szerepet kell vállalnia;
- a nemzeti kiberbiztonsági stratégia (2016) már a második ilyen ágazati stratégia;
- a legfontosabb stratégiai területek meghatározása Németország nemzetközi politikai és gazdasági rendszerben elfoglalt helyének és szerepének megfelelően történt;
- a stratégiai célok a fentieknek megfelelően a digitális önállóság megőrzése az ország számára, a köz- és magánszféra együttműködése, a megfelelő infrastruktúra és a nemzetközi kiberbiztonsági rendszerben az ország vezető szerepének hangsúlyozása;

- a stratégiai ezekhez a célokhoz megfelelő szervezetrendszert rendel hozzá.

Szlovákia stratégiáiból levonható következtetéseim:

- a második nemzeti biztonsági stratégia (2016) van életben, amely:
  - a kibertéri kihívások esetében a katonai veszélyeket is számba veszi;
  - a kibertér, mint hadviselési dimenzió is bekerül a stratégiába, amely kapcsán alapvetően a NATO kollektív védelmi elvét hangsúlyozza a dokumentum;
- a nemzeti kiberbiztonsági stratégia (2015) már az EU és a NATO kiberbiztonsági elveit (például az akkor még csak tervezett NIS irányelvet, vagy a kibertér, mint hadviselési dimenzió) is tartalmazza;
- számos feladatot határoz meg a jogszabályi háttér kidolgozása, a szervezeti háttér kialakítása, valamint az oktatás és tájékoztatási rendszer kiépítésére;
- szorgalmazza a K+F tevékenység növelését;
- szorgalmazza a nemzeti és nemzetközi együttműködés fokozását a kibertérben.

A megvizsgált országok nemzeti biztonsági és nemzeti kiberbiztonsági stratégiáiból levonható következtetések szintetizálása

A megvizsgált nagyhatalmak, valamint európai uniós országok nemzeti biztonsági stratégiáinak elemzése alapján kijelenthető, hogy azok gyakorlatilag mindegyike tartalmaz utalásokat a kiberbiztonságra, sőt némelyik egyenesen elrendeli a nemzeti kiberbiztonsági stratégia megalkotását. Ugyanakkor mivel több ország már a második, illetve esetenként a harmadik (például Hollandia) frissített, vagy alapjaiban megváltoztatott nemzeti kiberbiztonsági stratégiájának kiadásánál tart, ezért az időközben szintén frissülő nemzeti biztonsági stratégiák ezekben az országokban már visszamutatásokat is tartalmaznak ezek sikerességére, illetve hatékonyságára.

A különböző országok kiberbiztonsági stratégiáinak elemzéséből a stratégia felépítésére, illetve azok legfontosabb tartalmi elemeire a következők megállapításokat teszem.

A nemzeti kiberbiztonsági stratégia általában a következő elemekből épül fel:

- terminológiai gyűjtemény, amelyben a legtöbb esetben a kibertér, valamint a kiberbiztonság meghatározása is megtörténik;
- stratégiai környezet értékelése: a kibertéri veszélyek és kihívások bemutatása, illetve azok rövid stratégiai szempontú értékelése;

- olyan stratégiai célok meghatározása, amelyek a kiberbiztonság megteremtése és folyamatos emelése révén a nemzeti biztonsági stratégiai célok eléréséhez járulnak hozzá;
- a kiberbiztonság szervezeti hátterének megvalósítására vonatkozó stratégiai elképzelések;
- a kritikus információs infrastruktúrákra és ezáltal a kritikus infrastruktúrák védelmére vonatkozó meghatározások;
- kiberbiztonsággal kapcsolatos kutatás-fejlesztés-innováció stratégiai támogatása;
- a kiberbiztonság oktatásának stratégiája, amely sok esetben a kiberbiztonsági tudatosság fejlesztését, illetve növelését is célozza;
- a köz- és a magánszféra kiberbiztonság területén történő szoros és kölcsönös együttműködésének stratégiai ösztönzése;
- a nemzetközi kiberbiztonsági együttműködés iránti elkötelezettség és annak aktív támogatása;
- esetenként a stratégiai célok elérése érdekében történő akcióterv elkészítésének meghatározása.

A stratégiai célok elérése érdekében időszakos vizsgálatok elvégzésére kell, hogy sor kerüljön. Nyilvánvalóan ezzel kapcsolatban az egyik legfontosabb kérdés, hogy ezeket a vizsgálatokat ki végezze. E felülvizsgálat érdekében szükséges egy olyan független szakmai testület kinevezése, amelyben a kiberbiztonság különböző területeinek kompetens képviselői kapnak helyet. Ennek a testületnek a tagjai nemzetközi tapasztalatokkal és megfelelő szakmai ismeretekkel kell, hogy rendelkezzenek.

3.3. A nemzeti kiberbiztonsági stratégia modelljére tett javaslatom

Az elemzett nemzeti kiberbiztonsági stratégiákból levonható következtetésekre alapozva, figyelembe véve az eddigi modellalkotási példák összegzett tapasztalatait a következő általános érvényű javaslatot teszem a nemzeti kiberbiztonsági stratégia felépítésére, illetve annak legfontosabb tartalmi elemeire, majd a modell életciklusára.

Javaslat a nemzeti kiberbiztonsági stratégia felépítésére és annak legfontosabb tartalmi elemeire

Javaslatom alapján a nemzeti kiberbiztonsági stratégia a következő elemeket kell, hogy tartalmazza:

- terminológiai gyűjtemény, amelyben a kibertér, valamint a kiberbiztonság meghatározása is megtörténik;
- stratégiai környezet értékelése: a kibertéri veszélyek és kihívások bemutatása, illetve azok rövid stratégiai szempontú értékelése;
- olyan stratégiai célok meghatározása, amelyek a kiberbiztonság megteremtése és folyamatos emelése révén a nemzeti biztonsági stratégiai célok eléréséhez hozzájárulnak;
- a kiberbiztonság szervezeti hátterének megvalósítására vonatkozó stratégiai elképzelések;
- a kritikus információs infrastruktúrákra és ezáltal a kritikus infrastruktúrák védelmére vonatkozó meghatározások;
- kiberbiztonsággal kapcsolatos kutatás-fejlesztés-innováció stratégiai támogatása;
- a kiberbiztonság oktatásának stratégiája, amely a kiberbiztonsági tudatosság fejlesztését, illetve növelését is célozza;
- a köz- és a magánszféra kiberbiztonság területén történő szoros és kölcsönös együttműködésének (PPP) stratégiai ösztönzése;
- a nemzetközi kiberbiztonsági együttműködés iránti elkötelezettség deklarálása;
- a stratégiai célok elérése érdekében történő akcióterv elkészítésének meghatározása;
- értékelési rendszer kidolgozása, amely egyrészt a stratégiában, másrészt az akciótervben megfogalmazottak végrehajtásának ellenőrzéséhez ad mutatókat.

Mindezek mellett – nem átalános érvényű elemként, de – fontos hangsúlyozni, hogy az adott ország politikai döntésétől függően a hadsereg szerepe az ország kibervédelmében célszerűen megjelenítendő. Ez a következő kérdésekre (területekre és a hozzá kapcsolódó célokra) irányulhat:

- a hadsereg kiberműveleti képességeinek kialakítása, beleértve a kibertámadó képességeket is;
- a hadsereg feladatai az adott ország kibervédelmében és esetlegesen a kritikus infrastruktúrák és kritikus információs infrastruktúrák védelmében;

- a hadsereg feladatai egy, az adott országot érő kibertámadás során, amely akár válaszcsapás kialakítását is jelentheti;
- a hadsereg kiberműveleti képességei – a megfelelően robosztus állami kibervédelmi szervezetekkel és azok kibervédelmi képességeivel együtt – elrettentést jelentenek.

A fentieknek megfelelően a javasolt modell tartalmazza a kibertámadási képességekre vonatkozó meghatározást is. A hatékony kiberbiztonsági stratégiához szükséges, hogy az adott ország – nyilvánvalóan politikai döntéstől, illetve az adott ország alkotmányától függően – kialakítsa és rendelkezzen azokkal a kiberreagálási képességekkel, amelyek nem csak a támadások elhárítását, hanem az azokra adandó proaktív válaszokat, a korai előrejelzés képességét és akár a megelőző támadásokat is magába foglalják a potenciális támadókkal szemben (itt elsősorban az állami támogatású, a stratégiai fontosságú infrastruktúrákat célzó támadások elleni tevékenységre kell gondolni). Ezek a képességek befolyásolják, nagymértékben lerontják vagy megakadályozzák a szembenálló felet a támadások kivitelezésében, illetve abbéli képességeikben. A támadó képességek az elrettentés célját is szolgálják.

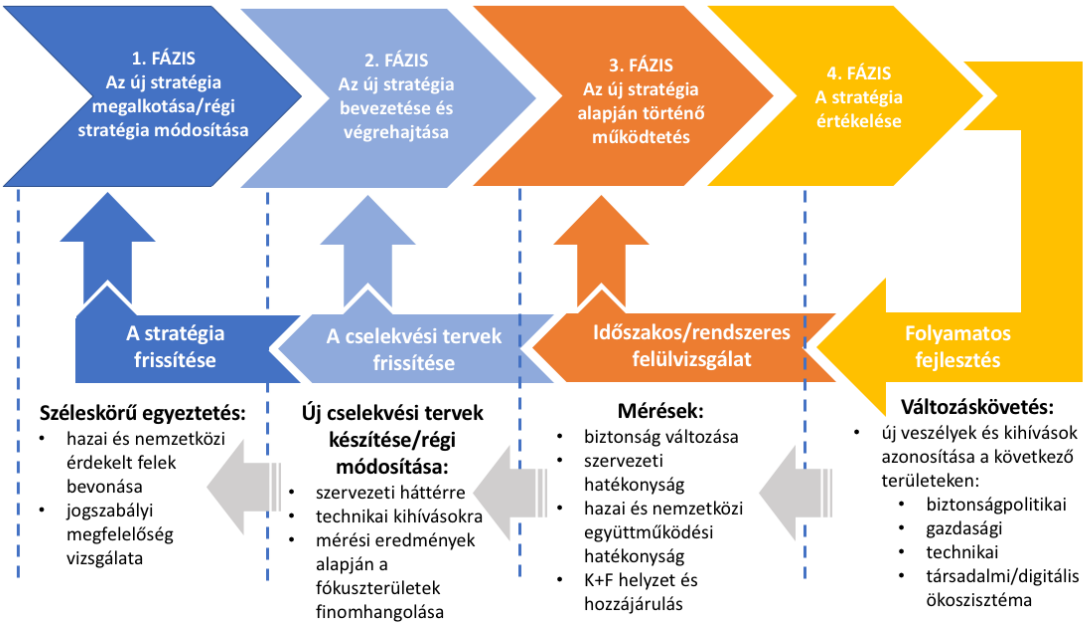
Javaslat a nemzeti kiberbiztonsági stratégia életciklusára

Az előzőekben megvizsgált nemzeti biztonsági stratégiák, valamint nemzeti kiberbiztonsági stratégiák, illetve a bemutatott kiberbiztonsági stratégiák kialakítását célzó modellek alapján egy általános érvényű nemzeti kiberbiztonsági stratégia modelljének életciklusára, valamint az abban szükséges tevékenységekre a következő formában teszek javaslatot.

A javasolt stratégia modellje abból az alapvetésből indul ki, hogy az európai országok mindegyike rendelkezik már nemzeti kiberbiztonsági stratégiával, sőt azok már egy, vagy akár több alkalommal felülvizsgálatra is kerültek. A másik alapvetés, hogy a nemzeti kiberbiztonsági stratégiának meg kell felelnie a nemzeti biztonsági stratégiában megfogalmazott céloknak, azokat a kiberbiztonság erősítésével és növelésével támogatniuk kell. Mindezeken túl a nemzeti kiberbiztonsági stratégiának azokat a képességeket is tartalmaznia kell, amelyeket a nemzeti biztonsági stratégia és/vagy esetlegesen a nemzeti katonai stratégia az ország fegyveres védelme érdekében meghatározott.

Az általam javasolt dinamikus modell életciklusa négy fázisból, valamint a fázisokhoz tartozó, az adott fázis követelményeihez alkalmazkodó, ennek megfelelően esetenként vagy folyamatosan – szintén dinamikusan – változó tevékenységeket tartalmaz. Mivel nemzeti

szintű stratégiáról beszélünk, ennek megfelelően a stratégia egészének megváltoztatása, azaz új stratégia készítése nem lehetséges rövid – azaz 2-3 évnél rövidebb – időintervallumon belül. Ezért a javasolt modell végrehajtása 3-4 év, de esetenként ennél is hosszabb ciklusra vonatkoztatható. A modell egyes fázisaiban lévő dinamikus változók – például mérési eredmények, vagy a veszélyek és kihívások felmérése és az azokhoz való alkalmazkodás – 3-4 éves ciklusban anélkül végrehajtható, hogy alapjaiban, például az alapvető kiberbiztonsági szervezeti háttér generális átalakításával kellene megváltoztatni azt. Nyilvánvalóan a kibertér jelenlegi és középtávra előre jelezhető változásai, valamint az abban lévő technikai és humán változások – például a már említett mesterséges intelligencia technikai alkalmazásokra, valamint közvetve és közvetett módon a humán környezetre gyakorolt esetleges hatásai miatt – a stratégia alapjainak felülvizsgálata 4-5 évente így is szükségessé válik.



9. ábra
A nemzeti kiberbiztonsági stratégia általam javasolt modelljéhez szükséges végrehajtási ciklus

szerkesztette: szerző

Fontos hangsúlyozni, hogy a javasolt modell nem egy statikus dokumentum elkészítését célozza, hanem az egy – akár nemzetközi együttműködésben elkészíthető –, a kibertérben megjelenő legváltozatosabb kihívásokat és veszélyeket dinamikusan kezelni képes, az adott ország kiberbiztonságának, és ezzel párhuzamosan az adott régió biztonságának emelni képes stratégiai elképzelések együttesét jelenti.

9. táblázat
Az általam javasolt nemzeti kiberbiztonsági stratégia modelljének egyes szakaszaihoz tartozó tevékenységek

Fázis / Visszacsatolás	*A modell szerint elvárt tevékenységek**
1. fázis: Az új stratégia megalkotása/régi stratégia módosítása	A stratégia általános céljának meghatározása, szükség esetén annak felülvizsgálata. A stratégiai célok meghatározása, azok pontosítása. Az érdekelt felek körének azonosítása, szükség szerinti felülvizsgálata, új szereplők szükség szerinti bevonása.
	A meglévő szakpolitikák, szabályzók felülvizsgálata és az ezek végrehajtásához szükséges képességek meghatározása.
	Nemzeti szintű kockázatértékelési és kockázatkezelési módszertan kialakítása és meghatározása.
	A kritikus információs infrastruktúrák védelmének növelése és interdependenciájuk felmérése.
	Az információmegosztási mechanizmusok felülvizsgálata, szükség esetén azok meghatározása vagy átalakítása.
	A kiberbiztonság növelése érdekében szükséges biztonsági követelmények megállapítása.
Az 1. fázishoz tartozó visszacsatolás: A STRATÉGIA FRISSÍTÉSE	Hazai és nemzetközi érdekelt felek azonosítása és bevonása. Nemzeti szintű kockázatelemzés elkészítése. Jogszabályi megfelelőség vizsgálat.
2. fázis: Az új stratégia bevezetése és végrehajtása (korábbi stratégia szükség szerinti módosítása)	Átlátható és a feladatokban/jogosultságokban egymást jelentősen nem átfedő irányítási és szervezeti struktúra kialakítása, illetve a felülvizsgálat eredményeként annak esetleges átalakítása.
	Kiberbiztonsági vészhelyzetkezelési tervek kidolgozása, pontosítása.
	A kiberbiztonságra vonatkozó értékelési séma (rendszer) kidolgozása, bevezetése és alkalmazása.

