PRO PATRIA AD MORTEM

Kiberbiztonság és -stratégia

KOVÁCS LÁSZLÓ

Dialóg Campus

Kovács László

Kiberbiztonság és -stratégia

Vákát oldal

Kovács László

KIBERBIZTONSÁG ÉS -STRATÉGIA

Dialóg Campus Kiadó ❖ Budapest

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú,
„A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű
kiemelt projekt keretében jelent meg.

Szakmai lektor
Krasznay Csaba

Tartalom

Vákát oldal

Bevezetés

A kibertér mindennapjaink meghatározó dimenziójává vált. Életünk minden szegmensére kihatással van, legyen szó gazdaságról, politikáról, kultúráról vagy akár a magánéletünk egyes elemeiről.

Azonban azok a szolgáltatások, amelyek a kiberteret alkotják és az ezeket lehetővé tevő eszközök egyre nagyobb függőséget jelentenek számunkra. Ezeknek a rendszereknek és szolgáltatásoknak a kiesése nemcsak, hogy komoly fennakadásokat okoz a mindennapokban, hanem ma már az anyagi károkon túl komoly veszélyt jelentenek az emberek életére is.

A kibertér és az abban megvalósítandó biztonság így minden ország számára elemi érdek. Ennek felismerése azonban csak az elmúlt egy-másfél évtizedben következett be. A 2000-es évek közepétől fokozatosan nő azoknak az országoknak a száma, amelyek ezt a felismerést állami szinten is képesek kezelni. A kibertér fontossága ma már nem kérdőjelezhető meg és nem is kerülhető meg. Ennek megfelelően a kibertérben megjelenő kihívásokra és veszélyforrásokra stratégiai szinten kell választ adni.

Ez az országok nemzeti kiberbiztonságról szóló stratégiai elképzeléseiben tükröződik a leginkább, hiszen a globális nagyhatalmak mellett a kisebb országok is nemzeti szinten igyekeznek a kibertérrel kapcsolatos biztonsági kérdésekre megoldásokat találni. Ezek a megoldások az egyes országokban látszólag eltérő válaszokat jelentenek, de egyvalami mégis összeköti őket: ez pedig a biztonság.

Az európai országok kiberbiztonsági stratégiáinak elemzésekor láthatjuk, hogy számos ország az első időkben az információs társadalom és annak biztonsági vetületei, más országok pedig a kritikus információs infrastruktúrák és azok biztonsági kérdései felől közelítették meg a kérdést. Ugyanakkor a legtöbb ország már a második

vagy akár a harmadik – esetenként frissített vagy néha alapjaiban megváltoztatott – kiberbiztonsági stratégiájának kiadásánál tart. Ennek oka az, hogy a kibertér egyre inkább meghatározó lett a legtöbb országban – a fenti utalás alapján ez igaz a gazdaság, a politika, az emberek mindennapjainak területére, de nyugodtan kijelenthetjük, hogy mindezek mellett már egy adott ország – és ezzel egy adott régió – jóléte is a kibertértől, illetve az abban meglévő zavartalanul működő rendszerektől és szolgáltatásoktól függ. Ennek megfelelően egyre inkább szükséges, hogy minden ország gondolkodjon és gondoskodjon a kibertér egészének biztonságáról. Ezt erősíti a technika korábban sosem látott ütemű fejlődése, amely azonban nemcsak pozitív tényezőket jelent a társadalom számára, hanem magában hordoz számos kihívást és veszélyt is. Napjaink technikai fejlődése során az egyik legnagyobb bizonytalanság a mesterséges intelligencia (MI) fejlődésében, illetve az általa nyújtott szolgáltatásokban van, hiszen ezek nehezen előrejelezhetőek. Ugyanakkor, ahogy arra Musk[1] és Hawking[2] is többször utalt: a nem teljesen átgondolt fejlesztések rendkívül nagy veszélyeket rejthetnek magukban, hiszen nem tudjuk, hogy az MI milyen funkciókra és milyen tudásra lesz képes, akár ellenünk is. (Cellan 2014) Ahogy egy családi beszélgetésen kissé viccesen elhangzott: „Az ilyen dolgoknak a filmekben mindig rossz vége van". Ám, hogy ez ne így legyen, minden országnak stratégiai szinten kell a kiberbiztonságról gondolkodnia, úgy, hogy abba a technikai fejlődés és annak bizonytalansága is bekerüljön, mint olyan tényezők, amelyek alapjaiban határozhatják meg a biztonságot.

A kérdés persze az, hogy a kibertér biztonsága megteremthető-e nemzeti szinten, hiszen a kibertérben nagyon nehezen értelmezhetők a földrajzi határok. Ennek megfelelően azt is meg kell vizsgálni, hogy egy olyan politikai-gazdasági szövetség, mint például az Európai Unió

[1] Elon Musk (eredeti nevén Elon Reeve Musk) dél-afrikai születésű, jelenleg az Egyesült Államokban élő feltaláló és technológiai befektető, a Tesla cég alapítója.

[2] Stephen Hawking (1942–2018) elméleti fizikus, aki nemcsak tudományos munkásságával, hanem tudománynépszerűsítő könyveivel is nagy sikert ért el.

vagy akár politikai-katonai szövetségként a NATO stratégiai szinten milyen megoldásokat lát a kibertér biztonságára nézve megvalósíthatónak.

Ugyanakkor sem a nemzeti, sem a szövetségi szinten történő kiberbiztonsági stratégiák kialakításakor nem elhanyagolható az, hogy ez az adott stratégia milyen kérdésekre tér ki, hogyan és milyen formában kívánja kezelni a kibertéri kihívásokat. Ezért szükséges számba venni azokat – az alapvetően nemzetközi szervezetek által készített – ajánlásokat és modelleket, amelyek alapul szolgálhatnak egy ország nemzeti kiberbiztonsági stratégiájának felépítéséhez és legfontosabb szabályozási kérdéseihez. Ezzel megteremthető annak a lehetősége is, hogy bár az országok nemzeti szinten alkotnak kiberbiztonsági stratégiát, azok mégis egymással összhangban, azonos filozófiai háttérrel készülhetnek, és így – többé-kevésbé függetlenül az adott ország érdekeitől és értékeitől – azonos irányba ható stratégiai elképzelések születnek. Ennek az azonos iránynak pedig egy célja lesz, ez pedig a biztonságos kibertér.

Mindezek alapján könyvünk hazánk kiberbiztonsági stratégiai gondolkodásának fejlődése mellett kitér néhány Magyarországhoz hasonló méretű ország kiberbiztonsági stratégiájára és politikájára, valamint bemutatja az Európai Unióban meghatározó olyan nagy országok, mint például Németország, Franciaország és az Egyesült Királyság[3] kiberbiztonságról alkotott stratégiai elképzeléseit. Ezek mellett, ahogy a fentiekben utaltunk rá, szükséges az Európai Unió és a NATO ilyen irányú irányelveit és dokumentumait is felvázolni, valamint azokat röviden elemezni, hiszen ezek kihatással vannak a szövetségek tagországainak nemzeti kiberbiztonsági stratégiáira is.

Ezt megelőzően, azaz mielőtt a nemzetek kiberteret érintő stratégiai elképzeléseit bemutatnánk, könyvünk felvázolja a kiberbiztonság legfontosabb összetevőit, majd bemutatja a kiberhadviselés elméletét. Ezt nem ok nélkül tesszük, hanem azért, mert számos ország esetében

[3] Az Egyesült Királyság a könyv írásának idején – 2018-ban – még az Európai Unió tagja.

láthatjuk, hogy ezekben az országokban a biztonság mellett megjelenik a kibertér katonai, illetve politikai célokra történő – és így nem mindig békés – alkalmazásának az igénye, sőt egyes esetekben ezekkel kapcsolatban már megtörtént eseteket is be tudunk mutatni.

A kibertér ilyenfajta felhasználása, nevezetesen a kiberhadviselés vagy egy másik ország politikai befolyásolása esetünkben azt is indukálta, hogy megvizsgáljuk azt, hogy a nagyhatalmak – az Egyesült Államok, Kína és Oroszország – milyen stratégiai gondolkodást és ezzel párhuzamosan milyen valós tevékenységet folytat a kibertérben. Így e három nagyhatalom kibertérrel kapcsolatos stratégiáinak bemutatása is bekerült könyvünkbe.

Természetesen a téma nagysága miatt némi lehatárolást, azaz témaszűkítést kell tennünk rögtön már a bevezetőben. Könyvünk nemcsak terjedelmi, hanem komoly szakértelmi hiányok miatt sem vállalkozhat a stratégiaalkotás minden elemének és számtalan összefüggésének bemutatására.[4] A stratégiakészítés önmagában is meglehetősen bonyolult folyamat, legyen szó egy egyszerű szervezetről vagy akár egy országról. Ráadásul minden egyes stratégiai területnek megvan a csak rá jellemző sajátossága. Természetesen vannak olyan elvek, amelyek közösek és általános érvényűnek tekinthetőek, így minden területen alapként funkcionálhatnak.

Mindezek alapján könyvünkben csak a kiberbiztonság legfontosabb összefüggéseire, illetve azoknak a különböző országok stratégiai dokumentumaiban való megjelenésére fókuszálunk.

A könyv számos – az eredeti stratégiai dokumentumokból származó – idézetet[5] tartalmaz. Bár ezek nyilvánvalóan eredeti szöveg-

[4] Mindezek mellett egy időbeni lehatárolást is szükséges megtennünk. Jelen könyv kézirata 2018 tavaszán-nyarán készült. Ebből következően az ezt követően megjelenő nemzeti stratégiák elemzését nem tartalmazhatja.

[5] Ezeket az idézeteket az eredeti stratégiai dokumentumok angol vagy esetenként német nyelvű változatainak felhasználásával jelen könyv szerzője fordította. Bár idézetekről van szó, néhány helyen a szó szerinti fordítás helyett az eredeti mondanivaló és gondolatok magyarul történő interpretálása miatt inkább azok értelmezése kapott szerepet.

környezetükből kiemelve jelennek meg könyvünkben, mégis bízunk benne, hogy hozzájárulnak az eredeti kiberbiztonsági stratégia vagy politika legfontosabb céljainak bemutatásához és megértéséhez.

Vákát oldal

1. A kiberbiztonság stratégiai alapjai

1.1. A kiberbiztonság meghatározása és lehatárolása

1.1.1. A kiberbiztonság összetevői és területei

A kiberbiztonság tárgyalásakor számos területet kell egészen pontosan definiálnunk ahhoz, hogy a nemzeti kiberbiztonsági stratégiák elemzéseihez hozzá tudjunk kezdeni, és azok ne fussanak már a kezdetek kezdetén rossz vágányra.

Ugyanakkor nagyon sok oka van annak, hogy mégsem tudunk egészen világos és mindenre kiterjedő meghatározásokkal szolgálni, még a kibertérre vonatkozóan sem. Az okok között szerepel a technika és a technológia hatalmas ütemű változása, amely olyan sebességgel történik, hogy akár néhány év alatt is alapjaiban változik meg a területről alkotott legalapvetőbb elképzeléseink többsége.[6] Egy másik ok pedig a technika hatása a társadalomra, amely hatás egy nagyon szoros interakció révén jön létre. Az információs technológiára épülő technika és az azon keresztül elérhető szolgáltatások természetszerűleg alakítják át a társadalom legalapvetőbb funkcióit is (gondoljunk csak például a kommunikációra, illetve az emberek egymással való kapcsolattartására), de megfigyelhető egy másik, az ellenkező irányban érvényesülő hatás is. Ez viszont a társadalom hatása a technikai fejlődésre,

[6] Erre utaltunk a bevezetőben, amikor megemlítettük a mesterséges intelligenciát és annak rohamos fejlődését. Ez az egyik olyan terület, amely esetében nagyon nehéz a biztonság bármely aspektusát előrejelzni, mert a mesterséges intelligencia jelenlegi fejlettségi szakaszában egyelőre csak az jelezhető előre, hogy magában a technológiában nagyon nagy a potenciál, valószínűsíthetően alapjaiban fogja meghatározni a jövőt, de ez lehet akár a védelem, akár a támadás oldalán is. Így ma nem mondható meg pontosan, hogy mire és hogyan fogjuk a jövőben használni.

hiszen nagyon sok esetben olyan technológiai újdonságok jutnak zsákutcába, amelyeknek a fejlesztők nagy jövőt jósoltak, csak éppen a társadalom igénye ezt nem igazolta; illetve olyan megoldások emelkednek fel és válnak világszinten népszerűvé, amelyekről első ránézésre ezt nem is gondoltuk volna, de a társadalom valamilyen oknál fogva mégis használatba veszi ezeket. Erre talán az egyik legjobb példa a közösségi médiumok sikertörténete.

Azonban van két fogalom, amelyet definiálnunk kell, amennyiben a kiberbiztonságot, illetve annak stratégiai vetületeit kívánjuk górcső alá venni. E két fogalom közül az egyik a kibertér. Ennek meghatározása sem egyszerű feladat azonban, hiszen ahogy Munk Sándor megfogalmazza egyik tanulmányában: „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)

A kibertér meghatározásával kapcsolatban van egy másik probléma is, amelyre az említett Munk-tanulmány is utal. Ez pedig nem más, mint az, hogy a számos kibertér-definíció nem is ugyanazon a szinten tárgyalja a fogalmat, hiszen egy részük a tartományt, egy részük a környezetet érti alatta, egy másik részük viszont hálózatok összességeként írja le. (Munk 2018)

Ugyanakkor a kibertérben megvalósítani kívánt biztonság stratégiai megközelítése okán célszerű a sok kibertéri megfogalmazásból egy olyat kiválasztanunk és a későbbi vizsgálataink során ezt használnunk, amely nyilvánvalóan stratégiai megközelítéssel tekint a kibertérre. Ennek az általunk felállított kritériumnak tökéletesen megfelel a 2013-as hazai Nemzeti Kiberbiztonsági Stratégiában használt megfogalmazás, amely szerint „[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]

A kibertér, illetve az azzal kapcsolatos fontos területek meghatározására születtek nagyon érdekes elképzelések is. Ezek azonban alapvetően valamely más, például nemzetközi jogi megközelítés miatt lehetnek hasznosak a számunkra. Az egyik ilyen elképzelés a külső űrrel kapcsolatos, illetve az erre a területre érvényes nemzetközi jogi szabályozás kialakulását és annak kibertéri relevanciáját, analógiáját vizsgálja. A külső űr és a kibertér vonatkozásában Nyman-Metcalf a következőket állapítja meg egy tanulmányában: „A kibertérrel való hasonlóság az alapüzenetben megtalálható: az emberiség valami olyan teljesen új korszakba lépett, elhagyva a föld korlátait, amely egy teljesen új jövőt jelent, amelyben 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)

A következő fogalom, amely könyvünk szempontjából különösen fontos, a kiberbiztonság. Ennek definiálásához a Nemzetközi Távközlési Egyesület (International Telecommunication Unit, ITU) által adott meghatározást hívjuk segítségül, amely 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 2017b)

Ezt a meghatározást alkalmazva levonhatjuk azt a következtetést, hogy a kiberbiztonság a jelenlegi és az előrejelezhető biztonsági kihívásokat kezeli, és biztosítja azt az állapotot, amelyben a szervezet működőképes, a felhasználó az eszközeit zavartalanul és biztonságosan tudja használni, hozzáfér az adataihoz és az információkhoz, valamint a szervezet különböző folyamatai az eredeti működési szándéknak megfelelő módon működnek. (ITU 2017b)

Ennek a meghatározásnak az alapgondolatai nagy mértékben tükröződnek a hazai kiberbiztonság területén fontos szerepet játszó információbiztonsági törvény[7] által adott meghatározásban, amely szerint a kiberbiztonság nem más, mint „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 1. § (1) bekezdés 26. pont]

A kiberbiztonsággal szorosan összefüggő információbiztonságban általában három olyan tényezőt határoznak meg, amelyekkel mérhető az adott szervezet biztonsága, illetve amely tényezőkre a biztonságnak ki kell térnie. Ez a három tényező a *bizalmasság,* a *sértetlenség* és a *rendelkezésre állás,* amelyek az angol terminológiában használt kifejezések: bizalmasság, azaz *confidentiality,* sértetlenség, azaz *integrity* és elérhetőség, azaz *availability* – a kezdőbetűk miatt ezt a tényezőhármast gyakran CIA-elvnek is hívják.

Ezek a biztonsági tulajdonságok jól jellemzik az adott szervezet információbiztonságát, ugyanakkor magáról a kiberbiztonságról még nem feltétlenül adnak teljes és jól áttekinthető képet. Ennek oka az, hogy a kiberbiztonság komplex tevékenységek sorozatával, több terület egymásra hatásával érhető csak el.[8]

A komplex információbiztonságra vonatkozóan is számos meghatározást találunk, attól függően, hogy az adott definíciót megalkotó milyen nézőpontból vizsgálja a kérdést. Így találunk a biztonságpolitika,

[7] A röviden csak információbiztonsági törvénynek vagy Ibtv.-nek nevezett jogszabály hivatalos címe a következő: Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény.

[8] E tevékenységek során azt is meg kell határoznunk, hogy mit értünk védelem és mit biztonság alatt. Kissé leegyszerűsítve kijelenthetjük, hogy a védelem olyan tevékenységek sorozatát jelenti, amely a biztonságot mint állapotot hozza létre.

de akár a kritikus információs infrastruktúra területéről indított meghatározásokat is.

Haig megfogalmazásában a komplex információbiztonság legfontosabb eleme annak céljában keresendő: „az információs társadalom információbiztonsága szempontjából tehát a fő cél a kritikus információk megóvása". (Haig 2015)

Mindezeknek megfelelően a komplex információbiztonságnak és így a kiberbiztonságnak is több területen végrehajtott védelmi tevékenységek egész sorozatát kell jelentenie. Ezek a területek a következők:

- személyi biztonság;
- fizikai biztonság;
- adminisztratív biztonság;[9]
- elektronikus információbiztonság. (Haig 2015)

Ahogy a fentiekben említettük, a kiberbiztonság a kritikus infrastruktúrák oldaláról is vizsgálható, és célszerű is ilyen szempontból vizsgálni. Ennek megfelelően az erre a területre vonatkozó definíciós készlet meghatározásához hívjuk segítségül a hazánk kritikusinfrastruktúra-védelmére vonatkozó, 2012-ben született törvényt, amely szerint a kritikus infrastruktúra:[10] „meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személyés 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]

[9] Korábban az adminisztratív biztonságot dokumentumbiztonságnak nevezték.

[10] A törvény – annak címéből következő módon – a *kritikus infrastruktúra* kifejezést a *létfontosságú rendszerelem* megnevezéssel azonosítja. [2012. évi CLXVI. törvény 1. § *f)* pont]

Mindezeken túl a törvény meghatározza az európai értelemben vett kritikus infrastruktúra[11] 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. törvény 1. § *c)* pont]

Ugyanakkor a kiberbiztonság szempontjából kiemelten lényeges kritikus információs rendszer és létesítmény[12] esetében is fontos a meghatározás áttekintése, amelyhez a kritikusinfrastruktúra-védelmi törvény végrehajtása érdekében kiadott kormányrendeletet hívjuk segítségül, amely így fogalmaz: „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]

1.1.2. Kiberbiztonsági fenyegetések

A kiberbiztonsági fenyegetések számbavétele és pontos felsorolása meglehetősen nehéz – és tegyük hozzá rögtön: kissé reménytelennek is tűnő – feladat, hiszen naponta jelennek meg újabb és újabb olyan támadási módok, amelyek a szoftver- és hardverkörnyezet sérülékenységeit sok esetben meglepően nagy hatékonysággal használják ki.

Ennek megfelelően nem célunk ezeknek a fenyegetések a teljesség igénye szerinti katalogizálása. Ez a kiberbiztonság stratégiai környezete szempontjából feltételezhetően nem is lenne olyan fontos. Ehe-

[11] A törvény az *európai létfontosságú rendszerelem* kifejezést használja az európai kritikus infrastruktúra vonatkozásában. [2012. évi CLXVI. törvény 1. § *c)* pont]

[12] A kormányrendelet a *létfontosságú információs rendszer és létesítmény* megnevezést használja. [65/2013. (III. 8.) Korm. rendelet 1. § 3. pont]

lyett néhány olyan trendre kívánjuk itt felhívni a figyelmet, amelyek szorosan összefüggnek a kiberbiztonság stratégiájának kialakításával, illetve amelyek alapvető hatással lehetnek azokra az elemekre, amelyeket egy-egy ilyen stratégiának tartalmaznia kell. Ezek a trendek – ha tetszik, területek, illetve legfontosabb kihívások – a következők:

- a kiberhadviselés megjelenése, valamint az ezzel összefüggő állami támogatású kibertámadások egyre növekvő száma;
- a politikai befolyásolás, amely során állami és nem állami támogatású csoportok hamis vagy álhírekkel különböző médiafelületeken nagy tömegben érik el a lakosságot, így formálva politikai és egyéb véleményüket;
- a kiberfegyverek terjedése, amelyek a kibertámadások mindennapos eszközeitől és megoldásaitól kezdődően az elsősorban állami célpontok elleni információszerző vagy a stratégiai fontosságú rendszereket célpontként támadó eszközökig terjednek;
- a kiberelrettentés, amely a legutóbbi időben megjelent – alapvetően stratégiai szinten jelentkező – kibereszközkészlet.

Kiberhadviselés

Az egyik legnagyobb fenyegetés, és talán nyugodtan kijelenthetjük, a jövőre nézve az egyik legnagyobb biztonságpolitikai kihívás a kiberhadviselés, így ennek rövid bemutatásával kezdjük a kibertéri kihívások elemzését.

A hadviselés folyamatos átalakulása nem új keletű dolog, hiszen a történelemben számos alkalommal láthattunk arra példát, hogy a korszerű eszközök és találmányok alapvetően alakították át a hadviselés addigi módszereit, de ugyanez igaz a társadalom átalakulására is, hiszen az is nagy hatással volt minden korban a hadviselésre. Persze ez fordítva is igaz, hiszen számos haditechnikai eszköz, amely megjelent a hadviselésben, később az élet számos területén bé-

később célok elérése vagy megvalósítása terén tűnt fel, például a civil alkalmazásban.

Ugyanakkor a 20. század végére és a 21. század elejére ez megváltozott. Már nem a haditechnikai fejlesztések és azok későbbi civil alkalmazása a jellemző, hanem fordítva, a civil fejlesztések és innovációk jelennek meg a katonai alkalmazásokban, amelyek nem mellesleg sokkal gyorsabban és rövidebb életciklussal követik egymást.

A kibertér és az azt megformáló információtechnológia azonban egy sosem látott mértékű változást hozott a hadviselésben. Ezt a forradalmi változást leginkább talán a *láthatatlan* és a *határtalan* jelzők jellemzik. Ugyanis ebben a térben nem látszik a támadó, nagyon sokszor nem látszik a támadás módszere sem, valamint a fizikai határok is csak nagyon nehezen értelmezhetők. Mindezeken túl a kiberhadviselés definíciós készlete sem alakult ki maradéktalanul eddig, hiszen – ahogy azt a későbbiekben látni fogjuk – a különböző országok még a kibertér definícióját is eltérő módon adják meg. Ennek megfelelően a kiberhadviselésre nagyon nehéz egységesen elfogadott meghatározást adni. Tegyük hozzá rögtön: *ma még.* Hiszen az már most is nagy bizonyossággal prognosztizálható, hogy az országok által támogatott kibertámadások számának növekedése és azok egyre súlyosabb következményei miatt hamarosan meg fog jelenni mind a különböző nemzetek, mind a NATO és az EU szótárában a kiberhadviselés többé-kevésbé egységes meghatározása.

Ezzel el is érkeztünk ahhoz, hogy ebben a térben megadjuk a kiberhadviselés legfőbb jellemzőit. Korábban számos kísérlet született a kiberhadviselés átfogó értelmezésére, amelyek közül az egyik – a 2011-ben született Haig, Kovács, Ványa által alkotott – megfogalmazás a következő: „Cyberhadviselésnek 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)

Ebben a megfogalmazásban azonban azon túl, hogy a *kiber* helyett az akkor használatos *cyber* idegen nyelvű kifejezés szerepel, még felfedezhető a hazai gondolkodás technikai alapú megközelítése, hiszen a szerzők ekkor még alapvetően nem mint biztonságpolitikai problémát, hanem mint katonai-műszaki kérdést és veszélyforrást azonosították a kiberhadviselést.

További probléma, hogy ebből a megközelítésből még alapvetően hiányzik az a tényező, amely napjaink legnagyobb veszélyévé teszi a kiberhadviselést. Ez pedig nem más, mint az, hogy kiberhadviselésről akkor beszélhetünk, amikor egy ország vagy országcsoport (esetleg ezekkel egyenértékű gazdasági vagy politikai hatalom) áll egy olyan kibertámadás, illetve kibertámadás-sorozat mögött, amelyek egy másik ország vagy országcsoport stratégiai fontosságú rendszerei ellen irányulnak.

Napjainkra sok olyan elmélet született, amely a kiberhadviselést a hagyományos hadviselés rendszerében helyezi el. Ezek között a legnagyobb átfedést az jelenti, hogy a hibrid jelzővel illetett, tehát a hagyományos hadviselési elemeket az újabb – nem konvencionális, de hadviselési célokra is alkalmazható – olyan tevékenységekkel, mint például a médiahadviselés vagy az általunk is említett politikai befolyásolás (akár a média felhasználásával, illetve annak csatornáin keresztül) eszközeit egyszerre alkalmazó, politikai és katonai célokat egyaránt elérni kívánó hadviselési keretek közé illesztik be a kiberhadviselést. (Fleming–Qualkenbush–Chapa 2017)

Ugyanakkor ez a hibrid jelző egyre inkább megfoghatatlan, és egyre inkább csak az olyan gyakorlati példákon keresztül érthető, mint az ukrajnai konfliktus. Azonban pont ezeken az eseteken 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 gazdasági és politikai értelemben vett fontosságára és jelentőségére már többször utaltunk a korábbiakban is, de később mind Kína, mind Oroszország esetében még vissza fogunk térni a kérdésre. Ám a kibertér és a demokrácia összefüggései, illetve a szabadságjogok korlátozásának, valamint esetenként más országok belügyeibe való beavatkozásoknak egyre sűrűsödő példáit látva szükséges egy látszólag nagyobb kitérőt tennünk a kiberbiztonság stratégiája felé haladó utunkon.

Erre a kis kitérőre pedig nem más vett rá minket, mint az, hogy Kofi Annan volt ENSZ-főtitkár egy meglehetősen éles kritikát fogalmazott meg a politika abbéli szándékával szemben, amely a szólásszabadságot és az internet szabadságát veszélyezteti, valamint az internet politikai – más államok befolyásolására irányuló – felhasználását célozza.

Annan 2018 februárjában a müncheni biztonságpolitikai konferencián elmondott beszédét nagyon sok sajtóorgánum közölte később. Az eredetileg *Az információtechnológia veszélyt jelent a demokráciára? (Has information technology become a threat to democracy?)* címmel megtartott beszédében a volt ENSZ-főtitkár kiállt a szólásszabadság, az internetes információ szabad áramlása és a demokrácia mellett. Ugyanakkor Annan abbéli véleményének adott hangot, amely szerint számos politikai vezető – és ebben sajnálatos módon vannak vezető globális hatalmak politikusai is – saját érdekei szerint és saját politikai előnyére használja, és ennek megfelelően kívánja átalakítani az internetet. Meg is nevez ezen országok közül néhányat: „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)

De persze a diplomata ellenpéldát is hoz: „Emlékezzünk 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)

Kofi Annan a demokrácia szemszögéből vizsgálja ezt a tevékenységet és ezeket a trendeket, majd felteszi a kérdést: ha a leginkább fejlett országok sem tudják megvédeni saját politikai és választási rendszerüket, akkor mit várhatunk a kevésbé fejlett országoktól?

A volt ENSZ-diplomata kitér a közösségi oldalak felelősségére is, hiszen az itt megjelenő vélemények óriási tömegekhez jutnak el nagyon rövid időn belül, és azonnal kifejtik befolyásoló hatásukat anélkül, hogy érdemi párbeszédre és érdemi vitára sor kerülhetne. Pedig – állítja Annan – ez lenne az igazi demokráciák alapja.

Kofi Annan írása nagyon jól rávilágít a kiberbiztonság legalapvetőbb összefüggéseire és mindazokra a részletekre is, amelyek a világon jelenleg mindenhol égető kérdésként merülnek fel. Az idézett írás is utal arra, hogy akár a terrorista propaganda, akár a politika, de akár a faji vagy a nemi gyűlöletbeszéd nagyon könnyen kiléphet a virtuális térből, és megjelenhet a fizikai dimenzióban, 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.