	A fő teljesítménymutatók (KPI) rendszerének kidolgozása.
	Incidenskezelési képességek kialakítása, fejlesztése.
	Kiberincidensek jelentési mechanizmusainak pontosítása.
	A kiberterületen folytatott K+F-tevékenység ösztönzőrendszerének kidolgozása, bevezetése, növelése.
	A kiberbűnözés elleni hatékony fellépés és tevékenység fokozása hazai és nemzetközi területen egyaránt.
	A kiberbiztonság területén nemzetközi együttműködésekben való aktív részvétel.
	A köz- és magánszféra közötti partnerség kialakítása.
	A közszféra intézményei közötti együttműködés hatékonyságának növelése.
	A magánszektor kiberbiztonsági területekbe való befektetésének ösztönzése.
A 2. fázishoz tartozó visszacsatolás: A CSELEKVÉSI TERVEK FRISSÍTÉSE	Akcióterv készítése (módosítása): • szervezeti háttér módosítása; • technikai kihívások kezelése; • mérési eredmények alapján a fókuszterületek finomhangolása.
3. fázis: Az új (módosított) stratégia alapján történő kiberbiztonsági rendszer működtetése	Kiberbiztonsági gyakorlatok megszervezése.
	A kiberképzési és -oktatási programok bevezetése és ösztönzése.
	Az állampolgárok kiberbiztonsági tudatosságának növelése.
A 3. fázishoz tartozó visszacsatolás: IDŐSZAKOS / RENDSZERES FELÜLVIZSGÁLAT	Kiberbiztonsági mérések a következő területeken: • a biztonság változása; • szervezeti hatékonyság; • hazai és nemzetközi együttműködés hatékonyság;

	• K+F helyzet és hatékonyság.
4. fázis: A stratégia, illetve annak hatékonyságának értékelése	A stratégia folyamatos fejlesztése.
	A nemzeti kiberbiztonsági stratégia finomhangolása a főbb teljesítménymutatók eredményeinek felhasználásával.
	A kibergyakorlatok során megszerzett tapasztalatok feldolgozása és ezek alapján hatékonyságnövelő intézkedések kidolgozása.
A 4. fázishoz tartozó visszacsatolás: FOLYAMATOS FEJLESZTÉS	Változáskövetés valamint az új veszélyek és kihívások azonosítása: • biztonságpolitikában; • gazdaságban; • IKT-ban; • társadalmi/digitális ökoszisztémában.

**Megjegyzés: A tevékenységek felsorolása esetén jelzett esetleges felülvizsgálatokat, illetve pontosításokat a már meglévő stratégiára kell vonatkoztatni.*

szerkesztette: szerző

A jelenlegi európai nemzetközi biztonsági struktúra szövetségi rendszerekre, így az Európai Unió, illetve a NATO által – sok esetben elrettentésre építő – biztonsági garanciáira, de mégis a tagállamok, azaz a nemzetállamok képességeire és politikai, gazdasági, valamint katonai képességeire épül.

Az általam javasolt stratégia modelljének egyes fázisait és az azokhoz tartozó tevékenységeket a következőkben mutatom be.

1. fázis: Az új stratégia megalkotása/régi stratégia módosítása

A széleskörű egyeztetés eredményeit, a cselekvési tervek frissítése során szerzett tapasztalatokat, az időszaki és rendszeres felülvizsgálat során keletkezett a stratégia folyamatába nem beépíthető elemeket, valamint a stratégiai szintű biztonságpolitikai, gazdasági, technológiai és társadalmi változásai generálta szükséges változásokat új vagy frissített stratégiában kell megjeleníteni. Ennek érdekében javaslatom szerint az első fázis a következő tevékenységeket foglalja magába

- a stratégia általános céljának meghatározása, szükség esetén annak felülvizsgálata;
- a stratégiai célok meghatározása, azok pontosítása:
  ennek szükségszerűen a nemzeti biztonsági stratégia célkitűzéseire kell épülnie, valamint más ágazati stratégiákkal harmonizált módon kell ezeket a célkitűzéseket támogatnia;
- az érdekelt felek körének azonosítása, szükség szerinti felülvizsgálata, új szereplők szükség szerinti bevonása;
- a meglévő szakpolitikák, szabályzók felülvizsgálata és az ezek végrehajtásához szükséges képességek meghatározása;
- nemzeti szintű kockázatértékelési és kockázatkezelési módszertan kialakítása és meghatározása, annak megléte esetén pontosítása:
  a kockázatmenedzsment, azaz a kockázatelemzés és a kockázatkezelés nemzeti szintű módszertanát kell kidolgozni. Ebben kockázatelemzésnek ki kell terjednie az azonosított érdekelt felekre és tartalmaznia kell a stratégiai szintű technikai és egyéb veszélyforrások jelentette fenyegetettségek bekövetkezése esetén jelentkező esetleges hatásokat (károkat). A kockázatelemzést rendszeres időközönként el kell végezni. A kockázatelemzés eredményeire épülő kockázatkezelési tervnek szintén nemzeti szinten tartalmaznia kell azokat a stratégiai terveket, amelyek mentén a kockázatok, illetve azok hatásai csökkenthetők. Mindezeket elősegítendő nemzeti szintű, többek között a kiberfenyegetések felderítése (threat intelligence) segítségével feltárt fenyegetéseket nemzeti adatbázis(ok)ba kell rendezni. A kockázatkezelésre stratégiai szinten is érvényes, hogy a kockázatkezelési módszereknek arányosnak kell lenniük a kockázatokkal. Ez azonban felveti annak a kérdését, hogy az üzemeltető és/vagy tulajdonos vagy az állam feladata-e a megfelelő – esetlegesen az adott rendszer vonatkozásában aránytalan – védelmi mechanizmus kiépítése. Ennek okán az állami szerepvállalás a stratégiai szintű kockázatok kezelésére elengedhetetlen még abban az esettben is, ha az adott kockázat magántulajdonban lévő rendszer, vagy rendszerelem vonatkozásában jelentkezik;
- a kritikus információs infrastruktúrák védelmének növelése és interdependenciájuk felmérése:

a kritikus információs infrastruktúrák védelmének növelése érdekében fel kell mérni azok egymás közötti függőségét, valamint azok védelme érdekében világos felelősségi köröket kell kijelölni. A kritikus infrastruktúrák stratégiai szintű meghatározása a nemzetbiztonság, a gazdaság működőképessége, illetve annak biztonsága, valamint a közbiztonság szempontjából fontos ágazatok és alágazatok csoportosításával lehetséges. A már meglévő kritikus infrastruktúra és kritikus információs infrastruktúra védelmi rendszer felülvizsgálata rendszeres időközönkét – többek között a fentiekben megfogalmazott kockázatelemzés eredményeire építve – szükséges. Ebben az egyik kiinduló pont a NIS irányelv által is előírt alapvető szolgáltatások, illetve azok üzemeltetőinek a meghatározása. A NIS alapvető szolgáltatásokat nyújtó szereplők azonosítására kritériumokat határozott meg. Az alapvető szolgáltatásokat kritikus ágazatonként számba kell venni és azokról nyilvántartást kell vezetni. Hasonlóan a kockázatkezeléshez itt is igaz, hogy a stratégiai szintű ágazatok esetében az állami szerepvállalás szükséges, amelyhez felelős állami szervezetet kell rendelni (például az adott ágazatért egyébként is felelős minisztérium, vagy kormányzati szerv). Fontos kérdés a köz- és a magánszféra kölcsönös bizalmon alapuló együttműködése ezen a területen is. Mindezeken kívül ezeknek az alapvető szolgáltatásoknak vagy rendszerelemeknek az egymásra gyakorolt hatásait fel kell mérni. A kritikus rendszerek esetében rendszeres védelmi gyakorlatokat kell tartani, amelyek során a különböző ágazatok egymásra gyakorolt hatása is mérhető;

- az információmegosztási mechanizmusok felülvizsgálata, szükség esetén azok meghatározása vagy átalakítása:

  a kiberbiztonságban érintett szereplők számára ki kell dolgozni egy rendszeres információmegosztási metódust, amelyben az érintett felek valós időben férhetnek hozzá a különböző információkhoz (nyilvánvalóan a jogosultságuk figyelembe vételével);
- a kiberbiztonság növelése érdekében szükséges biztonsági követelmények megállapítására vonatkozó feladat:

  ezeket a követelményeket nem szükségszerűen kell, hogy tartalmazza a stratégia. Azonban magának a feladatnak meg kell jelenni benne. A biztonsági követelmények megállapítása egységes keretet ad mind a köz-, mind a magánszféra számára a szükséges kiberbiztonsági szint eléréséhez (feladatokkal,

mérőszámokkal, szükséges szervezeti kialakításra tett javaslatokkal, képzési és oktatási feladatokkal).

2. fázis: Az új a stratégia bevezetése és végrehajtása (korábbi stratégia szükség szerinti módosítása)

Javaslatom szerint a második fázis a következő tevékenységeket foglalja magába:

- átlátható és a feladatokban/jogosultságokban egymást jelentősen nem átfedő irányítási és szervezeti struktúra kialakítása, illetve a felülvizsgálat eredményeként annak esetleges átalakítása;
- kiberbiztonsági vészhelyzetkezelési tervek kidolgozása, pontosítása:
  a stratégiai szintű ágazatokra nemzeti kibervészhelyzet-kezelési tervet kell készíteni, majd az ebben foglaltakat időszakosan tesztelni kell, például gyakorlatok levezetésével. Ezek lehetnek nemzeti (kiber)válságkezelési gyakorlatok, de az IKT rendszerek és a kritikus információs infrastruktúrák és szolgáltatások határokon átnyúló jellege miatt alapvető a nemzetközi gyakorlás szükségessége is;
- a kiberbiztonságra vonatkozó értékelési séma (rendszer) kidolgozása, bevezetése és alkalmazása;
- a fő teljesítménymutatók (KPI) rendszerének kidolgozása:
  amennyiben jelenleg nincs meg a kiberbiztonság reális felmérésére és folyamatos nyomon követésére kialakított mérő rendszer, vagy az nem megfelelő, akkor annak létrehozása (átalakítása) szükséges. A kiberbiztonság mérése, és így közvetett módon a kiberbiztonsági stratégia, illetve az abban foglalt (vagy akár az ehhez szorosan kapcsolódó akciótervben meghatározott) tevékenységek hatásainak, illetve hatékonyságának a mérésére a fő teljesítménymutatók alkalmasak;
- incidenskezelési képességek kialakítása, fejlesztése, valamint a kiberincidensek jelentési mechanizmusainak pontosítása:
  a nemzetközi incidensjelentési kötelezettségeket is figyelembe véve minden stratégiailag fontos szektorban szükséges meghatározni az incidensek jelentésének rendjét. Ehhez ki kell alakítani egy olyan incidensjelentési rendszert, amely a szektoriális incidensjelentésekkel együttműködésben képes az

incidensekről szóló információk az incidenskezelő, az incidens elemző rendszer, vagy akár ezen kívül szélesebb körben is – például a lakosság kiberbiztonsági tudatosságának növelése céljából – az érdekelt felek számára eljuttatni. Ennek a rendszernek további feladata meghatározott időszakonként – például negyedévente, vagy évente – statisztikai adatok formájában az incidensekről szóló adatokat közzétenni. Ezek az adatok felhasználhatók fenyegetettség-előrejelzés, egyéb elemzés, de akár az említett kiberbiztonsági tudatosság növelése céljából is fontosak. Szükséges egy nemzeti CERT vagy CSIRT kijelölése. Ez az EU-n belül a NIS irányelvekben meghatározottak miatt kötelező érvényű feladat is. Fontos a CERT-ek együttműködésének szabályozása, valamint kiemelten a nemzeti CERT vagy CSIRT nemzetközi incidenskezelési hálózatba való bekapcsolása, illetve az abban való aktív együttműködése;

- a kiberterületen folytatott K+F-tevékenység ösztönzőrendszerének kidolgozása és bevezetése:

  a kiberbiztonság K+F tevékenysége esetében is szükséges a stratégiai irányok, célok és prioritások kijelölése. Ebben az esetben is igaz, hogy a köz- és a magánszféra együttműködése elengedhetetlen, amely együttműködésbe az akadémiai szféra (például egyetemek, kutatóintézetek, laborok) bevonása szintén fontos. Ugyanakkor ezen a területen a K+F tevékenység eredményeinek (amelyek esetében szükséges megjegyezni, hogy csak versenyképes és piacképes eredmények lehetnek) megjelenése a piacon hasonló gyors ütemű kell, hogy legyen, mint az IKT szektor más ágazatai esetében. A kiberbiztonsági K+F nemzetközi piaci verseny kiélezett, de ennek ellenére vagy éppen ezért a nemzeti kiberbiztonsági kutatásokkal, fejlesztéssel és a termékek innovációjával foglalkozó cégek támogatása célszerű. Ennek és magának a K+F tevékenységnek a koordinációja az adott ország kormányzati szintjén kell, hogy megtörténjen;
- a kiberbűnözés elleni hatékony fellépés és tevékenység fokozása hazai és nemzetközi területen egyaránt:

  szükséges a bűnüldöző hatóságon belül dedikált, a kiberbűnözéssel foglalkozó egység(ek) létrehozása. Az ebben az egységben dolgozók, valamint a kiberbűncselekmények ellen fellépő ügyészek és bírák speciális felkészítése, szakmai továbbképzése kiemelt feladat, csakúgy, mint a kiberbűnözés elleni egységk technikai, illetve anyagi erőforrásainak biztosítása. A kiberbűnözés elleni hatékony fellépés csak nemzetközi együttműködésben valósítható meg, amelyhez

elengedhetetlen a kiberbűnözés elleni nemzetközi jogi egyezményekhez való csatlakozás, illetve azok hazai jogrendbe való átültetése és alkalmazása. A kiberbűnözés elleni hatékony fellépés a kiberbűncselekmények, illetve azok technikai és elkövetési módjainak a folyamatos nyomon követését, azok adatbázisokban való rögzítését is megköveteli. Az ezekből készülő időszakos jelentések az állampolgárok kiberbiztonsági tudatosságának növelése érdekében felhasználhatóak;

- a kiberbiztonság területén nemzetközi együttműködésekben való aktív részvétel:
  a kiberbiztonság területén megvalósítandó nemzetközi együttműködés több területen megvalósítandó feladatokat jelent. Egyrészt a nemzetközi kiberbiztonság növelése érdekében tevékenykedő szervezetekben való hatékony és konstruktív részvételt jelent, amely például a már többször említett nemzetközi jogszabályi keretek kialakítását és fejlesztését, vagy akár a kiberbűnözés elleni hatékony nemzetközi fellépést igyekszik kialakítani. Ezen kívül egy másik feladat a kiberveszélyek nemzetközi trendelemzésében, a nemzetközi kiberveszélyelőrejelző- és korai figyelmeztető rendszerhez való kapcsolódást is jelenthet. (Ez szükségszerűen adatcserével jár, amely során meg kell teremteni a minősített vagy politikai és/vagy gazdasági okok miatt érzékeny adatok kezelését is). Mindezek történhetnek centralizáltan, például a NIS direktíva által meghatározott nemzeti kontakt ponton keresztül, de történhet ágazati szinten a CIWIN mintája alapján is. Ezeken kívül a nemzetközi kutatás-fejlesztés programokban való részvétel, vagy az akadémiai szféra nemzetközi együttműködéseinek erősítése is stratégiai támogatást kell, hogy kapjon.
- a köz- és magánszféra közötti partnerség kialakítása:
  a nemzeti kiberbiztonsági stratégia végrehajtásának egyik alappillére a köz- és magánszféra közötti hatékony együttműködés kialakítása. Ennek oka többek között például a már említett kritikus infrastruktúra tulajdonosi és/vagy üzemeltetői körében keresendő. A köz- és a magánszféra közösen – de például a telekommunikációs infrastruktúra esetében túlnyomó többségben a magánszféra tulajdonában és kezelésében – lévő rendszerekről beszélhetünk. Így az együttműködés a két fél között elengedhetetlen. Ennek kialakításához nemzeti szintű stratégia, illetve terv szükséges, amelyben meghatározásra kerülnek például a magánszektor kritikus infrastruktúrákba, vagy kiberbiztonsági

rendszerekbe való invesztícióinak kérdései. A nagyvállalatok mellett szükséges a kis- és közepes vállalkozások bevonása is;

- a közszféra intézményei közötti együttműködés hatékonyságának növelése:
  ennek az együttműködésnek az intézményesített kereteit ki kell alakítani. Olyan rendszeresen ülésező fórumok, tanácsok és együttműködési hálózatok kialakítása a cél, amelyben a közszféra érintett szervezetein kívül a kiberbiztonsági hatóságok is aktívan részt vesznek. Ez a koordináción kívül az információáramlást is segítheti, valamint hozzájárulhat a kölcsönös bizalmon alapuló együttműködési hajlandóság növeléséhez;
- a magánszektor kiberbiztonsági területekbe való befektetésének ösztönzése:
  gazdaságpolitikai ösztönzés szükséges a kis- és közepes vállalatok, illetve az induló vállalkozások (startupok) kiberbiztonsági eszközökbe, illetve megoldásokba való befektetési kedvének és hajlandóságának a növelése érdekében. Ehhez adókedvezmények, munkatársak képzését szolgáló támogatások, vagy akár kedvezményes állami kölcsönök lehetnek célra vezetők.

3. fázis: Az új (módosított) stratégia alapján történő kiberbiztonsági rendszer működtetése

Javaslatom szerint a harmadik fázis a következő tevékenységeket foglalja magába:

- kiberbiztonsági gyakorlatok megszervezése:
  stratégiai szinten a számos kiberbiztonsági, illetve kibervédelmi gyakorlat koordinációja szükséges, illetve meg kell határozni, hogy ezek közül van-e olyan, amely céljait és eljárásait (volumenét) tekintve stratégiai szintű gyakorlat lehet. Ennek a gyakorlatnak a kiberválságkezelési-tervben kitűzött folyamatokat kell támogatniuk. A stratégiai szintű gyakorlat végrehajtásába lehetőség szerint minden érdekelt felet be kell vonni a köz- és a magánszférából egyaránt. Ezeknek a gyakorlatoknak a tapasztalatait fel kell használni a nemzeti szintű kiberbiztonsági stratégia fejlesztése során. Ezen kívül szektor specifikus gyakorlatokat kell tartani;
- a kiberképzési és -oktatási programok bevezetése és ösztönzése:
  a kiberbiztonsági képzések köz- és felsőoktatásban való megjelenését az adott ország oktatási stratégiájának részévé kell tenni. A legfiatalabb kortól kezdődően

az egyetemi oktatásig minden fiatal számára szükséges a kiberbiztonság – adott életkornak és az ahhoz a korhoz tartozó kihívásoknak és veszélyeknek megfelelni képes, illetve az azokra helyes válaszokat adó – rendszeres, intézményesített oktatás jelenléte. Ezekhez a képzésekhez meg kell teremteni a tanári és oktatói kar továbbképzését. Az olyan egyetemek, illetve kutatóintézetek, ahol kiberbiztonsági speciális képzés, illetve kutatás folyik azok dedikáltan tananyagok, illetve felkészítő anyagok elkészítésének feladatait kaphatják, vagy vállalhatják. Ezen kívül az iskolarendszerben nem részt vevők számára ingyenes képzések ajánlása szintén elengedhetetlen. Ezek lehetnek egyszeri előadások, de rendszeres előadás sorozatok is. Fontos, hogy ezek az oktatási programok a kiberbiztonsággal kapcsolatos jövőbeni szakemberek egyik toborzó helyévé is váljanak;

- az állampolgárok kiberbiztonsági tudatosságának növelése:
  az állampolgárok kiberbiztonsági tudatosságának növelése stratégiai cél, mert ezen keresztül növelhető a kibertér ellenállóképessége nem csak egy adott országban, hanem nemzetközi szinten is. Ennek érdekében külön stratégiai tervre van szükség, amelyben akár külön korosztályonként, akár gazdasági csoportonként (például kis- és közepesvállalkozások) lehet a célcsoportokat meghatározni, majd a számukra célzott kommunikációs kampányokat levezetni. A kommunikációs kampányoknak arra is ki kell terjedniük, hogy az állampolgárok, vagy a gazdasági szereplők képviselői hol és hogy a juthatnak a kiberbiztonságot érintő megbízható és hiteles információhoz, illetve hova fordulhatnak kiberbiztonságot érintő kérdéseikkel vagy esetleges problémáikkal. Ezeknek a kampányoknak a hatékonyságvizsgálata szintén fontos, mert a kampányok tartalmi része és/vagy kommunikációs eszközkészlete ezen visszajelzések alapján módosítható a megfelelő irányba.

4. fázis: A stratégia, illetve annak hatékonyságának értékelése

Javaslatom szerint a negyedik fázis a következő tevékenységeket foglalja magába:

- a stratégia folyamatos fejlesztése;
- a nemzeti kiberbiztonsági stratégia finomhangolása a főbb teljesítménymutatók eredményeinek felhasználásával:

a meghatározott KPI-k mellett a DESI index lehet egy olyan teljesítmény mutató, amely közvetve a kiberbiztonság hatékonyságának növekedését vagy csökkenését mutatja. Ezen eredmények alapján lehetséges az egyes kiberbiztonsági területek finomhangolása;

- a kibergyakorlatok során megszerzett tapasztalatok feldolgozása és ezek alapján hatékonyságnövelő intézkedések kidolgozása:
  a meghatározott időközönként megtartott nemzeti és nemzetközi gyakorlatok során megszerzett tapasztalatok, illetve az azokból levonható következtetések alapján a kiberbiztonság hatékonysága emelhető.

Mindezen feladatokon túl a nemzeti kiberbiztonsági stratégia magába kell, hogy foglalja a kiberválságkezelési-terv[114] elkészítésére vonatkozó feladatot is. Ez a terv, csakúgy, mint a stratégia végrehajtását leíró akcióterv egy különálló dokumentum. Ebben szükséges rögzíteni – a stratégiában meghatározottak szerint – a kibertér definíciós készletét. Fontos hangsúlyozni az együttműködés szükségességét, mert a kibertéri incidensek több szektort érintve – azok egymásra történő negatív hatásaikkal – elérhetik azt a szintet, amikor súlyos, illetve stratégiai szintű kiberválságról beszélhetünk. Ennek mérésére egy olyan mérőrendszer felállítása szükséges, amely a kritikus infrastruktúrákat érő kiberválságok hatásainak és azok következményeinek reális felmérését tudják elvégezni. Ugyanakkor a súlyos, illetve stratégiai szintű kiberválságok bekövetkezése okainak feltárása majd annak megszüntetése vagy mérséklése a kiberválságok bekövetkezésének valószínűségét csökkentik. Ebben a tevékenységben nem csak a technikai elemzés a kulcskérdés, hanem maga az idő. Minél rövidebb idő alatt sikerül a válság bekövetkezésének okait kideríteni, annál nagyobb a valószínűsége, hogy egy ugyanilyen vagy hasonló válság kiküszöbölhető. Külön kell választani a válság okainak elemzését és a válság kezelését, illetve a következmények felszámolását. Ugyanakkor mind az okok elemzéséhez, mind magához a válságkezeléshez hozzá kell rendelni a megfelelő anyagi erőforrásokat. Mindezeken túl szükséges az érdekelt felek azonosítása, bevonása, az együttműködésük jogszabályi

[114] Kiberválság alatt a súlyos kiberincidensek – kibertámadások, egyéb rosszindulatú kibertevékenységek – által bekövetkezett állapotot értem, amelyek stratégiai szintű infrastruktúrákra gyakorolt negatív hatásaikkal okoznak működésképtelenséget, technikai vagy esetleg humán kárt. A kibertérben történő incidensek sikeres és hatékony kezelése sok esetben megakadályozza a kiberválságok kialakulását. Azt a szintet, amely felett a kiberincidensek, illetve azok együttes hatása eléri a kiberválság szintjét a kiberválságkezelési-tervben kell megadni.

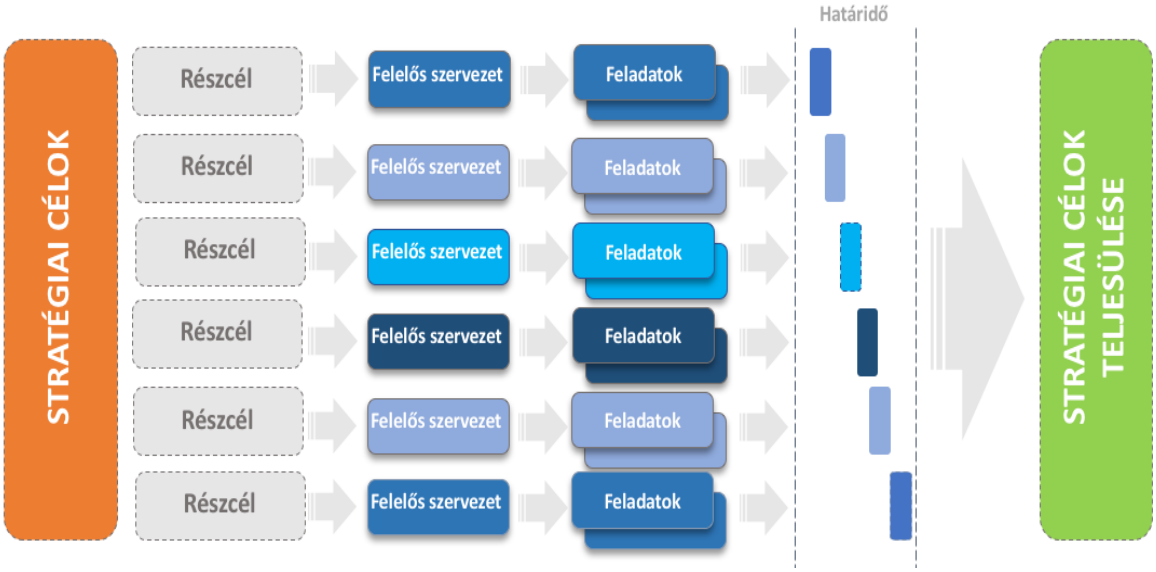
hátterének kidolgozása, valamint az információs és tájékoztatási, illetve koordinációs folyamatok kialakítása.

3.4. A nemzeti kiberbiztonsági stratégia végrehajtása érdekében elkészítendő akcióterv felépítésére vonatkozó javaslatom

A nemzeti kiberbiztonsági stratégia végrehajtása érdekében egy akciótervet kell meghatározni, amely a stratégiában megfogalmazott stratégiai célok végrehajtását operatív szinten, kézzelfogható feladatok elrendelésével támogatják. Az akciótervben megfogalmazott feladatokhoz felelős szervezeteket kell kijelölni, és meg kell határozni az adott feladat végrehajtásának határidejét. Fontos a feladatok közötti átfedések minimális szintre csökkentése, ugyanakkor a feladatok – stratégiai célok irányába történő – maximális hatásának elérése érdekében szükséges a feladatok összehangolása és koordinálása. Ehhez ki kell jelölni egy vezető szervezetet, amely szervezet megfelelő politikai-, gazdasági- és humánerőforrás birtokában van, illetve ezek a számára biztosíthatók.

Mindezeknek megfelelően a nemzeti kiberbiztonsági stratégia céljainak elérése és ez által a kiberbiztonság szintjének növelése érdekében megfogalmazott akciótervnek javaslatom szerint a következő elemekből kell állnia:

- a stratégiai célok végrehajtása érdekében minden célhoz felelős kormányzati szervezetet – például minisztériumot, központi ügynökséget, hivatalt stb. – kell hozzárendelni;
- a stratégiai célokat részcélokra kell osztani;
- mind a stratégiai célok, mind a részcélok esetében meg kell határozni a végrehajtás határidejét;
- a célok és részcélok elérése érdekében tevékenységeket (akciókat/feladatokat) kell azok mellé rendelni;
- a feladatok mellé anyagi erőforrásokat kell hozzárendelni;
- a feladatok végrehajtása érdekében humán erőforrásokat kell azokhoz rendelni;
- a célokhoz olyan mutatókat kell hozzárendelni, amelyekkel mérhető a célok elérése, illetve azoknak a tevékenységeknek a hatékonysága, amelyek ezen célok elérése érdekében meghatározásra kerültek;
- a végrehajtás hatékonysága mérésére alkalmazott mutatókat elemezni kell, majd az elemzések függvényében a stratégia egyes pontjai számára visszajelzéseket kell adni a finomhangolás vagy az esetleges nagyobb stratégiai korrekció végrehajtása érdekében.



10. ábra
A nemzeti kiberbiztonsági stratégiához kapcsolódó akcióterv folyamata

szerkesztette: szerző

Hangsúlyozni kell, hogy egy adott országon belül a kiberbiztonság megteremtése nem csak a nemzeti kiberbiztonsági szervezetek feladata, hanem összkormányzati, sőt össztársadalmi ügy és érdek is egyben. Ennek megfelelően a kiberbiztonság megteremtése, illetve annak fejlesztése érdekében az állampolgárok, a gazdasági élet szereplői és a kormányzati szervezetek – a kölcsönös bizalmon alapuló – tevékenysége szükséges. E filozófia mentén kell felépíteni a nemzeti kiberbiztonsági stratégiát, valamint annak végrehajtása érdekében azt az akciótervet, amely felépítésére a fentiekben javaslatot tettem.

3.5 A nemzeti kiberbiztonsági stratégia végrehajtása hatékonyságának mérésére szolgáló indikátor-rendszer elvi alapjaira tett javaslatom

Az eddigi kutatásaim eredményeinek összefoglalása révén jelen dolgozatban megfogalmazott javaslatok, amelyeket a nemzeti kiberbiztonsági stratégia elvi alapjaira és annak életciklusára, valamint a stratégia végrehajtása érdekében javasolt akciótervre tettem hozzájárulnak egy ország kiberbiztonsági szintjének emeléséhez. Azonban ennek a biztonsági szintnek az emelkedését (változását) szükséges folyamatosan figyelemmel kísérni és mérni, ahogy azt az általam javasolt kiberbiztonsági stratégia életciklusának 4. fázisa is tartalmazza. Ehhez a méréshez szükség van egy indikátor-rendszerre, amely a különböző célok eléréséhez rendelt feladatok hatékonyságát különböző mutatók (indikátorok) segítségével értékeli. A nemzeti kiberbiztonsági stratégia célja nyilvánvalóan a

kiberbiztonság, így a nemzeti biztonság emelése és annak növelése. Ugyanakkor sok esetben ennek egyes területein bekövetkezett változások jelenleg csak becsléssel, vagy rosszabb esetben szubjektív véleménnyel ítélhetők meg.

Mindezek alapján javaslatot teszek a nemzeti kiberbiztonsági stratégia végrehajtása hatékonyságának mérésére szolgáló indikátor-rendszer elvi alapjaira, amely a következő fő célterületeket foglalja magába[115]:

- a nemzeti kiberbiztonsági stratégia felülvizsgálata:
  - megtörtént-e;
  - van-e ehhez központi koordináló szervezet hozzárendelve és ehhez tartozik-e meghatározott eljárásrend;
  - stratégiai célok építenek-e a nemzeti biztonsági stratégia céljaira;
  - akcióterv hozzárendelésre került-e (célok, részcélok, felelősök, határidők);
  - nemzetközi követelmények beépítésre kerültek-e;
- a kiberbiztonság szervezeti háttere és annak képességei:
  - korai kiberveszély előrejelzést és elemzést végző szervezet és/vagy képesség megvan-e;
  - központi incidenskezelési szervezet megléte;
  - ágazati incidenskezelő szervezetek megléte;
  - az incidens kezelés átlagos ideje;
  - együttműködés hatékonysága: például az ágazati szinten bejelentett központi incidenskezelést igénylő esetekben ez mennyire valósul meg;
- kibertéri kockázatok és veszélyek felmérése:
  - nemzeti kockázatelemzési metódus megléte;
  - a nem kezelt súlyos kockázatok aránya;
- kritikus infrastruktúra védelem feladatai:
  - központi incidenskezelés megvalósul-e;
  - ágazati incidenskezelő szervezetek kialakultak-e;

[115] Az ezekhez a célterületekhez történő indikátorok meghatározása jelen értekezésben csak általánosan – modell értékűen – történhet meg. Ennek oka az, hogy még az európai országok is nagyon eltérő szinten vannak a digitális társadalom és gazdaság, valamint az ezekkel a tényezőkkel szorosan összefüggő kiberbiztonság területén. (Erre utalnak és ezt bizonyítják az 1. fejezetben bemutatott adatsorok, illetve az azokból levont következtetéseim is). Mindezeknek megfelelően a konkrét, az adott országra vonatkozó indikátorok meghatározását a kormányzat ambíciószintjének megfelelően, az érdekelt felek bevonásával a kiberbiztonságért felelős kormányzati szervnek vagy hatóságnak kell elvégeznie.

  - információs rendszer (sérülékenységekre figyelmeztető, tudatosító) működik-e;
  - az EU CIWIN hálózatban résztvevő kritikus infrastruktúra elemek száma;
  - sérülékenységek számának változása;
  - incidensek számának változása;
  - kritikus infrastruktúra IKT rendszereinek kiberbiztonsági megfelelőségi aránya;
- kiberbűnözés:
  - van-e a kiberbűncselekmények nyilvántartására központi adatbázis;
  - kiberbűncselekmények száma, illetve azok számának és/vagy súlyosságának változása;
  - jogi eljárás alá vont kiberbűncselekmények száma;
  - a kiberbűncselekményekkel szakmailag foglalkozó rendőri erők létszáma;
  - a kiberbűncselekményekkel szakmailag foglalkozó rendőri erők szakmai továbbképzéseinek száma;
  - a kiberbűncselekményekkel szakmailag foglalkozó bírók és ügyészek szakmai továbbképzéseinek száma;
- a hadsereg kiberműveleti kompetenciái:
  - a hadsereg kiberműveleti képességeihez szükséges szakemberek számának változása, beleértve az incidenskezeléshez, valamint a kibertámadó képességekhez szükséges szakembereket is;
  - a hadsereg kibertámadó képességeinek változása;
  - a hadsereg információs és vezetési rendszereit ért súlyos incidensek számának változása;
- kiberbiztonsági gyakorlatok:
  - hazai kiberbiztonsági gyakorlatok száma;
  - nemzetközi kiberbiztonsági gyakorlatok száma;
  - kiberbiztonsági versenyek száma;
- oktatás-képzés, tudatosítás:
  - a társadalom azon aránya, aki szerint biztonságos az IKT eszközök használata;
  - új, egyetemi szintű képzések száma;
  - új, a közoktatásba bevont kiberbiztonsági ismeretkörök száma;

  - továbbképzések száma a közigazgatás szereplői számára;
  - tudatosító kampányok száma;
- K+F tevékenység:
  - új, az IKT szektor biztonságával foglalkozó KKV-k száma;
  - elnyert nemzetközi források száma és összege;
  - hazai ösztönzőrendszer megléte és annak hatékonysága;
  - a közigazgatási IKT rendszerek fejlesztése során a kiberbiztonsági elemek megjelenése;
- nemzetközi együttműködés:
  - új bilaterális együttműködések száma;
  - új multilaterális együttműködések száma;
  - nemzetközi kiberbiztonsági fórumokban való részvétel.