Ez ismét egy példa arra, hogy a kibertér biztonságának megteremtése minden országban és nemzetközi szinten is stratégiai kérdés kell, hogy legyen. Ugyanakkor a nemzeti válaszok, tehát az egyes országok saját útkeresése mellett meg kell, hogy jelenjen egy akár globális stratégiai elképzelés, amely mentén az előbb említett kihívások és veszélyek egységesen és nem utolsósorban hatékonyan kezelhetők.

Nyilvánvalóan ennek a stratégiának ki kell térnie a jelenlegi helyzetben megjelenő veszélyekre, ugyanakkor fel kell térképeznie a közeli és a távolabbi jövő lehetséges kihívásait is. Ennek megfelelően a stratégiának választ kell adnia nemcsak a jelenlegi problémákra, hanem a jövő potenciális kihívásaira is. A kibertér jellegénél fogva

ez nem történhet meg csak nemzeti szinten, így a nemzetközi, akár globális összefogás elengedhetetlen a kiberbiztonság megteremtése vagy legalább növelése érdekében.

Kiberfegyverek

A kiberfegyverek esetében nem a fizikai dimenzióban működő, a valódi fegyverek hatásmechanizmusához hasonló eszközökre kell gondolnunk, hanem olyan szoftver- és hardvereszközökre, valamint ezek kibertéri alkalmazására, amelyekkel a kijelölt célpontok számára valamilyen mértékű kár okozható.

Ilyen fegyverek bevetésére már számos esetben volt példa. Az egyik korai, de pont emiatt az egyik legnagyobb visszhangot kiváltó kiberfegyver az Anonymous hacktivistacsoporthoz[13] köthető. Az Anonymous a Wikileaks támogatása érdekében vetette be ezt a fegyvert 2010-ben, amikor a kiszivárogtatások miatt több pénzügyi szolgáltató – köztük a PayPal és a Mastercard – zárolta a Wikileaks számláit. Ezeket a támadásokat az Anonymous egy nem túl kifinomult, de annál hatásosabb fegyverrel, az úgynevezett *Low Orbit Ion Cannon* szoftver segítségével valósította meg, amely: „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)

Ugyanakkor a kiberfegyverek megjelenése, azaz az információszerzésre, illetve a támadásra használható szoftvereszközök alkalma-

[13] A hacktivistacsoportok nevüket a *hacker* és az *aktivista* szavak összevonásából kapták. Ezek azok a csoportosulások, amelyek valamilyen politikai vagy más ügy melletti szimpátiájukat hackertudásukkal fejezik ki, azaz rendszereket törnek fel, vagy azok működését akadályozzák, ezzel kifejezve egy ügy melletti elkötelezettségüket vagy éppen az azzal szembeni kritikájukat.

zása óhatatlanul is kiberfegyverkezési versenyhez vezet. Ahogy Bruce Schneier fogalmazott egyik írásában ezzel kapcsolatban még 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)

Schneier a nemzetközi együttműködésben kialakított szabályozásban látta akkor a kiberfegyverek jelentette, egyre növekvő probléma megoldását: „A nemzetközi együttműködés és a nemzetközi szerződések jelentik az egyetlen módot 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)

Ez a fajta együttműködés – ahogy Schneier is utal rá – csak nemzetközi egyezmények alapján valósulhat meg.[14] Ennek megfelelően ez be kell, hogy kerüljön az egyes országok nemzeti kiberbiztonsági stratégiáinak prioritásai közé is.

[14] A Microsoft ennek érdekében hirdette meg az úgynevezett digitális genfi konvenció (Digital Geneva Convention) kezdeményezést, amelynek fő célja a felhasználók állami támogatású kibertámadásokkal szembeni védelme érdekében kialakítandó nemzetközi összefogás. (Microsoft 2018)

Ez annál is inkább égető kérdés, mert a 2010-es iráni atomlétesítmények elleni Stuxnet támadás[15] óta a kiberhadviselésre tett definíciós próbálkozásainkban szereplő állami támogatású kibertámadás már nem is példa nélküli, hiszen ebben az esetben pont stratégai – ráadásul – politikailag kiemelt – célpontja volt a támadásnak. (Brown–Metcalf 2014)

Természetesen a fentiekben bemutatott eseteken kívül is számos példát láthattunk az elmúlt időszakban a különböző kiberfegyverek alkalmazására. Ilyen volt a NoPetya zsarolóvírussal[16] elkövetett támadássorozat is 2017-ben, amely, ellentétben a néhány héttel korábban világméretű pánikot és hatalmas károkat okozó WannaCry-jal, nem véletlenszerűen, hanem célzottan támadta meg áldozatait. A támadókkal nem lehetett kapcsolatot teremteni, mert a vírus által megadott egyetlen e-mail-cím azonnal elérhetetlenné vált, ahogy annak szolgáltatója tudomást szerzett az akcióról. Alternatív elérési lehetőséget pedig a vírus nem adott. Elemzők szerint többek között ez is közvetett bizonyíték arra, hogy nem a pénzszerzés volt a NoPetya célja. A vírus terjedése Ukrajnában volt a leglátványosabb, hiszen eredete egy ukrán könyvelői program frissítéséhez volt köthető, amely mögött sokan Oroszországot sejtik. (Ivanov–Mamedov 2017)

Kiberelrettentés

Későbbi elemzéseinkben, illetve a szintén később bemutatott nemzeti kiberbiztonsági stratégiák esetében látni fogjuk, hogy ezek közül

[15] 2010-ben (egyes források szerint már 2009-ben) feltételezhetően amerikai és izraeli segítséggel egy olyan féregvírussal elkövetett támadássorozat zajlott, amely a Stuxnet nevet kapta, és amely elsősorban Irán bushehri atomerőművének, illetve a natanzi urándúsító centrifugáinak ipari vezérlőszoftvereit és azok eszközeit – például a Siemens által gyártott PLC-ket (Programmable Logic Controller) – támadta. (Kovács–Sipos 2010)

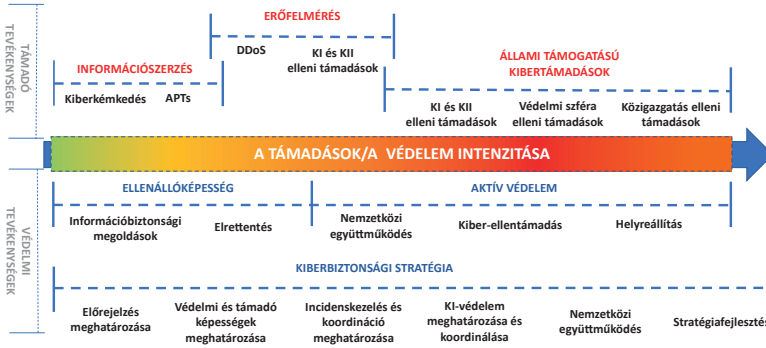
[16] A zsarolóvírusok – angol terminológiából eredő szóhasználattal ransomware-ek – a megfertőzött számítógépre jutva titkosítják a felhasználó fájljait. A titkosítás feloldásáért cserébe a támadó váltságdíjat kér, gyakran nehezen lenyomozható kriptovalutában.

sokban megjelenik az elrettentés, illetve a kiberelrettentés mint olyan eszköz, amellyel nyilvánvalóan nemcsak a kiberbiztonság, hanem közvetett módon az adott ország nemzeti biztonsága is garantálható, legalábbis bizonyos szintig.

A kiberelrettentés nagyon sok esetben levezethető a nemzeti biztonsági stratégiákban szereplő – elsősorban a katonai erő és az így megjelenő támadó képességek jelentette – fizikai elrettentésre vonatkozó megfogalmazásból. Ilyen, az elrettentést explicit módon tartalmazó doktrína az Egyesült Államok Nemzeti Védelmi Doktrínája. Az elrettentés a védelmi doktrína mellett az Egyesült Államok Védelmi Minisztériuma által kiadott kiberbiztonsági stratégiában is megjelenik: „A fokozódó fenyegetés, amellyel szembenézünk, szükségessé teszi, hogy a Védelmi Minisztérium hozzájáruljon egy átfogó kiberelrettentési stratégia kidolgozásához és végrehajtásához, annak érdekében, hogy megakadályozza a legfontosabb állami és nem állami szereplőket az amerikai érdekek elleni kibertámadások elkövetésében." (US DoD Cybersecurity Strategy 2015)

Ebben a kontextusban a kiberelrettentés nem jelent mást, mint egyrészt olyan kibervédelmi megoldások kialakítását az adott országban, amelyek áttörése nem, vagy csak komoly erőforrások segítségével lehetséges, másrészről olyan kibertámadó képességek kiépítését és felmutatását,[17] amelyek egy adott ellenséges kibertámadásra válaszul alkalmazhatók a támadóval szemben.

[17] Ez a felmutatás történhet indirekt módon úgy is, hogy a kiberbiztonsági stratégiába bekerül az *elrettentés* fogalma.



1. ábra

A kiberhadviselés lehetséges műveleteinek időbeni lefolyása és azok lehetséges elemei

Forrás: a szerző szerkesztése

A kiberelrettentés az USA mellett számos más ország nemzeti kiberbiztonsági stratégiájában is megjelenik. Ezekben visszatérő elem az azon képességek kiépítésére vonatkozó igény is, amellyel az ilyen elrettentést meg is lehet valósítani. Ilyen stratégia például az Egyesült Királyság Nemzeti Kiberbiztonsági Stratégiája, amely ezzel kapcsolatban a következőket fogalmazza meg: „A kibertér egy olyan szféra, amelyben meg kell védenünk érdekeinket és szuverenitásunkat. Ahogyan a fizikai dimenzióban tett lépéseink is relevánsak a kiberbiztonság és az elrettentés szempontjából, úgy a kibertéri cselekvéseinknek is hozzá kell járulniuk a szélesebb nemzeti biztonságunkhoz.” (Egyesült Királyság 2016)

Ugyanakkor néhány kutató felhívja a figyelmet arra a tényre, hogy az elrettentés nem szükségszerűen működik minden esetben. Erre utal Burton egyik tanulmányában, amelyben többek között Oroszország Krím félszigetet érintő annektálását hozza fel példaként: „A Putyin-kormány akciói alapvető kihívásként értelmezhetők a hidegháború utáni európai rend számára. Ezek az akciók az elrettentés kudarcát is jelzik.” (Takács 2017, idézi: Burton 2018)

Kissé árnyalják azonban a képet az olyan kibertéri akciók, mint amelyeket egyes elemzések szerint szintén Oroszország követett el 2015, majd 2016 telén. Ezekkel az akciókkal az ukrajnai villamosenergia-rendszer irányítását támadták.

2015. december közepén az egyik ukrán regionális villamosenergia-elosztó és villamosenergia-átviteli vállalat rendszereit megtámadták, és a cég számítógépeibe, valamint SCADA (Supervisory Control and Data Acquisition, azaz felügyeleti, irányító és adatgyűjtő) rendszereibe is behatoltak. A támadók hét 110 kV-os, valamint közel kéttucatnyi 35 kV-os alállomást értek el a rendszerirányító cég számítógépein keresztül, majd ezek segítségével lekapcsolták a területen a villamosenergia-szolgáltatást. A támadások ezek után több más rendszerirányító cégre is kiterjedtek, amelyek során az áramszolgáltatásban bekövetkezett kiesések miatt közel 225 ezer fogyasztó nem jutott áramhoz. (SANS 2016)

Ahogy a későbbiekben látni fogjuk, bár nincsenek egyértelmű bizonyítékok a támadások elkövetőivel szemben, és gyakran nem is lehet a támadók kilétét megállapítani, ezek a támadások mégis szolgálhatják az elrettentés céljait. Még ha vannak is politikai vagy gazdasági veszteségek, ezekben a támadásokban nem a károkozás az igazi cél, hanem sokkal inkább annak a demonstrálása, hogy a támadó – alapvetően állami támogatással – technikailag képes azokat megvalósítani és kivitelezni. Így a kibertámadások és persze nem utolsósorban azok hatásainak bemutatása stratégiai kommunikációs célt és bizonyos fokú elrettentést is jelent.

1.2. A kiberbiztonság stratégiájának általános elvei

A kiberbiztonság számos kapcsolódó területet meghatároz. Ennek megfelelően nyilvánvalóan nemcsak a szűkebb értelemben vett kiberbiztonság és annak stratégiája, hanem – ahogy arra a definíciós készlet meghatározásakor már utaltunk – az olyan kapcsolódó területek, mint a kritikus

infrastruktúra, illetve a kritikus információs infrastruktúra-védelem vagy akár a kiberbűnözés elleni tevékenység áttekintése is szükséges.

Mindezeken túl fontos hangsúlyozni azt a korábban már megállapított tényt is, hogy nagyon sokszor a digitális gazdaság és digitális társadalom fejlettsége paradox módon együtt jár a kiberbiztonság felértékelődésével. Minél fejlettebb digitális gazdasággal és társadalommal rendelkezik egy adott ország vagy akár egy régió, annál inkább ki van téve a kibertérből érkező fenyegetéseknek. Ebből következően a fejlett digitális infrastruktúrával és digitális gazdasággal rendelkező országok természetszerűleg nagyobb figyelmet kell, hogy fordítsanak a kibertér védelmére. A paradoxon pedig pont ebben van: a technológia fejlődésével egyenes arányban kellene fejlődnie a kiberbiztonságnak is, de ez ma még koránt sincs így.

Ugyanakkor egy adott ország kiberbiztonsági stratégiájának számos olyan kérdést is tartalmaznia kell, amely a stratégia eredeti céljain jóval túlmutat. Ilyenek lehetnek a stratégiában megfogalmazott olyan kérdések, amelyek az adott ország biztonsági stratégiájának támogatására, az abban foglalt célok eléréséhez mintegy kiegészítő kül- vagy belpolitikai eszközkészletet adnak. Erre utal Valeriano, Jensen és Maness a kiberstratégiáról írt könyvükben: „A kiberműveletek inkább kiegészítik az állam hagyományos eszközeit, semmint leváltják azokat. Úgy találjuk, hogy a kibereszközök a külpolitikai eszközkészlet hozzáadott adalékanyagaként szolgálnak a modern stratégiai versenyben." (Valeriano–Jensen–Maness 2018)

A fentieknek megfelelően könyvünk következő fejezetében áttekintjük a legfontosabb nemzetközi szervezetek, mint például az ITU, az Európai Unió Hálózat- és Információbiztonsági Ügynökség (European Union Agency for Network and Information Security, ENISA), illetve a NATO Kiberbiztonsági Kiválósági Központ (Co-operative Cyber Defence Centre of Exellence, CCDOE) különböző, a kiberbiztonsági stratégiákat meghatározó, azok alapjaira, célszerű felépítésére és egyes esetekben implementációjára adott javaslatait és ajánlásait.

A kiberbiztonság megteremtése csak rendszerben képzelhető el, azaz egy adott ország vagy az említett nemzetközi szervezetek biztonsági stratégiai elképzelései egyik pillérét kell, hogy képezzék a kiberbiztonságra irányuló stratégiai prioritások. Ahogy egy ország esetében is az alkotmányból vagy az alaptörvényből, illetve az ott megfogalmazott nemzeti értékek és érdekek védelméből eredeztethető, illetve vezethető le a nemzeti biztonsági stratégia, úgy a nemzeti biztonsági stratégia pillérei a különböző ágazati stratégiák. Ilyen ágazati stratégia lehet például a katonai stratégia, a kiberbiztonsági stratégia, az energiabiztonsági stratégia vagy akár a gazdaságbiztonsági stratégia. Ez természetszerűleg nemcsak egy országra, hanem a különböző nemzetközi szervezetekre is igaz.

Ennek megfelelően a nemzetközi ajánlások tanulmányozása előtt szükséges áttekintenünk, hogy a stratégiai dokumentumok rendszere általában milyen felépítésben jelenik meg, milyen stratégiák, doktrínák és jogszabályok mentén határozható meg és alakítható ki a biztonság egy adott országban.

1.2.1. A stratégiai dokumentumok rendszere

Mielőtt belevágnánk a kiberbiztonság stratégiájának, illetve annak nemzeti szinten meghatározó jelentőségű elemeinek ismertetésébe, érdemes nagyon röviden áttekinteni, hogy mit is jelent a *stratégia* kifejezés. Ez azért is fontos, mert ha a stratégia mögöttes tartalmát meg szeretnénk ismerni, szükséges magának a kifejezésnek a pontosabb ismerete, hiszen enélkül a kiindulópontunkat sem lennénk képesek jól meghatározni.

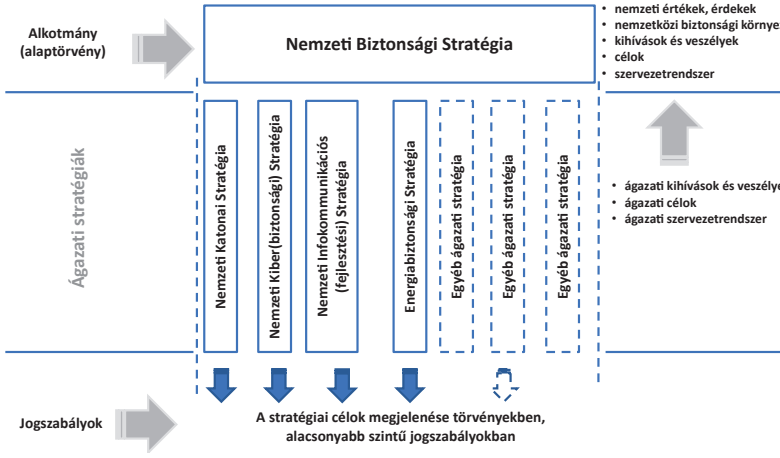
A *stratégia* szó, illetve maga a fogalom az ókori görög időkből, a *stratēgos* kifejezésből származtatható, jelentése: a legfőbb katonai vezető. Nagyon sokáig a katonai hadműveletek megtervezésének és a katonai csapatok tervszerű mozgatásának jellemzésére használták a stratégia kifejezést.

Természetesen az idő előrehaladtával már nemcsak katonai területen, hanem például a gazdaságban és a vállalatok vezetésében, irányításában is helyet kapott ez a fogalom.

Amíg tehát korábban a stratégia alapvetően és majdnem kizárólag csak a katonai terület meghatározó fogalma volt, addig ez mára alaposan megváltozott. Amennyiben a stratégia államok közötti kapcsolatrendszerét vagy annak biztonságpolitikai vonatkozását kívánjuk feltárni, akkor nagyon jó összefoglalását kapjuk mindennek a következő gondolatban: „Modern 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)

Ma már a stratégiai dokumentumok viszonylag jól körülhatárolható rendszerét tudjuk megadni, és egymáshoz való viszonyukat is fel tudjuk vázolni. A stratégiai dokumentumok egyik legmagasabb szintjét az adott nemzet érdekeinek és értékeinek meghatározása adja, amelyet általában az adott ország alaptörvényében, illetve alkotmányában is rögzítenek. Ezek azok a legfontosabb tényezők, amelyek érvényre juttatása, valamint folyamatos védelme az egyik legfontosabb prioritás az adott ország szemszögéből. Nyilvánvalóan a nemzetközi környezetben az adott ország érdekei és értékei, azok elérése, megvédése vagy biztosítása csak más országokkal való különböző interakciók útján képzelhető el. Ez azt is jelenti, hogy az erre utaló szándék, azaz annak definiálása, hogy milyen nemzetközi politikai és/vagy gazdasági környezetben és együttműködési rendszerben kíván egy adott ország élni, szintén meg kell, hogy jelenjen a legfelső szintű stratégiai dokumentumban. Ez a dokumentum legtöbbször nem más, mint a nemzeti biztonsági stratégia. Ebben a stratégiában az adott ország rögzíti mindazon értékek és érdekek védelmét, amelyeket az alkotmányban meghatároztak. Ezt követően e stratégia megvizsgálja azt a környezetet, amelyben ezeket az értékeket és érdekeket érvényesíteni szükséges. Ez magában kell, hogy foglalja azoknak a kihívásoknak

és veszélyeknek a számbavételét és értékelését is, amelyek az említett értékeket és érdekeket, illetve azok elérését befolyásolhatják.



2. ábra

A stratégiai dokumentumok rendszere

Forrás: a szerző szerkesztése

Természetesen 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 azokban foglaltakat.

1.2.2. A kiberbiztonsági stratégia általános felépítése: nemzetközi ajánlások

Az előzőekben bemutatott visszásságok, azaz például az a tény, hogy nemhogy nemzetközileg egységesen elfogadott meghatározások nem

léteznek a kibertérre és annak biztonságára vonatkozóan, de az országok többségében még csak nem is találunk egyértelmű definíciós készletet minderre, szükségessé teszi, hogy megvizsgáljuk azokat az eszközöket, amelyeket a kiberbiztonságra vonatkozó stratégiai elképzelések – azaz a nemzeti szintű kiberbiztonsági stratégia megalkotása, majd bevezetése és a stratégiában foglaltak alapján a kiberbiztonság rendszerének működtetése során – mégis egységesen alkalmazhatók.

Ehhez segítségül hívjuk a NATO CCDCOE,[18] az ENISA,[19] valamint az ITU[20] egy-egy olyan tanulmánygyűjteményét, amelyek egyrészt tudományos módszerekkel filozófiai alapokat nyújtanak, másrészt meghatározzák azoknak az ajánlásoknak a halmazát, amelyek célszerűen egy nemzeti biztonsági stratégia részét kell, hogy képezzék.

[18] A NATO CCDCOE egy olyan kutatóközpont és koordináló szervezet egyben, amely a kibertér jogi kérdéseitől kezdve a technikai védelem megvalósításáig számos területen ajánlásokat és javaslatokat dolgoz ki a szövetségnek és a tagálamoknak egyaránt. Magyarország 2010 óta a kiválósági központ teljes jogú tagja. (CCDCOE 2018)

[19] Az Európai Unió egyik legfontosabb kiberbiztonsági szervezete az ENISA, amely 2004-es alapítása óta részt vesz a nemzeti CSIRT-ek (Compurter Security Incident Response Team, azaz számítógép-vészhelyzeti reagálócsoport) együttműködésének szervezésében, és azok képességeinek fejlesztéséhez szintén hatékonyan hozzájárul. Az ENISA fontos szerepet tölt be a tagállamok nemzeti kiberbiztonsági stratégiáinak kialakítása során, mert konzultációs szervezetként a nemzetközi jó gyakorlatokkal és tanácsokkal járul hozzá azokhoz. Az ENISA központja Krétán, Heraklionban van, de az ügynökség egy athéni operatív irodával is rendelkezik. (Enisa 2017a)

[20] Az ITU az ENSZ távközlésre szakosodott szervezete, amelynek fő feladata a távközlés és az IKT (Infokommunikációs Technológia) szektorok nemzetközi koordinációja. A 193 országot és több mint 800 akadémiai, valamint gazdasági szervezetet tagjai sorában tudó ITU három nagy szakmai részre tagozódik: az ITU-R-re (ITU Radiocommunication Sector), azaz a rádikommunikációért felelős szervezetre, az ITU-T-re (ITU Telecommunication Standardisation Sector), azaz a nemzetközi telekommunikáció egységesítéséért és szabványosításáért felelős szervezetre, valamint az ITU-D-re (ITU Development Sector), azaz a nemzetközi infokommunikációs fejlesztésekért felelős szervezetre. (ITU 2017a)

Az ENISA ajánlásai: avagy hogyan készítsünk nemzeti kiberbiztonsági stratégiát?

A korábbiakban felvázolt kérdések egész sora arra késztette az ENISA-t, hogy azonosítsa a már meglévő nemzeti kiberbiztonsági stratégiákban azokat a közös elemeket, amelyek alapjai lehetnek egy olyan modellnek, amelyre építve egységes és rádadásul hatékony válasz adható a kiberbiztonsági kihívásokra. (ENISA 2012)

Ezt a célt konkrétan meg is fogalmazta a szervezet: „Ebben az összefüggésben az ENISA számos olyan konkrét intézkedést határozott meg, amelyek megvalósulása koherens és holisztikus nemzeti kiberbiztonsági stratégiát eredményez." (ENISA 2012)

Annak érdekében, hogy a kibertér folyamatosan változó jellege, a mind technikai, mind politikai értelemben egyre megújuló, új és még újabb kihívások ellenére egy ország megfelelő módon legyen képes válaszokat adni a kibertérben megjelenő fenyegetésekre, az államoknak rugalmas és dinamikus kiberbiztonsági stratégiákra van szükségük. Ehhez természetszerűleg a kibertér jellegéből adódóan a nemzetközi együttműködés elengedhetetlen, hiszen olyan tényezőkre kell figyelemmel lenni, mint a nyitottság, a globális jelleg, a kézzelfogható (ország)határok hiánya stb.

Nyilvánvalóan a nemzetközi együttműködés egyik alapfeltétele, hogy az országok olyan kiberbiztonsági irányelvekkel, valamint az azokat végrehajtani is képes szervezeti rendszerrel rendelkezzenek, amelyeket átfogó stratégiákban rögzítettek. Ugyanakkor egy átfogó terminológiai egységesítés is üdvös lenne, mert ahogy nap mint nap megállapítjuk, és ahogy arra az ENISA is rámutatott a 2012-ben kiadott ajánlásgyűjteményében, az országok még az olyan egyszerűnek tűnő fogalmak alatt is mást értenek, mint például a kibertér. Az pedig, hogy a terminológia is eltér, nagyban befolyásolja a nemzeti kiberbiztonságról alkotott elképzeléseket is. (ENISA 2012)

Mindezekhez az ENISA az említett iránymutatás-gyűjteményében pontról pontra végigvette, hogy melyek lehetnek a leginkább

célravezető lépések egy nemzeti szintű kiberbiztonsági stratégia kialakításához. A dokumentumnak akár a *Hogyan készítsünk nemzeti kiberbiztonsági stratégiát?* címet is adhatnánk.

Az iránymutatás egyes elemeinek kifejtése után az akkor már meglévő nemzeti szintű kiberbiztonsági stratégiákból a dokumentum példákat is hoz, amelyeket jó gyakorlatként mutat be. (ENISA 2012)

Az ENISA a kiberbiztonságot meghatározó stratégiát egy olyan, két fázisból álló életciklushoz hasonlítja, amelyben az első fázis a stratégia megalkotása és bevezetése (majd nyilvánvalóan az abban megfogalmazott elvi, jogszabályi és szervezeti keretrendszer szerinti működtetése), majd a második fázis a stratégia felülvizsgálata, fejlesztése és az így levont következtetések és tapasztalatok alapján a stratégia szükségszerű átalakítása. (ENISA 2012)

Ez nagyban hasonlít ahhoz a PDCA-elvhez,[21] illetve -modellhez, amelyet egyébként számos nemzetközi minőségbiztosítási, illetve információbiztonsági szabvány és ajánlás is követ. Ilyen például az ISO/IEC 27001-es nemzetközi szabvány, amely az információbiztonság-irányítási rendszer kialakítására, bevezetésére és annak fejlesztésére fogalmaz meg ajánlásokat. (ISO 27001)

Az említett két fázist az ENISA különböző megközelítésekben látja kivitelezhetőnek. Az első megközelítés olyan lineáris gondolkodásmódot követel meg, amely szerint a kiberbiztonságra vonatkozó stratégiát a korábban említett szakaszokban kell végrehajtani, azaz ki kell dolgozni a stratégiai dokumentumot, végre kell hajtani az abban foglaltakat, majd értékelni kell az eredményeket, és végezetül meg kell azt szüntetni, vagy le kell cserélni egy új stratégiára. A második megközelítés sokkal inkább hasonlít egy életciklus-alapú megközelítésre,

[21] *PDCA:* Plan, Do, Check, Act, azaz 'megtervezni, végrehajtani, ellenőrizni, beavatkozni' modell, amely eredetileg PDSA volt (amelyben az *S* jelentése 'study', azaz 'tanulmányozni, következtetéseket levonni'), és Edward Denning vezetéselméleti tudós nevéhez fűződik. Ugyanakkor az eredeti PDSA-modellt Japánban az 1950-es években kissé átalakítva már PDCA-modellnek hívták. (Moen é. n.)

amely szerint az értékelési szakasz eredményeként megjelenő tapasztalatokat a stratégia fenntartására vagy ha kell, akkor annak kisebb-nagyobb módosítására kell felhasználni. Ugyanakkor létezik egy harmadik – hibrid – megközelítés is, amely alapján több folyamatos fejlesztési ciklust kell létrehozni különböző szinteken, és ezeket nemcsak, hogy harmonizálni kell egymással, de szükségszerűen az egymásra gyakorolt hatásukat is figyelembe kell venni. (ENISA 2012)

A kiberbiztonság stratégiájának kialakítása során az ENISA ajánlásában húsz, logikusan egymásra – és nem utolsósorban az említett PDCA-modellre épülő – lépést mutat be, amelyek a következők:

1. A stratégia hatókörének (annak, hogy mire vonatkozik a stratégia, mely területeket fedi le), céljainak és prioritásainak meghatározása.
2. Nemzeti szintű kockázatértékelési módszertan kialakítása és meghatározása.
3. A meglévő szakpolitikák, szabályzók és képességek felmérése.
4. Világos irányítási struktúra kialakítása.
5. Az érintettek azonosítása és bevonása.
6. A megbízható információmegosztási mechanizmusok létrehozása.
7. Kiberbiztonsági vészhelyzetkezelési tervek kidolgozása.
8. Kiberbiztonsági gyakorlatok megszervezése.
9. Alapszintű biztonsági követelmények megállapítása.
10. Kiberincidensek jelentési mechanizmusainak kialakítása.
11. Az állampolgárok információbiztonsági tudatosságának növelése.
12. A kiberterületen folytatott K+F tevékenység ösztönzése.
13. A kiberképzési és -oktatási programok bevezetése és ösztönzése.
14. Incidenskezelési képességek kialakítása, fejlesztése.
15. A kiberbűnözés elleni hatékony fellépés és tevékenység kialakítása.