Az általam javasolt nemzeti kiberbiztonsági stratégia végrehajtása hatékonyságának mérésére szolgáló indikátor-rendszer és annak mutatói

Fő cél	**Cél elérése érdekében meghatározott feladat**	**Indikátor**	**Meglévő érték**	**Elvárt érték**
			kiinduló év	+három év
1. A nemzeti kiberbiztonsági stratégia felülvizsgálata				
	1.1. Megtörtént-e a nemzeti kiberbiztonsági stratégia felülvizsgálata?	Igen/Nem	igen	igen
	1.2. Van-e ehhez központi koordináló szervezet kinevezve és ehhez tartozik-e meghatározott eljárásrend?	Igen/Nem	nem	igen
	1.3. A nemzeti kiberbiztonsági stratégia épít-e a nemzeti biztonsági stratégiára? (Vannak-e a nemzeti biztonsági stratégia által megfogalmazott stratégiai célok között a kiberbiztonságra vonatkozó célok, ha igen, azok megjelennek-e a kiberbiztonsági stratégiában?	Igen/Nem	nem	igen

	1.4. Készült-e akcióterv a nemzeti kiberbiztonsági stratégia végrehajtásához?	Igen/Nem	nem	igen
	1.5. Nemzetközi követelmények beépítésre kerültek-e a stratégiába (pl. NIS direktíva)?	Igen/Nem	nem	igen
2. A kiberbiztonság szervezeti háttere és annak képességei fejlesztése				
	2.1. Korai kiberveszély előrejelzést és elemzést végző szervezet és/vagy képesség van-e?	Igen/Nem	nem	igen
	2.2. Központi incidenskezelési szervezet megléte?	Igen/Nem	nem	igen
	2.3. Ágazati incidenskezelő szervezetek megléte?	Igen/Nem/Részben	nem/ részben	igen
	2.4. Az incidens kezelés átlagos ideje?	Óra	jelenleg szükséges idő	a korábbinál rövidebb idő
	2.5. Együttműködés hatékonysága: pl. ágazati szinten bejelentett központi incidenskezelést igénylő esetek?	Darab	jelenleg bejelentett incidensek száma	bejelentett incidensek számának növekedése

3. Kibertéri kockázatok és veszélyek felmérésének fejlesztése				
	3.1. Nemzeti kockázatelemzési metódus megléte?	Igen/Nem	nem	igen
	3.2. A nem kezelt súlyos kockázatok aránya?	Összes súlyos kockázat %-os értéke	70%	40%
4. A kritikus infrastruktúra védelem javítása				
	4.1. Központi incidenskezelés megvalósul-e?	Igen/Nem	nem	igen
	4.2. Ágazati incidenskezelő szervezetek kialakultak-e?	Igen/Nem/Részben	nem/ részben	igen
	4.3. Információs rendszer (sérülékenységekre figyelmeztető, tudatosító) működik-e?	Igen/Nem/Részben	nem/ részben	igen
	4.4. EU CIWIN hálózatban résztvevő kritikus infrastruktúra elemek aránya a teljes (azonosított és kijelölt) kritikus infrastruktúra számhoz viszonyítva?	%	50%	90%

	4.5. Felismert sérülékenységek számának változása?	%	jelenleg felismert sérülékenységek (100%)	150 %
	4.6. Bekövetkezett, felismert és kezelt incidensek számának változása?	%	jelenleg bekövetkezett, felismert és kezelt sérülékenységek (100%)	75%
	4.7. Kritikus infrastruktúra IKT rendszereinek kiberbiztonsági megfelelőségi aránya?	%	50%	100%
5. Kiberbűnözés visszaszorítása				
	5.1. Kiberbűncselekmények központi adatbázisa?	Igen/Nem	nem	igen
	5.2. Kiberbűncselekmények számának változása?	%	jelenlegi kiberbűncselekmények száma (100%)	-40%
	5.3. Jogi eljárás alá vont kiberbűncselekmények számának változása?	%	jelenleg jogi eljárás alá vont kiberbűncselekmények száma (100%)	60%

	5.4. A kiberbűncselekményekkel szakmailag foglalkozó rendőri erők létszámának változása?	%	jelenlegi erők száma (100%)	140%
	5.5. A kiberbűncselekményekkel szakmailag foglalkozó rendőri erők szakmai továbbképzéseinek száma?	%	jelenlegi továbbképzések száma (100%)	130%
	5.6. A kiberbűncselekményekkel szakmailag foglalkozó bírók és ügyészek szakmai továbbképzéseinek száma?	%	jelenlegi bírók és ügyészek száma (100%)	140%
6. A hadsereg kiberműveleti kompetenciái				
	6.1. A hadsereg kiberműveleti képességeihez szükséges szakemberek számának változása, beleértve az incidenskezeléshez, valamint a kibertámadó képességekhez szükséges szakembereket?	%	jelenlegi szakemberek száma (100%)	140%
	6.2. A hadsereg kibertámadó képességeinek változása?	%	jelenlegi képességek (100%)	140%
	6.3. A hadsereg információs és vezetési rendszereit ért súlyos incidensek számának változása?	%	jelenlegi incidensek száma (100%)	-50%

7. Kiberbiztonsági gyakorlatok növelése				
	7.1. Hazai kiberbiztonsági gyakorlatok száma?	darab	jelenlegi gyakorlatok száma (X)	4X
	7.2. Nemzetközi kiberbiztonsági gyakorlatok száma?	darab	jelenlegi gyakorlatok száma (X)	2X
	7.3. Kiberbiztonsági versenyek száma?	darab	jelenlegi versenyek száma (X)	5X
8. Oktatás-képzés, tudatosítás növelése				
	8.1. A társadalom azon aránya, aki szerint biztonságos az IKT eszközök használata?	%	40%	75%
	8.2. Új egyetemi szintű képzések száma?	darab	jelenlegi képzések száma (X)	5X
	8.3. Új, a közoktatásba bevont kiberbiztonsági ismeretkörök száma?	darab	jelenlegi ismeretkörök száma (X)	15X
	8.4. Továbbképzések száma a közigazgatás szereplői számára?	darab	jelenlegi továbbképzések száma (X)	3X

	8.5. Tudatosító kampányok száma?	darab	jelenlegi kampányok száma (X)	5X
9. K+F tevékenység növelése				
	9.1. Új KKV-k száma?	trend	-	növekedés
	9.2. Elnyert nemzetközi források száma és mértéke?	trend	-	növekedés
	9.3. Hazai ösztönzőrendszer és megoldások száma?	trend	-	növekedés
	9.4. A közigazgatási IKT rendszerek fejlesztése során kiberbiztonsági elemek megjelenése?	Igen/Nem/Részben	nem/részben	igen
10. Nemzetközi együttműködés fokozása				
	10.1. Bilaterális együttműködések száma?	darab	jelenlegi együttműködések száma (X)	5X
	10.2. Multilaterális együttműködések száma?	darab	jelenlegi együttműködések száma (X)	2X

	10.3. Nemzetközi kiberbiztonsági fórumokban való részvétel?	Igen/Nem	nem	igen

ÖSSZEGZETT KÖVETKEZTETÉSEK

Kutatómunkám során kiberbiztonság különböző területeit vizsgáltam. Jelen dolgozatban a korábbi kutatási eredményeimet szintetizáltam és tettem megállapításokat a területtel kapcsolatosan. Az első ilyen fontos megállapítás az, hogy a digitális technológia innovációja, az IKT eszközök és rendszerek elterjedése azt eredményezték, hogy a társadalom egyre nagyobb igényt támaszt az új digitális eszközök és szolgáltatások zavartalan működésére. Mindezek azt is jelentik, hogy napjainkra egyre több országban alakul ki a digitális ökoszisztéma.

Azonban ennek a digitális ökoszisztémának a biztonsága alapvető fontosságú a társadalmi funkciók zavartalan ellátásához. Ebben a biztonságban kiemelt helyet kell, hogy kapjon azoknak az infrastruktúráknak a védelme, amelyeken keresztül a digitális ökoszisztéma megvalósul és az abban lévő szolgáltatások működnek.

A digitális technológia ennek megfelelően komoly hatással volt a társadalomra és át is alakította azt. A digitális technika és technológia hatásának mérése több módszerrel történhet, de ezek csak közvetett módon lehetnek alkalmasak a kiberbiztonság szintjének bemutatására.

A kibertérben jelentkező stratégiai kihívások számbavételekor megállapítottam, hogy számos olyan új veszély jelentkezett az elmúlt fél évtized során, amelyek az állami támogatású kibertámadásokban összegezhetők. Az olyan, már-már klasszikusnak mondható kibertéri veszélyek, mint a kiberbűnözés, a hacktivizmus vagy a kiberkémkedés mellett kialakult és rendszeressé vált a kibertérben folytatott politikai és gazdasági befolyásolás, valamint a kiberhadviselés. Mindezek stratégiai szintű védelmi megoldásokat kívánnak nemzeti és szövetségi szinten egyaránt. A védelem egyik megoldásaként azonosítottam a kiberelrettentést.

A nemzeti biztonsági stratégia és a nemzeti kiberbiztonsági stratégia összefüggéseinek elemzése során megállapítottam, hogy a nemzeti biztonsági stratégia legfontosabb célkitűzései megvalósítása érdekében a kiberbiztonság ma már az egyik legfontosabb tényező.

Kutatómunkám során megvizsgáltam három nagyhatalom – Kína, Oroszország és az Amerikai Egyesült Államok – nemzeti szintű biztonsági, katonai és kiber stratégiáit. Ezek alapján megállapítottam, hogy mind a három nagyhatlom eltérő módon közelíti meg a kiberteret. Ugyanakkor az elvégzett elemzéseim alapján azt a következtetést vonom le, hogy a nagyhatalmak is a nemzeti biztonságuk alapvető összetevőjeként tekintenek a kibertérre és

annak biztonságára. Mindezeken túl a kibertérben folytatott információszerző, befolyásoló és támadó tevékenységükkel, illetve e tevékenységekkel kapcsolatos képességeikkel a nemzetközi biztonsági, gazdasági és politikai viszonyrendszerben is számítanak.

Az egyes európai országok kiberbiztonsági stratégiái elemzése során megállapítottam, hogy bár ezek az országok is eltérő módon közelítik meg a kibertér biztonságát, de annak stratégiai megközelítésében számos olyan elem azonosítható, amelyek nagyban hasonlítanak egymásra. Megállapítottam, hogy ezek az azonos elemek, függően azok szerepétől és azok hatékonyságától alapjai lehetnek egy nemzeti kiberbiztonsági stratégia modelljének. Ennek alapján, felhasználva a közös elemek vonatkozásában tett megállapításaimat, valamint a vizsgált országok kiberbiztonsági tevékenysége során feltárt hatékony és valóban működő elemeket, javaslatot tettem a nemzeti kiberbiztonsági stratégia összetevőire, legfontosabb elemeire, valamint a stratégia életciklusára.

A nemzeti kiberbiztonsági stratégia azonban csak különböző – jól definiált – tevékenységek és feladatok során valósítható meg. Ennek érdekében – kiindulva a korábbi megállapításaimból és javaslataimból – kidolgoztam és javaslatot tettem egy akciótervre. Az akcióterv olyan elemeket tartalmaz, amely konkrét feladatokat, a feladatokhoz meghatározott felelős szervezeteket és nem utolsó sorban határidőket tartalmaz.

Az akcióterv a korábban ismertetett életciklus egyik fontos, de nem elégséges eleme. A konkrét feladatok hatékonyságát, majd ezek összesített eredményét szükséges mérni ahhoz, hogy a kiberbiztonsági stratégia céljainak megvalósulására visszaigazolást nyerjünk, vagy szükség esetén korrekciós döntést lehessen hozni. Ennek megfelelően kidolgoztam egy, a kiberbiztonsági stratégia hatékonyságának mérését lehetővé tevő indikátor-rendszert. Az ebben foglalt mutatók (indikátorok) közvetlenül az adott ország kiberbiztonsági helyzetét mutatják, ugyanakkor közvetett módon alkalmasak a nemzeti kiberbiztonsági stratégia egyes elemeinek – az abban foglalt célok elérése hatékonyságának – mérésére.

TUDOMÁNYOS EREDMÉNYEK

A korábbi kutatásaimra, valamint jelen dolgozatban megfogalmazott szintetizált következtetésekre építve a következő tudományos eredményekkel, valamint az azokban megfogalmazott javaslatokkal kívánok a kiberbiztonság stratégiai szintű növeléséhez hozzájárulni:

1. A kutatómunkám során elemzett nemzeti kiberbiztonsági stratégiák és politikák alapján **kidolgoztam** és javaslatot tettem egy általános érvényű **nemzeti kiberbiztonsági stratégia modelljére.** Ezen belül **azonosítottam azokat a tartalmi elemeket**, amelyek egy hatékony nemzeti **kiberbiztonsági stratégia kialakítása során szükségesek**.

2. **Kidolgoztam** és javaslatot tettem a **nemzeti kiberbiztonsági stratégia életciklusára**.

3. **Kidolgoztam** és javaslatot tettem a nemzeti kiberbiztonsági stratégia végrehajtása érdekében szükséges **akcióterv tartalmi elemeire**.

4. **Kidolgoztam** és javaslatot tettem a nemzeti kiberbiztonsági stratégia végrehajtása hatékonyságának mérésére szolgáló **indikátor-rendszerre és annak mutatóira**.

RÖVIDÍTÉSEK JEGYZÉKE

Rövidítés	Idegen nyelvű kifejtés	Magyar nyelvű kifejtés
AFCYBER	Air Force Cyber Command	Légierő Kiberparancsnoksága
ANSSI	Agence nationale de la sécurité des systèmes d'information	Nemzeti Információbiztonsági Ügynökség
APCIP	Programm zum Schutz kritischer Infrastrukturen	Kritikus infrastruktúra védelmi terv
APT	Advanced Persistent Threat	Célzott, folyamatosan fennálló, fejlett támadás
ARCYBER	Army Cyber Command	Hadsereg Kiberparancsnoksága
ASP	Application Service Provider	Alkalmazásszolgáltatási modell
BBC	British Broadcasting Corporation	Brit közszolgálati műsorszolgáltató
BCP	Business Continuity Plan	Üzletmenetfolytonossági terv
BM		Belügyminisztérium
BS	British Standard	Brit szabvány

BSI	Bundesamt für Sicherheit in der Informationstechnik	Szövetségi Információs Biztonsági Hivatal
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik	Törvény a Szövetségi Információs Biztonsági Hivatalról
C2	Command & Control	Vezetés és irányítás
C4	Cyber Crime Competence Center	Kiberbűnözés kompetencia központ
C4I	Command, Control, Communication, Computer, Intelligence	Katonai információs rendszer
CCA	Centre for Cyber Assessment	Nemzeti Kiberbiztonsági Elemző Központ
CCDCoE	Co-opreative Cyber Defence Centre of Exellence	Kiberbiztonsági Kiválósági Központ (NATO)
CEPOL	European Union Agency for Law Enforcement Training	Európai Rendőrakadémia
CERT	Computer Emergency Response Team	Számítógép-vészhelyzeti reagáló csoport
CERT.LV	Computer Emergency Response Team Latvia	Lett számítógép-vészhelyzeti reagáló csoport
CERT-UK	UK's Computer Emergency Response Team	Egyesült Királyság CERT-je
CESG	Communications-Electronic Security Group	Kommunikációs és elektronikai biztonsági csoport

CGCYBER	Coast Guard Cyber Command	Partiőrség Kiberparancsnoksága
CIA	Confidentiality, Integrity, Availability	Bizalmasság, sértetlenség, rendelkezésre állás
CIA	Central Intelligence Agency	Központi Hírszerző Ügynökség
CIP	Critical Infrastructure Protection	Kritikusinfrastruktúra-védelem
CIS	Communication and Information System	Kommunikációs és információs rendszer
CIT	Cyber Intelligence Team	Kiberfelderítési csoport
CIWIN	Critical Infrastructure Warning Information Network	Kritikus infrastruktúrákra figyelmeztető információ hálózata
CMF	Cyber Mission Force	Kiberműveleti csoport
CNA	Center for Naval Analyses	Haditengerészeti Kutatások Központja
CNDSP	Computer Network Defense Service Provider	Védelmi Minisztérium számítógép-hálózat védelmi szolgáltatója
CNN	Cable News Network	Amerikai kábeltelevízió és hírszolgáltató
CNO	Computer Network Operations	Számítógép-hálózati műveletek

CPNI	Centre for the Protection of National Infrastructure	Nemzeti Infrastruktúra Védelmi Központ
CPT	Cyber Protection Team	Kibervédelmi Csoport
CSDP	Common Security and Defence Policy	Közös európai biztonság- és védelempolitika
CSIRT	Computer Security Incident Response Team	Számítógép-biztonsági incidenskezelő csoport
DDoS	Distributed Denial of Service	Elosztott túlterheléses támadás
DHS	Department of Homeland Security	Belbiztonsági Minisztérium
DJP		Digitális Jóléti Program
DNS	Domain Name Service	Domainnév-szolgáltatás
DoD	Department of Defense	Védelmi Minisztérium (USA)
DoDIN	DoD information network	Védelmi Minisztérium információs hálózata
DoS	Denial of Service	Túlterheléses támadás
DRP	Disaster Recovery Plan	Katasztrófavédelmi terv

DTC	Digital Trust Center	Digitális Megbízhatósági Központ
EBESZ		Európai Biztonsági és Együttműködési Szervezet
EC3	European Cybercrime Centre	Európai kiberbűnözés elleni központ
ECI	European Critical Infrastructures	Európai kritikus infrastruktúrák
ECOSEC	Economic and Social Council	ENSZ Gazdasági és Szociális Tanácsa
EDA	European Defence Agency	Európai Védelmi Ügynökség
EEAS	European External Action Service	Európai Külügyi szolgálat
EECSP	Energy Expert Cyber Security Platform	Energiaipari kiberszakértői platform
EFTA	European Free Trade Association	Európai Szabadkereskedelmi Társulás
EK		Európai Közösség
EMPACT	European Multidisciplinary Platform Against Criminal Threats	Európai multidiszciplináris platform a bűncselekmények fenyegetettsége ellen

ENISA	European Union Agency for Network and Information Security	Európai Hálózat- és Információbiztonsági Ügynökség
ENSZ		Egyesült Nemzetek Szervezete
EP3R	European Public-Private Partnership for Resilience	Európai köz- és magánszféra együttműködés az ellenállóképességért
EPCIP	European Programme for Critical Infrastructure Protection	Kritikusinfrastruktúra-védelem Európai Programja
EU	European Union	Európai Unió
EWI	EastWest Institute	Kelet-Nyugat Intézet
FAO	Food and Agriculture Organisation	ENSZ Élelmezési és Mezőgazdasági Szervezete
FBI	Federal Bureau of Investigation	Szövetségi Nyomozó Iroda
FBS	Foreign Broadcast Information Service	CIA külföldi információs szolgálata
FLTCYBER	Fleet Cyber Command	Haditengerészet Kiberparancsnoksága
FOC	Full Operational Capability	Teljes Műveleti Képesség

FSZB	Fegyeralnaja Szluzsba Bezopasznosztyi Rosszijszkoj Fegyeracii	Szövetségi Biztonsági Szolgálat
FTP	File Transfer Protocol	Fájl átviteli protokoll
GCA	Global Cybersecurity Agenda	Globális Kiberbiztonsági Program
GCHQ	Government Communications Hedquarters	Nemzeti Kommunikációs Központ
GCI	Global Cybersecurity Index	Globális kiberbiztonsági index
GCSC	Global Commission on the Stability of Cyberspace	Globális Bizottság a Kibertér Stabilitásáért
GDP	Gross Domestic Product	Nemzeti össztermék
GDPR	General Data Protection Regulation	Általános adatvédelmi rendelet
GovCERT	Government Computer Emergency Response Team	Kormányzati eseménykezelő csoport
HÁEIEK		Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ
HCSS	The Hague Centre for Strategic Studies	Hágai Stratégiai Tanulmányok Központ

HM		Honvédelmi Minisztérium
HTML	HyperText Markup Language	Hiperszöveges jelölőnyelv
HTTP	HyperText Protocol	Hyperszöveg protokoll
Ibtv.		Információbiztonsági törvény (2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról)
ICANN	Internet Corporation for Assigned Names and Numbers	Internet Név és IP cím kezelő szervezet
ICO	Information Commissioner's Office	Információs jogokkal foglalkozó iroda
ICT	Infocommunication Technology	Infokommunikációs technológia
ICS	Industrial Command System	Ipari vezérlőrendszer
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team	Ipari Irányító Rendszerek Kiber Vészhelyzeti Reagáló Csoport
IDS	Intrusion Detection System	Behatolásdetektáló rendszer
IEC	International Electrotechnical Commission	Nemzetközi Elektrotechnikai Tanács

IG	Internet Governance	Internet irányítás
IGF	Internet Governance Forum	Internet Irányítás Fórum
IKT		Infokommunikációs technológia
ILO	International Labour Organisation	Nemzetközi Munkaügyi Szervezet
IOCTA	Internet Organised Crime Threat Assessment	Internetes szervezett bűnözéssel kapcsolatos fenyegetésértékelés
IoT	Internet of Things	A dolgok internete
IoT-GSI	Global Standards Initiative on Internet of Things	A dolgok internetének globális szabványa
IP	Internet Protokol	Internetprotokoll
ITU	International Telecommunication Union	Nemzetközi Telekommunikációs Szervezet
ITU-D	ITU Development Sector	A Nemzetközi Telekommunikációs Szervezet fejlesztésekért felelős ágazata
ITU-R	ITU Radiocommunication Sector	A Nemzetközi Telekommunikációs Szervezet

ITU-T	Telecommunication Standardisation Sector	A Nemzetközi Telekommunikációs Szervezet telekommunikáció egységesítésért és szabványosításért felelős ágazata
IXP	Internet Exchange Point	Internet csatlakozási pont
J-CAT	Joint Cybercrime Action Taskforce	Egyesített kiberbűnözés elleni akciócsoport
K+F		Kutatás-fejlesztés
KB		Központi Bizottság
KKP		Kínai Kommunista Párt
KKV		Kis- és közepes vállalkozások
KNBSZ		Katonai Nemzetbiztonsági Szolgálat
KÖFOP		Közigazgatás- és Közszolgáltatás-fejlesztési Program
KPI	Key Performance Indicator	Fő teljesítménymutató rendszer

KSH		Központi Statisztikai Hivatal
LOIC	Low Orbit Ion Cannon	Alacsony Orbitális Ionágyú
LRLIBEK		Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja
MARFORCYBER	Marine Forces Cyber Command	Tengerészgyalogság Kiberparancsnoksága
MI		Mesterséges intelligencia
milCERT	Military Computer Emergency Response Team	Katonai számítógépes vészhelyzeti reagáló csoport
MiLCERT	Military Cyber Emergency Readiness Team	Katonai kibervészhelyzeti készenléti csoport
MIRT	Mobile Incident Response Team	Mobil incidenskezelő csoport
NASA	National Aeronautics and Space Administration	Nemzeti Repülési és Űrhajózási Hivatal
NATO	North Atlantic Treaty Organisation	Észak-atlanti Szerződés Szervezete
NBF		Nemzeti Biztonsági Felügyelet

NBSZ		Nemzetbiztonsági Szakszolgálat
NCCIC	National Cybersecurity and Communications Integration Center	Nemzeti Kiberbiztonsági és Kommunikáció Integrációs Központ
NCIRC	NATO Cyber Incident Response Capability	NATO kiberincidensreagáló képesség
NCSC	National Cyber Security Centre	Nemzeti Kiberbiztonsági Központ
NCP	National Cybercontingency Plan	Nemzeti kiberkészenléti terv
NCU	National Cyber Crime Unit	Nemzeti Kiberbűnözés Elleni Egység
NEGS	Nationalen E-Government-Strategie	Nemzeti e-Kormányzati Stratégia
NEIH		Nemzeti Elektronikus Információbiztonsági Hatóság
NHS	National Health Service	Nemzeti Egészségügyi Szolgálat (UK)
NIS	Network and Information System	Hálózati és információs rendszer
NKI		Nemzeti Kibervédelmi Intézet
NOCP	National Offensive Cyber Programme	Nemzeti Kiber Támadási Program

NSA	National Security Agency	Nemzetbiztonsági Ügynökség
OECD	Organisation for Economic Co-operation and Development	Gazdasági Együttműködési és Fejlesztési Szervezet
OKF		Országos Katasztrófavédelmi Főigazgatóság
PDCA	Plan-Do-Check-Act	Tervezés-cselekvés-ellenőrzés-beavatkozás
PLA	People's Liberation Army	Kína Népi Felszabadítási Hadsereg
PLC	Programmable Logic Controller	Programozható kontroller
POP3	Post Office Protocol version 3	Levelező protokoll 3-as verzió
PPP	Public Private Partnership	Köz- és a magánszféra közötti partnerség
PSSIE	Politique de sécurité des systèmes d'information	Nemzeti Információs Rendszerek Biztonsági Politikája
RFID	Radio Frequency Identification	Rádiófrekvenciás azonosítás
RIA	Riigi Infosüsteemi Amet, RIA	Észt Információs Rendszer Hatóság
RNC	Republican National Committe	Republikánus Nemzeti (Választási) Tanács

RPOC	Rządowy Program Ochrony Cyberprzestrzeni	Kormányzati kiberbiztonsági cselekvési terv
RSA	Rivest–Shamir–Adleman	Aszimmetrikus titkosító algoritmus (megalkotók neveinek kezdőbetűiből alkotott rövidítés)
RTU	Remote Terminal Unit	Távoli elérést biztosító terminálóknak
SCADA	Supervisory Control and Data Acquisition	Felügyeleti, irányító és adatgyűjtő
SCO	Shanghai Cooperation Organisation	Sanghaji Együttműködési szervezet
SGDSN	Secrétaire général de la défense et de la sécurité nationale	Védelmi Minisztérium
SHAPE	Supreme Headquarters Allied Powers Europe	Szövetséges Erők Európai Főparancsoksága
SIGINT	Signals Intelligence	Rádióelektronikai felderítés
SMB	Server Message Block	Szerver üzenet blokk (alkalmazásréteg protokoll)
STEM	Science, Technology, Engineering and Mathematics	Műszaki tudományok és matematika
SZTAKI		Számítástechnikai Automatizálási Kutatóintézet

SZVR	Szluzsba Vnyesnyej Razvedki	Külső Hírszerző Szolgálat
TLD	Top Level Domain	Felső szintű tartomány
UN GGE	United Nations Group of Governmental Experts	ENSZ Kormányzati Szakértői Csoport
UK	United Kingdom	Egyesült Királyság
URL	Uniform Resource Locator	Egységes erőforráshely
US GAO	United States Government Accountability Office	Egyesült Államok Kormányzati Elszámoltatási Hivatala
US-CERT	United States Computer Emergency Readiness Team	Egyesült Államok Számítógép Vészhelyzeti Reagáló Csoport
USCYBERCOM	United States Cyber Command	Egyesült Államok Kiberparancsnoksága
USCYCOM	United States Cyber Command	Egyesült Államok Kiberparancsnoksága
USSTRATCOM	US Strategic Command	Egyesült Államok Stratégiai Parancsnoksága
V4	Visegrad Four	Visegrádi négyek

ZITiS	Zentral Stelle für Informationstechnik im Sicherheitsbereich	Biztonsági szektor információtechnológiai központja

ILLUSZTRÁCIÓK JEGYZÉKE

1. ÁBRA *AZ EURÓPAI UNIÓ ORSZÁGAINAK DESI INDEXE 2018-BAN* 30

2. ÁBRA *AZ ITU GCI INDEXÉNEK MÉRŐSZÁM-CSOPORTJAI* 34

3. ÁBRA *A KIBERTÉRBEN MEGJELENŐ KIHÍVÁSOK ÉS VESZÉLYEK HATÁS ÉS KÖVETKEZMÉNY SZERINTI INTERPRETÁLÁSA* 38

4. ÁBRA *A STRATÉGIAI DOKUMENTUMOK RENDSZERE* 56

5. ÁBRA *AZ USA LEGFONTOSABB STRATÉGIAI DOKUMENTUMAINAK RENDSZERE* 57

6. ÁBRA *A NEMZETI KIBERVÉDELMI INTÉZET PILLÉREI ÉS KAPCSOLÓDÁSAI* 148

7. ÁBRA *A 2015-ÓTA MŰKÖDŐ HAZAI ÁLLAMI KIBERVÉDELMI SZERVEZETEK* 149

8. ÁBRA *A SZLOVÁK KIBERBIZTONSÁGI SZEREZETEK KAPCSOLATAI* 162

9. ÁBRA *A NEMZETI KIBERBIZTONSÁGI STRATÉGIA ÁLTALAM JAVASOLT MODELLJÉHEZ SZÜKSÉGES VÉGREHAJTÁSI CIKLUS* 201

10. ÁBRA *A NEMZETI KIBERBIZTONSÁGI STRATÉGIÁHOZ KAPCSOLÓDÓ AKCIÓTERV FOLYAMATA* 214

TÁBLÁZATOK JEGYZÉKE

1. TÁBLÁZAT *A HAZAI KRITIKUS INFRASTRUKTÚRA ÁGAZATOK ÉS ALÁGAZATOK* 20

2. TÁBLÁZAT *A NIS-DIREKTÍVA ÁLTAL MEGHATÁROZOTT ALAPVETŐ SZOLGÁLTATÁSOKAT NYÚJTÓ SZEREPLŐK* 24

3. TÁBLÁZAT *A VILÁG INTERNETPENETRÁCIÓJA* 26

4. TÁBLÁZAT *MAGYARORSZÁG DESI INDEXE 2017-BEN ÉS 2018-BAN* 30

5. TÁBLÁZAT *MAGYARORSZÁG DESI INDEXE INDIKÁTORCSOPORTONKÉNT 2018-BAN* 31

6. TÁBLÁZAT *AZ EGYESÜLT ÁLLAMOK KIBERBIZTONSÁGRA ÉS KRITIKUS INFRASTRUKTÚRÁKRA VONATKOZÓ FONTOSABB STRATÉGIÁI ÉS TÖRVÉNYEI 2000-2018*..... 63

7. TÁBLÁZAT *AZ EGYESÜLT ÁLLAMOK VÉDELMI MINISZTÉRIUMÁNAK KIBERSTRATÉGIÁJÁNAK STRATÉGIAI CÉLJAI ÉS AZ AZOKAT TÁMOGATÓ TEVÉKENYSÉGEK* 66

8. TÁBLÁZAT *AZ ITU NEMZETI KIBERBIZTONSÁGI PROGRAM ELEMEIRE VONATKOZÓ AJÁNLÁSÁNAK ÖSSZEFOGLALÁSA*..... 185

9. TÁBLÁZAT *AZ ÁLTALAM JAVASOLT NEMZETI KIBERBIZTONSÁGI STRATÉGIA MODELLJÉNEK EGYES SZAKASZAIHOZ TARTOZÓ TEVÉKENYSÉGEK* 202

IRODALOMJEGYZÉK

1035/2012. (II.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

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

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2015. évi CXXX. törvény az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról

2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programról

223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

A Kormány 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról

Annan, Kofi (2018): *Has information technology become a threat to democracy? Forrás*: http://www.kofiannanfoundation.org/supporting-democracy-and-elections-with-integrity/msc-technology-democracy/ (Letöltés ideje: 2018. 10. 11.)

ANSSI (2018): *Our Audiences and Our Activities*. Forrás: https://www.ssi.gouv.fr/en/mission/audiences-and-activities/ (Letöltés ideje: 2018. 10. 11.)

Ausztria (2013a): *Österreichische Sicherheitsstrategie Sicherheit in einer neuen Dekade – Sicherheit gestalten.* Forrás: https://www.bmi.gv.at/502/files/130717_Sicherheitsstrategie_Kern_A4_WEB_barrierefrei.pdf (Letöltés ideje: 2018. 10. 11.)

Ausztria (2013b): *Austrian Security Strategy Security in a New Decade—Shaping Security.* Forrás: http://www.bundesheer.at/pdf_pool/publikationen/sicherheitsstrategie_engl.pdf (Letöltés ideje: 2018. 10. 11.)

Ausztria (2013c): *Österreichische Strategie für Cyber Sicherheit*. Forrás: https://www.bmi.gv.at/504/files/130416_strategie_cybersicherheit_WEB.pdf (Letöltés ideje: 2018. 10. 11.)

Ausztria (2013d): *Austrian Cyber Security Strategy*. Forrás: https://www.digitales.oesterreich.gv.at/documents/22124/30428/AustrianCyberSecurityStrategy.pdf/35f1c891-ca99-4185-9c8b-422cae8c8f21 (Letöltés ideje: 2018. 10. 11.)

Bencsik Balázs (2015): *GovCERT-Hungary bemutatása*. Előadás, Budapest, Nemzeti Kibervédelmi Intézet.

Biztonságpolitikai Szakkollégium (2010): *NATO stratégiai koncepciója 2010 a Biztonságpolitikai szakkollégium fordításában*. Forrás: http://www.biztonsagpolitika.hu/documents/1291766875_NATO_Strat_Koncepcio_2010_hun_BSZK.pdf (Letöltés ideje: 2018. 10. 11.)