16. A kiberbiztonság területén nemzetközi együttműködésekben való aktív részvétel.
17. A köz- és magánszféra közötti partnerség kialakítása.
18. Az állampolgárok jogainak tiszteletben tartása és a biztonsági intézkedések közötti egyensúly megteremtése.
19. A kiberbiztonságra vonatkozó értékelési séma (rendszer) kidolgozása, bevezetése és alkalmazása.
20. A nemzeti kiberbiztonsági stratégia finomhangolása. (ENISA 2012)

Ezeknek az ajánlásoknak megfelelően a kiberbiztonság stratégiájának kialakítása során az első lépés nyilvánvalóan a legfontosabb célok meghatározása kell, hogy legyen. Ezeket a célokat priorizálva, hierarchikus rendszerben célszerű megadni. Az ENISA a célok meghatározásához feladatokat is hozzárendel, amelyek a következőek:

- Meg kell határozni a stratégia legfontosabb célját és azokat a területeket, amelyekre a stratégia vonatkozik. Mindezekhez egy időintervallumot is célszerű hozzárendelni, azaz szükséges annak meghatározása, hogy az adott stratégiai célok mennyi időn belül érhetőek el. Ez általában 5–10 évet jelent.
- Meg kell határozni a stratégia hatálya alá tartozó üzleti szektorokat és szolgáltatásokat.
- Átfogó nemzeti kockázatértékelést kell végezni a stratégia céljainak és hatókörének meghatározásához.
- A társadalomra, a gazdaságra és a polgárokra gyakorolt hatást tekintve prioritásokat kell kitűzni.
- Figyelembe kell venni a jelenlegi szabályozási és működési környezetet.
- A folyamat elejétől kezdődően az érdekelt feleket meg kell nyerni a stratégiai célkitűzések támogatására.
- A stratégia végrehajtásához ütemtervet kell felállítani, amely célszerűen a következő lépésekből kell, hogy álljon:

– olyan konkrét tevékenységeket kell meghatározni, amelyek megfelelnek a stratégia célkitűzéseinek, és a stratégia végrehajtására vonatkozó akciótervet kell kidolgozni;
– a stratégia végrehajtására, értékelésére és fenntartására vonatkozó irányítási (keret) rendszert kell kialakítani;
– konkrét cselekvési tervet kell kidolgozni minden egyes tevékenységre;
– meg kell határozni és ki kell alakítani a stratégia értékelésének főbb lépéseit, illetve annak szervezeti elemeit feladatokkal együtt. Azaz meg kell határozni, hogy mely kulcsfontosságú teljesítménymutatót kinek kell értékelnie. (ENISA 2012)

Nem túl meglepő módon az ENISA ajánlása a kockázatelemzéssel kapcsolatosan is megfogalmaz számos feladatot. Ez azért nem meglepő, mert az információbiztonság szervezeti szinten való kialakítása során ez ma már nemcsak, hogy elvárás, hanem kötelező érvényű feladat. A nemzeti szintű kockázatelemzés során külön ki kell térni a kritikus infrastruktúrákra, valamint a kritikus információs infrastruktúrákat fenyegető kockázatokra, mert ezek a területek lesznek nemzeti szinten a stratégiai jelentőségű tényezők. A kockázatelemzést egy kockázatkezelési tervnek, illetve az arra vonatkozó külön stratégiának kell követnie. (ENISA 2012)

A kockázatkezelési stratégia a kritikus infrastruktúrák vonatkozásában ágazati megközelítésű kell, hogy legyen. Ennek kialakításához az ENISA szintén számos javaslatot fogalmazott meg, amelyek első körben a kritikus ágazatok meghatározását, majd az ágazatspecifikus védelmi tervek kialakítását igénylik. Ennek során a következő feladatokat kell végrehajtani:

• azonosítani kell a társadalom és a gazdaság megfelelő működéséhez szükséges kritikus eszközöket és szolgáltatásokat (ez feleltethető meg a szervezetre vonatkozó információbiztonság során alkalmazott kockázatelemzés során a vagyonelemek felmérésének);

- fel kell mérni a kritikus eszközöket érintő összes kockázatot, be kell sorolni azokat hatásuk szerint, és lehetőség szerint meg kell becsülni azok bekövetkezési valószínűségét;
- egyeztetni kell azokkal a magánszektorbeli érdekeltekkel[22] is akik érintettek ezen infrastruktúrák, illetve elemek tulajdonlásában és/vagy működésében, és meg kell osztani velük a kockázatelemzés eredményeit, valamint ha szükséges, akkor korrigálni kell azokat az érdekeltek megállapításaival;
- meg kell határozni a kezelendő kockázatok körét, azaz ki kell jelölni azokat a kockázatokat, amelyek mérsékelhetők, de még vállalhatók, illetve meg kell határozni azokat a kockázatokat, amelyek már nem vállalhatók, és így már nem is kezelendők (nyilvánvalóan annak megadásával és indoklásával, hogy mindennek mi az oka, azaz milyen tényezőket vett figyelembe az adott döntéshozó, amikor ezeket a kockázatokat megjelölte);
- egy olyan nemzeti kockázati nyilvántartást kell kidolgozni, amely rögzíti az azonosított kockázatokat, és amely nyilvántartás folyamatos naprakészsége biztosított, és amelyben így megjelennek a legújabb és legfrissebb kockázatok is;
- az újonnan megjelenő, illetve a potenciális fenyegetések és sebezhetőségek folyamatos megfigyelésére egy szervezett, nemzeti szintű (megfelelő nemzetközi kapcsolatrendszerrel rendelkező) folyamatot kell kialakítani, amelyhez nyilvánvalóan egy szervezetrendszer is kell, hogy társuljon. (ENISA 2012)

A legfontosabb célok meghatározása és a kockázatelemzés után, a kiberbiztonság területén megvalósítani kívánt célok részletes megha-

[22] Itt szükséges megjegyezni, hogy a kritikusinfrastruktúra- és kritikus információs infrastruktúra-védelem területén az egyik legnagyobb kihívás, hogy az ágazatok, illetve alágazatok egyes rendszerei (esetenként azok többsége) nem állami, hanem magántulajdonban vannak. Ennek megfelelően a tulajdonosok, illetve az említett üzemeltetők bevonása a kockázatelemzés folyamatába nemcsak, hogy szükséges, de egyben elkerülhetetlen feladat is.

tározása előtt fontos a jelenlegi helyzet felmérése, amelybe beleértendő a jelenlegi szabályozási környezet is. Az ENISA ajánlásában ehhez tipizált feladatokat rendelt hozzá. Ezek a feladatok a következő területekre kell, hogy kiterjedjenek:

- meg kell határozni és fel kell mérni az elmúlt években a kiberbiztonság vagy kapcsolódó területein született szabályozásokat, illetve jogszabályokat (ilyen szabályozások lehetnek az információbiztonság, az elektronikus kereskedelem vagy akár az adatvédelem területén);[23]
- azonosítani kell a különböző ágazatokban eddig alkalmazott összes szabályozási intézkedést és azok hatását a kiberbiztonság szintjének emelésére (ilyenek például az elektronikus hírközlési ágazatban kötelező incidensjelentések és azok hatásai);
- fel kell mérni a már működő kiberbiztonsági kihívások kezelésére kialakított és már meglévő képességeket (például nemzeti vagy kormányzati CERT-eket);
- fel kell mérni az egyéb, már meglévő szabályozó mechanizmusokat (például a köz- és a magánszféra közötti partnerségi kapcsolatokat), majd ezeket abból a szempontból kell értékelni, hogy azok milyen mértékben érték el céljaikat, azaz milyen mértékben járultak hozzá a kiberbiztonság szintjének emeléséhez;
- elemezni kell a már meglévő kiberbiztonsági politikákkal, szabályozásokkal és műveletekkel foglalkozó állami szervek szerepét és felelősségi körét (például az energiaszabályozó hatóságokat, az elektronikus hírközlési hatóságokat, az adatvédelmi hatóságokat, a nemzeti számítógépes bűnözési központokat), majd azonosítani kell az ezek közötti felelősségi körökben és esetlegesen a hatósági jogkörökben meglévő átfedéseket vagy éppen hiányosságokat;

[23] Az ENISA ajánlása itt hangsúlyozza, hogy ezeknek a szabályozásoknak, de kiemelten a kiberbiztonság nemzeti szintű szabályozásának összhangban kell lennie a nemzeti biztonságot meghatározó dokumentumokban – nevezetesen az adott ország nemzeti biztonsági stratégiájában – megfogalmazott célkitűzésekkel.

- fel kell mérni, hogy a meglévő szakpolitikai, szabályozási és működési környezet milyen mértékben felel meg a stratégia célkitűzéseinek és hatókörének, valamint azonosítani kell a fennálló hiányosságokat. (ENISA 2012)

Az ENISA mindezen lépések megtételét követően egy világosan átlátható, letisztult felelősségi és hatáskörökkel rendelkező kormányzati, a kiberbiztonság különböző területeit átlátni, ott hatékony szabályozási és beavatkozási lépéseket megtenni képes struktúra kialakítását javasolja. Ugyanakkor a stratégia kialakításához – annak teljes életciklusát menedzselő – kormányzati koordináló szerv vagy munkacsoport kijelölése, illetve (ha kell) létrehozása szükséges.

Természetesen ennek a munkacsoportnak a felállításához és munkájához is eligazítást ad az ENISA, amelyet a következőkben foglal össze:

- meg kell határozni, hogy ki a felelős a stratégia kialakításának az irányításáért és annak értékeléséért. Itt célszerű a nemzeti kiberkoordinátort erre a feladatra kinevezni (felkérni), hiszen – bár országonként eltérő módon, de – rendszerint ő az a személy, aki a legmagasabb szintű felhatalmazással (például miniszterelnöki vagy a kiberbiztonságért felelős miniszteri kinevezéssel) látja el az adott országban a kibertérben megjelenő érdekelt felek – az állami szereplők, a magánszféra, az akadémiai szféra – közötti egyeztetéseket és koordinációt;
- meg kell határozni az irányítási struktúrát. Ennek során egy olyan tanácsadó testületet kell létrehozni, amely tanácsokat ad a stratégiával kapcsolatosan a kiberkoordinátor számára. Ezen kívül meg kell határozni az érintett és a munkába bevonni kívánt kormányzati és magánszektor szereplőit. Ez általában a nemzeti kiberbiztonsági koordinációs tanácson keresztül történik, amelyben mind a köz-, mind a magánszektor képviselteti magát. Mindezt úgy célszerű megtenni, hogy a munkába bevont résztvevők a kiberbiztonság legszélesebb spektrumát fedjék le;

- deklarálni kell a felállított tanácsadó testület mandátumát (annak szerepét, felelősségét, folyamatait, döntési jogát) és feladatait (ilyen feladatok például a nemzeti kockázatkezelés, a felmerülő veszélyek értékelése, a kritikus helyzetekre történő reagálás, a nemzetközi együttműködést elősegítése stb.);
- meg kell határozni (vagy meg kell erősíteni) a kiberbiztonság politikájának és szabályozásának kezdeményezéséért és fejlesztéséért felelős szervezetek mandátumát és feladatait. E lépés során figyelemmel kell lenni arra, hogy ezek a szervezetek hogyan hatnak egymásra, és hogyan járulnak hozzá a tanácsadó testület munkájához;
- ki kell alakítani a nemzeti – azaz stratégiai fenyegetések és sebezhetőségek feltárásáért és azok összegyűjtéséért (monitorozásáért) felelős – szervezeteket, majd meg kell bízni őket a feladattal. A fenyegetések feltárása mellett a kibertámadásokra való reagálásra (incidenskezelésre), valamint a válságkezelés megerősítésére is ügyelni kell, úgy, hogy ez a szervezet is hozzá kell, hogy járuljon a tanácsadó testület munkájához, illetve közreműködjön abban. Ilyen szervezetek célszerűen a nemzeti incidenskezelési központ(ok) és/vagy a nemzeti (kritikus) információs infrastruktúrák védelmét ellátó szervezetek;
- elemezni kell és meg kell határozni a meglévő, országos kiberbiztonsági és incidensreagáló csoportok (CERT-ek) szerepét mind a köz-, mind a magánszférában. A nemzeti vagy kormányzati CERT feladata lehet a felügyeleti tevékenységek mellett az információmegosztás, illetve a kritikus információs infrastruktúrák védelme. A CERT-ek kulcsszerepet játszhatnak a más, hasonló szervezetekkel való együttműködésben és információcserében nemzeti és nemzetközi szinten egyaránt. (ENISA 2012)

Ahhoz, hogy a kialakítandó kiberbiztonsági stratégia végrehajtható és sikeres is legyen, sok összetevőre van szükség. Ezek közül

a fentiekben ismertetett ENISA-ajánlás számos szükséges tényezőt felsorolt. Ezeken kívül talán az egyik legfontosabb kérdés a kiberbiztonság megteremtésében és kialakításában, valamint annak folyamatos fejlesztésében érdekelt felek azonosítása. Bár ezt már a korábbiakban is láthattuk, az említett ajánlásgyűjtemény ehhez célszerű feladatokat is hozzárendelt. A felek azonosítása után szükséges az ő bevonásuk a stratégia kialakításába, és szükséges annak megvalósítása során a partneri, együttműködői viszony kialakítása és fenntartása.

Ahogy a már többször idézett ajánlásgyűjtemény fogalmaz: „Az állami érdekeltek általában politikai, szabályozási és működési mandátummal rendelkeznek. Biztosítják a nemzet kritikus infrastruktúráinak és szolgáltatásainak biztonságát. A kiválasztott magánentitásoknak is célszerű a fejlesztési folyamat részét képezniük, mivel valószínűleg ők a legfontosabb információs infrastruktúrák és szolgáltatások tulajdonosai." (ENISA 2012)

Ez azonban azonnal rávilágít egy komoly problémára is. Ez pedig nem más, mint a kritikus infrastruktúrák és kritikus információs infrastruktúrák tulajdonosi, illetve üzemeltetői struktúrája. Az említett rendszereknek, illetve rendszerelemeknek csak egy bizonyos hányadát tulajdonolja az állam vagy állami háttérrel rendelkező vállalat, és ugyanez igaz ezen rendszerek üzemeltetőire is. A kérdés ebben az esetben az, hogy a szabályozásba hogyan lehet bevonni a magánvállalkozásokat, amelyek első körben nyilván ebben ellenérdekelt felek lesznek, hiszen a kiberbiztonsággal (információbiztonsággal, kritikus infrastruktúrák és kritikus információs infrastruktúrák védelmével) kapcsolatos bármilyen tevékenység és szabályozás, illetve az azokban megfogalmazottak megvalósítása plusz erőforrásokat igényel akár a tulajdonos, akár az üzemeltető részéről.

Ugyanakkor a sikeres kiberbiztonsági stratégia kialakítása és az azzal kapcsolatos tevékenységek végrehajthatósága érdekében be kell vonni a magánszférát is, és törekedni kell a velük való együttműködésre. Ennek során lehetséges annak a tudatosítása, hogy önmagában egy-egy tulajdonos vagy üzemeltető a legmagasabb szintű

védelem kialakítása mellett sem lesz képes a rendszerek interdependenciájának, azaz a rendszerek vagy rendszerelemek egymásra hatásának a semlegesítésére. Ezért szükséges az együttműködés és a közös tevékenység, valamint a lehetőleg állami szinten koordinált védelem. Abban az esetben, ha a stratégiaalkotás folyamatába már annak kezdetén bevonják a magánszektor érdekelt feleit, akkor valódi együttműködés és végső soron magasabb kiberbiztonság érhető el.

Mindezek érdekében a következő feladatokat célszerű végrehajtani:

- a kritikus infrastruktúrák és szolgáltatások tulajdonosainak azonosítása;
- meg kell határozni azokat a közigazgatási szereplőket, akik a kiberbiztonsági politika és szabályozás kezdeményezéséért és fejlesztéséért felelősek, és akiknek megvannak a magánszférában lévő partnereik (ilyenek lehetnek például a telekommunikációs terület hatósági szervei, akiknek a magánszférabeli partnerei nyilvánvalóan a telekommunikációs cégek vagy a nemzeti infrastruktúrák védelmének központi szervei, illetve hatóságai, akiknek a magánszféra részéről a partnerei a kritikus infrastruktúra magántulajdonosai és/vagy üzemeltetői lesznek);
- mind a köz-, mind a magánszféra érdekelt feleit be kell vonni a stratégiaalkotás folyamatába, úgy, hogy egyértelműen meg kell határozni a szerepüket és a felelősségüket is. Például ilyen feladat- és felelősségikör-meghatározás lehet, ha tisztázódik, hogy a magánszféra megvédi (akár állami segítséggel) az infrastruktúráját, de közös felelősségük van a nemzetbiztonság területén;
- ki kell dolgozni azt az ösztönzőrendszert, amely alapján biztosítható mind a magán-, mind a közszféra érdekeltjeinek részvétele a stratégiai folyamatokban. Itt nyilvánvalóan a köz- és a magánszféra akár egymásnak ellentmondó érdekeit is figyelembe kell venni (lásd korábbi megjegyzésünket). (ENISA 2012)

A megfelelő érdekelteket a nemzeti szintű kiberbiztonsági stratégia egyes szakaszaiba a megfelelő időben és a megfelelő módszerrel

célszerű bevonni. Amennyiben minden érdekelt fél látja a stratégiaalkotás és -végrehajtás során a saját szerepét és nem utolsósorban azokat az előnyöket, amelyek ebből a számára megjelennek, akkor nyilvánvalóan elkötelezettek lesznek annak kialakítása és végrehajtása során. Amennyiben ez az elkötelezettség kialakul, abban az esetben az együttműködés is könnyebbé vállhat a magán- és a közszféra között. Ebben az együttműködésben a kormánynak is nagy szerepe van, hiszen már a stratégiaalkotás során is a kormány lesz az, aki a legfontosabb célokat kijelöli. Mindezek mellett a kormány lesz az is, aki akár a hazai, akár a nemzetközi együttműködés során a célok eléréséhez szükséges tevékenységek kereteit megadja.

Az ENISA ajánlása is kitér a civil társadalom és a civil szervezetek bevonásának szükségességére, amelyet már a kiberbiztonsági stratégia megalkotása során célszerű megtenni. A civil társadalom hatalmas szerepet játszik a stratégia végrehajtása során is. Ebben az állampolgárok részéről jelentkező biztonságtudatosság meghatározó, hiszen a kibertérben az egyik legfontosabb szereplő maga az állampolgár, legyen szó annak az állammal (például e-kormányzati szolgáltatás igénybevétele útján), a magánszektorral (például vásárlás esetén) vagy a kritikus infrastruktúrával kapcsolatos interakciójáról (annak bármely ágazatát vagy alágazatát vagy akár csak egyik rendszerelemét használva). Ennek megfelelően a biztonságtudatosság növelése már állampolgári szinten is stratégiai jelentőségű. Amennyiben az állampolgárok, azaz a kibertér legfontosabb szereplői[24] jobban megértik a kiberteret érintő kockázatokat, fenyegetéseket és veszélyeket, akkor lehetőség van arra, hogy – ahogy az ENISA-ajánlás is fogalmaz – proaktív módon intézkedéseket hozzanak a kockázatok csökkentésére vagy azok enyhítésére. (ENISA 2012)

[24] Az állampolgárok ebben az értelemben azért nevezhetőek a kibertér legfontosabb szereplőinek, mert az Európában jelenleg átlagosnak tekinthető 80%-os internetpenetráció mellett az állampolgárok azok, akik a legtöbbször – ráadásul a legvédtelenebb módon – használják a kiberteret és annak legkülönfélébb szolgáltatásait.

Az is nyilvánvaló, hogy akár az állampolgárok biztonságtudatosságának növelését, akár a köz- illetve a magánszféra érdekeltjeinek valódi együttműködésre való hajlandóságát nagymértékben növeli a megfelelő információáramlás. A megbízható információmegosztási rendszer kialakítása, amelyben minden érdekelt fél – természetesen a rá vonatkozó mértékig – hozzáférhet, illetve megkaphatja a kiberbiztonsággal kapcsolatos szükséges információkat, nagyban hozzájárulhat ahhoz, hogy a kiberbiztonsági kihívásokról és veszélyekről az érdekelt felek időben tudjanak tájékozódni. Ez az információáramlási rendszer lehetőséget ad arra is, hogy amennyiben ebben helyet kap valamilyen kibertéri korai előrejelző rendszer, akkor annak adatai – feldolgozás és szanitizálás[25] után – az érdekeltekhez eljussanak, így akár a felkészülés, akár az incidenskezelés – amelyekben egyébként rendszerint az idő az egyik legfontosabb tényező – megfelelő módon megtörténhessen. Természetszerűleg az információmegosztási rendszerbe a különböző kormányzati szerveket – mint például a nemzetbiztonsági szolgálatokat, a CERT-eket, illetve amennyiben működnek, akkor a nemzeti kiberkoordinációs testületet vagy tanács munkacsoportjait – is célszerű bevonni.

Ahogy az ENISA ajánlása is fogalmaz, szükséges a nemzeti kiberbiztonsági stratégia részét képező úgynevezett nemzeti kiberkészenléti tervet vagy terveket (National Cybercontingency Plan, NCP) készíteni, amelyek alapján a kritikus információs infrastruktúrákat érintő, súlyos kiberbiztonsági események kezelhetők, és amelyek mentén azok működőképessége visszaállítható. Ennek a tervnek – azon túl, hogy része kell, hogy legyen a nemzeti kiberbiztonsági stratégiának – a nemzeti készenléti tervekbe is bele kell illeszkednie, hiszen nagyon sok olyan terület van, amelyet érint, és amelyre hatással van egy esetleges nemzeti szintű kiberbiztonsági esemény. Ehhez a tervhez definiálni kell, hogy mit jelent

[25] A szanitizálás az információnak a forrásától való elválasztását jelenti, ami kizárja, hogy az információ forrására vagy annak különböző paramétereire vonatkozó következtetéseket lehessen levonni.

a súlyos kiberincidens, és melyek azok a területek – alapvetően stratégiai fontosságuk miatt –, amelyeket szükséges a kiberkészenléti terv hatálya alá vonni. Mivel minden fejlett infrastruktúrával rendelkező ország rendelkezik azok védelmére, illetve védelmi célú felkészítésére vonatkozó valamilyen szintű és típusú tervvel, ezért a kiberkészenléti terveknek ezekkel harmonizálniuk kell. (ENISA 2012)

Ezeknek a terveknek csakúgy, mint az említett információmegosztási rendszernek, hasonlóan a kiberbiztonsági stratégia többi eleméhez, a gyakorlatban is kipróbált módon kell működniük. Ehhez célszerű kiberbiztonsági gyakorlatokat szervezni és végrehajtani. Ezekkel a gyakorlatokkal kapcsolatosan az ENISA ajánlása a következőket fogalmazza meg: „A gyakorlatok lehetővé teszik az illetékes hatóságok számára, hogy teszteljék a meglévő vészhelyzeti terveket, rámutassanak a konkrét hiányosságokra, fokozzák az együttműködést a különböző ágazatok között, azonosítsák a kölcsönös függőségeket, előmozdítsák a működésfolytonosság tervezésének javítását, és kialakítsák az együttműködés kultúráját a rugalmasság növelése érdekében. A kibergyakorlatok fontos eszközül szolgálnak annak felmérésére, hogy az adott közösség menynyire felkészült a természeti katasztrófák, a technológiai hibák, a kibertámadások és a vészhelyzetek kezelésére.” (ENISA 2012)

A nemzeti kiberbiztonsági stratégiának tartalmaznia kell az alapvető biztonsági követelményeket is. E követelményeknek mind az állami, mind a magánszervezetek számára kötelező érvényűnek kell lenniük. Kialakításuk azonban meglehetősen összetett feladat, hiszen számos olyan tényezőt kell figyelembe venni, mint például a szervezetek eltérő technikai és technológiai fejlettsége, azok nagysága, összetétele (állami vagy nem állami szféra), a különböző ágazatok számára már meglévő, de eltérő biztonsági sztenderdek stb. Ugyanakkor ezen alapvető biztonsági követelmények alapján az érintett szervezeteknek a releváns kockázatokkal és sérülékenységekkel szemben a szükséges (kiber)védelmi intézkedéseket az elvárt szinten meg kell tenniük. Az ENISA-ajánlás szerint ezek a biztonsági követelmények az adott iparág által széles körben elismert, meglévő hazai vagy nemzetközi biztonsági szabványokon, ajánlá-

sokon vagy jó gyakorlatokon célszerű, hogy alapuljanak. Ezek az adott ágazatra vonatkozó alapszintű biztonsági követelmények meghatározzák azt a minimális biztonsági szintet is, amelynek az ágazat valamennyi szervezetének meg kell felelnie.

A kiberbiztonsági stratégia ki kell, hogy térjen a kiberincidensek jelentési mechanizmusainak kialakítására is. Az esetleges incidensekről szóló információknak nagyon fontos szerepe van a hatékony védelem kialakításában, illetve azok elemzése után a későbbi incidensek elkerüléséhez – esetlegesen azok következményeinek legalább csökkentéséhez – szükséges felkészülésben. Az időtényező, ahogy korábban említettük, ebben az esetben kiemelten fontos, hiszen minél gyorsabban lehet egy-egy incidens esetén annak forrásáról, felépítéséről, támadási mechanizmusáról vagy a megtámadott entitásokról reális képet alkotni, annál hatékonyabb lehet az adott támadással szemben alkalmazott incidenskezelés is. A későbbi incidensekre való felkészülésben, illetve az ezekre irányuló hatékony reagálóképesség kialakításában szintén nagy szerepe van az információáramlásnak.

Az információáramlási rendszer kialakítása mellett, azzal bizonyos átfedésben szükséges az állampolgárok információbiztonsági tudatosságának növelése. Ennek során meg kell tanítani akár az egyéni felhasználókat, akár a munkavállókat azokra a releváns fenyegetésekre – azok felismerésére, kezelésére, bekövetkezésük esetén a következmények csökkentésére –, amelyekkel a különböző infokommunikációs eszközök, rendszerek és szolgáltatások használata során találkozhatnak. Ez a tanítás azonban nem egy egyszeri folyamat, hiszen az újabb és újabb kiberbiztonsági veszélyek megjelenése azt is megköveteli, hogy az állampolgárok figyelmét újra és újra ráirányítsuk ezekre a veszélyekre, illetve azok elkerülésének módjaira. Az információbiztonsági tudatosság növelésére sok eszköz és megoldás létezik a különböző médiakampányoktól kezdve a személyre vagy adott szolgáltatásra szabott figyelmeztetéseken át az iskolarendszerű oktatásig.

Ezek mellett szükséges a kiberképzési és -oktatási programok bevezetése, amelyre már stratégiai szinten is utalni kell. Ez egyrészt

a már említett biztonságtudatosság növeléséhez járulhat hozzá, másrészt annak a hatalmas problémának a kezeléséhez, amely a kiberbiztonsággal foglalkozó szakemberek jelenleg tapasztalható hiányából ered. Ennek megfelelően a nemzeti kiberbiztonsági stratégiának tartalmaznia kell az arra vonatkozó elképzelést – és ennek akár stratégiai célként meg is kell jelennie –, hogy az adott ország milyen módon kívánja a terület szakembereinek utánpótlását biztosítani. Természetszerűleg ennek átfedésben és szoros együttműködésben kell lennie az adott ország felső- és szakoktatási stratégiájával.