BMI (2018): *Critical infrastructure protection*. Forrás: https://www.bmi.bund.de/EN/topics/civil-protection/critical-infrastructure-protection/critical-infrastructure-protection-node.html (Letöltés ideje: 2018. 06. 11.)

Brown, Gary D.–Metcalf, Andrew O. (2014): *Easier Said Than Done: Legal Reviews of Cyber Weapons.* Forrás: http://jnslp.com/wp-content/uploads/2014/02/Easier-Said-than-Done.pdf (Letöltés ideje: 2018. 10. 11.)

Brzezinski, Zbiegniew (1999): *A nagy sakktábla.* Európa.

BSI (2018a): *Organisationsübersicht des BSI.* Forrás: https://www.bsi.bund.de/DE/DasBSI/Aufgaben/aufgaben_node.html (Letöltés ideje: 2018. 10. 11.)

BSI (2018b): *Organisational Chart*. Forrás: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/org_chart_IFG_pdf.pdf?__blob=publicationFile&v=7 (Letöltés ideje: 2018. 10. 11.)

BSI-Gesetz (2009): *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG).* Forrás: https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf (Letöltés ideje: 2018. 061011.)

Burton, Joe (2018): *Cyber Deterrence: A Comprehensive Approach?* Forrás: https://ccdcoe.org/sites/default/files/multimedia/pdf/BURTON_Cyber_Deterrence_paper_April2018.pdf (Letöltés ideje: 2018. 10. 11.)

Butrimas, Vytautas (2015): *National Cyber Security Organisation: Lithuania.* CCDCOE, Tallinn. Forrás: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_LITHUANIA_092015.pdf (Letöltés ideje: 2018. 10. 11.)

Carr, Jefrrey (2011): *Inside Cyber Warfare: Mapping the Cyber Unerworld.* Sebastopol, O'Reilly Media.

Castells, Manuel (2005): *A hálózati társadalom kialakulása – Az információ kora.* I. kötet. Budapest, Gondolat–Infonia.

CCDCOE (2018): *About Us: History.* Forrás: https://ccdcoe.org/history.html (Letöltés ideje: 2018. 10. 19.)

Cellan-Jones, Rory (2014): Stephen Hawking warns artificial intelligence could end mankind. *BBC,* 2014. 12. 04. Forrás*:* www.bbc.com/news/technology-30290540 (Letöltés ideje: 2018. 10. 11.)

CERT GOV.PL (2017): *System ARAKIS-GOV*. Forrás: www.cert.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html (Letöltés ideje: 2018. 10. 11.)

Cheng, Ron (2016): China Passes Long-Awaited Cyber Security Law. *Forbes*, 2016. november 9. Forrás: https://www.forbes.com/sites/roncheng/2016/11/09/china-passes-long-awaited-cyber-security-law/#537c0c9524d2 (Letöltés ideje: 2018. 10. 12.)

China Law Translate (2015): *National Security Law.* Forrás: https://www.chinalawtranslate.com/2015nsl/?lang=en#_Toc423592311 (Letöltés ideje: 2018. 10. 11.)

CIA (2018): *The World Factbook: Central Asia: Russia.* Forrás: https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html (Letöltés ideje: 2018. 10. 11.)

Clapper, James R. (2016): *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community. Senate Armed Services Committee*. Forrás: https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf. (Letöltés ideje: 2018. 10. 11.)

Connell, Michael – Vogler, Sarah (2017): *Russia's Approach to Cyber Warfare.* CNA. Forrás: https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf (Letöltés ideje: 2018. 10. 11.)

CRC-ICS (2015): *Cyber Research Center - Industrial Control Systems*. Forrás: https://www.crc-ics.net/research.html (Letöltés ideje: 2018. 10. 05.)

Critical Foundations (1997): *Critical Foundations – Protecting Americe's Infrasctructures, The Report of the President's Commission on Critical Infrastructure Protection.* Forrás: https://www.nist.gov/sites/default/files/documents/2017/04/26/keyes_part2_032613.pdf (Letöltés ideje: 2018. 10. 11.)

Cseh Köztársaság (2015a): *Bezpečnostní strategie České republiky.* Forrás: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf (Letöltés ideje: 2018. 10. 11.)

Cseh Köztársaság (2015b): *National Security Strategy of Czech Republic.* Forrás: http://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf (Letöltés ideje: 2018. 10. 11.)

Cseh Köztársaság (2015c): *Národní strategie kybernetické bezpečnosti České republiky pro období od roku 2015 do roku 2020.* Forrás: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf (Letöltés ideje: 2018. 10. 11.)

Cseh Köztársaság (2015d): *National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020.* Forrás: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (Letöltés ideje: 2018. 10. 11.)

Cseh Köztársaság (2015e): *Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020.* Forrás: https://www.govcert.cz/download/gov-cert/container-nodeid-578/ap-cs-2015-2020-en.pdf (Letöltés ideje: 2018. 10. 29.)

Csiki Tamás (2008): A stratégiai dokumentumok rendszere. *Nemzet és Biztonság.* 2008. szeptember. Forrás: http://www.nemzetesbiztonsag.hu/cikkek/csiki_tamas-a_strategiai_dokumentumok_rendszere.pdf (Letöltés ideje: 2018. 10. 11.)

Department of Defense (2015): *The Department of Defense Cyber Strategy*. Forrás: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (Letöltés ideje: 2018. 10. 11.)

Department of Defense (2018a): *Summary of the 2018 National Defense Strategy of The United States of America – Sharpening the American Military's Competitive Edge.* Forrás: http://nssarchive.us/wp-content/uploads/2018/01/2018-National-Defense-Strategy-Summary.pdf (Letöltés ideje: 2018. 10. 11.)

Department of Defense (2018b): *The Department of Defense Cyber Strategy 2018.* Forrás: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (Letöltés ideje: 2018. 09. 21.)

Department of Homeland Security (2018a): *Cybersecurity.* Forrás: https://www.dhs.gov/topic/cybersecurity (Letöltés ideje: 2018. 10. 11.)

Department of Homeland Security (2018b): *Cyber Incident Response.* Forrás: https://www.dhs.gov/cyber-incident-response (Letöltés ideje: 2018. 10. 11.)

DHS (2009): *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*. Forrás: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf (Letöltés ideje: 2018. 10. 11.)

Digitális Megújulás Cselekvési Terv 2010–2014. DMCST (2010). Forrás: 2010-2014.kormany.hu/download/7/0d/30000/Digitalis_Megujulas_Cselekvesi_Tervull.pdf (Letöltés ideje: 2018. 11. 14.)

Egyesült Királyság (2010): *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* Forrás: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (Letöltés ideje: 2018. 10. 11.)

Egyesült Királyság (2011): *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world.* Forrás: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (Letöltés ideje: 2018. 10. 11.)

Egyesült Királyság (2015): *National Security Strategy and Strategic Defence and Security Review 2015 A Secure and Prosperous United Kingdom.* Forrás: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf (Letöltés ideje: 2018. 10. 11.)

Egyesült Királyság (2016): *National Cyber Security Strategy 2016-2021*. Forrás: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (Letöltés ideje: 2018. 10. 11.)

ENISA (2012): *National Cyber Security Strategies Practical Guide on Development and Execution*. Forrás: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport (Letöltés ideje: 2018. 10. 11.)

ENISA (2014): *An evaluation Framework for National Cyber Security Strategies.* Forrás: https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport (Letöltés ideje: 2018. 10. 11.)

ENISA (2016): *NCSS Good Practice Guide. Designing and Implementing National Cyber Security Strategies*. Forrás: https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport (Letöltés ideje: 2018. 10. 11.)

ENISA (2017a): *About Enisa.* Forrás: www.enisa.europa.eu/about-enisa (Letöltés ideje: 2018. 10. 11.)

Enisa (2017b): *Actionable Information for Security Incident Response.* Forrás: http://www.enisa.europa.eu/publications/actionable-information-for-security (Letöltés ideje: 2018. 10. 25.)

ENSZ (2013): *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* Forrás: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 (Letöltés ideje: 2018. 10. 11.)

ENSZ (2015)*: Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*. Forrás: http://repository.un.org/bitstream/handle/11176/158448/A_69_723-EN.pdf?sequence=3&isAllowed=y (Letöltés ideje: 2018. 06. 11.)

ENSZ DESA (2018): *World Urbanization Prospects, The 2018 Revisions.* Forrás: https://population.un.org/wup/Publications/Files/WUP2018-KeyFacts.pdf (Letöltés ideje: 2018. 11. 01.)

Európai Bizottság (2018a): *DESI 2018.* Forrás: https://digital-agenda-data.eu/charts/desi-composite#chart={%22indicator%22:%22DESI_SLIDERS%22,%22breakdown%22:{%22DESI_1_CONN%22:5,%22DESI_2_HC%22:5,%22DESI_3_UI%22:3,%22DESI_4_IDT%22:4,%22DESI_5_DPS%22:3},%22unit-measure%22:%22pc_DESI_SLIDERS%22,%22time-period%22:%222018%22} (Letöltés ideje: 2018. 10. 01.)

Európai Bizottság (2018b): *A digitális gazdaság és társadalom fejlettségét mérő mutató (DESI), 2018, Magyarországról szóló országjelentés.* Forrás: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=52334 (Letöltés ideje: 2018. 10. 01.)

Európai Bizottság (2018c): *The Digital Economy and Society Index (DESI). DESI 2018.* Forrás: https://ec.europa.eu/digital-single-market/en/desi (Letöltés ideje: 2018. 10. 01.)

Európai Unió Kiberbiztonsági Stratégiája (2013): *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Forrás: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (Letöltés ideje: 2018. 10. 01.)

Európa Tanács (2001): *Convention on Cybercrime.* Forrás: www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (Letöltés ideje: 2018. 10. 25.)

Európa Tanács (2017): *Chart of Signatures and Ratifications of Treaty 185.* Forrás: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (Letöltés ideje: 2018. 10. 25.)

Észtország (2010): *National Security Concept of Estonia.* Forrás: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf (Letöltés ideje: 2018. 10. 11.)

Észtország (2011): *National Defence Strategy Estonia*. Forrás: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf (Letöltés ideje: 2018. 10. 11.)

Észtország (2014a): *Küberjulgeoleku strateegia 2014-2017*. Forrás: https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf (Letöltés ideje: 2018. 10. 11.)

Észtország (2014b): *Cyber Security Strategy 2014-2017*. Forrás: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf (Letöltés ideje: 2018. 10. 11.)

Europe 2020 Strategy (2010): *Europe 2020 – A Strategy for Smart, Sustainable and Inclusive Growth.* Forrás: http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf (Letöltés ideje: 2018. 10. 11.)

Európai Bizottság (2004): *Critical Infrastructure Protection in the Fight Against Terrorism.* Forrás: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33259&from=GA (Letöltés ideje: 2018. 11. 11.)

Európai Bizottság (2005): *Zöld Könyv egy Kritikus Infrastruktúra Védelmi Európai Programról.* Forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52005DC0576&from=EN (Letöltés ideje: 2018. 11. 11.)

Európai Bizottság (2006): *Létfontosságú infrastruktúrák védelmére vonatkozó európai program.* Forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l33260&from=EN (Letöltés ideje: 2018. 11. 11.)

Európai Bizottság (2015a): *A Digital Single Market for Europe*. Forrás: https://ec.europa.eu/commission/sites/beta-political/files/2-years-on-dsm_en_0.pdf (Letöltés ideje: 2018. 10. 11.)

Európai Bizottság (2015b): *A bizottság közleménye az európai parlamentnek, a tanácsnak, az európai gazdasági és szociális bizottságnak és a régiók bizottságának. Európai digitális egységes piaci stratégia.* Forrás: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:52015DC0192 (Letöltés ideje: 2018. 10. 11.)

Európai Bizottság (2015c): *The European Agenda on Security.* (Letöltés ideje: 2018. 06. 11.) Forrás: ec.europa.eu/anti-trafficking/sites/antitrafficking/files/eu_agenda_on_security_en.pdf (Letöltés ideje: 2018. 10. 11.)

Európai Bizottság (2016): *What is the Digital Economy and Society Index?* Forrás: http://europa.eu/rapid/press-release_MEMO-16-385_en.htm (Letöltés ideje: 2018. 11. 15.)

Európai Bizottság (2017a): *Az Unió helyzetéről szóló 2017. évi beszéd – Kiberbiztonság: a Bizottság megerősíti a kibertámadásokkal szembeni uniós reagálási képességet.* Forrás: http://europa.eu/rapid/press-release_IP-17-3193_hu.htm (Letöltés ideje: 2018. 10. 11.)

Európai Bizottság (2017b): *Kiberbiztonsági reform Európában 2017*. Forrás: http://www.consilium.europa.eu/hu/policies/cyber-security (Letöltés ideje: 2018. 10. 11.)

Európai Bizottság (2017c): *Az európai digitális menetrend.* Forrás: https://europa.eu/european-union/file/1515/download_hu?token=BR0rWYPW (Letöltés ideje: 2018. 10. 11.)

Európai Bizottság (2017d): *The Digital Economy and Society Index (DESI) Country Profiles.* Forrás: https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2017 (Letöltés ideje: 2018. 11. 11.)

Európai Bizottság (2017e): *Digital Single Market Bringing Down Barriers to Unlock Online Opportunities.* Forrás: https://ec.europa.eu/commission/priorities/digital-single-market_en (Letöltés ideje: 2018. 11. 15.)

Európai Bizottság (2018a): *Critical Infrastructure.* Forrás: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en (Letöltés ideje: 2018. 11. 15.)

Európai Bizottság (2018b): *Critical Infrastructure Warning Information Network (CIWIN).* Forrás: https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en (Letöltés ideje: 2018. 11. 15.)

Európai Bizottság (2018c): *The Digital Economy and Society Index (DESI).* Forrás: https://ec.europa.eu/digital-single-market/en/desi (Letöltés ideje: 2018. 11. 15.)

Európai Bizottság (2018d): *Magyarország DESI indexe.* Forrás: https://ec.europa.eu/digital-single-market/en/scoreboard/hungary (Letöltés ideje: 2018. 11. 15.)

Európai Parlament (2018): *Copyright in the Digital Single Market.* Forrás: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0337+0+DOC+PDF+V0//EN (Letöltés ideje: 2018.10. 01.)

Európai Tanács (2014): *EU Cyber Defence Policy Framework.* Forrás: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyb

erdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf (Letöltés ideje: 2018.11. 15.)

Európai Unió (2016): *Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy.* Forrás: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf (Letöltés ideje: 2018. 10. 18.)

Europol (2017a): *European Cybercrime Centre - EC3. Combating Crime in a Digital Age.* Forrás: www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Letöltés ideje: 2018. 10. 11.)

Europol (2017b): *Strategic Analysis. Complementing Operational Analysis.* Forrás: www.europol.europa.eu/activities-services/services-support/strategic-analysis (Letöltés ideje: 2018. 10. 11.)

Fireeye (2014): *APT28: A Window Into Russia's Cyber Espionage Operations?* Forrás: www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf (Letöltés ideje: 2018. 10. 11.)

Fireeye (2016): *Red Line Drawn: China Recalculates its Use of Cyber Espionage*. Forrás: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf (Letöltés ideje: 2018. 10. 11.)

Fireeye (é.n.): *APT1 Exposing One of China's Cyber Espionage Units.* Forrás: www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (Letöltés ideje: 2018. 10. 11.)

Fleming, T. Casey – Qualkenbush, Eric L. – Chapa, Anthony M. (2017): The Secret War Against the United States The Top Threat to National Security and the American Dream Cyber and Asymmetrical Hybrid Warfare An Urgent Call to Action. *The Cyber Defense Review,* 2. évfolyam, 3. szám. Forrás: https://cyberdefensereview.army.mil/Portals/6/Documents/CDR-FALL2017.pdf?ver=2017-11-21-092725-887 (Letöltés ideje: 2018. 10. 11.)

Franciaország (2013a): Livre Blanc: Défense et Sécurité Nationale 2013. Forrás: http://www.defense.gouv.fr/content/download/206186/2286591/file/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf (francia) (Letöltés ideje: 2018. 10. 11.)

Franciaország (2013b): *French White Paper – Defence and National Security 2013.* Forrás: http://www.defense.gouv.fr/content/download/215253/2394121/file/White%20paper%20on%20defense%20%202013.pdf (Letöltés ideje: 2018. 10. 11.)

Franciaország (2014): *La Politique de Sécurité des Systèmes d'Information de l'État (PSSIE).* Forrás: https://www.ssi.gouv.fr/entreprise/reglementation/protection-des-systemes-dinformations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/ (Letöltés ideje: 2018. 10. 11.)

Franciaország (2015a): *Stratégie nationale pour la sécurité du numérique.* Forrás: http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf (Letöltés ideje: 2018. 10. 11.)

Franciaország (2015b): *French National Digital Security Strategy*. Forrás: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf (Letöltés ideje: 2018. 10. 11.)

Franciaország (2017): *Defence and National Security Strategic Review 2017.* Forrás: https://www.defense.gouv.fr/layout/set/popup/content/download/520198/8733095/version/2/file/DEFENCE+AND+NATIONAL+SECURITY+STRATEGIC+REVIEW+2017.pdf (Letöltés ideje: 2018. 10. 11.)

Gallagher, Sean (2017): Apple Deleted Server Supplier after Finding Infected Firmware in Servers. *Arstechnica.com*, 2017. 02. 24. Forrás: https://arstechnica.com/information-technology/2017/02/apple-axed-supermicro-servers-from-datacenters-because-of-bad-firmware-update (Letöltés ideje: 2018. 10. 19.)

Gallagher, Ryan (2018): Google Plans to Launch Censored Search Engine in China, Leaked Documents Reveal. *The Intercept,* 2018. augusztus 1. Forrás: https://theintercept.com/2018/08/01/google-china-search-engine-censorship/ (Letöltés ideje: 2018. 10. 12.)

GAO (2013): *Report to Congressional Addressees – Cybersecurity National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented.* Forrás: https://www.gao.gov/assets/660/652170.pdf (Letöltés ideje: 2018. 10. 11.)

GAO (2018): *Weapon Systems Cybersecurity. DOD Just Beginning to Grapple with Scale of Vulnerabilities.* Forrás: https://www.gao.gov/assets/700/694913.pdf (Letöltés ideje: 2018. 10. 12.)

Garamone, Jim (2018): *DoD Official: National Defense Strategy Will Enhance Deterrence. F*orrás: https://www.defense.gov/News/Article/Article/1419045/dod-official-national-defense-strategy-will-enhance-deterrence/ (Letöltés ideje: 2018. 06. 11.)

GCSC (2018): *The Global Commission on the Stability of Cyberspace (GCSC): The Commission.* Forrás: https://cyberstability.org/about/ (Letöltés ideje: 2018. 06. 11.)

Haig Zsolt – Kovács László – Ványa László (2011): Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. *Felderítő Szemle,* 10. évf. 1–2. sz. 183–209.

Haig Zsolt (2015): *Információ, társadalom, biztonság*. Budapest, NKE Szolgáltató Kft.

Hannas, William C. – Mulvenon, James C. – Puglisi, Anna B. (2013): *Chinese Industrial Espionage: Technology Acquisition and Military Modernization.* Routledge.

Harold, Scott W. (2016): The U.S.-China Cyber Agreement: A Good First Step. *RAND Blog*. Forrás: https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html (Letöltés ideje: 2018. 10. 11.)

Heath, Timothy R. – Gunness, Kristen – Coope, Cortez A. (2016): *The PLA and Military Strategies, Deterrence Concepts, and Combat Capabilities.* RAND Corporation. Forrás, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1402/RAND_RR1402.pdf (Letöltés ideje: 2018. 10. 11.)

Hollandia (2011): *The National Cyber Security Strategy (NCSS).* Forrás: https://english.nctv.nl/binaries/cyber-security-strategy-uk_tcm32-83648.pdf (angol) (Letöltés ideje: 2018. 10. 11.)

Hollandia (2013a): *Nationale Cybersecurity Strategie Van bewust naar bekwaam.* Forrás: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2013/10/28/nati

onale-cyber-security-strategie-2/rapport-nationale-cybersecurity-strategie-2-2.pdf (Letöltés ideje: 2018. 10. 11.)

Hollandia (2013b): *National Cyber Security Strategy 2: From awareness to capability.* Forrás: Forrás: https://english.nctv.nl/binaries/national-cyber-security-strategy-2_tcm32-84265.pdf (Letöltés ideje: 2018. 10. 11.)

Hollandia (2018a): *Wereldwijd voor een veilig Nederland Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022.* Forrás: https://www.eerstekamer.nl/overig/20180327/_wereldwijd_voor_een_veilig/document3/f=/vkn0m270yrz6.pdf (holland) (Letöltés ideje: 2018. 10. 11.)

Hollandia (2018b): *Cyber Security Raad: Over de CSR.* Forrás: https://www.cybersecurityraad.nl/005_OverdeCSR/index.aspx (Letöltés ideje: 2018. 06. 11.)

Hollandia (2018c): *National Cyber Security Centrum: Incident Response.* Forrás: https://www.ncsc.nl/english/Incident+Response/24-hour-support.html (Letöltés ideje: 2018. 10. 11.)

Hollandia (2018d): *Nederlandse Cybersecurity Agenda Nederland digitaal veilig.* Forrás: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig/CSAgenda_def_web.pdf (holland) (Letöltés ideje: 2018. 10. 11.)

HSD Foundation (2018): *Minister Grapperhaus Launched the Dutch Cyber Security Agenda.* Forrás: https://www.thehaguesecuritydelta.com/news/newsitem/1072-minister-grapperhaus-launched-the-dutch-cyber-security-agenda (Letöltés ideje: 2018. 10. 11.)

HSDL (2018): *National Strategy Documents*. Forrás: https://www.hsdl.org/?collection&id=4 (Letöltés ideje: 2018. 10. 11.)

ICANN (2018): *The IANA Functions: An Introduction to the Internet Assigned Numbers Authority (IANA) Functions.* Forrás: https://www.icann.org/en/system/files/files/iana-functions-18dec15-en.pdf (Letöltés ideje: 2018. 10. 11.)

Internet World Stats (2018*): Internet Usage Statistics. The Internet Big Picture World Internet Users and 2018 Population Stats.* Forrás: www.internetworldstats.com/stats.htm (Letöltés ideje: 2018. 10. 19.)

ITU (2017a): *Definition of Cybersecurity.* Forrás: www.itu.int/en/ITU-/studygroups/com17/Pages/cybersecurity.aspx (Letöltés ideje: 2018. 10. 11.)

ITU (2017b): *Global Cybersecuriy Index:* Forrás: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (Letöltés ideje: 2018. 09. 15.)

ITU (2018a): *Global Cybersecurity Agenda (GCA).* Forrás: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx (Letöltés ideje: 2018. 10. 11.)

ITU (2018b): *Global Cybersecurity Index (GCI).* Forrás: https://www.itu.int/en/ITU-D/Cybersecurity/PublishingImages/GCA-GCI_091.png (Letöltés ideje: 2018. 10. 01.)

Ivanov, Anton – Mamedov, Orkhan (2017): *In ExPetr/Petya's shadow, FakeCry ransomware wave hits Ukraine.* Forrás: https://securelist.com/in-expetrpetyas-shadow-fakecry-ransomware-wave-hits-ukraine/78973 (Letöltés ideje: 2018. 10. 25.)

Jacobs, Andrew (2009): China Fears Ethnic Strife Could Agitate Uighur Oasis. *New York Times,* 2009. július 22. Forrás: https://www.nytimes.com/2009/07/23/world/asia/23kashgar.html?scp=1&sq=Uighur%20internet%20&st=cse (Letöltés ideje: 2018. 10. 11.)

JP 3-12 (2018): *Joint Publications 3-12 Cyberspace Operations.* Forrás: https://fas.org/irp/doddir/dod/jp3_12.pdf (Letöltés ideje: 2018. 10. 25.)

KIBEV (2018): *Célok és alapvetések.* Forrás: http://www.kibev.hu/ (Letöltés ideje: 2018. 10. 11.)

Kína kiberbiztonsági törvénye (2016): *Kiberbiztonsági törvény*. Forrás: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm (nem hivatalos fordítás: https://www.chinalawtranslate.com/cybersecuritylaw/?lang=en) (Letöltés ideje: 2018. 10. 12.)

Klimburg, Alexander ed. (2012): *National Cyber Security Framwork Manual.* Tallin, NATO CCDCOE. Forrás: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (Letöltés ideje: 2018. 10. 11.)

Kormányzati Eseménykezelő Központ (2009): *PTA CERT-Hungary Központ, mint Nemzeti Hálózatbiztonsági Központ.* Forrás: www.cert-hungary.hu/node/65 (Letöltés ideje: 2018. 10. 11.)

Kormányzati Eseménykezelő Központ (2017): *Magunkról.* Forrás: www.cert-hungary.hu/node/1 (Letöltés ideje: 2018. 10. 11.)

Kovács László – Krasznay Csaba (2017): „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *NKE Stratégiai Védelmi Kutatóközpont Elemzések,* 2017/9.

Kovács László – Sipos Marianna (2010): A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. *Hadmérnök,* 5. évf. 4. sz. 163–172. Forrás: www.hadmernok.hu/2010_4_kovacs_sipos.pdf (Letöltés ideje: 2018. 10. 11.)

Kovács László (2009a): Információs hadviselés kínai módra. *Nemzet és Biztonság: Biztonságpolitikai Szemle*, 2. évfolyam 7. szám (Letöltés ideje: 2018. 10. 11.)

Kovács László (2009b): Obama's new cybersecurity policy. *Hadtudományi Szemle*, 2. évfolyam 3. szám. Forrás: http://archiv.uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2009/2009_3/2009_3_hm_kovacs_laszlo_15_20.pdf (Letöltés ideje: 2018. 10. 11.)

Kovács László (2011): Kiberháború?: Internetes támadások a Wikileaks ellen és mellett. *Nemzet és Biztonság,* 4. évf. 1. sz. 3–8.

Kovács László (2012): Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése. *Hadmérnök,* 7. évf. 2. sz. 302–311.

Kovács László (2014): Az e-közszolgálat fejlesztés nemzetbiztonsági és hadtudományi kérdései. In Nemeslaki András szerk.: *E-közszolgálat fejlesztés: Elméleti alapok és tudományos kutatási módszerek.* Budapest, Nemzeti Közszolgálati Egyetem. 227–248.

Kovács László (2017): Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12 évfolyam 1. szám. Forrás: http://www.hadmernok.hu/171_17_kovacs.pdf (Letöltés ideje: 2018. 10. 15.)

Kovács László (2018a): *A kibertér védelme.* Dialóg-Campus.

Kovács László (2018b): *Kiberbiztonság és -stratégia.* Dialóg-Campus. Forrás: https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_Kiberbiztonsag_es_strategia.pdf (Letöltés: 2018. 11. 22.)

KPMG (2017): *Overview of China's Cybersecurity Law.* Forrás: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf (Letöltés ideje: 2018. 10. 12.)

Larson, Christina (2018): Who needs democracy when you have data? *MIT Techology Review,* 2018. augusztus 20. Forrás: https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/ (Letöltés ideje: 2018. 10. 12.)

Lengyelország (2014a): S*trategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Forrás*: https://www.bbn.gov.pl/ftp/SBN%20RP.pdf (Letöltés ideje: 2018. 10. 11.)

Lengyelország (2014b): *National Security Strategy of the Republic of Poland.* Forrás: https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf (Letöltés ideje: 2018. 10. 11.)

Lengyelország (2017a): K*rajowe ramy polityki bezpieczeństwa cybernetycznego Rzeczypospolitej Polskiej na lata 2017-2022.* Forrás: https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/0bbc7a32-64df-b45e-b08c-dac59415f109 (Letöltés ideje: 2018. 10. 11.)

Lengyelország (2017b): *National Framework of Cybersecurity Policy of the Republic Of Poland for 2017-2022.* Forrás: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf (Letöltés ideje: 2018. 10. 11.)

Lété, Bruno – Chase, Peter (2018): *Shaping Responsible State Behavior in Cyberspace.* Forrás: https://nato-engages.org/wp-content/uploads/2018/07/Shaping-Responsible-State-Behavior-in-Cyberspace.pdf (Letöltés ideje: 2018. 10. 06.)

Lettország (2014): *Cyber Security Strategy of Latvia 2014-2018*. Forrás: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/latvian-national-cyber-security-strategy/view/++widget++form.widgets.file/@@download/LV_NCSS.pdf (Letöltés ideje: 2018. 10. 11.)

Lettország (2015): *The National Security Concept (informative section)*. Forrás: http://www.mod.gov.lv/~/media/AM/Par_aizsardzibas_nozari/Plani,%20koncepcijas/NDK/NDK_ENG_final.ashx (Letöltés ideje: 2018. 10. 11.)

Lettország (2018): *Ministry of Defence of Republic of Latvia. The National Security Concept of the Republic of Latvia.* Forrás: http://www.mod.gov.lv/Par_aizsardzibas_nozari/Politikas_planosana/Koncepcijas/Nac_dros.aspx (Letöltés ideje: 2018. 10. 11.)

Liang, Qiao – Xiangsui, Wang (2002): *Unrestricted Warfare: China's Masterplan to Destroy America.* Pan American Publishing Company, Panamy City.

Liddell Hart, B.H. (2002): *Stratégia.* Európa.

Lindsay, Jon R. – Ming, Cheung Tai – Reveron, Derek S. (szerk.) (2015): *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.* Oxford University Press

Litvánia (2011): *Government of The Republic of Lithuania Resolution no 796 of 29 June 2011 on the approval of the programme for the development of electronic information security (cyber-security) for 2011–2019.* Forrás: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/programme-for-the-development-of-electronic-information-security-cyber-security-for-2011-2019-2011/view/++widget++form.widgets.file/@@download/LT_NCSS.pdf (Letöltés ideje: 2018. 10. 11.)

Litvánia (2017): *National Security Strategy of the Republic of Lithunia*. Forrás: https://kam.lt/download/57457/2017-nacsaugstrategijaen.pdf (Letöltés ideje: 2018. 10. 11.)

MITS (2003): *Magyar Információs Társadalom Stratégia.* Forrás: itf.njszt.hu/23r4r23r/uploads/2013/08/MITS-magyar.pdf (Letöltés ideje: 2018. 09. 14.)

Microsoft (2018): Forrás: A Digital Geneva Convention to protect cyberspace. *Microsoft Policy Papers*. Forrás: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH (Letöltés ideje: 2018. 10. 11.)

Military Ballance (2018): *The Military Ballance 2018: Chapter 5. Russia-Eurasia.* Forrás: https://www.iiss.org/en/publications/military%20balance/issues/the-military-balance-2018-545f/mb2018-05-russia-eurasia-dcce (Letöltés ideje: 2018. 10. 15.)

Miller, Alice (é.n.): The CCP Central Committee's Leading Small Groups. *China Leadership Monitor No.* 26. Forrás: https://www.hoover.org/sites/default/files/uploads/documents/CLM26AM.pdf (Letöltés ideje: 2018. 10. 11.)

Mills, Elinor (2016): Google to censor China Web searches Search giant agrees to censorship laws, reasoning that people getting limited access to content is better than none. *Cnet,* 2006. 01. 25. Forrás: www.cnet.com/news/google-to-censor-china-web-searches/ (Letöltés ideje: 2018. 10. 11.)

Mod PRC (2015): *National Security Law of the People's Republic of China (2015).* Forrás: http://eng.mod.gov.cn/publications/2017-03/03/content_4774229.htm (Letöltés ideje: 2018. 10. 11.)

MoD PRC (2018): *Central Military Commission.* Forrás: http://eng.mod.gov.cn/leadership/index.htm (Letöltés ideje: 2018. 10. 11.)

Munk, Sándor (2018): A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány*, 2018/1.

Munoz, Arturo G. (2013): *Intelligence in Public Media: Review on Chinese Industrial Espionage: Technology Acquisition and Military Modernization by William C. Hannas, James Mulvenon, and Anna B. Puglisi. Central Intelligence Agency.* Forrás: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-

studies/studies/vol-59-no-4/pdfs/Munoz-Chinese-Industrial-Espionage.pdf (Letöltés ideje: 2018. 10. 11.)

Nádudvari Anna (2018): A 2017-es francia stratégiai felülvizsgálat eredménye. *Stratégiai Védelmi Kutatóközpont Elemzések*, 2018/2.

NATO (2002): *Prague Summit Declaration.* Forrás: www.nato.int/cps/en/natohq/official_texts_19552.htm (Letöltés ideje: 2018. 10. 11.)

NATO (2010): *A NATO 2010-es új stratégiai koncepciója: Aktív Szerepvállalás, Modern Védelem Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságáról.* Forrás: 2010-2014.kormany.hu/download/b/52/20000/nato_strategiai_koncepcio.pdf (Letöltés ideje: 2018. 10. 14.)

NATO (2012): *Chicago Summit Declaration.* Forrás: https://www.nato.int/cps/en/SID-D95FAE1D-99C8ECE1/natolive/official_texts_87593.htm (Letöltés ideje: 2018. 10. 11.)

NATO (2016a): *Warsaw Summit Communiqué.* Forrás: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (Letöltés ideje: 2018. 10. 11.)

NATO (2016b): *Cyber Defence Pledge.* Forrás: https://www.nato.int/cps/su/natohq/official_texts_133177.htm (Letöltés ideje: 2018. 10. 11.)

NATO (2017): *Press conference by NATO Secretary General Jens Stoltenberg following the the meeting of the North Atlantic Council at the level of Defence Ministers.* Forrás: https://www.nato.int/cps/en/natohq/opinions_148417.htm (Letöltés ideje: 2018. 10. 11.)

NATO (2018a): *Cyber Defence.* Forrás: https://www.nato.int/cps/en/natolive/topics_78170.htm (Letöltés ideje: 2018. 10. 11.)