Az oktatásra és képzésre vonatkozó stratégiai elképzelések mellett kiemelten fontos a K+F tevékenység ösztönzése. Ennek a kiberbiztonsági vetülete az, amelyet a stratégiába be kell építeni. A stratégiai céloknak tartalmazniuk kell az arra vonatkozó elképzeléseket, hogy a különböző IKT-eszközök és -rendszerek tervezése és gyártása során a biztonság hangsúlyosan jelenjen meg, legyen szó az alkalmazás során a potenciális veszélyekkel szembeni ellenálló képességről vagy akár a felhasználók személyes adatainak védelméről.

A stratégia fontos elemét képezik az incidenskezelési képességek kialakítására és fejlesztésére vonatkozó célok. Ennek során a nemzeti, illetve kormányzati CERT-ek kialakítása és fejlesztése kulcsfontosságú. Ezek a szervezetek azok, amelyek képesek nemzeti szinten koordinálni az incidensek kezeléséhez szükséges szervezeteket. Mindezeken túl a nemzeti CERT-ek tartják a kapcsolatot más országok nemzeti vagy a nemzetközi szervezetek incidenskezelési központjaival.[26] (ENISA 2012)

Hasonlóan fontos feladat a kiberbűnözés elleni hatékony fellépés és tevékenység kialakítására irányuló stratégiai elképzelések

[26] A nemzeti, illetve a kormányzati incidenskezelő csoportok legfontosabb képességei kialakításához az ENISA már 2009-ben kiadott egy ajánláscsomagot, amelyben az egyik legfontosabb problémára kívánnak választ adni, amely a tagországokban meglévő, nagyon eltérő incidenskezelési képességek területén jelentkezik. Az eltérő képességek ugyanis nagyban akadályozzák, hogy megfelelő hatékonysággal lehessen kezelni a kibertér jellegéből adódó – határokon átnyúló – kiberincidenseket. (ENISA 2018)

és célok megjelenítése a kiberbiztonsági stratégiában. Ahogy a különböző kiberincidensek kezelése során, úgy a kiberbűnözés elleni tevékenység során is elengedhetetlen a nemzetközi együttműködés, hiszen ezen a területen is jellemző az, hogy nem léteznek a hagyományos értelemben meglévő fizikai határok. Meg kell azonban jegyezni, hogy paradox módon a nemzetközi térben megjelenő kiberbűnözés elleni jogszabályi környezet ezt mintha nem venné tudomásul.

A már említett nemzetközi együttműködés a kiberbiztonság számos egyéb területén is elengedhetetlen abból az egyszerű tényből kiindulva, amelyet a kiberbiztonság tárgyalásakor már említettünk, nevezetesen hogy a kiberbiztonsági kihívások és veszélyek többsége nemzetközi. Ennek megfelelően az ezekre adandó válaszok csak nemzetközi együttműködési keretben képzelhetők el. A kiberbiztonsági stratégiának tehát tartalmaznia kell azt is, hogy mindezek milyen eljárásrendszerben valósíthatók meg az adott ország vonatkozásában. Az Európai Unió 2016-ban megjelent úgynevezett NIS-irányelve, amelyet a későbbeikben részletesen is bemutatunk, ehhez kötelező érvényűen nemzeti kapcsolattartó pont kijelölését is meghatározza. (NIS Directive 2016)

Az ENISA ajánlásgyűjteménye a kiberbiztonsági stratégiával kapcsolatosan különösen nagy hangsúlyt fektet a köz- és a magánszféra közötti partnerség (Public Private Partnership, PPP) kialakítására. Ennek során közös célok és akciótervek kialakítását szorgalmazza a dokumentum, amelyek alapján a PPP-ben megvalósuló tevékenységek a biztonság és az ellenálló képesség különböző szempontjaira összpontosíthatnak. Ezek közül a legfontosabbak a következők:

- elrettentés (a támadók visszatartása érdekében);
- védelem (új fenyegetések és az azokkal szembeni tevékenység felkutatása);
- észlelés (információcsere az új fenyegetések kezelésére);
- reagálás (annak érdekében, hogy az adott szervezet képes legyen kezelni az eseményt már annak kezdetén);

- helyreállítás (az esetlegesen bekövetkezett támadások következményeinek felszámolása). (ENISA 2012)

Az ENISA megállapítja, hogy az ilyen konstrukcióban kialakított együttműködés például a kritikus infrastruktúrák védelme során már bizonyított. (Ne feledkezzünk meg arról a korábban már megállapított tényről, hogy a kritikus infrastruktúrák az egyik olyan terület, ahol jellemzően nem állami tulajdonosokat, illetve üzemeltetőket találunk.) (ENISA 2012)

A 21. század biztonsági környezetében az egyik legnagyobb kihívás az állampolgárok jogainak tiszteletben tartása és a biztonsági intézkedések közötti egyensúly megteremtése. Akár a kiberbűnözés elleni tevékenység, akár a terrorizmus elleni intézkedések során az állampolgárok személyiségi jogai nagyon sokszor komolyan sérülhetnek, hiszen a mindenre kiterjedő adat- és információgyűjtés sokszor a személyes adatok olyan kezelését is magával hozza, amelyről az állampolgárok nem is biztos, hogy tudnak. Ilyenek lehetnek a biometrikus adatok vagy akár a közösségi oldalak használata során a felhasználóról gyűjtött adatok. Az Európai Unió nagy hangsúlyt fektet erre a kérdésre, és ennek érdekében számos olyan közösségi szabályozás is született, amely biztosíthatja az állampolgári személyes adatok kezelésének elvárható szintjét. Talán ebben a kérdésben az egyik legfontosabb szabályozó az EU általános adatvédelmi rendelete (General Data Protection Regulation, GDPR), amely többek között a kibertérben megjelenő magán- és személyes adatok kezelésére ír elő – minden európai uniós tagország számára – kötelező szabályokat.[27] (ENISA 2012; 2016/679 EK európai parlamenti és a tanácsi rendelet)

Az ENISA 2016 novemberében felülvizsgálta a fentiekben többször idézett, a nemzeti kiberbiztonsági stratégiákra vonatkozó ajánlás-

[27] Az Európai Parlament és az Európai Tanács 2016 áprilisában fogadta el a GDPR-t (General Data Protection Regulation), amely az EU általános adatvédelmi rendelete. A 2018. május 25-én életbe lépő GDPR óriási változást hozott az adatvédelem területén minden uniós országban, de hatásait tekintve számos más térségben is. (2016/679 EK európai parlamenti és a tanácsi rendelet)

gyűjteményét. Ebben már figyelembe vették 17 ország[28] (16 EU-tagország, és az EFTA-státusszal rendelkező Svájc) meglévő és esetenként frissítésen, illetve módosításon átesett nemzeti kiberbiztonsági stratégiáját. Az új útmutató a 2012-es tanulmány eredményeire építve, az eltelt időszak tapasztalatait figyelembe véve ad eligazítást a nemzeti kiberbiztonsági stratégiák kialakításához, bevezetéséhez és fenntartásához. Az első ajánlásgyűjtemény óta eltelt időszak tapasztalatait a vizsgált országok kiberbiztonsággal foglalkozó hatóságainak képviselői, nemzeti kiberbiztonsági szakértői, illetve a tagországok egyéb – releváns – hatóságainak képviselői biztosították az ENISA számára. (ENISA 2016)

A frissített ajánlásgyűjteményben az ENISA egy, a kiberbiztonsági stratégiára vonatkozó életciklust határozott meg, amelyet négy fő fázisra osztott. Az első fázis a stratégia kialakítása, azaz a stratégia kifejlesztésének fázisa. A második életciklusszakasz a stratégia bevezetése és működtetése. A harmadik lépcső az értékelési szakasz, majd ezt követi a fenntartási fázis. Mind a négy fázishoz tartozik visszacsatolás is, amely során a stratégia folyamatos fejlesztése az egyik legfontosabb prioritás. Ezek a visszajelzések lehetőséget (de ugyanakkor a stratégiáért felelős szervezet számára feladatokat is) jelentenek, hiszen rendszeres időközönként felül kell vizsgálni és frissíteni kell a stratégiát, valamint frissíteni kell az akcióterveket is. (ENISA 2016)

[28] Ez a 17 ország a következő volt: Ausztria, Belgium, Bulgária, Horvátország, Dánia, Észtország, Finnország, Franciaország, Görögország, Magyarország, Írország, Luxemburg, Málta, Szlovénia, Spanyolország, Svédország, illetve EFTA-országként Svájc. (ENISA 2016)

3. ábra

Az ENISA nemzeti kiberbiztonsági stratégiák életciklusára kiadott ajánlása

Forrás: ENISA 2016, a szerző szerkesztése

Az eredeti, 2012-es ajánlás még 20 lépést tartalmazott a kiberbiztonsági stratégia kialakításához, bevezetéséhez, illetve annak hatékony fenntartásához, de az a fenti életciklusból csak az első két fázisra koncentrált. (Igaz ez még akkor is, ha nyilvánvalóan az említett 20 lépésből álló tevékenységsorozat a stratégai értékelésének és fenntartásának fázisához ad eligazítást, és azokban is alkalmazható.).

Ugyanakkor a 2016-os, frissített kiadás már egy jóval letisztultabb és sok tekintetben strukturáltabb rendszert mutat be. Ebben már az említett életciklusszakaszokra bontva találhatók meg az ajánlott feladatok, amelyek egy valóban működő és hatékony nemzeti kiberbiztonsági stratégiához szükségesek. Ráadásul időközben az Európai Unióban egy igen markáns szabályozás is megszületett, amely nem más, mint a NIS-direktíva (NIS Directive – Network and Information Systems Directive, azaz hálózat és információs rendszerek irányelv). Erről később az Európai Unió kiberbiztonsági stratégiai szabályozása kapcsán részletesen is szólunk majd. A NIS jellegénél és az EU-s tagországokra nézve kötelező érvényű volta miatt meg kell, hogy jelenjen a nemzeti kiberbiztonsági stratégiákban is. Így az ENISA 2016-os ajánlása már tartalmazza az e direktíva bevezetése és végrehajtása szem-

pontjából legfontosabb olyan tennivalókat, amelyeket a nemzeti szintű kiberbiztonsági stratégiában szükséges rögzíteni.

1. táblázat

A nemzeti kiberbiztonsági stratégia lehetséges összetevői az ENISA-ajánlás alapján

Terület/fázis	*Az ENISA ajánlása szerint szükséges tevékenység*
1. fázis: a nemzeti kiberbiztonsági stratégia megtervezése és kialakítása	A stratégia hatókörének (annak, hogy mire vonatkozik a stratégia, mely területeket fedi le), 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
2. fázis: a nemzeti kiberbiztonsági stratégia implementálása (bevezetése)	Kiberbiztonsági vészhelyzetkezelési tervek kidolgozása
	A kritikus információs infrastruktúrák védelme
	Kiberbiztonsági gyakorlatok megszervezése
	Alapszintű biztonsági követelmények megállapítása
	Kiberincidensek jelentési mechanizmusainak kialakítása
	Az állampolgárok információbiztonsági tudatosságának növelése
	A kiberképzési és -oktatási programok bevezetése és ösztönzése
	A kiberterületen folytatott K+F-tevékenység 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 közszféra intézményei közötti együttműködés intézményesítése
	A magánszektor kiberbiztonsági területekbe való befektetésének ösztönzése

Terület/fázis	*Az ENISA ajánlása szerint szükséges tevékenység*
3. fázis: a nemzeti kiberbiztonsági stratégia értékelése	A kiberbiztonságra vonatkozó értékelési séma (rendszer) kidolgozása, bevezetése és alkalmazása
	A fő teljesítménymutatók (KPI) rendszerének kidolgozása
4. fázis: a nemzeti kiberbiztonsági stratégia fenntartása	A nemzeti kiberbiztonsági stratégia finomhangolása a főbb teljesítménymutatók eredményeinek felhasználásával
	A stratégia folyamatos fejlesztése

Forrás: ENISA 2016, a szerző szerkesztése

Ahogy korábban már utaltunk rá, az új ajánlásgyűjtemény a kiberbiztonsági stratégia életcikluselemei közül már nemcsak a stratégia megalkotására és bevezetésére, hanem a stratégia alapján működő szervezetek, folyamatok és azok hatásainak értékelésére és fenntartására is nagy hangsúlyt fektet. A stratégia értékelése során egy úgynevezett fő teljesítménymutató rendszer (Key Performance Indicator, KPI) kialakítását és bevezetését javasolja az ENISA. E teljesítménymutatók alapvetően a stratégia legfontosabb céljainak elérését hivatottak mérni. Ezek alapján lehetséges annak felmérése, hogy a legfontosabb célkitűzések közül melyeket sikerült elérni, és melyek elérése nem, vagy nem a megfelelő módon történt meg.[29]

Ehhez a munkához az ENISA szintén készített egy ajánlásgyűjteményt, amely *A kiberbiztonsági stratégiák értékelésének keretrendszere* címet viseli, és a nemzeti kiberbiztonsági szakpolitikát tervező, végrehajtó és értékelő szakértők és kormányzati tisztviselők számára készült. A dokumentumban megfogalmazottak szerint ennek a célja egy olyan rugalmas és pragmatikus eszközkészlet kialakítása, amely alapvetően sokkal inkább a főbb filozófiai elveket határozza meg a stratégiában foglaltak végrehajtásának felmérésére, semmint a kötelező érvényűen végrehajtandó ellenőrző listákat. Az ENISA által kidolgozott értékelési keretrendszer egy olyan logikai modellt mutat be, amely különböző lépéseken keresztül veszi végig a lehetséges teljesít-

[29] Meg kell jegyezni, hogy az ajánlásgyűjtemény ezen indikátorok alapján az említett országok vonatkozásában el is végezte a legfontosabb stratégiai célok megvalósulásának értékelését, amelyet térképes formában be is mutatott. Hazánk ebben az értékelésben, ha nem is kiemelkedően, de meglehetősen jól szerepelt. (ENISA 2016)

ménymutatókat (KPI-ket). Ezek az ajánlott KPI-k az értékelési modell célkitűzéseihez lettek hozzárendelve, megkönnyítve ezzel az érdekeltek számára, hogy prioritásuk alapján kiválasszák a számukra leghasznosabbakat. A teljesítménymutatók minőségi, és nem mennyiségi mutatók. (ENISA 2014)

A mutatókat öt nagy csoportra osztotta az ENISA, amely csoportokban az adott mérendő, illetve értékelendő terület főbb mutatói kaptak helyet. Ezek a csoportok a következők:

- a kibervédelmi politikák és képességek fejlesztése;
- a kiberellenálló képesség elérése: képességek és hatékony együttműködés kialakítása az állami és a magánszektorban;
- kiberbűnözés csökkentése;
- a kiberbiztonság ipari és technológiai alapjainak (hátterének) fejlesztése;
- biztonságos kritikus információs infrastruktúra. (ENISA 2014)

A következő táblázatokban az öt fő indikátorcsoport mérendő részterületeit mutatjuk be.

2. táblázat

Az ENISA nemzeti kiberbiztonsági stratégiára megadott fő teljesítménymutatói a kibervédelmi politikák és képességek fejlesztése területen

Fő teljesítménymutató	*Mérendő terület (tények, bizonyítékok)*
A kibervédelemre vonatkozó stratégiai nemzeti terv (doktrína, fogalmak, érdekelt felek, konkrét feladatok) létezése	Egy ilyen terv, illetve tevékenységi jelentések, cselekvési tervek és felelősségek lehatárolásának létezése és státusza
Az uniós kibervédelmi kezdeményezésekben való részvétel mértéke (képességfejlesztés)	A részvétel jelzése, a részvétel szintje
A katonai CERT (milCERT) azonosítása és felépítése, annak a katonai politikában (stratégia, doktrína) való megjelenési szintje	Kapacitásértékelések; dokumentumok (stratégia, doktrína); belső működési dokumentumok
A képzés megléte (a szükséges személyi feltételekkel) és annak hatása	Kapacitásértékelések; dokumentumok; belső működési dokumentumok

Fő teljesítménymutató	*Mérendő terület (tények, bizonyítékok)*
Interoperabilitás (milyen mértékben van együttműködés a kibervédelmi képességekben a katonai területen kívül)	Kapacitásértékelések; dokumentumok; belső működési dokumentumok
Együttműködéssel és új eszközökkel megnövelt ellenálló képesség a katonai kibertámadásokkal szemben (gyorsabb észlelés, válaszadás és helyreállítás a kifinomult támadásokkal szemben, költséghatékony fejlesztés az együttműködésen keresztül, megfelelő és elérhető kommunikációs csatornák)	Kapacitásértékelések; incidensjelentések; tevékenységjelentések

Forrás: ENISA 2014, a szerző szerkesztése

3. táblázat

Az ENISA nemzeti kiberbiztonsági stratégiára megadott fő teljesítménymutatói a kiberellenálló képesség elérése: képességek és hatékony együttműködés kialakítása az állami és a magánszektorban területen

Fő teljesítménymutató	*Mérendő terület (tények, bizonyítékok)*
CERT-ek és/vagy nemzeti biztonsági ügynökségek felállítása	Ezeknek az intézményi szereplőknek a megléte és megbízatása (hatásköre, mandátuma)
A köz- és a magánszféra együttműködése (PPP) a kiberbiztonsági területen	Ezeknek az együttműködéseknek az azonosítása, szerkezete, a bevont szervezetek és azok szerepe, tevékenységjelentések
Kockázatok és veszélyek feltérképezése	Kockázatelemzés, fenyegetéselemzés (a CERT-ek vagy a nemzeti biztonsági ügynökségek vezetésével)
Nemzeti szintű kiberbiztonsági gyakorlatok létezése	Tevékenységjelentések
Továbbfejlesztett képességek: szervezett tréningek a köz- és magánszektor számára, kölcsönös képzések (workshopok és konferenciák)	Tevékenységi jelentések, események címei, részt vevő vállalatok/érdekeltek
A végfelhasználók tudatosságát növelő tevékenységek (anyagok, kampányok, események)	A felhasználók számára kiadott anyagok, kampányok/események szervezése, az állampolgárok biztonságtudatosságának felmérése
Nemzeti koordinációs intézkedések a nemzeti kiberbiztonság területén (nemzeti biztonsági ügynökségek)	Tevékenységi jelentések, megbízások, együttműködési tevékenységek

Fő teljesítménymutató	*Mérendő terület (tények, bizonyítékok)*
A fejlett válaszkészségek megléte (reagálási-helyreállítási tervek, korai figyelmeztető rendszerek stb.)	Védelmi, észlelési, reagálási, visszaállítási tervek, korai figyelmeztető rendszerek és szimulációs modellek, tevékenységi jelentés
A nyilvános informatikai rendszerek biztonságának növelése	Sérülékenységvizsgálatok (CERT vagy nemzetbiztonsági ügynökség jelentései), a szoftverfrissítések/-javítások gyakoriságának dokumentáltsága, azok végrehajtása, az IKT-rendszerek biztonsági szabványainak elfogadása, bevezetése

Forrás: ENISA 2014, a szerző szerkesztése

4. táblázat

Az ENISA nemzeti kiberbiztonsági stratégiára megadott fő teljesítménymutatói a kiberbűnözés csökkentése területen

Fő teljesítménymutató	*Mérendő terület (tények, bizonyítékok)*
A kiberbűnözés csökkentésére irányuló nemzeti intézményi keretek (például rendőrségi szervezetek, CERT-ek)	Strukturált és dokumentált keretrendszer
Rendőrségi szervezetek fejlesztése (hiányfelmérés, szükségletek azonosítása, technika jelenlegi állása, bevált gyakorlatok alkalmazása)	Azonosított hiányosságokról szóló dokumentáció, valamint az ezek csökkentésére irányuló tevékenységekkel támogatott kiberbűnözés elleni rendőrségi szervezetek, a képességek felmérésének dokumentációja, a legjobb gyakorlatok jegyzéke, a folyamatok dokumentálása
Az EC3, a CEPOL, a Eurojust és más tagállamokkal történő együttműködési mechanizmusok megléte	Tevékenységjelentések és közös akciók
Nemzeti kiberbűncselekmények adatbázisa	Rendőrségi statisztikák a kiberbűncselekményekről (nyomozások száma, megoldott esetek száma stb.)
Nemzetközi együttműködés (a kiberbűnözés elleni, határokon átnyúló küzdelem fokozása; a korszerű eszközökhöz való hozzáférés; alacsonyabb költségek)	A határokon átnyúló kiberbűncselekmények elleni nyomozások száma, statisztikai adatai, költségvetések
Biztonságosabb kibertér minden felhasználó számára	Statisztikai adatok

Forrás: ENISA 2014, a szerző szerkesztése

5. táblázat

Az ENISA nemzeti kiberbiztonsági stratégiára megadott fő teljesítménymutatói a kiberbiztonság ipari és technológiai támogatása területen

Fő teljesítménymutató	*Mérendő terület (tények, bizonyítékok)*
A szabványosítás, valamint a megbízhatósági és biztonsági címkék fejlesztésének támogatása	A szabályozó hatóságok által bevezetett biztonsági szabványok, ellenőrzések és tanúsítási mechanizmusok betartása, szabványok elfogadási aránya és biztonsági címkék megléte
A kutatás finanszírozása EU-s és nemzeti kutatási programok felhasználásával	EU-kutatásiprojekt-adatbázisok, tudományos finanszírozásra szakosodott ügynökségek megléte
Új intézkedések kidolgozása a kiberbiztonság keresleti oldalára (például beszerzésekre)	Politikák és kormányzati IKT-követelmények megléte
Az e-kereskedelem innovációjának és költséghatékonyságának támogatása	Innovatív e-kereskedelmi megoldások bevezetése és megléte
A vásárlók szélesebb körű hozzáférése a biztonságos technológiához	Piackutatási jelentések

Forrás: ENISA 2014, a szerző szerkesztése

6. táblázat

Az ENISA nemzeti kiberbiztonsági stratégiára megadott fő teljesítménymutatói a kritikus információs infrastruktúra területen

Fő teljesítménymutató	*Mérendő terület (tények, bizonyítékok)*
A kritikus információs infrastruktúrák azonosítása, azaz a kritikus eszközök, sebezhetőségek, függőségek, kockázatok felmérése	A nemzeti kritikus információs infrastruktúrák listája, a nemzeti kritikus eszközök és azok függőségeinek listája, kockázatok és sebezhetőségi nyilvántartások (CERT, kormányzati ügynökség, nemzeti biztonsági hatóság megléte)
Kockázatértékelési és kockázatkezelési eljárások/tervek	A követendő feladatok és eljárások megosztása (beleértve a frissítések gyakoriságát)
Az eseménybejelentési és az értesítési eljárások kialakítása	Az eljárások leírása a szerepek és felelősségek, valamint az érintett szervek megnevezésével, az országok közötti együttműködés leírásával

Fő teljesítménymutató	*Mérendő terület (tények, bizonyítékok)*
Olyan eszközök tervezése és megvalósítása, amelyek a piaci hiányosságokat kompenzálják (PPP-k, szabálysértésekre vonatkozó szabályozások)	Stratégiai programdokumentumok; megvalósítási útmutatók
A kritikus infrastruktúrák üzletmenet-helyreállítási és folytonossági tervei	Stratégiai dokumentumok, végrehajtási útmutatók, érintett szervek, feladatok és szerepek a különböző testületek számára
Sikeres információmegosztás és megbízható együttműködés a különböző szereplők között	Megbízható kommunikációs csatornák, rendszeres találkozók, érdekelt felek bevonása
Gyorsabb és hatékonyabb válasz nemzeti szintű incidens esetén (kevesebb támadás/incidens esetén kevesebb leállás)	A reakció sebességének csökkentése; a válasz bizonytalanságának csökkenése
A rendszerek átláthatósága és elszámoltathatósága	A nyilvánosság számára hozzáférhető dokumentáció száma és típusa, az emberek tudatosságának mérése

Forrás: ENISA 2014, a szerző szerkesztése

Mindezeken túl az ajánlás általános értelemben vett indikátorokra, illetve mutatókra is javaslatokat tesz. Ezek az általános mutatók magának a nemzeti kiberbiztonsági stratégiának, illetve annak végrehajtásának egységes megítéléséhez adnak támpontokat.

7. táblázat

Az ENISA nemzeti kiberbiztonsági stratégiára megadott fő teljesítménymutatói a nemzeti kiberbiztonsági stratégia értékelésének területére

Fő teljesítménymutató	*Mérendő terület (tények, bizonyítékok)*
A nemzeti kiberbiztonsági stratégia értékelései (stratégiai szint)	KPI-k és egyéb mutatók, megvalósult eredmények (a programért felelős szakpolitikai egység, ellenőrző szervek)
A megvalósítás értékelése (végrehajtási szint)	KPI-k és egyéb mutatók, megvalósult eredmények (a programért felelős szakpolitikai egység, ellenőrző szervek)
Nemzetközi és nemzeti jogi kötelezettségek	A kötelezettségek végrehajtási aránya (az európai jogszabályok átültetése vagy nemzeti jogszabályoknak való megfelelés)

Fő teljesítménymutató	*Mérendő terület (tények, bizonyítékok)*
Költségvetés (a nemzeti kiberbiztonsági politika költségeinek átláthatósága)	Pénzügyi ellenőrzés a kiberbiztonsági cselekvési terv tevékenységeivel összefüggő konkrét tevékenységekkel kapcsolatosan
Az államok együttműködnek a kibertérben a közös normáknak megfelelően, így támogatják a közös értékeket a kibertérben	Az együttműködés és közös tevékenység szintje

Forrás: ENISA 2014, a szerző szerkesztése

Az ITU kiberbiztonsági stratégiával kapcsolatos ajánlásai

Az Egyesült Nemzetek Szervezetének Közgyűlése 2001-ben egy Információs Társadalom Világ-csúcstalálkozó (World Summit on Information Society, WSIS) létrehozásáról döntött. A két fázisban megvalósítandó projekt első részére Genfben, 2003. december 10. és 12., míg a második részére Tunéziában, 2005. november 16. és 18. között került sor. (ITU 2003a)

A 2003-as genfi rendezvényen több mint 11 ezren vettek részt. Az eseményen 175 ország kormánya, civil szervezetek egész sora, az üzleti világ, technológiai cégek, az akadémiai szféra és természetesen számos nemzetközi szervezet képviseltette magát. (ITU 2003a)

A fórum zárónyilatkozata, avagy a hivatalos megfogalmazás szerint az *Alapelvek nyilatkozata* (Declaration of Principles) három fő részben összesen 67 olyan alapelvet azonosított, amelyek az információs társadalom kialakításához, fejlesztéséhez, az infokommunikációs technológia előnyeinek kihasználásához, valamint mindezek alapján a tudásmegosztáshoz járulhatnak hozzá. (ITU 2003b)

A zárónyilatkozat már tartalmaz utalásokat a biztonságra vonatkozóan, de alapvetően még az infokommunikációs eszközök és rendszerek biztonságos használata, illetve az információbiztonság jelenik meg biztonsági tényezőként. Emellett azonban nagyon előremutató, hogy a nyilatkozat már tartalmazza a kiberbiztonság kifejezést, bár azt

még elsősorban a globális kiberbiztonsági kultúra, valamint az adatok és a magánélet vonatkozásában használja.