NATO (2018b): *Brussels Summit Declaration.* Forrás: https://www.nato.int/cps/ic/natohq/official_texts_156624.htm (Letöltés ideje: 2018. 10. 25.)

NCSI (2018): National Cyber Security Index. Forrás: https://ncsi.ega.ee/ (Letöltés ideje: 2018. 10. 01.)

Németország (2009): *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. Forrás: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1 (Letöltés ideje: 2018. 10. 11.)

Németország (2011): *Cyber-Sicherheitsstrategie für Deutschland*. Forrás: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile (Letöltés ideje: 2018. 10. 11.)

Németország (2015): *Nationale E-Government-Strategie Fortschreibung.* Forrás: https://www.it-planungsrat.de/SharedDocs/Downloads/DE/NEGS/NEGS_Fortschreibung.pdf?__blob=publicationFile&v=4 (Letöltés ideje: 2018. 06. 11.)

Németország (2016a): *Weissbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr. F*orrás: https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf (Letöltés ideje: 2018. 10. 11.)

Németország (2016b): *Cyber-Sicherheitsstrategie für Deutschland 2016. Forrás:* https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (Letöltés ideje: 2018. 10. 11.)

Nemzeti Infokommunikációs Stratégia (2014): *Az infokommunikációs szektor fejlesztési stratégiája (2014-2020) v7.0.* Forrás: http://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf (Letöltés ideje: 2018. 10. 11.)

NITS (2001): *Nemzeti Információs Társadalom Stratégia.* Forrás: http://itf.njszt.hu/23r4r23r/uploads/2013/08/nits_kesz.doc (Letöltés ideje: 2018. 09. 14.)

NIS Direktíva (2016): *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.*

Nyman-Metcalf, Katrin (2018): *A Legal View on Outer Space And Cyberspace: Similarities and Differences.* Tallinn Papers No10. CCDCOE. Forrás: https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper_10_2018.pdf (Letöltés ideje: 2018. 10. 11.)

Orosz Föderáció (2014): *Военная доктрина Российской Федерации.* Forrás: https://rg.ru/2014/12/30/doktrina-dok.html (Letöltés ideje: 2018. 11. 08.)

Orosz Föderáció (2015): Стратегия национальной безопасности Российской Федерации. Forrás: http://static.kremlin.ru/media/events/files/ru/l8iXkR8XLAtxeilX7JK3XXy6Y0AsHD5v.pdf (Letöltés ideje: 2018. 10. 11.)

Orosz Föderáció (2016): *Doctrine of Information Security of the Russian Federation*. Forrás: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 (Letöltés ideje: 2018. 11. 08.)

Osula, Anna-Maria (2015): *National Cyber Security Organisation: Estonia.* CCDCOE, 2015. Forrás: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ESTONIA_032015_1.pdf (Letöltés ideje: 2018. 10. 11.)

Pagliery, Jose (2015): Sniper attack on California power grid may have been 'an insider,' DHS says. *CCN Tech,* 2015. október 17. Forrás: http://money.cnn.com/2015/10/16/technology/sniper-power-grid/index.html (Letöltés ideje: 2018. 10. 11.)

PPD-41 (2016): *Presidential Policy Directive - United States Cyber Incident Coordination. Presidential Policy Directive / PPD-41.* Forrás: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident (Letöltés ideje: 2018. 11. 11.)

Raud, Mikk (2016): *China and Cyber: Attitudes, Strategies, Organisation.* CCDCOE, Tallinn. Forrás: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf (Letöltés ideje: 2018. 10. 11.)

Rothenpieler, Samuel (2016): *National Cyber Security Strategy 2016.* Forrás: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/april-2017/170426-bsi-enisa-nlo-presentation-v2.pdf (Letöltés ideje: 2018. 10. 11.)

Sanger, David E. – Perlroth, Nicole (2014): N.S.A. Breached Chinese Servers Seen as Security Threat. *New York Times*, 2014. március 22. Forrás: https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=0 (Letöltés ideje: 2018. 10. 11.)

SANS (2016): *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Forrás: https://ics.sans.org/media/E-SAC_SANS_Ukraine_DUC_5.pdf (Letöltés ideje: 2018. 11. 15.)

Schmitt, Michael N. ed. (2013): *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York, Cambridge University Press.

Schmitt, Michael N. ed. (2016): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* New York, Cambridge University Press.

Schneier, Bruce (2012): Cyberwar Treaties. *Schneier on Security,* 2012. 06. 14. Forrás: https://www.schneier.com/blog/archives/2012/06/cyberwar_treati.html (Letöltés ideje: 2018. 10. 11.)

Spiegel (2007): Innenministerium bestreitet Schäden durch Hackerangriffe. *Der Spiegel,* 2007. augusztus 25. Forrás: http://www.spiegel.de/netzwelt/tech/infizierte-regierungscomputer-innenministerium-bestreitet-schaeden-durch-hackerangriffe-a-502008.html (Letöltés ideje: 2018. 10. 11.)

Spiegel (2013): Cyber-Spionage Chinesische Hacker greifen EADS und ThyssenKrupp an. *Der Spiegel,* 2013. február 24. Forrás: http://www.spiegel.de/netzwelt/web/it-sicherheit-chinesische-hacker-greifen-eads-und-thyssenkrupp-an-a-885189.html (Letöltés ideje: 2018. 10. 11.)

Stratcom (2018): *United States Cyber Command.* Forrás: http://www.stratcom.mil/Portals/8/Documents/CYBERCOM_Fact_Sheet.pdf (Letöltés ideje: 2018. 10. 11.)

Szlovákia (2015a): *Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020.* Forrás: http://www.nbusr.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf (Letöltés ideje: 2018. 10. 11.)

Szlovákia (2015b): *Cyber Security Concept of the Slovak Republic for 2015 – 2020.* Forrás: http://www.nbusr.sk/wp-content/uploads/cyber-security/Cyber-Security-Concept-of-the-Slovak-Republic-for-2015-2020.pdf (Letöltés ideje: 2018. 10. 11.)

Szlovákia (2016a): *Biela kniha o obrane Slovenskej republiky*. Forrás: http://www.mod.gov.sk/data/BKO2016_LQ.pdf (Letöltés ideje: 2018. 10. 11.)

Szlovákia (2016b): *White Paper on Defence of the Slovak Republic*. Forrás: http://www.mosr.sk/data/WPDSR2016_LQ.pdf (Letöltés ideje: 2018. 10. 11.)

Szlovákia (2016c): *Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015-2020.* Forrás: http://www.nbusr.sk/wp-content/uploads/cyber-security/Action-Plan-for-the-Implementation-of-the-Cyber-Security-Concept-of-the-Slovak-Republic-for-2015-2020-_3_.pdf (Letöltés ideje: 2018. 10. 11.)

Takacs, D. (2017): Ukraine's deterrence failure: Lessons for the Baltic States. *Journal on Baltic Security*, Vol. 3 No. 1.

US DHS–FBI (2016): *US Department of Homeland Security and Federal Bureau of Investigation (2016): JAR-16-20296. GRIZZLY STEPPE – Russian Malicious Cyber Activity.* Forrás: www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (Letöltés ideje: 2018. 10. 15.)

US DoD Cybersecurity Strategy (2015): *The DoD Cyber Strategy*. Forrás: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (Letöltés ideje: 2018. 10. 11.)

USCC (2008): *2008 Report to Congress of the U.S.-China Economic and Security Review Commission One Hundred Tenth Congress Second Session.* U.S. Government Printing Office, Washington. Forrás: https://www.uscc.gov/sites/default/files/annual_reports/2008-Report-to-Congress-_0.pdf (Letöltés ideje: 2018. 10. 11.)

USCC (2017): *2017 Report to Congress of the U.S.-China Economic and Security Review Commission One Hundred Tenth Congress Second Session. U.S. Government Printing Office, Washington.* Forrás: https://www.uscc.gov/sites/default/files/annual_reports/2017_Annual_Report_to_Congress.pdf (Letöltés ideje: 2018. 10. 11.)

USCYBERCOM (2018): Achieve and Maintain Cyberspace Superiority Command Vision for US Cyber Command. Forrás: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010 (Letöltés ideje: 2018. 10. 21.)

Wamala, Frederick (2011): *The ITU National Cybersecurity Strategy Guide.* Forrás: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf (Letöltés ideje: 2018. 10. 11.)

White House (2017): *National Security Strategy of the United States of America*. Forrás: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (Letöltés ideje: 2018. 10. 11.)

White House (2018): *National Cyber Strategy of the United States of America*. Forrás: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf 0905.pdf (Letöltés ideje: 2018. 10. 26.)

Wong, Edward (2015): China Approves Sweeping Security Law, Bolstering Communist Rule. *New York Times*, 2015. július 1. Forrás: https://www.nytimes.com/2015/07/02/world/asia/china-approves-sweeping-security-law-bolstering-communist-rule.html (Letöltés ideje: 2018. 10. 11.)

Yarger, Harry R. (2006): Strategic Theory for the 21st Century: The Little Book on Big Strategy. *The Letort Papers*, US War College Forrás: https://www.files.ethz.ch/isn/20753/Strategic%20Theory%20for%20the%2021st%20Century.pdf (Letöltés ideje: 2018. 10. 12.)

Yuan, Li (2018): Young people in China don't know the internet we do – and they like it that way. *Independent,* 2018. szeptember 5. Forrás: https://www.independent.co.uk/life-style/gadgets-and-tech/features/china-internet-social-media-great-firewall-of-china-censorship-apps-a8510036.html (Letöltés ideje: 2018. 10. 12.)

ZITiS (2018): *Über Uns.* Forrás: https://www.zitis.bund.de/DE/ZITiS/Ueber_Uns/ueber_uns_node.html;jsessionid=96BB2385345B065ED4537A388F651F6F.2_cid377 (Letöltés ideje: 2018. 10. 11.)

AZ ÉRTEKEZÉS TÉMÁJÁBAN SZÜLETETT FONTOSABB TUDOMÁNYOS PUBLIKÁCIÓIM JEGYZÉKE

Monográfia, könyv

Kovács László (2018): *Kiberbiztonság és -stratégia*. Budapest: Dialóg Campus Kiadó; Nordex Kft., 350 p. ISBN 978-615-5920-93-6

Kovács László (2018): *A kibertér védelme*. Budapest: Dialóg Campus Kiadó; Nordex Kft., 354 p. ISBN 978-615-5889-63-9

Haig Zsolt, Kovács László, Ványa László, Vass Sándor, Németh András (szerk.) (2014): *Elektronikai hadviselés.* Budapest: Nemzeti Közszolgálati Egyetem, 271 p. ISBN 978-615-5305-87-0

Haig Zsolt, Kovács László, Munk Sándor, Ványa László, [Kovács László, Tózsa István (szerk.)] (2013): *Az infokommunikációs technológia hatása a hadtudományokra.* Budapest: Nemzeti Közszolgálati Egyetem, 173 p. ISBN 978-615-5305-02-3

Könyvfejezet / Szerkesztett könyvben cikk

Kovács László (2014): *Az e-közszolgálatfejlesztés nemzetbiztonsági és hadtudományi kérdései*. In: Nemeslaki András (szerk.) E-közszolgálatfejlesztés: Elméleti alapok és tudományos kutatási módszerek. 353 p. Budapest: Nemzeti Közszolgálati Egyetem, pp. 227-248.

Kovács László (2013): *Cyber challenges to the armed forces.* In: Marek Kulczkycki (szerk.) Armed Forces in the system of international security. 223 p. Wrocław: Wroclaw University Press, pp. 157-173. ISBN 978-83-63900-52-6

Haig Zsolt, Kovács László (2008): Energiaellátó rendszerek rendszerirányítása: 3.7.4. fejezet. In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 51-75. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): Internet Magyarországon: 3.7.5. fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 77-100. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): Védelmi szféra infrastruktúrák: 3.7.6. fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 101-136. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): A vezetékes távközlő rendszerek áttekintése: 5.3.3 fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 1-5. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): A mobil cellás rádiótelefon rendszerek áttekintése és néhány gyakorlati alkalmazás: 5.3.4 fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 1-22. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): Kritikus információs infrastruktúrák elleni fenyegetések: 3.7.7. fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 137-148. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): Kritikus információs infrastruktúrák védelme: 3.7.8. fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 149-170. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): Műholdas távközlési rendszerek: 5.3.5. fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 1-8. ISBN 963 9313 12 2

Nemzetközi folyóiratcikk

Kovács László (2018): Cyber Security Policy and Strategy in the European Union and NATO. *Revista Academiei Fortelor Terestre / Land Forces Academy Review*, XXIII. 1 (89) pp. 16-24.

Kovács László (2018): National Cyber Security as the Cornerstone of National Security. *Revista Academiei Fortelor Terestre / Land Forces Academy Review*, XXIII. 2. (90) pp. 113-120.

Kovács László (2018): Comparative Study on Digital Economy and Society of Austria and the Visegrad Countries. *Economics and Management,* 2017. 2. pp. 36-47.

Haig Zsolt, Kovács László (2007): New Way of Terrorism: Internet- and cyber-terrorism. *Military Technical Academy Review*, 17. 2. pp. 125-137.
chnical Academy Review, 17. 2. pp. 125-137.

Hazai folyóiratcikk

Kovács László, Krasznay Csaba (2017): Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Stratégiai Védelmi Kutató Központ (Elemzések) / Center for Strategic and Defense Studies Analyses*, 2017. 9. pp. 1-11.

Kovács László, Krasznay Csaba (2017): Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság: Biztonságpolitikai Szemle*, 2017. 1. pp. 3-16.

László Kovács, András Nemeslaki, Ákos Orbók, András Szabó (2017): Structuration Theory and Strategic Alignment in Information Security Management: a Comprehensive Research Approach and Program. *Academic and Applied Research In Military And Public Management Science*, 16. 1. pp. 5-16.

Nagyné Takács Veronika, Kovács László (2015): Az információbiztonság vezető szakirányú továbbképzés tapasztalatai. *Pro Publico Bono: Magyar Közigazgatás*, 2015. 4. pp. 85-99.

Kovács László (2012): Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I. *Hadmérnök*, VII. 2. pp. 302-311.

Haig Zsolt, Kovács László, Ványa László (2011): Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. *Felderítő Szemle*, 10. évf. 1-2.sz. pp. 183-209.

Kovács László, Illési Zsolt (2011): Cyberhadviselés. *Hadtudomány*. XXI. 1-2. pp. 29-41.

Kovács László, Sipos Marianna (2011): A Stuxnet és ami mögötte van II.: Célok és teendők. *Hadmérnök*, VI. 1. pp. 222-231.

Kovács László (2011): Kiberháború? Internetes támadások a Wikileaks ellen és mellett. *Nemzet és Biztonság: Biztonságpolitikai Szemle*, 2011. 1. pp. 3-8.

Kovács László, Krasznay Csaba (2010): Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság: Biztonságpolitikai Szemle*, 2010. 1. pp. 44-56.

Kovács László, Sipos Marianna (2010): A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. *Hadmérnök,* V. 4. pp. 163-172.

Kovács László (2009): Electronic warfare and the asymmetric challenges. *Bolyai Szemle*, 2009. 3. pp. 135-151.

Kovács László (2009): Információs hadviselés kínai módra. *Nemzet és Biztonság: Biztonságpolitikai Szemle*, 2. 7. pp. 35-44.

Kovács László (2009): Obama's new cybersecurity policy. *Hadtudományi Szemle,* 2. 3. pp. 15-20.

Haig Zsolt, Kovács László (2008): Fenyegetések a cybertérből. *Nemzet és Biztonság: Biztonságpolitikai Szemle,* 1. 5. pp.

Kovács László (2008): Az információs terrorizmus elleni tevékenység kormányzati feladatai. *Hadmérnök*, 2008. 2. pp. 138-148.

Kovács László (2008): Kritikus információs infrastruktúrák Magyarországon. *Hadmérnök*, 2007. (Különszám) pp. 1-20 p.

Kovács László (2007): Az információs terrorizmus eszköztára. *Hadmérnök*, 2007. 1. pp. 1-18.

Konferencia kiadványban megjelent cikk

Kovács László (2013): Cyberterrorizmus: valós vagy túldimenzionált veszély? *Magyar Rendészet,* XIII. (különszám) pp. 85-93.

Tanulmány

Kovács László, Szentgáli Gergely (2015): *National Cyber Security Organisation: Hungary*. NATO CCDCOE, Észtország, pp. 1-14.

Haig Zsolt, Kovács László, Ványa László (szerk.) (2012): Kritikus infrastruktúrák és kritikus információs infrastruktúrák, Tanulmány. Budapest: Nemzeti Közszolgálati Egyetem, 2012. 298 p.

Haig Zsolt, Hajnal Béla, Kovács László, Muha Lajos, Sik Zoltán Nándor (2009): *A kritikus információs infrastruktúrák meghatározásának módszertana*. Budapest: ENO Advisory Kft. 198 p.

Budapest, 2018. november 21.