Így a kiberbiztonság stratégiai megfontolásai ugyan még nem szerepelnek a dokumentumban, de az mindenképpen figyelemre méltó, hogy az ENSZ kiáll az IKT-eszközök és -rendszerek olyan célú használata mellett, amely a nemzetközi térség biztonságát nem veszélyezteti, így ez akár stratégiai célkitűzésként is értelmezhető: „támogatjuk az Egyesült Nemzetek azon tevékenységeit, amelyek megakadályozzák az IKT potenciális felhasználását olyan célokra, amelyek nem állnak összhangban a nemzetközi stabilitás és biztonság fenntartásának célkitűzéseivel" (ITU 2003b)

A genfi csúcstalálkozó résztvevői a zárónyilatkozat mellett egy akciótervet is elfogadtak. Ebben az akciótervben már hangsúlyosan megjelenik a biztonság mint az információs társadalom építésének és fejlesztésének egyik alappillére. Az IKT használata során a bizalmat és a biztonságot hivatottak növelni azok a célok, amelyeket az akcióterv ezzel kapcsolatosan megfogalmaz:

- nemzetközi együttműködésekkel kell előmozdítani a felhasználók IKT-eszközökkel és -rendszerekkel szembeni bizalmának növelését;
- fel kell mérni az infokommunikációs eszközökkel és rendszerekkel szemben meglévő és lehetséges fenyegetéseket;
- a kormányoknak a magánszektorral együttműködve kell kezelniük a számítógépes bűnözést, beleértve a megfelelő jogszabályalkotást, a visszaélések hatékony kivizsgálását és a büntetőeljárást;
- támogatni kell a hatékony nemzetközi együttműködésen alapuló kölcsönös segítségnyújtást a kiberbűncselekmények megelőzésére, felderítésére és visszaszorítására;
- támogatni kell a felhasználók oktatását és ismereteik bővítését az online magánélet védelméről és a magánélet védelmének módjáról, valamint a számítógépes bűncselekmények kapcsán a biztonságtudatosságuk fejlesztését;

- ösztönözni kell a nemzeti szintű jogszabályok olyan átalakítását, hogy azok lehetővé tegyék, illetve megkönnyítsék az elektronikus szolgáltatások igénybevételét;
- ösztönözni kell a valós idejű incidensek kezelésére és reagálására szakosodott intézmények felállítását, valamint azok nemzetközi hálózatának kialakítását;
- az online tranzakciók megkönnyítése érdekében támogatni kell a biztonságos és megbízható alkalmazások további fejlesztését;
- minden országot ösztönözni kell, hogy aktívan járuljanak hozzá az információs és kommunikációs technológiák biztonságát célzó ENSZ-tevékenységekhez. (ITU 2003c)

Amennyiben végignézzük a fenti – a biztonság érdekében megfogalmazott – feladatokat, akkor nyugodtan kijelenthetjük, hogy azok valóban előremutatóak, hiszen ne feledjük, már 2003-ban megjelent a kiberbűnözéssel (illetve az akkori terminológiával élve számítástechnikai bűnözéssel), a koordinált és nemzetközi szinten is megvalósuló incidenskezeléssel vagy éppen a felhasználók biztonságtudatosságának növelésével kapcsolatos elképzelések és követelmények egész sora. Amennyiben ezeket a feladatokat 15 év távlatából nézzük, akkor megállapíthatjuk, hogy ma is ugyanúgy érvényesek, és most is kiemelt feladatnak számítanak.

Az ENSZ Információs Társadalom Világ-csúcstalálkozó második fázisára, ahogy az az említett genfi akcióterv utolsó részébe feladatként be is került, Tuniszban, 2005 novemberében került sor. Ezen a rendezvényen már több mint 19 ezer fő vett részt.

A csúcstalálkozó döntött egy úgynevezett Internetirányítás (Internet Governance, IG) kezdeményezésről, amely munkájának támogatására az ENSZ-főtitkár által felállított munkacsoport (Working Group on Internet Governance, WGIG) volt hivatott. A munkát az Internetirányítási Fórum (Internet Governance Forum, IGF) koordinálta, eredményeit pedig számos workshop és egyéb rendezvény keretében mutatták be. (ITU 2003a)

Az Internetirányítás a hivatalos megfogalmazás szerint egy munkacím, amely alatt az ENSZ a következőket érti, illetve értette: „a kormányok, a magánszektor és a civil társadalom szerepének, közös alapelveinek, normáinak, szabályainak, döntéshozatali eljárásainak és programjainak fejlesztése és alkalmazása, amelyek az internet fejlődését és használatát befolyásolják." (ITU 2005)

A csúcstalálkozó számos akciótervet fogalmazott meg, amelyek vezetésére, illetve menedzselésére ki is jelölte azok felelős ENSZ-szervezeteit.

8. táblázat

Az ENSZ Információs Társadalom Világ-csúcstalálkozón meghatározott akciótervek és azok felelős szervezetei

Akcióterv		Lehetséges moderátor/felelős
C1.	A közigazgatási szervezetek és minden érintett szerepe az IKT-fejlesztésben	ECOSOC/ENSZ regionális bizottságai/ ITU
C2.	Információs és kommunikációs infrastruktúra	ITU
C3.	Az információhoz és a tudáshoz való hozzáférés	ITU/UNESCO
C4.	Képességfejlesztés	UND/UNESCO/ITU/UNCTAD
C5.	Bizalom és biztonság kialakítása az IKT-eszközök és -rendszerek alkalmazása során	ITU
C6.	Az alkalmas környezet kialakítása	ITU/UNDP/ENSZ regionális bizottságai/UNCTAD
C7.	IKT-eszközök: • e-kormányzás • e-business • e-learning • e-egészségügy • e-munka • e-környezet • e-mezőgazdaság • e-tudomány	IKT-eszközök: • UNDP/ITU • WTO/UNCTAD/ITU/UPU • UNESCO/ITU/UDINO • WHO/ITU • ILO/ITU • WHO/WMO/UNEP/ICAO • FAO/ITU • UNESCO/ITU/UNCTAD
C8.	Kulturális sokszínűség és identitás, nyelvi sokszínűség és helyi tartalom	UNESCO
C9.	Média	UNESCO

Akcióterv		Lehetséges moderátor/felelős
C10.	Az információs társadalom etikai dimenziója	UNESCO/ECOSEC
C11.	Nemzetközi és regionális együttműködés	ENSZ regionális bizottságai/UNDP/ ITU/ UNESCO/ECOSEC

Forrás: ITU 2005, a szerző szerkesztése

Ezekben az akciótervekben (Action Lines) található a már a genfi csúcstalálkozó zárónyilatkozatában is szereplő, de itt ismét visszaköszönő, *az információs és kommunikációs technológiák használatának bizalmát és biztonságát* (amelynek a hivatalos angol címe: *Building confidence and security in the use of ICTs*) célzó feladategyüttes. Ezeknek a feladatoknak a koordinálására, illetve a feladatok facilitátorának az ENSZ a Nemzetközi Távközlési Egyesületet (International Telecommunication Unit, ITU) kérte fel. (ITU 2005)

Mindezek alapján az ITU 2007-ben elindította a Globális Kiberbiztonsági Programot (Global Cybersecurity Agenda, GCA). A GCA a tuniszi WSIS-csúcstalálkozón megfogalmazottak és az ott kapott felhatalmazás alapján az információs társadalom biztonságának fokozására irányuló nemzetközi együttműködés keretrendszere. A GCA öt pillére – nevezetesen a jogi intézkedések, a műszaki és eljárási intézkedések, a szervezeti struktúrák, a kapacitásbővítés, valamint a nemzetközi együttműködés elősegítése és fokozása – az információs társadalom biztonságának hatékony, a különböző területek és tevékenységek közötti átfedéseket minimalizáló, nemzetközi együttműködésre épülő fejlesztését célozta meg. (ITU 2018)

A GCA-ra épülve az ITU 2011 szeptemberében kiadott egy saját nemzeti kiberbiztonsági stratégiákkal kapcsolatos útmutatót. A kiadvány célja annak megfogalmazása szerint a következő: „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)

A referenciamodellt bemutató ajánlás egy globális kiberbiztonsági helyzetelemzéssel kezdődik, amely a globális és nemzeti gazdasági helyzetet, illetve az azt nagymértékben meghatározó kiberteret és annak rendszereit, illetve szolgáltatásait elemzi. A globális helyzetelemzés alapvetően az ENSZ információs társadalom és kiberbiztonság területén meglévő tevékenységeit mutatja be. Ezekre röviden a későbbiekben jelen könyvben mi is kitérünk.

Ezt egy nemzeti kiberbiztonsági kontextus bemutatása követi, ahol a fő hangsúly a kritikus infrastruktúrákra, illetve a kritikus információs infrastruktúrákra helyeződik.

Mindezekre építve jelenik meg a dokumentumban egy ajánlás a nemzeti kiberbiztonsági stratégia modelljére vonatkozóan. A modell stratégiai összefüggésben, holisztikus megközelítéssel mutatja be a kiberbiztonság nemzeti stratégiájának javasolt struktúráját. A stratégiai kapcsolatok bemutatása a nemzetközi szerződések és egyezmények, a nemzeti érdekek, valamint a kibertér veszélyeinek és kihívásainak a felmérésével kezdődik, majd azoknak a tényezőknek a meghatározásával folytatódik, amelyek nemzeti szinten befolyásoló tényezőként jelentkeznek a kiberbiztonság egyes tevékenységeiben. Természetesen a dokumentum bemutatja a nemzeti kiberbiztonsági stratégia legfontosabb célkitűzéseit és prioritásait is. (Wamala 2011)

A bemutatott holisztikus, a lehető legtöbb érdekelt felet integráló nemzeti kiberbiztonsági stratégia, illetve az annak kialakítására alkalmazandó program sok helyen átfedést mutat a korábban bemutatott és elemzett ENISA-ajánlással. A következő táblázat az ITU – nemzeti kiberbiztonsági stratégia kialakítását célzó – programjának elemeit mutatja be összefoglaló módon.

9. 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 program: • 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, a szerző szerkesztése

A NATO Kibervédelmi Kiválósági Központjának ajánlásai: filozófiai alapok

Az említett két nemzeti kiberbiztonsági stratégia kialakítását segíteni hivatott ajánlásgyűjtemény mellett 2012-ben a NATO tallinni székhelyű Kibervédelmi Kiválósági Központja szintén jelentkezett egy meglehetősen vaskos kiadvánnyal, amelynek címe *Nemzeti kiberbiztonsági keretrendszer kézikönyv* (National Cyber Security Framework Manual) volt. A számos neves szerzőt felvonultató tanulmánygyűjtemény önnön célját a következőképpen fogalmazta meg: „nem törekszik arra, hogy egy egységes, általánosan alkalmazható ellenőrző listát adjon azokra a dolgokra, amelyeket meg kell fontolni egy nemzeti kiberbiztonsági stratégia kidolgozása során. Inkább részletes információs elméleti keretet és hátteret nyújt, amely segít az olvasónak megérteni a nemzeti kiberbiztonság különböző szempontjait különböző politikai szinteken." (Klimburg 2012)

Ebből a nagyon világos célmeghatározásból következik, hogy ez a kiadvány valójában inkább egy tanulmánygyűjtemény, amelyben a különböző fejezetek egy stabil elméleti és filozófiai hátteret adnak a nemzeti kiberbiztonsági stratégia kialakításához, illetve annak elkészítéséhez.

A dokumentum struktúrája is ezt támasztja alá, hiszen a tanulmánykötet egy áttekintő résszel kezdődik, amelyben a terminológiai felvezetés után annak a nem egyszerűen kibogozható kérdésnek igyekszik utánajárni, hogy a nemzeti biztonság és a kiberbiztonság egy adott országban hogyan függenek össze. Ezekre az összefüggésekre számos példát is bemutat a kötet, hiszen 2007 után nagyon sok ország nemzeti biztonsági stratégiájába már explicit módon bekerültek a kibertérben megjelenő fenyegetések, illetve azok kezelésének szüksége.

A könyv ezt követően áttekinti a nemzeti kiberbiztonsági stratégia koncepcionális felépítését, nevezetesen azt, hogy milyen céljai legyenek, kinek szóljon – azaz ki legyen a stratégia célközönsége –, illetve mit is tartalmazzon maga a stratégia a különböző – kormányzati, nemzeti,

illetve nemzetközi – dimenziókban. Figyelemre méltó annak a kérdésnek a vizsgálata, hogy mely területekre vonatkozzon a stratégia. A tanulmány itt öt különböző területet vizsgál: a kiberbiztonság katonai vetületeit (például kiberhadviselés, kiberfegyverek); a kiberbűnözést (nemcsak a hagyományos bűnözés kibertérben való megjelenése, hanem akár a kiberbűnözés és a kiberterrorizmus kapcsolata is ide tartozhat); a kiberhírszerzést és -elhárítást (a szellemi tulajdon ellopása mellett az állami szervezetek elleni kémkedés nagymértékű növekedése, illetve az ilyen akciók elleni elhárítótevékenység fontosságának hangsúlyozása mellett); a kritikusinfrastruktúra-védelmet (mint nemzetbiztonsági érdek megjelenését); a nemzeti krízismenedzsmentet, valamint kiberdiplomáciát és internetkormányzást (azaz a diplomácia transzferálását a kibertérbe). (Klimburg 2012)

Ugyanakkor a fenti felosztásból is világosan látszik, ahogy azt az ajánlásgyűjtemény a korábban elemzett másik két dokumentumhoz (ENISA, illetve ITU) hasonló módon meg is jegyzi, hogy ezek a területek különböző szereplőket jelentenek, így még az állami szegmensen belül is különböző csoportok és együttműködők bevonása, illetve azok koordinált együttműködésének megteremtése szükséges ahhoz, hogy a nemzeti kiberbiztonsági stratégia megalkotása egyáltalán elkezdődhessen.

A CCDCOE-tanulmány az állam oldaláról mindezekhez még egyéb más fontos kérdéseket is felvet. Öt olyan dilemmát azonosít, amelyek befolyásolják az említett nemzeti biztonsági stratégiáról való legalapvetőbb kérdések megvitatását is. Ezeknek a kérdéseknek egy része az adott országon belül, de egy részük az országon kívül, azaz nemzetközi viszonylatban merül fel, hiszen egy ország biztonságában bekövetkező esetleges fejlődés vagy akár éppen annak ellenkezője, azaz egy esetleges biztonsági helyzet romlása természetszerűleg magával hozza az adott ország nemzetközi környezetének változását is. (Klimburg 2012)

Az első ilyen kérdés vagy dilemma nem más, mint az, hogy a gazdaság versenyképességének növelése szemben áll-e a nemzeti

biztonsággal. Ez többek között abból a szempontból merülhet fel komoly kérdésként, hogy az információtechnológia fejlődési sebessége, amely technológia alapvető szükséglet és sok esetben a gazdaság motorja is, jóval gyorsabb, mint a védelmének fejlődése. Ráadásul a vállalkozások – de akár a közigazgatás is – nagyon sokszor a versenyképességük biztosítása érdekében gyors ütemű információtechnológiai fejlesztéseket hajtanak végre, de ezekkel a fejlesztésekkel nincsenek arányban – sem mennyiségben, sem minőségben – az információbiztonsági fejlesztések. (Klimburg 2012)

Ez annak a veszélyét hordozza magában, hogy a gyorsan fejlődő IKT-rendszerek számos sérülékenységet és sebezhetőséget rejtenek magukban, amelyek kihasználása, azaz a kibertámadások végrehajtása már nemcsak az adott üzleti vállalkozást (vagy az adott közigazgatási szolgáltatást) fogja negatívan érinteni, hanem ezen rendszerek összekapcsoltsága (interdependenciája) révén kihatással lesz más rendszerekre is. Ez olyan mértékű rendszerkieséseket és működésképtelenségeket okozhat, amelyek már nemzetbiztonsági kockázatot jelentenek. Ugyanilyen probléma lehet, amikor a védelmi megoldásokat (vagy akár a tervezett teljes IKT rendszer kiépítését) olyan cégre bízzák, amelyet nem megfelelően és nem kellő körültekintéssel választottak ki. Ez egyaránt igaz a gazdasági szférára és a közigazgatásra is, hiszen számos olyan példát látunk, amikor a látszólag megbízható cég mögött homályos, nem azonosítható tulajdonosi struktúra áll. A túl gyors és nem körültekintő, a védelemi szempontokat gazdasági vagy egyéb okok miatt nélkülöző vagy az azokat nem megfelelő módon kezelő fejlesztések tehát potenciális veszélyforrások. Ezzel kapcsolatban az idézett CCDCOE-tanulmány a következő kérdést veti fel: „Ebben az esetben a nemzetbiztonság vonatkozásában három kérdés játszik központi szerepet: a kormány biztosítja-e az alapvető szolgáltatások elérhetőségét? Biztosítja-e a szellemi tulajdon védelmét? Hogyan őrzi meg a polgárok bizalmát (és a biztonságot), amikor az részt vesz az internetes gazdaságban?” (Klimburg 2012)

Ez tehát az a dilemma, amelyre figyelmet kell fordítani és amelyre nyilván adekvát válaszokat kell adni a nemzeti kiberbiztonsági stratégia megalkotása, majd bevezetése során.

A következő dilemma az, hogy az infrastruktúra modernizációja magában hordozza-e a kritikus infrastruktúrák sebezhetőségének, illetve sérülékenységének növekedését. Ez a kérdés számos olyan kérdést is magában foglal, amelyek nagyban hasonlítanak a fentiekben tárgyalt IKT-eszközök gyors modernizációja és a nemzetbiztonság egymásra hatása esetében bemutatott problémára. Ezek egyrészt a fejlesztések és a védelem megteremtésének eltérő sebességében, másrészt abban keresendők, hogy minél fejlettebb és összetettebb egy IKT-eszköz vagy -rendszer, annál többe kerül hozzá a biztonság megteremtése.

Ugyanakkor az infrastruktúrák esetében az eltérő fejlettségű rendszerelemek szintén komoly kihívást jelentenek, hiszen az eltérőség nemcsak az üzemeltetés, de az egységesen kialakítandó biztonsági rendszer, illetve annak irányítása számára is kihívásokat hordoz magában. Mindezeken túl az anyagi erőforrások szűkössége sok esetben azt okozza, hogy az infrastruktúra-tulajdonosok és/vagy az infrastruktúrák üzemeltetői olyan eszközökkel fejlesztik a rendszert, azaz olyan rendszerelemek kerülnek be az infrastruktúrába, amelyek pont amiatt olcsóbbak, mert a fejlesztésük és a gyártásuk során teljes körű ellenőrzésükre nem került sor (például a gyors ütemű fejlesztés és a gyors piacra dobás piaci kényszere miatt).

Persze a modernizáció már önmagában is számos kérdést vet fel, hiszen ha egy hagyományos – például vezetékes kommunikációt használó – infrastruktúra esetén korszerűbb és hatékonyabb (nagyobb sávszélességű, vezeték nélküli, így kényelmesebb és nem utolsósorban olcsóbb kiépítésű) eszközöket és elemeket illesztenek a rendszerbe, mint amelyekre a SCADA-rendszerek esetében gyakori új szenzorok alkalmazásával már sok példa van, akkor, mivel azok távolról könnyebben elérhetők, támadhatóvá válnak.

Ugyanakkor a dilemma itt nemcsak az infrastruktúra-tulajdonosok és -üzemeltetők, hanem az állam részéről is felmerül, hiszen az egyes infrastruktúrákban keletkező, akár csak időszakos kiesés is dominószerű hatásokat fejthet ki más rendszerekkel szemben. Ezen a területen az állam nemcsak koordináló, de a védelem megvalósításának és garantálásának a legfontosabb és egyben a legmagasabb szintű szereplője is. Emellett ma már az is nyilvánvaló tény, hogy gyakorlatilag minden kritikus infrastruktúra önmagában is tartalmaz infokommunikációs rendszert, sőt rendszereket, többek között az adott rendszer vezérlésére és irányítására. Így ezeknek az IKT-eszközöknek és -rendszereknek a biztonsága stratégiai szinten is fontos kérdés.

A következő dilemma, amely már a korábban elemzett ENISA-kiadványban is hangsúlyosan jelent meg, a köz- és a magánszektor kapcsolata. Ez a kérdés jóval mélyebb, és jóval túlmutat azon a problémakörön, amely a kritikus infrastruktúra tulajdonlásában és annak üzemeltetésében jelenik meg. A magánszektor jellegénél fogva, illetve az üzleti megtérülés és az anyagi haszon megteremtése miatt majdnem elsődleges és kizárólagos szerepet játszik az olyan területeken, mint a szoftverek vagy hardverek kutatás-fejlesztése, illetve azok gyártása. Ez versenyhelyzetet is jelent, amely egyrészt nyilvánvalóan egy sor pozitív jelenséggel is együtt jár – ilyen például a gyors alkalmazkodás a piaci, illetve felhasználói igényekhez vagy a legújabb technológiák alkalmazása –, ugyanakkor számos veszélyt és kihívást is rejt magában, hiszen a gyors ütemű fejlesztés, illetve pont a piaci versenyhelyzet teremtette időhiány sok esetben a biztonság rovására megy. Nincs idő a részegységek, modulok vagy infrastruktúra-elemek egymásra gyakorolt hatásának átgondolt és mindenre kiterjedő vizsgálatára. Vagyis a tervezés és a gyártás során sokszor nincs idő a biztonság megteremtésére. E kérdés vizsgálata során egy másik komoly szempont – ahogy azt az említett tanulmánykötet is megjegyzi –, hogy a kritikus infrastruktúrák számára rendszereket, illetve rendszerelemeket gyártók sok esetben kiemelt célpontjai a kibertámadásoknak, a kiberbűnözésnek. A kibertámadások jelentős részben arra irányulnak, hogy

már a gyártás, sőt ha lehet, akkor a tervezés során olyan hibákat, illetőleg olyan rosszindulatú programokat helyezzenek el a majdani kritikus rendszereket vezérlő és irányító számítógépekben, amelyekkel azok kompromittálhatók és rávehetők a hamis, rossz vagy téves vezérlésre egy adott pillanatban – és természetesen, ha ez lehetséges, akkor mindez távolról, távirányítással történjen. A kiberbűnözés alapvetően ebben a szegmensben a szellemi termékek eltulajdonításában és az információszerzésben (ipari kémkedés) jelentkezik, hiszen itt a tervezés és a gyártás a legköltségesebb folyamatok egyike. A tervezés során eltulajdonított adatokkal pedig a konkurencia – legyen az egy másik vállalat vagy akár egy másik ország – jóval költséghatékonyabb módon tudja megkezdeni magát a gyártást, hiszen viszonylag alacsony költséggel vagy akár költségek nélkül jut a gyártást lehetővé tevő adatokhoz, információkhoz, míg az eredeti fejlesztő nemcsak a nagyobb költséggel, de a támadás során bejuttatott eszközökkel is szembe kell, hogy nézzen. (Klimburg 2012)

Mindezeknek megfelelően nem túlzás azt állítani, ahogy azt a fenti tanulmány is idézi, hogy akár a kritikus infrastruktúrákról, akár az itt is nagyon erősen jelen lévő kiberbiztonságról van szó, közös felelősséget kell vállalnia az államnak, azaz a közszférának és a magánszférának. Az erre való utalásnak vagy akár szabályozásnak be kell kerülnie a nemzeti kiberbiztonsági stratégiába. Az persze kérdéses, hogy a kötelező érvényű szabályozást vagy a megengedőbb javaslati szintű megoldást részesíti előnyben egy-egy ország, mint ahogy ezek hatásai is eltérők lehetnek. Ezt így fogalmazta meg a CCDCOE-tanulmány, hivatkozva egy olyan 2009-ben készült elemzésre,[30] amely az európai uniós kritikus információs infrastruktúra-védelmi terveket hasonlította össze: „a vizsgált 16 EU-tagállam közül körülbelül azok fele fogalmaz meg inkább önkéntes, mint kötelező elveket a kritikus

[30] A tanulmány itt a következő elemzésre hivatkozik: Booz & Company, Comparison and Aggregation of National Approaches (JLS/2008/D1/019 – WP 4) (2009). 28.

információs infrastruktúra védelmi programjában, körülbelül hat kiegyensúlyozott az önkéntes és a kötelező jogi intézkedések között, és csak két tagállam alkalmazza a teljesen kötelező érvényű szabályozást. Azonban nagyon valószínű, hogy ezek a számok változnak, tekintettel a legutóbbi európai trendre, amely egyre inkább a jogszabályok alkalmazását jelenti ezen a területen." (Klimburg 2012)

Egy biztos, az azóta eltelt időszakban, mint ahogy azt a következő részekben az Európai Unió tagországainak nemzeti kiberbiztonsági stratégiáinak elemzésekor látni fogjuk, nagyon sok ország pont ezt a szabályozási elvet, és nem az önkéntességet vette alapul. Ennek oka sokrétű, de elsősorban az olyan uniós szabályozásban keresendő, mint például az uniónak a már szintén említett, de a későbbiekben részletesen is bemutatni kívánt NIS-direktívája, amely konkrét szabályozási lépések megtételét irányozza elő – alapvetően az információs rendszerek vonatkozásában – minden tagország számára, ráadásul mindezt kötelező érvényű módon.

A következő dilemma az adatok védelmének és az információk szabad áramlásának látszólagos vagy éppen ellenkezőleg: tényleges szembenállásáról szól. Persze mint minden eddig bemutatott dilemma, ez sem olyan egyszerű, mint ahogy az a fenti kérdésben felvetődik. Az állampolgárok jogos igénye, hogy egy olyan nyílt társadalomban éljenek, ahol az információk szabad áramlása alapvető jog, ugyanakkor joggal merül fel a részükről az igény, hogy az adataik mind az állam, mind a magánszektor vállalatai és egyéb szereplői részéről védettek legyenek. Ez azt is jelenti, hogy akár a kiberbűnözés elleni tevékenység, akár napjainkban a terrorizmus elleni fellépésben olyan információk cseréje is meg kell, hogy valósuljon, amelyek mind ez idáig az állampolgárok és az állam, illetve annak néhány hatósága között nem voltak napi rendszerességgel jelen. Ez sok esetben olyan személyes adatokat és információkat is jelent, amelyek nyilvánvalóan szükségesek például a kiberbűnözés elleni fellépéshez, de nyilvánosságra kerülésük kerülendő, mert akár üzleti hátrányt is okozhatnak, vagy az állampolgárok kárára elkövetett visszaélésekre adhatnak alkalmat.

Másik kérdés ezen a dilemmán belül, hogy az állam vagy annak egyes szereplői milyen gyorsan és milyen volumenben képesek megosztani például olyan kiberbiztonsági veszélyekre figyelmeztető információkat, amelyek alapján akár az állampolgárok, akár a magánszféra képes hatékonyan kibervédelmi intézkedéseket megtenni, vagy amelyek alapján legalább a kibervédelemre történő felkészülést meg tudja kezdeni. Ehhez egyrészt olyan szervezetrendszer kell, amely képes a kiberbiztonsági veszélyeket folyamatosan nyomon követni, másrészt megvan a kapcsolatrendszere és nem utolsósorban a kommunikációs hálózata ahhoz, hogy az ezekről szóló elemzések és tájékoztatók el is jussanak mind a közszféra, mind a magánszféra érdekelt szervezeteihez. Ennek a szervezetrendszernek a biztosítására, kiépítésére, illetve működtetésére a tanulmánykötet az incidenskezelő központokat (például a CERT-eket) látja a legalkalmasabbnak. Ennek megfelelően az ilyen CERT-ek feladatainak meghatározása a nemzeti kiberbiztonsági stratégiába is be kell, hogy kerüljön. (Klimburg 2012)

Az ötödik és egyben utolsóként megfogalmazott dilemma a véleménynyilvánítás szabadságának és a politikai stabilitásnak a kérdése. Ez a látszólag szintén nagyon egyszerű kérdés azonban számos problémát felvet. Nyugati világunkban az információszabadság és a véleménynyilvánítás a legfontosabb alapelvek közé tartoznak. Az infokommunikációs eszközök alkalmazásával az állampolgároknak megvan az a lehetőségük, hogy a politikai döntések meghozatalában akár közvetlen módon részt vegyenek. Az állampolgárok ezeknek az eszközöknek és rendszereknek a segítségével minden eddiginél hatékonyabban fejezhetik ki szimpátiájukat és támogatásukat vagy éppen nemtetszésüket és ellenérzéseiket egy-egy politikai döntés mellett vagy az ellen. Ugyanakkor például a szerzői jogok kérdése esetén már nem ilyen egyszerű az információ szabad áramlása, hiszen az állampolgárok egy része jelentős nemtetszését fejezte ki az olyan oldalak és szolgáltatások korlátozásával szemben, ahonnan filmeket, zenét lehetett letölteni. Az ő értelmezésükben, mivel a technológia ezt

lehetővé tette, a szerzői jogokat egészen más módszerekkel kell vagy kellene érvényesíteni.

Egy másik olvasata ennek a problémának a köz- és magánszféra kapcsolatában keresendő. Például joga van-e (azaz megfelelően van-e szabályozva) egy térfigyelő rendszert üzemeltető magánvállalkozásnak ahhoz, hogy egy utcai – esetlegesen az aktuális kormány egyes döntései ellen szervezett – tüntetés résztvevőiről készült képeket és felvételeket átadja a rendvédelmi vagy nemzetbiztonsági szerveknek? Ugyanez a kérdés felmerül – természetesen más platformokon és más típusú adatokkal – az internetszolgáltatók esetében is, például abban a vonatkozásban, hogy az adott politikai erő ellen véleményt kifejtő internetes fórum vagy blog felhasználójának adatai milyen mértékben és kinek adhatók át. (Klimburg 2012)

Később utalni fogunk rá, hogy ez, bár sok ország kiberbiztonsági stratégiájában megjelenik, elsősorban mégsem kiberbiztonsági, hanem politikai, illetve jogi, jogszabályi kérdés. Ezzel kapcsolatosan a 2016-os amerikai, később 2017-ben a német, illetve francia elnökválasztás mindenképpen ide kapcsolódik. Ugyanis egy komoly változás következett be az említett tanulmány megszületésének ideje és napjaink között. Ez pedig nem más, mint a közösségi média megjelenése és annak politikai célú, nagy tömegeket érintő, manipulatív kihasználása. (Kovács–Krasznay 2017)

A CCDCOE-tanulmány felvázolja azokat a politikai célokat és politikai módszereket, amelyek szükségesek a nemzeti kiberbiztonsági stratégia megalkotása során. A dokumentum készítői megvizsgálták 19 ország nemzeti kiberbiztonsági stratégiáját, illetve ezekkel párhuzamosan ezen országok nemzeti biztonsági stratégiáit. A nemzeti biztonsági stratégiák természetesen minden ország esetében feltárják azokat a veszélyforrásokat, amelyekkel az adott országnak számolnia kell. Ilyen – több ország esetében is megjelenő, nyilvánvalóan nem is új – veszélyforrás többek között a tömegpusztító fegyverek elterjedése, a terrorizmus, az állam működésének akadályozása stb. Ennek oka abban keresendő, hogy a nemzeti biztonsági stratégiák

jelentős része az 1990-es évek elején, közepén vagy jó esetben az évtized végén született, így azok természetszerűleg az akkor legfontosabb veszélyeket tartalmazzák.

Ugyanakkor már az is megfigyelhető, hogy számos ország olyan releváns fenyegetésként értékeli a kibertérben megjelenő kihívásokat, amelyek a hagyományos kihívásokkal azonos szinten jelennek meg, így bekerülnek a nemzeti biztonsági stratégia által tárgyalt kihívások közé. Mindezek a kibertéri veszélyek esetenként már úgy is megjelennek, hogy világos a kritikus infrastruktúrák egyes ágazataira – például az energia-, a pénzügyi ágazatra, a kommunikációra – kifejtett negatív hatása.

Az említett stratégiák vizsgálata arra is rávilágított, hogy még mindig csak korlátozott a politikai akarat a kibertérben megjelenő veszélyek kezelésére. Ezt elsősorban a probléma megértésének és teljesen világossá válásának nehézségeiben azonosították a szerzők.

Az is nyilvánvalóvá vált, hogy a nemzeti kiberbiztonsági stratégiát számos ország olyan eszköznek szánja, amellyel kijelölhetők a legfontosabb irányok, a kiberbiztonság területén megvalósítandó politikai célok, és ezek alapján akár az anyagi erőforrások elosztása is megtörténhet a felvázolt feladat- és szervezetrendszer kialakításával együtt. (Klimburg 2012)

Ezzel kapcsolatban meg kell jegyezni, hogy a kiberbiztonsági szervezetrendszer felállítása, illetve e szervezetek feladatainak a meghatározása megjelenik a 2013-ban kiadott magyar kiberbiztonsági stratégiában, illetve az erre épülő információbiztonsági törvényben is, de számos – tegyük hozzá rögtön jogos – kritika is éri mind a stratégiát, mind a törvényt azért, mert az anyagi erőforrások feladatokhoz történő hozzárendelése ugyanakkor nem történt meg.

A CCDCOE-tanulmány megállapítja, hogy a vizsgált országok nemzeti kiberbiztonsági stratégiái eltérő definíciós készlettel dolgoznak a kibertér és a kiberbiztonság meghatározása kapcsán is: „A 19 nemzeti kiberbiztonsági stratégia vizsgálata azt sugallja, hogy a kibertér fogalmi meghatározásai különböznek egymástól. Egyesek

az internethez szorosan illeszkedőnek tartják, míg mások szélesebb értelemben használják a definíciót. A vizsgált nemzeti kiberbiztonsági stratégiák kevesebb mint felében definiálják csak a kiberbiztonságot." (Klimburg 2012)

A tanulmánykötetben nagyon előremutató a nemzeti kiberbiztonsági stratégia legfontosabb céljai és azok elérésében a legkiemeltebb szereplők azonosítása. Ezzel kapcsolatban a dokumentum kitér arra, hogy a stratégiának azonosítania kell a különböző érdekeltségi területeket, azok szerepét, ráadásul ezt mind támadó, mind védelmi kibertéri műveletek esetében meg kell tenni. Ezen a helyen is fontos hangsúlyozni, hogy a kibertéri támadó műveletek nagyon sokáig – és ez még napjainkra is igaz sok esetben – mintha tabunak számítanának. Nyilvánvaló, hogy sok ország nemzeti biztonsági stratégiája – hasonlóan Magyarországéhoz – alapvetően védelmi jellegű filozófiát követ. Ugyanakkor a kibertérben a védelem sok esetben nem képzelhető el támadó, illetve megelőző támadó képességek megléte nélkül.

Ahogy korábban utaltunk rá, a dokumentum a nemzeti kiberbiztonsági stratégia kidolgozása során az érdekelt feleket három dimenzióban látja azonosíthatónak. Ez a három dimenzió a kormányzati, a nemzeti (társadalmi) és a nemzetközi szereplők által meghatározott dimenzió. Nyilvánvalóan ezek közül a kormány az, amely a koordinációt el kell, hogy végezze az érdekelt felek, illetve a kiberbiztonság szereplői közül. A nemzeti kiberbiztonsági stratégia legfontosabb céljait bemutatva a tanulmány 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 rendszereit;

- nemzeti kiberbiztonsági stratégiák kialakításakor gyakran tapasztalható, hogy a különböző megközelítések – például a katonai és a sokszor ezzel szembenálló vagy legalábbis az ezzel nem teljesen harmonizáló civil vagy akár a kiberbűnözés elleni szervezetek által követett irányok – feszültségekhez vezetnek. Hasonló feszültséget okozhat az, 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)

A kiberbiztonság nemzeti szintű szervezeti rendszerének kialakításával kapcsolatban a tanulmánykötet szintén megfogalmaz számos olyan kérdést, amelyek mind a stratégia kialakításkor, mind annak végrehajtása során fontos tényezőként jelennek meg. Ilyen kérdések a következők:

- 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 jönnek létre nem megfelelő feladatokkal, funkciókkal és képességekkel;
- 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)

Mindezeken túl a tanulmánykötet egy nagyon érdekes felvetéseket tartalmazó részt is tartalmaz, amelyben a különböző kötelezettségvállalásokkal – például a nemzetközi szerződésekkel és egyezményekkel – kapcsolatos megfontolásokat igyekszik számba venni. Ennek során a dokumentum 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 meglévő, olyan nemzeti szintű 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 (itt a szerzők nagy valószínűséggel a Budapest Konvencióra utalnak) 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)

Az ENISA, az ITU és a CCDCOE ajánlásgyűjteményeinek összehasonlításából levonhatjuk azt a következtetést, hogy amíg az ENISA egészen konkrét lépéseket javasol a nemzeti szintű kiberbiztonsági stratégia kialakítása és működtetése során, addig az ITU egy átfogóbb, inkább modellértékű javaslatcsomaggal állt elő. Ugyanakkor mindkét dokumentum épít azokra az elvekre, amelyek megfogalmazódnak a CCDOE ajánlásaiban.

A fentiekből is kitűnik, hogy a tanulmányok számos olyan alaposan átgondolt javaslatot tartalmaznak, amelyek valóban alapul szolgálhatnak, és akár sorvezetőként is használhatók egy nemzet döntéshozói részéről az adott ország kiberbiztonsági stratégiájának kialakításához vagy a már meglévő stratégia felülvizsgálatához.

2. Kiberstratégia szövetségben

A nemzeti kiberbiztonsági stratégiákra adott ajánlások után a hazánk vonatkozásában is meghatározó olyan nemzetközi szervezetek, mint az Európai Unió és a NATO kiberbiztonsággal kapcsolatos elgondolásait, illetve esetenként stratégiai elképzeléseit, valamint ezek meghatározó dokumentumokban való megjelenését mutatjuk be, amelyek a korábban is említett tényezők miatt az egyes országok nemzeti kiberbiztonsági stratégiáira is hatással vannak.

Az EU és a NATO kiberbiztonsági stratégiái mellett nagyon röviden bemutatjuk az ezekhez kapcsolódó dokumentumok lényeges elemeit, amelyek meghatározó módon épülnek a kibertér egyes részeire és rendszereire. Ilyen terület például a már többször említett kritikus infrastruktúrák és azok védelmi megoldásai. Ennek oka az, hogy nagyon nehéz elképzelni ma – és ez a jövőben meglehetősen jól prognosztizálható módon, várhatóan még inkább igaz lesz – olyan, a társadalom számára valóban létfontosságú rendszereket vagy akár ezeknek egyes elemeit is, amelyek ne épülnének vagy ne működnének legalább közvetett módon a kibertér egyes összetevőire.

2.1. Az Európai Unió kiberbiztonsági stratégiája

Az Európai Bizottság 2010-ben meghirdetett Európa 2020 stratégiája öt fő célkitűzést és ezen belül számos pillért tartalmazott. A stratégia az európai gazdaság kitettségének és sérülékenységének csökkentése, valamint az EU versenyképességének növelése érdekében született. A stratégia a versenyképesség növelése mellett a sérülékenységek csökkentését irányozta elő. Az Európa 2020 egyik pilléreként az európai digitális menetrend az EU olyan, a digitális területen meglévő

kihívásaira kíván egységes választ adni, mint a digitális piac megosztottsága, az interoperabilitási problémák, a kiberbűnözés rendkívül gyors ütemű terjedése, az alacsony szintű K+F és az erre épülő beruházások elmaradása vagy a digitális írástudás régónként eltérő és sok esetben nagyon alacsony szintje. (European Commission 2017c)

Az hamar világossá vált az Európai Bizottság és a tagországok döntéshozói számára is, hogy a kibertér biztonságának megteremtése nélkül a fenti célok nem, vagy csak részben valósíthatók meg. Ennek megfelelően olyan stratégiára volt szükség, amellyel az unió döntéshozói még adósak voltak, így 2013-ban megszületett az EU kiberbiztonsági stratégiája.

A stratégia kialakítása sok vitával és egyeztetéssel járt, így a konkrét szövegére tett javaslatot csak 2013 februárjában tették közzé. A két részből álló javaslat első része maga a kiberbiztonsági stratégia, amely hivatalos formában az Európai Bizottság és a külügyi és biztonságpolitikai főképviselő közleménye,[31] a második rész pedig a NIS-irányelvre tett javaslat volt, amely az Európai Bizottság olyan határozott szándéka a hálózat- és az információbiztonság növelésére, amely a 28 tagállam mindegyikében egységes elveken nyugszik.

Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér

A javaslatokat konkrét döntések is követték, így 2013-ban elfogadták a stratégiát. Ennek hivatalos címe rendkívül érdekes, hiszen a magyar változat az alábbi: *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér*. (European Commission 2013) Bár ez a cím magában hordoz némi ellentmondást (hiszen ami nyílt, az nem feltétlenül jár együtt a megbízhatósággal és a biztonsággal), de

[31] A hivatalos cím szerint: *Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának*. Brüsszel, 2013.2.7. JOIN(2013) 1 final.

nagyban utal azokra a célokra, amelyek elérése érdekében a stratégia megszületett.

A stratégia általános értelemben is megfogalmazza 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. (European Commission 2013).

Az elfogadott európai uniós kiberbiztonsági stratégia öt alapelvre épül, amelyek egyben az unió prioritásai is. Az öt alapelv a következő:

- a kibertámadásokkal szembeni ellenálló képesség megteremtése;
- a kiberbűnözés (a stratégiában használatos kifejezéssel élve számítástechnikai bűnözés) nagyarányú visszaszorítása;
- a kibervédelmi politika kidolgozása úgy, hogy az a közös biztonság- és védelempolitikára épüljön;
- a kiberbiztonsághoz szükséges ipar és technológia fejlesztése;
- a kibertérre vonatkozó olyan nemzetközi szakpolitika meghatározása, amely a tagállamok mindegyike számára érvényes, és amely támogatja az alapvető uniós értékeket. (European Commission 2013)

A stratégia ezeket a prioritásokat intézkedésekkel támogatja. A kibertámadásokkal szembeni ellenálló képesség megteremtése érdekében a stratégia három nagy területen lát szükségesnek intézkedéseket hozni:

- *a 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 – ideértve a kiberbűnözés elleni hatékony fellépést is – fejlesztésre szorul;
- *a jogalkotás területe:* ennek ki kell terjednie a nemzeti stratégia és nemzeti együttműködési terv elkészítésére, valamint azoknak a minimumkövetelményeknek a megfogalmazására, amelyek alapján többek között a nemzeti kiberhatóságok kijelölhetők, valamint megalakíthatók a nemzeti CERT-ek. (European Commission 2013)

A köz- és a magánszektor összefogásának hiányát a stratégia alapvető veszélyforrásként is értékeli: „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." (European Commission 2013)

Ennek megoldására született többek között a NIS-irányelv javaslat, amely közel 3 évvel a kiberbiztonsági stratégia megjelenése után, 2016 közepi elfogadása után – módosításokkal ugyan, de – a tagországokra nézve – 22 hónapos felkészülési időt követően – kötelező érvényű direktívává is vált 2018-ban.

A stratégia az ellenálló képesség megteremtése érdekében nemcsak a fenti – az Európai Parlament és az Európai Tanács felé intézett –, a NIS elfogadását sürgető kérést fogalmazott meg, hanem felhívta az ENISA-t, hogy támogassa a nemzeti képességek kialakítását, ami a stratégiában megfogalmazottak szerint a következőket jelenti: „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." (European Commission 2013)

A fenti megfogalmazásból is kitűnik, hogy az Európai Unió a kiberbiztonsági stratégiában egy olyan holisztikus megközelítést alkalmaz, amely jóval túlmutat a kibertéren, hiszen az olyan kapcsolódó területek biztonságának növelését is célul tűzte ki, mint a kritikus infrastruktúrák területe.

Az ellenálló képesség terén a stratégia kiemeli a kiberbiztonsági tudatosság fejlesztését, amelyben a felhasználók internetes tevékenységeinek minél nagyobb biztonságát hangsúlyozza. E cél megvalósítása érdekében a stratégia ismét segítségül hívja az ENISA-t, de az Europolt és az Eurojustot is.

A tudatosság növelésének egyik jó példája az ENISA által kezdeményezett és szervezett európai kiberbiztonsági hónap rendezvénysorozat, amelyhez a 2013-as első megrendezése óta Magyarország is minden évben többtucatnyi rendezvénnyel kapcsolódik. (European Commission 2013)

A kiberbűnözés drasztikus csökkentése érdekében a stratégia szigorúbb és hatékonyabb jogszabályok meghozatalát és azok betartását kéri a tagországoktól. A dokumentum itt utal a Budapest Konvencióra,[32] amely a tagországok számára megfelelő keretet jelenthet a saját kiberbűnözés elleni jogszabályaik kidolgozásához. A kiberbűnözés elleni hatékonyabb uniós szintű koordináció érdekében a stratégia támogatja az EUROPOL-on belül létrejött Számítástechnikai Bűnözés

[32] A 2001-ben született Budapest Konvenció fő célja a kiberbűnözés és a kiberbűncselekmények elleni tevékenység nemzeti jogszabályokban rögzített harmonizációja. (Council of Europe 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, néhány állam, mint például Oroszország vagy India számos kifogást emelve ezt nem tette meg.

Elleni Európai Központtal (European Cyber Crime Center, EC3)[33] és az Eurojusttal való közös munkát. Az EC3 lehet a központja a kiberbűnözés elleni hírszerzésnek, elemző munkának és operatív beavatkozásoknak.

A stratégia a közös európai biztonság- és védelempolitika (Common Security and Defence Policy, CSDP) részének tekinti a kiberbiztonságot is. Ennek megfelelően a kibertér biztonságának megteremtése – elsősorban a veszélyek és kihívások sokszínűsége és sokfélesége miatt – a polgári és a katonai módszerek együttes alkalmazását igényli. Ezért az Unió a NATO-val közös tevékenységeket tervez a kormányzati hálózatok és védelmi információs rendszerek biztonságának növelése érdekében. Ennek érdekében a stratégia a következő feladatot fogalmazza meg a NATO-val való együttműködés keretében: „Hatékony 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." (European Commission 2013)

A kiberbiztonsági ipari és technológiai erőforrások fejlesztése érdekében a stratégia hangsúlyozza a már meglévő és a jövőben megjelenő termékek számára biztosítandó egységes piac megteremtésének fontosságát, amely során a NIS-ben megfogalmazottak alkalmazása kiemelt szerepet kap. A stratégia ösztönzi a K+F-célú beruházásokat és az innovációt. A stratégia alapján az Európai Bizottság támogatja biz-

[33] Az EC3 az EUROPOL szervezeteként 2013 januárja óta három nagy területen végzi a kiberbűnözés elleni tevékenységet. Kriminalisztikai vizsgálatokat (IT Forensics) vége közreműködik a kiberbűnözés elleni stratégiaalkotásban, és nyomoz a kiberbűncselekmények felderítése érdekében. A stratégiaalkotás, illetve a stratégiák fejlesztése területeken az EC3 két csoportja is dolgozik. Az első csoport feladata a tájékoztatás és támogatás, így az koordinációs segítséget nyújt az EU-tagországoknak, más bűnüldöző hatóságoknak, nemzetközi szervezeteknek, illetve akadémiai és gazdasági együttműködőknek. A másik csoport a kiberbűnözés elleni stratégiai elképzelések kidolgozásáért és azok fejlesztéséért felelős. Ezen belül stratégiai elemzéseket, politikai és jogalkotási intézkedések megfogalmazását, illetve szabványosított képzések fejlesztését is végzik. (Europol 2017a; Europol 2017b)

tonsági szabványok és minősítési rendszerek kialakítását a felhőalapú szolgáltatásokra. Ebben a feladatban is komoly szerepet kap az ellátási lánc, valamint a kritikus infrastruktúra biztonságának növelése.

A stratégia következő kiemelt célja olyan nemzetközi szakpolitika létrehozása, amely a már meglévő nemzetközi szabályozásokra építve járul hozzá az uniós alapértékek biztosításához. Ennek során a következő területeket hangsúlyozza a stratégia:

- 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. (European Commission 2013)

A stratégiában megfogalmazott fő célkitűzések elérése és így az unió kiberbiztonságának növelése érdekében a bizottság mind uniós, mind nemzeti szinten meghatározta azokat a legfontosabb szereplőket és legfontosabb felelősségi köreiket, amelyek nemcsak a kiberbiztonsághoz, hanem a nemzeti biztonsághoz, ugyanakkor így a tagországok összességében az Európai Unió biztonságához is hozzájárulnak. A három pillérre épített szervezeti rendszer a következő:

- hálózati és információbiztonság:
  - EU-szinten: Európai Bizottság, ENISA, EU-CERT, illetékes hatóságok hálózata, EP3R;
  - nemzeti szinten: nemzeti CERT-ek, NIS szempontjából illetékes hatóságok;
- kiberbűnözés elleni fellépés:
  - EU-szinten: EUROPOL EC3, CEPOL, Eurojust;
  - nemzeti szinten: nemzeti kiberbűnözés elleni szervezetek;
- kibervédelem:
  - EU-szinten: EEAS, EDA;
  - nemzeti szinten: nemzeti védelmi és biztonsági hatóságok. (European Commission 2013)

A 2013-ban született uniós kiberbiztonsági stratégia azonban – figyelembe véve a bekövetkezett technikai, politikai és gazdasági változásokat, valamint az ezeken a területeken megjelent új kihívásokat és fenyegetéseket – felülvizsgálatra szorul. A felülvizsgálatot az is sürgeti, hogy a stratégia végrehajtása nem minden területen és nem minden tagországban ment zökkenőmentesen. Jean-Claude Juncker, az Európai Bizottság elnöke az unió helyzetéről szóló szokásos éves beszámolójában 2017 szeptemberében erről a következőket mondta: „Az 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 támadásokkal szembeni védelem megerősítésére, többek között egy európai kiberbiztonsági ügynökség létrehozását." (European Commission 2017a)

Mindezek alapján az Európai Bizottság egy új javaslatcsomagot terjesztett elő, amelyet gyakran a Cybersecurity Act, azaz kiberbiztonsági törvény névvel illetnek, és amely az európai kiberbiztonság teljes reformját irányozta elő. A javaslatcsomag többek között tartalmazza egy új *Európai Uniós Kiberbiztonsági Ügynökség* felállítását is. Ez az új ügynökség ENISA-ra épülve a tagállamok számára nyújt segítséget a kibertámadások megelőzésében és az azokra való reagálásban. Az ügynökség feladatai közé fog tartozni az európai kiberbiztonsági gyakorlatok megszervezése és levezetése. Ezek mellett a javaslatcsomag a digitális termékek és szolgáltatások biztonságos használatát lehetővé tevő és az azokat garantáló új európai tanúsítási rendszer kidolgozását is felvázolja. (European Commission 2017a)

A NIS-irányelv

Ahogy korábban utaltunk rá, az Európai Unió kiberbiztonsági stratégiája két részből áll, amelyből az első rész maga az unió kiberbiz-

tonságra vonatkozó stratégiája, a második rész pedig az úgynevezett NIS-irányelv.

Az irányelv gyakran használatos címe a NIS, amely az angol Network and Information Systems Directive, azaz hálózati és információs rendszerek kifejezésekből ered. Ugyanakkor 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.*[34] (NIS Directive 2016)

A 2013-as NIS-re tett javaslat után közel kettő és fél évre, valamint nagyon kemény tárgyalássorozatra volt szükség ahhoz, hogy magát az irányelvet 2016 júliusában az Európai Parlament és az Európai Tanács elfogadja. (European Commission 2017b)

A nemzeti hálózati és információs rendszerekre vonatkozólag a direktíva egyik legfontosabb előírása a tagállamok számára kötelező: „Valamennyi tagállam elfogad egy hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát, amelyben meghatározza a stratégiai célokat, valamint a hálózati és információs rendszerek magas szintű biztonságának megteremtéséhez és fenntartásához szükséges megfelelő szakpolitikai és szabályozási intézkedéseket, legalább a II. mellékletben említett ágazatokra és a III. mellékletben említett szolgáltatásokra vonatkozóan." (NIS Directive 2016)

Az idézetből is kitűnik, hogy azon kívül, hogy nemzeti szinten létre kell hozni kiberbiztonsági stratégiát, az említett mellékletek előremutató módon tartalmazzák azokat a hálózati és információs rendszereket, azaz kicsit leegyszerűsítve azokat a kritikus infrastruktúra ágazatokat, amelyekre a nemzeti stratégiának ki kell térnie.

A NIS meghatározza azokat a területeket is, amelyeket az említett nemzeti stratégiának tartalmaznia kell. Azaz – ha egy kissé

[34] 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.

továbbgondoljuk ezt a kérdést, akkor – javaslatokat fogalmaz meg arra, hogy milyen tématerületek kerüljenek a nemzeti kiberbiztonsági stratégiába. Ezek a területek a következők:

- 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;
- azok az intézkedések, amelyek a 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 Directive 2016)

A fenti területeket a hazai nemzeti kiberbiztonsági stratégia felülvizsgálata során is azonosítani kell. Bár később részletesen is szólunk Magyarország nemzeti kiberbiztonsági stratégiájáról, az már elöljáróban is elmondható, hogy annak 2013-as megjelenésével számos olyan elem jelen volt a hazai kiberbiztonságban, amelyeket a NIS-en keresztül az Európai Unió csak 2016-tól, illetve a NIS 2018. májusi hatálybalépésétől fogva szabályoz.

A NIS az unión belüli együttműködés biztosítása érdekében egy együttműködési csoport felállítását határozza meg. Az együttműködési csoport 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.

A NIS előírja nemzeti illetékes hatóságok kialakítását és nemzeti kapcsolattartó pont létrehozását, amelyek fő feladata a korábban emlí-

tett – külön meghatározott – ágazatok esetében a hálózati és információs rendszerek biztonságának megteremtése. A hatóságokon kívül létre kell hozni nemzeti és ágazati szinten is számítógép-biztonsági eseményekre reagáló csoportokat (CSIRT-eket, vagy CERT-eket), amelyek mellé megfelelő erőforrásokat, biztonságos kommunikációs és információmegosztási megoldásokat kell biztosítani. A nemzeti kapcsolattartó pont egy központi szervezet kell, hogy legyen, amely az ágazati CSIRT-ek közötti koordinációt, valamint a többi tagország felé a kommunikációt biztosítja. Ennek az úgynevezett egyedüli kapcsolattartó pontnak évente összefoglaló jelentést kell benyújtania az együttműködési csoport felé.

Természetesen a NIS meghatározza a hálózati és információs szolgáltatásokat nyújtó számára is a legfontosabb követelményeket. Ennek megfelelően a direktíva külön kitér azokra a feladatokra, amelyeket az alapvető szolgáltatásokat nyújtó szereplőknek, valamint a digitális szolgáltatóknak kell megtenniük a hálózati és információs rendszerek biztonsága érdekében. (NIS Directive 2016)

2.2. A NATO kibervédelmi stratégiája

A NATO mint politikai és katonai szövetség több évtizedes fennállása során 2007-ben szembesült először azzal a nagyon nehéz politikai és stratégiai dilemmával, amelyet az orosz–észt incidens[35] okozott. A szövetség fennállása alatt ez volt az első olyan – nem a fizikai

[35] Ma már egyre inkább történelmi, illetve klasszikus példaként említik a 2007-es orosz–észt incidenst, amely során 2007. április közepétől közel három héten át – alapvetően DDoS-támadásokkal – a már akkor is igen fejlett észt közigazgatási, banki és egyéb civil információs rendszereket támadták. Ezek a támadások a komoly anyagi károkon kívül nagy társadalmi károkat is okoztak, hiszen egyrészt a kormányzatba vetett bizalom is alaposan megrendült (az átlagállampolgár véleménye teljesen jogos: nem képes a kormányzat, sem a Szövetség – hiszen Észtország ebben az időben már NATO-tag – megvédeni az alapvető információs rendszereket és szolgáltatásokat, és mindamellett a konfliktus komoly biztonságpolitikai percepcióváltozást is okozott. (Kovács 2014)

dimenzióban bekövetkező – támadás, amely a szövetség egyik tagországát érte. Ezzel egy új korszak nyílt, hiszen világossá vált, hogy egy ország már nemcsak a korábban jól meghatározható és jól jellemezhető hagyományos dimenziókban – szárazföld, levegő, tenger, űr –, hanem a kibertéren át is támadható.

Bár a 2002-es prágai NATO-csúcsértekezletet zárónyilatkozatába már bekerült a veszélyek meghatározásánál a kibertámadások növekvő száma és az azokkal szembeni védelem fontossága, mégis az orosz–észt incidens utáni felismerés vezetett a szövetségben arra, hogy a 2010-es lisszaboni NATO-csúcstalálkozó után a szervezet stratégiai koncepciójába is bekerüljön a katonai információs és kommunikációs rendszerek (Communication and Information System, CIS) védelmének feladata. (NATO 2002; NATO 2010)

A lisszaboni csúcstalálkozó után kiadott stratégiai koncepció – a hazai Biztonságpolitikai Szakkollégium fordítását segítségül hívva – így fogalmaz: „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)

Ezt követően a NATO kibervédelem területén meghozott egyik legfontosabb döntésére 2011. június 8-án került sor. Ekkor írták alá a NATO-tagországok védelmi miniszterei a szövetség új kibervédelmi politikáját. Ez a dokumentum nemcsak a kibervédelemre vonatkozó stratégiai elképzeléseket tartalmazta, hanem már magában foglalt egy olyan kibervédelmi cselekvési tervet is, amelynek a részletes programját 2011 októberében fogadták el. (Kovács 2014) Ennek egyik pontja alapján 2012 februárjában elindult a NATO kiberincidens-kezelési képességének (NATO Cyber Incident Response Capability,

NCIRC)[36] teljes kiépítése, amellyel egy időben egy úgynevezett kiberfenyegetés-előrejelző központ (Cyber Threat Awareness Cell) kialakítása is megkezdődött. (NATO 2018; Kovács 2014)

A 2012-es chicagói csúcstalálkozó tovább erősítette a NATO kibervédelmi tevékenységét, amely a stratégia mellett konkrét, kézzelfogható képességfejlesztést is jelentett. A csúcstalálkozó után kiadott hivatalos állásfoglalás szerint: „Építve 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 véghezvisszük 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 a NATO is szembesült azzal a ténnyel, hogy az eltérő technikai fejlettségű országok eltérő módon kezelik a kiberbiztonságot és a kibervédelmet is. Ez nagy kockázatot jelent, amelynek felszámolása azóta is prioritást élvez. Ennek megfelelően a szövetség arról határozott, hogy a nemzeti kibervédelmi képességek fejlesztéséhez minden olyan tagország esetén hozzájárul, ahol ez szükséges. Ez a feladat a chicagói csúcstalálkozó zárónyilatkozatába is bekerült: „Tovább 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)

[36] Az NCIRC technikai központját a koordinációért felelős szervezettel együtt a NATO SHAPE kötelékében Mons-ban, Belgiumban állították fel. Az NCIRC legfontosabb feladata a NATO saját információs rendszereinek és számítógép-hálózatainak védelme. (NATO 2018)

Mindezeken túl a NATO is kifejezte együttműködési szándékát az olyan nemzetközi szervezetekkel, mint például az ENSZ, az EU, az Európai Tanács vagy az EBESZ. Ehhez a munkához hozzájárul a tallinni Kibervédelmi Kiválósági Központ és az az által létrejött szakértelem is. A kiválósági központ volt az egyik kezdeményezője annak a tanulmánykötetnek is, amely a kiberhadviselés nemzetközi jogi szabályozását vizsgálta. A *Tallinn Manual*t, azaz magyarul a *Tallinni Kézikönyv*et 2013-ban adták ki. A tanulmánykötet egyik legfontosabb célja volt, hogy a kiberhadviselés területén alkalmazható nemzetközi jogi és nemzetközi hadijogi kérdéseket megvizsgálja. A vizsgálatok számos egyetem és kutatóintézet közreműködésével készültek, és ezek eredményeit két nagy részre osztva mutatták be. A nemzetközi kiberbiztonsági jog (International Cyber Security Law), illetve a kiberhadijog (The Law of Cyber Armed Conflict) 7 fejezetében összesen 95 úgynevezett szabályt azonosítottak a tanulmány készítői a nemzetközi jog területén. (Schmitt 2013)

Az első kiadást követően 2016-ban jelent meg a *Tallinn Manual 2.0,* amely tartalmazza az első részt is, de annak jelentősen kibővített változatában kapunk választ a nemzetközi jog kiberműveletekben való alkalmazhatóságára. Ez a tanulmánykötet már 154 olyan szabályt elemez, amelyek a nemzetközi jogból levezetve alkalmazhatóak a kiberműveletekben. (Schmitt 2016)

A szövetség 2014-es walesi csúcstalálkozója után egy felülvizsgált kibervédelmi politikát fogadtak el, amelyet 2017-ben egy új akcióterv is követett. A politika rögzíti, hogy a kibervédelem a NATO legfontosabb kollektív védelmi feladatainak része. (NATO 2018)

2016 azonban gyökeres változást hozott a kibervédelem és a NATO viszonyában. Ez az áttörés a 2016-os varsói csúcstalálkozóhoz köthető. Ekkor deklarálta a szövetség hivatalosan is, hogy a kibertér műveleti dimenziónak tekinthető, tehát a kibertér hadviselési dimenzióvá vált. Ennek kapcsán a csúcstalálkozó hivatalos zárónyilatkozata a következőképpen fogalmaz: „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."[37] (NATO 2016a)

Ezzel egy időben a tagországok egy NATO kibervédelmi felajánláscsomagot (NATO Cyber Defence Pledge) is elfogadtak. Ebben az országok a következő képességek és feladatok kialakítását vállalták:

- a nemzeti információs infrastruktúrák és számítógép-hálózatok védelmének teljes körű 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;

[37] Az eredeti angol nyelvű szöveg: "Cyber attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea." (NATO 2016a) Meg kell jegyezni, hogy mivel a NATO-nak nincsenek olyan képességei, amelyek az űrben lennének alkalmazhatóak, ezért az űr hiányzik a hagyományos dimenziók felsorolásából.

- felgyorsítják a kötelezettségvállalások végrehajtását, beleértve azoknak a nemzeti rendszerek körét is, amelyekre a NATO is támaszkodik;
- a felajánláscsomagban foglaltak végrehajtásának nyomon követésére mutatókon alapuló értékelést készítenek, amelyet a következő csúcsértekezleten megvizsgálnak. (NATO 2016b)

Hangsúlyozni kell, hogy a kibervédelem kérdésére a szövetség alapvetően mint a tagországok kötelezettségére tekint. Ugyanakkor mivel az is teljesen világos, hogy a kibervédelmet egy-egy tagország egyedül nem képes nemzetközi együttműködés nélkül megvalósítani, ezért a tagországok összefogása és folyamatos párbeszéde elengedhetetlenül fontos. Ennek 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.

2017 decemberében a NATO főtitkára, Jens Stoltenberg bejelentette, hogy a szövetség tagországainak védelmi miniszterei megállapodtak abban, hogy egy kibervédelmi műveleti központot állítanak fel, amely a NATO parancsnoki struktúrájának része lesz: „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)

Amennyiben ez a kiberműveleti központ megkezdi munkáját, akkor a NATO kiberteret érintő történetében egy új korszak nyílik, hiszen már nemcsak nemzeti, de szövetségi szinten is lesz olyan képesség, amely a meghatározott jogi keretek között képes lesz a szövetség közös érdekei és értékei védelme érdekében kibertevékenységeket folytatni.

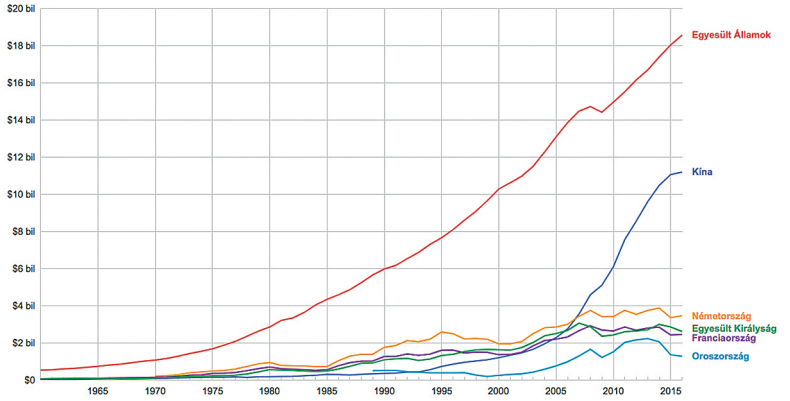
3. Nagyhatalmak kiberbiztonsági stratégiái

Mielőtt megvizsgálnánk a kiberbiztonságot és annak szabályozását néhány globálisan is jelentős ország – nevezetesen Kína, Oroszország és az Egyesült Államok – vonatkozásában, érdemes egy pillantást vetnünk ezeknek az országoknak a gazdasági teljesítőképességére is. A könnyebb összehasonlíthatóság érdekében – és nem utolsósorban a kontraszt érzékeltetése miatt – feltüntettük néhány szintén jelentős gazdasági szereplő – Németország, az Egyesült Királyság, illetve Franciaország – teljesítményét is.[38] Ez jól érzékelteti azoknak a nagyhatalmaknak a gazdaságát, azok egymáshoz való viszonyát, amelyeket be kívánunk mutatni a következőkben.

Mindhárom vizsgált ország esetében megvizsgáljuk – ahogy ezt a később a bemutatni kívánt európai uniós tagországok esetében is megtesszük –, hogy az adott ország teljes lakosságának számához viszonyítva hányan és milyen arányban használják az internetet, azaz mekkora az adott ország internetpenetrációja. Ez sok esetben egyenes arányban van az adott ország digitális gazdaságával és digitális társadalmával, de nagybani következtetéseket tudunk levonni az adott ország kibertérrel kapcsolatos viszonyát illetően is. Természetesen ezen kívül sok olyan egyéb tényezőt is figyelembe kellene még venni, mint például az adott ország digitális infrastruktúrájának fejlettsége vagy a digitális gazdaság teljes gazdaságban betöltött szerepe, azonban ezek egyrészt nagyon gyorsan változnak, másrészt nem járulnak hozzá érdemben jelenlegi – kiberbiztonsági stratégiákat érintő – vizsgálatainkhoz.

---

[38] Természetesen egy adott ország gazdasági teljesítőképessége sok tényező vizsgálata alapján mutatható csak be. Itt azonban csak a bruttó hazai összтermék, azaz a GDP értékét adjuk meg az amerikai dollár aktuális árfolyamán. Ezek az értékek nincsenek az inflációhoz igazítva.



4. ábra

Az Egyesült Államok, Kína, Oroszország, valamint Németország, Franciaország és az Egyesült Királyság nemzeti összтermékének alakulása 1990 és 2015 között

Forrás: Google 2018

3.1. Kína és a kiberbiztonság

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) Pedig másfél évtizede még nem is keltett nagy visszhangot a volt amerikai elnöki nemzetbiztonsági tanácsadó, Zbigniew Brzezinski figyelmeztetése, amely szerint az Egyesült Államok legnagyobb vetélytársa és az egyik meghatározó világhatalom az akkor még csak közelgő új évezred elejére Kína lesz. (Brzezinski 1999; Kovács 2009a)

10. táblázat

Kína internetpenetrációja 2016-ban és 2017-ben

Kína			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	1382	721,4	52,2%
2017	1388	738,5	53,2%
Világ			
2017	7519	3885	51,7%

Forrás: www.internetlivestats.com/internet-users/china/, www.internetworldstats.com/asia.htm#cn, a szerző szerkesztése

Ugyanakkor Brzezinski jóslata ma már nemcsak gazdasági téren látszik beigazolódni, hanem a katonai potenciál különböző szegmenseiben is. Ennek igen szembetűnő jelét adják azok a kínai törekvések, amelyek az információs technológia polgári felhasználása mellett azok egyre több katonai alkalmazásában figyelhetők meg. Olyan új kínai haditechnikai eszközök jelennek meg a hagyományos fegyverek területén is, amelyek alapvetően az információtechnológiára alapozva jöhettek létre, és akkor még nem is beszéltünk a kínai kiberfegyverekről.

Mindezek alapján teljesen nyilvánvaló, hogy Kína a kibertér minden szegmensére rendkívül nagy hangsúlyt fektet. Ennek köszönhetően már ma is meghatározó és megkerülhetetlen világméretű kibertéri szereplő ez a hatalmas ország, hiszen 2017-ben a kínai internetfelhasználók száma közel 740 millió fő volt, ami a világ összes internethasználójának közel 20%-a. Ezen kívül egyre dominánsabb a kínai információtechnológiai vállalatok világszintű technológiai fejlettsége, amellyel ezek a cégek ma már a világ élmezőnyébe kerültek.

3.1.1. Kína viszonya a kibertérhez

Az információtechnológia robbanásszerű fejlődése talán pont Kína esetében volt a legmarkánsabban nyomon követhető. A gazdasági fejlődés egyik motorja az információtechnológia és közvetett módon az internet lett az elmúlt évtizedben. Ez számos kérdést felvetett a kommunista berendezkedésű, de gazdaságát kapitalista módon kezelő és menedzselő rezsim életében.

Bár 2013-ban az ENSZ egyik szakértői csoportjának jelentésében, amelyet Kína is támogatott, megállapította, hogy az államok kibertérben történő tevékenységének szabályozására az *ENSZ Alapokmánya,* valamint a nemzetközi jog teljes mértékben alkalmazható (United Nations 2013), Kína mégis egy meglehetősen érdekes felvetést tett ezzel kapcsolatban 2011-ben, amelyet azután 2015-ben ki is egészítettek. (United Nations 2015, idézi: Raud 2016) Kína ugyanis a Shanghaji Együttműködési Szervezeten (Shanghai Cooperation Organisation – SCO) keresztül többek között Oroszországgal, valamint számos közép-ázsiai országgal – például Kazahsztánnal, Kirgizisztánnal, Tádzsikisztánnal és Üzbegisztánnal – közösen az ENSZ 2011-es közgyűlésén egy saját információbiztonságra vonatkozó nemzetközi magatartási kódexet nyújtott be. 2015-ben ezt az eredeti dokumentumot kissé átdolgozva és kiegészítve ismét az ENSZ közgyűlése elé tárták. A közleményben megfogalmazottak szerint az új internetes magatartási kódex célja, hogy „az információs térben azonosítsa az államok jogait és felelősségét, előmozdítsa a konstruktív és felelősségteljes magatartásukat, valamint fokozza együttműködésüket az információs térben jelentkező közös fenyegetések és kihívások kezelésében" (United Nations 2015)

A magatartási kódex önkéntes alapon várta azoknak az országoknak a csatlakozását, amelyek elkötelezettek a fentiekben megfogalmazott alapelvek mellett. A dokumentum 13 pontban rögzítette azokat a főbb megállapításokat, amelyeket a csatlakozó országok magukra nézve kötelező érvényűnek tekintenek. Ilyen elvek például az *ENSZ*

*Alapokmányá*ban foglaltak egyetemleges teljesítése vagy például annak vállalása, hogy „nem alkalmaznak információs és kommunikációs technológiákat, valamint információs és hírközlési hálózatokat abból a célból, hogy megzavarják más ország belső ügyeit, vagy hogy aláássák annak politikai, gazdasági és társadalmi stabilitását." (United Nations 2015)

Ez különösen annak fényében érdekes, hogy Oroszország – többé-kevéssé bizonyítottan – beavatkozott a 2016-os amerikai, illetve a 2017-es francia és német elnökválasztásokba. (Kovács–Krasznay 2017)

Az nyilvánvalóan az idézett javaslatot megfogalmazó országok felsorolásánál is látszik, hogy azok nemzetállami mivolta nagyon hangsúlyos, azaz ezt a kibertérre lefordítva: ezen országok nagyon érzékenyek a kibertér nemzetközi szintű szabályozására, amely szerintük az adott ország feladata és felelőssége kell, hogy legyen. Ennek megfelelően ez a kibertérben is megjelenik az említett országok vonatkozásában. Kína esetében ez két komoly következményt is magában hordoz. Az egyik: a kibertérben megjelenő felhasználók irányítását és ellenőrzését az államnak kell végeznie. A másik: a kibertér szuverenitása közvetlenül az adott ország, tehát ebben az esetben Kína szuverenitását is meghatározza. Így annak szabályozása nem történhet külső szervezet – például az ICANN[39] (Internet Corporation for Assigned Names and Numbers) – vagy külső jogrend alapján.

Kínának a kibertér nemzetközi szabályozását illető álláspontját, azaz egy sokkal szélesebb nemzetközi irányításra való igény megfogalmazását sok elemző osztja, hiszen jelenleg ezen a téren az USA dominanciája – például a nagy nemzetközi szervezetek vezetésében vagy a nemzetközi jog meghatározásában – nagyon erős. Ennek ellenpólusa

[39] Az ICANN egy nonprofit közhasznú társaság, amelynek résztvevői a világ minden tájáról biztosítják az internet biztonságos, stabil és interoperábilis működését. A szervezet előmozdítja a versenyt és fejleszti az internet egyedi azonosítókkal kapcsolatos politikáját. Az internet elnevezési rendszerének koordinációs szerepén keresztül fontos hatással van az internet bővítésére és fejlődésére. (ICANN 2018)

lehetne egy Kína által javasolt közös és integrált globális internetes irányítás. (Raud 2016)

3.1.2. Kína és a kibertér szabályozása

Az információ szabad áramlásának kérdése sokáig komoly dilemma volt a kínai vezetés előtt. A megoldandó kérdés ugyanis sokáig az volt, hogy hogyan lehet akár valós időben ellenőrizni azt, hogy a kínai állampolgárok az internet segítségével milyen információkhoz jutnak hozzá. (Raud 2016) Ennek megoldása, tehát az internet szabályozása persze nem az első olyan kérdés, amely meglehetősen egyedülálló volt Kínában.

Kína a webes cenzúra biztosítására egy, a nyugati országokban csak Kínai Nagy Tűzfalnak nevezett saját rendszert fejlesztett ki, amelyet annak 2003-as indulása óta folyamatosan használ. Azonban ez csak egy része, illetve egy speciális eleme a hivatalos nevén *Aranypajzsnak* (Jindun gongcheng) nevezett hardver- és szoftveregyüttesnek, amelyet a kínai Közbiztonsági Minisztérium tart fent. Az Aranypajzs hivatalos kínai megnevezése *Nemzeti Közbiztonsági Információs Technológia,* amely mellett számos más biztonsági – „arany" – rendszer is működik, mint például az *Aranyhíd* rendszer, amely egy gazdasági információs rendszer, az *Arany szokások* rendszer, amely a külföldi üzleteket felügyelő rendszer, vagy az *Aranyadó* rendszer, amely nevéből adódóan is az adózást felügyelő rendszer.

Amíg korábban a 300 millió kínai internetfelhasználót 50 ezer „netrendőr" ellenőrizte folyamatosan, azaz ennyi ember működött közre többek között a Kínai Nagy Tűzfal üzemeltetésében, addig az internetfelhasználók számának növekedésével – ne felejtsük el, hogy 2017-ben már közel 740 millió fő internetezett Kínában – ez a szám is nyilvánvalóan együtt növekedett. (Kovács 2009a)

A rendszer által korábban a leggyakrabban cenzúrázott tartalmak közé tartoztak az olyan politikailag betiltott csoportok, mint a Falun

Gong vagy az olyan hírforrások, amelyek például az 1989-es Tienanmen téri tüntetéssel foglalkoztak. Mindezek mellett cenzúrázzák a tajvani kormány hivatalos oldalait, a pornográf webes tartalmakat, illetve a Tibet függetlenségéhez kapcsolódó információkat. Ehhez számos technikai megoldást alkalmaznak, többek között például az IP-címek blokkolását. Ez nem jelent mást, mint azt, hogy a gyanús, illetve nem kívánatos IP-címek esetében blokkolják a HTTP, az FTP vagy akár a POP3 protokollokat. Amennyiben egy szerver több weblapot hosztol, és azok akár egyikén is van olyan tartalom, amely tiltott, akkor az összes hosztolt oldalt elérhetetlenné teszik. Hasonló technikai lehetőség a nem kívánt tartalmak elérhetőségének korlátozására a DNS-szűrés és -átirányítás, amely során az olyan tartományneveket, amelyeken tiltott tartalom van, a DNS-szerver egyáltalán nem oldja fel, vagy hibás IP-címet küld vissza a felhasználónak. Egy másik szűrési megoldás a kulcsszavak alapján történő csomagszűrés, amely URL esetében is jól működik. Ez azt jelenti, hogy az előre meghatározott szavakra vagy fogalmakra történő keresés esetén a rendszer blokkolja a kapcsolatot. Ez korábban már a keresőmotorok esetében is működött. (Kovács 2009a)

Természetesen a cenzúráról nem áll rendelkezésre nagyon sok és részletes hivatalos információ, de látható, hogy a kínai állam számos feltételt szab a nyugati – és így az olyan nagy technológiai cégek számára is –, amelyek többek között előírják, hogy a blogok használata regisztrációhoz kötött, a felhasználók adatait pedig a szolgáltatók kötelesek átadni a hatóságoknak. Persze erre van hivatalos magyarázat, miszerint minderre a felhasználók védelme érdekében van szükség, azaz így kívánják megvédeni az állampolgárokat a kiberbűnözéstől és az egyéb olyan veszélyektől, amelyek a felhasználók biztonságát fenyegethetik.

Több mint egy évtizede a Google is arra a következtetésre jutott, hogy ha Kínában jelen akar lenni, akkor el kell fogadnia a kínai állam feltételeit. 2006-ban, a keresőóriás kínai változatának, a google.cn-nek az elindításakor Andrew McLaughlin, a Google kormányzati

kapcsolatokért felelős vezetője a következőket mondta: „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)

Mindezek mellett Kína sokkal drasztikusabban is fellép a neki nem tetsző helyzetekben. Erre az egyik legmarkánsabb példa a 2009 nyarán Hszincsiang tartomány fővárosában, Urumcsiben kitört ujgur zavargások után az adott területen az internet-hozzáférés korlátozása és a nemzetközi telefonvonalak lekapcsolása volt. Ennek kiváltó oka az volt, hogy a kínai kormány feltételezése szerint a szeparatista Ujgur Világkongresszus vezetője – Rebija Kadír – az internet segítségével szervezte és irányította a tüntetéseket. (Jacobs 2009)

Persze más hasonló lépéseket is gyakran megtesznek a kínai hatóságok. A Tienanmen téri tüntetések több évfordulója alkalmával is megtörtént, hogy az olyan közösségi weboldalakat – például a Twittert –, amelyeken a megemlékezésekkel kapcsolatos beszámolók nyilvánosságra kerültek, egyszerűen blokkolták. Emellett több esetben előfordult korábban, hogy zavarták a BBC, a CNN és a TV5 Monde kínai adásait is, amelyek a Tienanmen téri tüntetések évfordulója alkalmából tudósítottak volna. (MTI–Origó 2009)

3.1.3. Kémek a kibertérben: a katonai kapcsolat és a korlátlan hadviselés elmélete

A kibertér, illetve annak biztonsága területén a 2000-es évek legelején Kínában alapvetően a katonai gondolkodás dominált. Információbiztonsággal kapcsolatos publikációk alapvetően csak katonai folyóiratokban jelentek meg.

Ugyanakkor figyelemreméltó egy 1999 februárjában megjelent könyv, amelyet részben a modern kínai katonai gondolkodás és stra-

tégia alapjának is tekintenek. A könyv, amelynek angolra fordított címe *Unrestricted Warfare* (magyarul: korlátlan hadviselés) két kínai ezredes – Qiao Liang és Wang Xiangsui – neve alatt jelent meg a Kínai Népi Felszabadítási Hadsereg hivatalos kiadója gondozásában. A könyvet az amerikai FBIS (Foreign Broadcast Information Service), azaz a CIA külföldi információs szolgálata fordította és jelentette meg angolul 2000 januárjában.

Ezt követően 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. Ez a kiadás már jóval az Egyesült Államokat ért 2001. szeptember 11-i terrortámadások után, de még a támadások okozta közvetlen sokkhatás idején jelent meg. Talán ennek is köszönhető a könyv hátsó borítóján lévő ajánlások legkevésbé sem visszafogott hangneme, amelyek összefüggést véltek felfedezni 9/11 és a kínai korlátlan hadviselés között.

Pedig a könyv egy nagyon mély katonai-szakmai alapossággal megírt mű, mondhatnánk, hogy egy igazi átfogó, hadtudományi elemzés, amelyben kétségtelenül megjelenik az Egyesült Államok, de alapvetően az USA haderejének az elmúlt idők fegyveres küzdelmeiben és háborúiban játszott szerepe, az azokban alkalmazott stratégiájának és a katonai vezetésének elemzése kap fő hangsúlyt. A könyv számos kritikát is megfogalmaz az amerikai fegyveres erők vezetési rendszerével szemben, kezdve a második világháborútól Grenadán át az Öböl-háborúig. Persze nagyon nehéz európai szemmel és gondolkodással a könyv mondanivalóját és főbb gondolatmeneteit követni, hiszen a több ezer éves kínai hagyományokkal rendelkező gondolkodók sokszor egészen más értelmet adnak azoknak a képeknek és metaforáknak, amelyeket a nyugati világban megszoktunk, illetve alkalmazunk. Erre az egyik legjobb példa a könyvből a következő idézet: „A háborút a legnehezebb megmagyarázni és megérteni. A háborúnak szüksége van a technika támogatására, de a technológia nem helyettesítheti a morált és a stratégiát; szüksége van művészi inspirációra,

de elutasítja a romantikát és a szentimentalizmust; matematikai pontosságra van szüksége, de a pontosság néha mechanikus és merev; filozófiai absztrakcióra van szüksége, de a tiszta gondolkodás nem segíti a rövid életű lehetőségeket a vas és a tűz közepette." (Liang–Xiangsui 2002)

Az öbölháborúval kapcsolatban pedig a nagyon beszédes, *A légi-szárazföldi csatán túl* című alfejezetben a következő gondolat jelenik meg: „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 világűrben és a kibertérben történő harcot, illetve azok megszállását is." (Liang–Xiangsui 2002)

A tanulmány leszögezi, hogy a technológiai fejlődés, valamint a korszerű haditechnikai eszközök alkalmazása nemcsak, hogy szükséges a korszerű háborúban, hanem majdhogynem elengedhetetlen. Ugyanakkor az amerikai technológiába vetett hitet, illetve a „technika majd mindent megold és győzelemre vezet minket"-elvet kerülendőnek tartja, és sok esetben ebben látja az amerikai katonai vezetés egyik legnagyobb hibáját: „Az összhaderőnemi műveletektől a minden dimenzióban háború [elméletéig] csak egy lépés megérteni azt, ami az amerikai katonai gondolkodás mögött, azaz a relatív technológiai fölény mögött van. A feltételezett jövőbeni háborúkban más országokkal összehasonlítva az amerikai katonai gondolkodást teljes mértékben áthatja a high-tech technológia szemlélete." (Liang–Xiangsui 2002)

Bár a könyv nem szól konkrét kibertevékenységekről, hiszen a 90-es évek végén járunk még csak, de már sok helyen hangsúlyozza a kibertér fontosságát, valamint az ott folytatott műveleteket.

Pedig Kína már ebben az időben is jelen volt a kibertér különböző műveleteiben. Ezek azonban nem mindig katonai műveletek, sőt ellenkezőleg, alapvetően még nem katonai célból és nem feltétlenül katonai célpontok ellen irányuló műveleteket jelentettek. Az pedig ekkor még végképp nem volt, hogy ezeket a kibertéri műveleteket a kínai hadsereg hajtaná végre, ráadásul akkoriban még ennek az állami támogatású mivoltára sem utalt semmi.

Azóta persze Kínát sokszor éri az a vád, illetve a gyakran kézzel fogható bizonyítékok hiányában egyelőre csak 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)

Ezekre a gyanús tevékenységekre világított rá az Egyesült Államok Kongresszusa számára 2008 őszén készült jelentés, amelyben annak készítői megállapították, hogy már 2002-től kezdődően számos Kínának tulajdonítható informatikai behatolássorozatot észleltek az USA-ban. Ezek a kiberkémkedési akciók a katonai, kormányzati és kormányhoz közel álló közepes és nagyvállalatok számítógépes rendszereit és hálózatait érintették. Az egyik legnagyobb ilyen akció később a Titan Rain (Titán Eső) nevet kapta. Ez egy egészen hosszú és jól felépített kiberkémkedési akciósorozat volt, amely során – feltételezhetően – kínai hackerek közel 20 terabyte-nyi adathoz fértek hozzá. A 2000-ben kezdődött támadást csak 2003-ban fedezték fel egy véletlennek köszönhetően. A támadás célpontjai között a NASA mellett egyértelműen olyan hadiipari nagyvállalatok voltak, mint például az amerikai légierő számára harci repülőgépeket fejlesztő Lockheed Martin vagy a Redstone Arsenal, amely vállalat az egyik legfontosabb amerikai rakétavédelmi rendszert gyártja.

A Titan Rain támadássorozat 2002-ben kezdődött, de elemző cégek még 2005-ben is találtak arra utaló nyomokat, hogy elsősorban kínai területről érkeztek illegális számítógépes behatolások olyan

nagyvállalatok és kutatóintézetek rendszereibe, mint például a SANS Institute, a Lockheed Martin, a Sandia National Laboratories, a Redstone Arsenal vagy a NASA. Természetesen a Pentagon különböző rendszereit is érintették a támadások. Ugyanakkor itt is megfigyelhető volt, hogy elsősorban a nem titkos rendszerekből töltöttek le adatokat a hackerek. (Kovács 2009a)

Az említett kongresszusi jelentés kiemeli, hogy a Titan Rain alatt ellopott adatmennyiség összehasonlítható a világ legnagyobb könyvtárában, azaz a Kongresszusi Könyvtárban tárolt összes könyv digitalizációja esetén megjelenő adatmennyiséggel, amely körülbelül 10 terabyte-nyi adatot tesz ki. (USCC 2008)

2013-ban a Mandiant nevű, jelenleg a FireEye (USA) információbiztonsági csoporthoz tartozó, fő profiljában kiberbiztonsági elemzésekkel foglalkozó vállalat egy jelentésben foglalta össze Kína kiberkémkedéssel kapcsolatos tevékenységeit. (FireEye 2017)

A jelentés, amelynek címe *APT1, Exposing One of China's Cyber Espionage Units,* azaz magyarul *APT1, Kína egyik kibertérben működő kémszervezetének bemutatása,* kiemeli, hogy 2006 és 2013 között közel 200 APT- (Advanced Persistent Threat, azaz fejlett, folyamatosan fennálló) támadásra szakosodott csoportot azonosítottak, amelyek közül 20 volt Kínához köthető. Ezek közül az egyik az APT1 nevet kapta (erre utal a jelentés címe is). A közel 7 évig tartó vizsgálatsorozat során sikerült az APT1 közel 150 áldozatát felderíteni és azonosítani.

A Mandiant megállapította, hogy az APT1 négy sanghaji hálózathoz köthető, és az általuk infrastruktúra és a támadások kivitelezésének módjai is elkülöníthetők, így az azok mögött álló támadók is jól azonosíthatók. A cég azt a következtetést vonta le, hogy az APT1 a hivatalos kínai kormány által támogatott csoport. Erre a megállapításra közvetett bizonyítékként szolgál az, hogy az APT1 sokáig tartó és kiterjedt kémkedést hajtott végre állami és katonai célpontok ellen. Az elemzés azonban ennél tovább is megy, és kijelenti, hogy az APT1 mögött a Kínai Népi Felszabadítási Hadsereg (People's Liberation Army, PLA) Vezérkarának 2. Csoportfőnöksége alatt működő

61398 nevet viselő egység áll. Ezt természetesen vizsgálati eredményeikre alapozva tették meg, és a vizsgálat során megállapították, hogy az APT1 és a 61398 egység Shanghaj ugyanazon negyedében, ugyanabban az utcában, sőt ugyanabban az épületben található. Mindezeken túl a két szervezet hasonló feladatokat lát el, nagyon hasonló képességekkel és erőforrásokkal bír. A jelentés összességében azt a konzekvenciát vonta le, hogy a csoport alapvetően a hadsereghez köthető, mégis a fő cél a különböző cégektől és szervezetektől való szellemi tulajdon ellopása volt. (FireEye é. n.)

A jelentés szerint az APT1 demonstrálta azt a képességét is, hogy egyidejűleg több tucat szervezettől is képes adatokat lopni, valamint azt, hogy miután az APT1 hozzáférést biztosított a megtámadott rendszerhez, ezt a hozzáférést több hónapon át vagy akár több évig is fenntartották. Volt olyan célpont, amely esetében közel 4 évig volt hozzáférése a támadóknak. Az átlagos hozzáférési idő is igen hosszú volt, hiszen azt APT1 átlagosan 356 napig volt jelen egy-egy rendszerben. (FireEye é. n.)

Egyes jelentések szerint az APT1 mellett már 2008-ban megközelítőleg 250 olyan hackercsoport volt Kínában, amelyek nemcsak, hogy államilag megtűrtek és támogatottak voltak, hanem ezek közül számos egyenesen a kínai hadsereghez volt köthető. (USCC 2008)

Persze már a Mandiant elemzése előtt is voltak hírek a kínai kiberkémkedésről. Az egyik ilyen nagy visszhangot kiváltott eset 2007 augusztusában Németországban történt, amikor több kormányzati számítógépen is kínai kémprogramokat találtak. Ez az ügy azért vált különösen érdekessé, mert mindez néhány nappal Angela Merkel német kancellár hivatalos kínai útja előtt került napvilágra. Természetesen a hivatalos szervek igyekeztek az esemény volumenét és az általa okozott károkat minimalizálni, de a Német Szövetségi Alkotmányvédelmi Hivatal egyik korábbi jelentésében már utalt arra, hogy Németország kiemelt célpontja a kínai – elsősorban gazdasági – kémkedésnek. Az eset után a *Der Spiegel* szakértőkre hivatkozva jelentette, hogy az ügy kirobbanása után a hatóságoknak sikerült megakadályozniuk

egy 160 gigabyte-os adatcsomag elindítását a kínai IP-cím felé. (Der Spiegel 2007, idézi Kovács 2009a)

Ezek a támadások egészen újszerűek voltak, hiszen ezt megelőzően elsősorban az ipari kémkedés és a szellemi tulajdon ellopása volt jellemző. Ezek a támadások Németország esetében több milliárd dollár kárt okoztak, és feltételezhetően most is okoznak évente. (Der Spiegel 2013)

Egy másik fajta támadásra 2008 áprilisában került sor, amikor kínai hackerek összehangolt támadást terveztek a CNN hírcsatorna ellen. A támadás azokra a kritikus hangvételű riportokra adott válasz volt, amelyek a pekingi olimpia előtt kialakult tiltakozó megmozdulások hivatalos kínai kezelését mutatták be. (CNN 2008)

Ennél sokkal súlyosabb támadás történt azonban, amikor kínai (és feltehetően orosz) hackerek behatoltak az Egyesült Államok villamosenergia-irányító rendszerébe 2009-ben, amely során a támadók számos rendszerelemet elértek, és bár a támadók nem okoztak nagy kárt, de az nyilvánvaló volt, hogy a rendszerek sok gyenge és sebezhető pontját feltérképezték. Nem ez volt azonban az első ilyen támadás, hiszen a kaliforniai elektromos rendszerbe már 2001-ben behatoltak hackerek, de nem is ez volt az utolsó támadás, mert azóta is számos alkalommal – a nyilvános híradások szerint 2013-ban, 2015-ben és 2017-ben is – történtek ilyen, az egyik legfontosabb kritikus infrastruktúrát, illetve kritikus információs infrastruktúrát célzó támadások. Persze rögtön hozzá kell tenni, amit már többször hangsúlyoztunk, hogy az elkövetők kilétének bizonyítása nagyon nehéz, főleg, ha belső munkatárs is segíti őket. (Pagliery 2015)

Ahogy utaltunk rá, a fent bemutatott támadásoknál nem minden esetben sikerült 100%-ig bizonyítani, hogy azok kínai eredetűek, de közvetett bizonyítékok sok esetben rendelkezésre állnak. A *New York Times* számolt be először arról az Edward Snowden által kiszivárogtatott dokumentumról, amely szerint az NSA (National Security Agency, Nemzeti Biztonsági Ügynökség) már 2010-ben megfigyelte a kínai Kuangtun tartományban székelő, ezen belül is sencseni

központú világméretű IT-vállalat, a Huawei belső kommunikációját. (Sanger–Perlroth 2014, idézi: Raud 2016) Az NSA műveletének, amely a Shotgiant nevet viselte, legfontosabb célja az volt, hogy feltárja és bizonyítsa a Huawei és a Kínai Népi Felszabadítási Hadsereg közötti kapcsolatokat. Az amerikai titkosszolgálat persze ennél többet is el szeretett volna érni, nevezetesen azt, hogy az általuk a Huawei-eszközökben elhelyezett kódok segítségével azokban az országokban, ahol nem amerikai hálózati és egyéb informatikai eszközöket használnak, meg lehessen figyelni a hálózati forgalmat és a kommunikációt. (Sanger–Perlroth 2014, idézi: Raud 2016)

Ezen kívül az amerikai titkosszolgálatok több mint 20 kínai hackercsoport aktivitását kísérik figyelemmel. Nyilvánvalóan az amerikai hivatalos álláspont szerint ezek a kibertámadások és betörések csak törvényes módon, nemzetbiztonsági okok miatt történtek, és ahogy az említett *New York Times*-cikk idézi: „Mi nem az amerikai vállalatok versenyképességének javítása vagy azok megsegítése miatt gyűjtünk hírszerzési adatokat. Sok ország ezt nem mondhatja el magáról." (Sanger–Perlroth 2014)

2015 őszén azonban Barack Obama amerikai és Hszi Csin-ping (pinjin átírásban: Xi Jinping) kínai elnök tárgyalóasztalhoz ült. A tárgyalások során a tárgyaló felek kötelezettséget vállaltak arra, hogy nem támogatják a kibertérben elkövetett, a szellemi tulajdonra, a kereskedelmi titkokra vagy a bizalmas üzleti információkra vonatkozó lopásokat. (Raud 2016)

Az amerikai–kínai csúcstalálkozót követően számos elemzés rámutatott, hogy valóban csökkent az amerikai cégek elleni kibertámadások száma, azonban rögtön azt is sietve hozzáteszik, hogy ez az elkövetések sokkal szofisztikáltabbá válásának, azaz nehezebb felderíthetőségének vagy akár más országok célpontként való megjelenésének is betudható. (Harold 2016, idézi: Raud 2016) (FireEye 2016)

3.1.4. Kína amerikai nézőpontból

Az Amerikai Egyesült Államok Kongresszusának egyik bizottsága, amely az *Egyesült Államok és Kína gazdasági és biztonsági felülvizsgálati bizottság* nevet viseli, 2000 óta minden évben értékeli a két ország kapcsolatát. Az értékelés számos területen vizsgálja a kínai politikai, gazdasági és katonai képességeket, lehetőségeket és az esetleges műveleteket, azoknak az Egyesült Államok biztonságára, gazdaságára és katonai tevékenységére gyakorolt hatásai alapján. A jelentés kitér Kínának az energia és a természeti erőforrások területén meglévő lehetőségeire és az e területeken meglévő kihívásaira; értékeli Kína kül- és katonai politikáját, ezen belül részletesen bemutatja az ország katonai terveit és doktrínáját, a hadsereg felépítését és szervezetét, illetve annak fejlesztési elképzeléseit. Külön elemzés tárgya Kína katonai döntéshozatali folyamata, valamint a polgári és katonai vezetés közötti kölcsönhatás. (USCC 2015)

A jelentések külön értékelik Kína kibertérben játszott szerepét. Ennek során a Kongresszus részletesen megismerheti Kína kiberképességeinek és kiberműveleteinek stratégiai, gazdasági és biztonsági vonatkozásait, nyilvánvalóan amerikai szemszögből vizsgálva. (USCC 2017)

A 2017-es jelentésben ez utóbbi, azaz Kína kibertéri tevékenysége *A kínai belföldi információellenőrzés, a globális médiabefolyás és a kiberdiplomácia* című fejezetben kapott helyett. Önmagában már ennek a fejezetnek a címe is nagyon beszédes, de ha vetünk egy pillantást a fejezet legfontosabb megállapításaira, akkor tovább erősödhet bennünk az a kép, amely Kínával kapcsolatban az eddig elmondottakból már nagy vonalakban rendelkezésre állhatott. A kongresszusi jelentés legfontosabb – az információ ellenőrzésére, a média befolyásolására, valamint a kibertér egyéb tevékenységeivel kapcsolatban tett – megállapításai a következők:

- Kína jelenlegi információ-ellenőrzési gyakorlata, valamint a kormány újmédia-ellenőrzési terve jelentős (negatív) előrelé-

pést jelent a hatósági cenzúra, az emberek megfigyelése és a magánélet megsértése területén;

- a kínai újságírók állami elnyomása ma már egyre inkább kiterjed a külföldi újságírókra és azok Kínában dolgozó munkatársaira. Ebből következően a politikailag érzékeny történetek 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 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 kínai ügyekben;
- a kínai kormány hivatalosan az internet szuverenitását hangsúlyozza, ezzel igazolja, illetve gyakorlatilag legitimálja a szólásszabadság korlátozását az országban. Ugyanakkor mindez kereskedelmi céllal akadályozza az amerikai vállalatok határokon átnyúló adatátvitelét, ami 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)

Mindezekkel a megállapításokkal összefüggésben a vizsgálat, illetve az annak eredményét összefoglaló kongresszusi jelentés számos ajánlást fogalmaz meg az Egyesült Államok számára. Ezek között olyan fontos javaslatok is vannak, amelyek például az említett amerikai

médiavállalkozásokban meglévő kínai jelenlétet igyekeznek feltérképezni és szabályozni úgy, hogy legyen bejelentési kötelezettsége az ilyen cégeknek, ezzel átláthatóbbá téve az amerikai területen vagy amerikai érdekeltségek ellen folytatott esetleges kínai információs műveleteket. Hasonlóan fontos javaslat a média kínai befolyásolásának ellensúlyozására vagy lehetőség szerinti ellensúlyozására a szövetségi kommunikációs szabályokban olyan változtatások megtétele, amelyek előírnák a kínaiak által szponzorált médiatartalom feltüntetését. (USCC 2017)

A fentiek mellett az amerikai hadsereg is megkülönböztetett figyelmet szentel a kínai hadsereg által támogatott kiberhadviselési csoportoknak és szakértőknek. Ez természetszerűleg adódik abból, hogy egyrészt az amerikai infrastruktúra és információs rendszerek védelme kiemelt feladat, másrészt az olyan sérülékeny katonai információs rendszerek védelméről is gondoskodni kell, mint amilyen a NIPRNet[40] (Nonsecure Internet Protocol Router Network). Ez a hálózat az amerikai hadsereg békeidejű és háborús műveleteiben a nem titkos, de szenzitív harctámogatási információk szétosztására szolgál. Mivel a rendszer a nyílt internethez kapcsolódik, természetszerűleg sérülékeny. A már említett amerikai kongresszusi jelentés is utal rá, hogy ennek a rendszernek a gyenge pontjait a kínaiak már feltérképezték, így fennáll annak a veszélye, hogy adott körülmények között képesek abban komoly károkat is okozni. (USCC 2008)

Ebből azt a következtetést is levonhatjuk, hogy ha Kína hozzáfér a NIPRNet-hez vagy az ahhoz hasonló katonai hálózatokhoz, az lehetővé teszi Kína számára, hogy az Egyesült Államok logisztikai rendszerétől kezdve a harctámogatás különböző elemein át számos egyéb rendszert kielemezzen. Amennyiben ezt továbbgondoljuk, akkor arra a következtetésre juthatunk, hogy Kína rendelkezhet azzal a képes-

[40] Az NIPRNett-el párhuzamosan működik az SIPRNet (Secret Internet Protocol Router Network), amelynek fő feladata elsősorban a minősített információk szétosztása egy különválasztott titkosított hálózaton.

séggel, hogy ezekbe a rendszerekbe beavatkozva azok működését korlátozza vagy akadályozza. Így mindez komoly biztonságpolitikai és egyben stratégiai kérdéssé is válik. (Kovács 2009a)

3.1.5. Kína és a kiberbiztonsági stratégia

A kínai kiberbiztonsági stratégia nem egy jól körülhatárolható és világos célokat megfogalmazó dokumentumra épül. Már a kiberteret és a kiberbiztonságot jellemző terminológia megfogalmazása és annak értelmezése is eltér az Európában, illetve az Egyesült Államokban megszokottól.

Kína az információs tér és az információs társadalom kialakításának oldaláról közelíti meg a kérdést. 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)

Ebből következően a kiberbiztonság is sokszor az információs tér biztonságával kapcsolódik össze. Ugyanakkor nagyon nehéz szétválasztani a közigazgatási (kormányzati) és a katonai tevékenységet[41] ezen a területen.

[41] A kínai hadsereg vagy hivatalos nevén a Kínai Felszabadítási Hadsereg különválasztása a kormánytól meglehetősen furcsának tűnhet a nyugati gondolkodásban. Ugyanakkor a kínai hadsereg a Kínai Kommunista Párt alárendeltségében, hatalmas politikai erővel rendelkezik. Gyakran az állam az államban kifejezéssel is illetik. A hadsereg vezetése annak angol nyelvű tájékoztatója szerint a Kínai Kommunista Párt Központi Katonai Bizottsága alá tartozik (amely nem ugyanaz, mint a Párt Központi Bizottsága), és amelynek elnöke a Kínai Kommunista Párt főtitkára (könyvünk írásakor Xi Jinping), aki egyben a Kínai Népköztársaság elnöke és a KKP Politikai Bizottsága Állandó Bizottságának elnöke is. Rajta kívül két alelnökből és négy tagból áll a Központi Katonai Bizottság. Mind a hat tag katona, tábornoki rendfokozatban. (MoD PRC 2018; Lindsay–Ming–Reveron 2015)

Kína nemzetbiztonsági törvénye, amelynek hivatalos címe *A Kínai Népköztársaság Nemzetbiztonsági Törvénye,*[42] és amelyet a Kínai Népköztársaság tizenkettedik Népi Nemzeti Kongresszusa 2015. július 1-jei Állandó Bizottságának 15. ülésén fogadtak el, a kibertérről nem rendelkezik explicit módon. Ugyanakkor ennek a törvénynek a 25. cikkelye[43] egy olyan hálózati és információbiztonsági rendszer kialakítását irányozza elő, amelynek 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)

Az idézett cikkely legalább két következtetés levonását teszi lehetővé számunkra. Az egyik, amely tényre korábban már utaltunk, az, hogy a kínai gazdaság és társadalmi-politikai élet nagyban függ az információtechnológiától, illetve a számítógép-hálózatoktól. Ennek felismerése a kínai legfelsőbb politikai szinten is megtörtént már. A másik következtetés pedig az, hogy mind a külső, mind a belső információáramlást a kínai politika továbbra is – sőt, ha lehet, akkor még erőteljesebb módon – ellenőrzése alatt akarja tartani.

[42] A törvény azon három törvény egyike, amelyek újraírják Kína biztonságról alkotott jogszabályi és szervezeti felépítését. A másik két törvénnyel – a külföldi nem-kormányzati szervezetekről szóló törvénnyel, valamint a terrorizmus ellen törvénnyel – együtt ez a törvény az elnök közvetlen irányítása alá tartozó Központi Biztonsági Ügynökség hatáskörét hatalmas mértékben kiterjeszti, beleértve a hadsereget is. (Wong 2015)

[43] A törvénynek a kínai Védelmi Minisztérium hivatalos honlapján elérhető angol nyelvű változata csak az első 24 cikkelyt tartalmazza. Ugyanakkor más forrásokból elérhető a teljes szövege. (China Law Translate 2015)

Ugyanakkor Kína kiberteret érintő stratégiai elgondolásainak hátterében nagyon sok elemző az úgynevezett 27-es Dokumentumot tekinti meghatározónak. Ez a dokumentum, illetve az abban foglaltak azonban egy kis felvezetést igényelnek, amelyben a kínai politikai elit döntéshozatali mechanizmusát mutatjuk be.

Bár hivatalosan Kínában is többpártrendszer van, a hatalmat igen erősen centralizált formában a Kínai Kommunista Párt (KKP) gyakorolja. A KKP-n belül is központosított a hatalom. A KKP központi szervezetei közül elvileg a legfontosabb plénum a pártkongresszus, amely ötévente ülésezik. A pártkongresszus alatt található – annak iránymutatásai alapján működve – a Központi Bizottság (KB), de az igazi hatalmat a KB Politikai Bizottságának 4–7 főből álló úgynevezett Állandó Bizottsága gyakorolja. (Lindsay–Ming–Reveron 2015)

Ugyanakkor a különböző szinteken számos úgynevezett *vezető csoport* található. Ezek kis létszámú, szakértői csoportok, amelyek közvetlenül a Politbüro számára végeznek támogatói munkát. (Miller é. n.)

A kiberbiztonság kérdését több vezető csoport is tárgyalta, hiszen – ahogy arra mi is utaltunk a fenti következtetéseinkben – annak hatása a nemzetbiztonságra vagy akár közvetlenül a belpolitikára és a gazdaságra egyre inkább előtérbe került az utóbbi időben. Xi Jinping elnök 2014-ben újjászervezte a vezető csoportokat, amely során a kiberbiztonság területén egy új vezető csoport jött létre. Azonban 2014 előtt az Állami Információs-fejlesztési Vezető Csoport és az Államtanács Információs Irodája voltak a terület fő felelősei. Az elnök vezette Állami Információs-fejlesztési Vezető csoport Kína nemzeti információtechnológiai tervét dolgozta ki 2001-ben. Ennek a csoportnak az egyik munkacsoportja – az Állami Hálózati és Információbiztonsági Koordinációs Munkacsoport – adta ki 2003-ban az úgynevezett 27-es Dokumentumot, amely alapvetően a terület biztonságának meghatározó irányelveit tartalmazta. Ezek között az irányelvek között voltak a többszintű védelmi séma kialakítására, a kriptográfiára, az információbiztonság monitoringrendszerére, a kritikus

infrastruktúrák védelmére, a terület terminológiájára, illetve a kutatás-fejlesztésre vonatkozó konkrét feladatok. (Lindsay–Ming–Reveron 2015)

Ezt követően a 27-es Dokumentum főbb irányelveit részletesen is kidolgozták, de a munkacsoport egyre kevesebbet szerepelt ezekben. Pedig a kínai információtechnológia ekkor indult el robbanásszerű fejlődési pályáján. Számos olyan információtechnológiai cég született ebben az időben – azaz 2007 és 2010 között –, amelyek azóta a világ élvonalába kerültek. (Lindsay–Ming–Reveron 2015)

Lindsay és társai tanulmánya részletes elemzést készített azokból a nyilvánosan elérhető információkból és adatokból, amelyek a jelenlegi hivatalos kínai kiberbiztonsági szereplőket mutatja be hierarchikus felépítésben. Ennek csúcsán a már említett – a Kínai Kommunista Párt közvetlen irányítása alatt működő – Állami Információs-fejlesztési Vezető csoportot találjuk, de számos jel mutat arra, hogy a kínai hadsereg is meghatározó szerepet kap a területen. A kínai hadsereg a rádióelektronikai felderítés (Signals Intelligence, SIGINT) és az elektronikai hadviselés mellett a korábban bemutatott akciókkal és tevékenységekkel nagyon hangsúlyosan van jelen a kibertérben. (Lindsay–Ming–Reveron 2015)

A kínai hadsereg vezérkarának harmadik csoportfőnöksége felel a felderítésért, a negyedik pedig az elektronikai hadviselésért. Katonai körzetenként vannak felderítő főnökségek. A kínai hadsereg számos egyetemet, illetve ott folyó kutatás-fejlesztési tevékenységeket támogat. Az egyetemek feltételezhetően sokszor szoros kapcsolatokat ápolnak a kibermilíciákkal, azaz azokkal a civil hackerekből álló szervezetekkel, akik képesek komoly informatikai támadásokat kivitelezni akár külföldi célpontok ellen is.

3.2. Oroszország és a kiberbiztonság

Oroszország esetében is igaz az a korábban Kína esetében tett megállapítás, amely szerint mind politikai, mind katonai potenciálját tekintve a világ egyik vezető hatalmáról beszélhetünk. Ezt nyilvánvalóan sokan regionális szintre igyekeznek korlátozni, de amennyiben Oroszország meglévő katonai erejét,[44] illetve annak erőkivetítő képességét megnézzük, akkor talán nem tévedünk nagyot akkor, amikor a világ egyik vezető katonai hatalmaként aposztrofáljuk.

Oroszország kibertérhez való viszonya, az ott folyó egyre aktívabb és világszerte jelen lévő tevékenysége, valamint az ország kiberbiztonsági stratégiájának vizsgálata előtt szükséges egy pillantást vetnünk az ország nemzeti biztonsági stratégiájára, csakúgy, mint katonai stratégiájára. Ezen meghatározó dokumentumok áttekintése mellett azok kiberbiztonságra, valamint a kibertéri tevékenységek szabályozására utaló meghatározásait keressük.

3.2.1. Oroszország nemzeti biztonsági stratégiája

A 2015. év végén, egészen pontosan 2015. december 31-én adták ki Vlagyimir Putyin elnök aláírásával az Orosz Föderáció Nemzeti Biztonsági Stratégiáját. Az új stratégia a korábbi, 2009-es – akkor szintén elnöki rendeletben kiadott – nemzeti biztonsági stratégiát váltotta fel.

Az új stratégia megfogalmazása szerint: „magában 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)

[44] Ezt a katonai erőt jól jellemzi, hogy a Military Ballance adatai szerint az orosz fegyveres erők létszáma több mint 1 millió főt számlál, (Military Ballance 2018) a CIA évenkénti országértékelésének adatai alapján a katonai kiadások pedig 2016-ban elérték a GDP 5,4%-át. (CIA 2018)

A stratégia az *Oroszország a modern világban* című fejezetben felméri mindazokat a veszélyeket, amelyekkel az országnak szembe kell néznie. Ebben sok egyéb mellett – például a többközpontú világrendből adódó instabilitás, támadó fegyverek korszerűsítésére való törekvés, az Afrikából és a Közel-Keletről érkező migrációs nyomás, illetve az európai országok erre adott elégtelen válasza – megjelenik az információs technológia jelentette kihívás is: „Jogellenes 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)

A stratégia a *Nemzeti érdekek és stratégiai nemzeti prioritások* című fejezetben felsorolja mindazokat az érdekeket és célokat, amelyeket Oroszország hosszú távon a legfontosabbaknak tart. Ezek az érdekek és célok (avagy prioritások, ahogy a dokumentum fogalmaz) természetszerűleg egymásra épülnek. A stratégiában megfogalmazott legfontosabb hosszú távú érdekek a következők:

- az ország védelme, az Orosz Föderáció alkotmányos rendjének sérthetetlenségének, szuverenitásának, függetlenségének, valamint nemzeti és területi integritásának biztosítása;
- a nemzeti együttműködés erősítése, a politikai és társadalmi stabilitás, valamint a demokratikus intézmények fejlesztése, az állam és a civil társadalom közötti együttműködési mechanizmusok javítása;
- az életszínvonal emelése, a lakosság egészségének javítása és az ország stabil demográfiai fejlődésének biztosítása;
- a kultúra és a hagyományos orosz szellemi és erkölcsi értékek megőrzése és fejlesztése;
- a nemzetgazdaság versenyképességének növelése;
- az Orosz Föderáció vezető világhatalmának megszilárdítása, amellyel a policentrikus világban megvalósuló stratégiai sta-

bilitás és a kölcsönösen előnyös partnerségek megőrzése a cél. (Orosz Föderáció 2015)

A dokumentum szerint ezek az érdekek a következő nemzeti prioritások szem előtt tartásával valósíthatók meg:

- nemzetvédelem;
- állam- és közbiztonság;
- gazdasági növekedés;
- tudomány, technológia és oktatás;
- egészségügyi ellátás;
- kultúra;
- az élő rendszerek ökológiája és a természeti erőforrások racionális felhasználása;
- stratégiai stabilitás és egyenlő stratégiai partnerség. (Orosz Föderáció 2015)

Ugyanakkor nem teljesen koherens és következetes a stratégia felépítése. Addig, amíg az állam és a közbiztonság területén számos közvetlen veszélyforrást sorol fel a dokumentum (például az állam biztonságával szemben nagyon markáns veszélyforrásként jelöli meg a külföldi hírszerző szolgálatok információszerző tevékenységét vagy a terror és egyéb extrémista szervezetek jelenlétét és esetleges akcióit vagy a közbiztonság területén a korrupciót, illetve a szervezett bűnözést is kiemeli), addig a nemzetvédelem területén a stratégia csak általános értelemben vett veszélyeket mutat be.

Mindezek mellett azonban az álampolgárok életszínvonalának emelése érdekében a stratégia az információs technológia alkalmazását és annak szélesebb körű elterjedésének támogatását is célul tűzi ki, amikor kijelenti, hogy „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)

A stratégia kitér azokra a negatív hatásokra és következményekre, amelyek a nemzetközi közösség Oroszországgal szemben bevezetett szankciói miatt alakulhattak ki többek között az olyan területeken, mint a tudományos és technológiai kutatások vagy éppen az ezekre alapozott oktatás. A stratégia veszélyforrásként értékeli a szankciók miatt importtilalommal sújtott tudományos és tesztberendezések, elektronikai alkatrészek, számítógépes hardver- és szoftverösszetevők hiányát, de kitér arra is, hogy ezeknek a szankcióknak, illetve az így nem megfelelő módon fejlődő tudományos-technológiai kutatásoknak negatív hatásai vannak nemcsak a tudományra, az innovációra és az ipari technológiai kutatásokra, hanem az a tanári és a mérnöki szakma presztízsének csökkenését is magával hozza, sőt mindezeken túl a műszaki és tudományos, valamint az általános és középfokú szakképzés és a felsőoktatás minőségében is csökkenést eredményez. (Orosz Föderáció 2015)

Ennek megfelelően a stratégia a nemzeti biztonság növelésének egyik legfőbb területének a technológiai biztonságot tekinti, amelybe beletartozik az információs tér is: „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)

Ebből kiindulva a stratégia számos olyan nemzetbiztonsági feladatot határoz meg, amellyel a tudomány, a technológia és az oktatás színvonala biztosítható vagy emelhető. Ilyen feladat például a tudományos potenciál átfogó fejlesztése és a teljes tudományos termelési ciklus visszaállítása, a nemzeti innovációs rendszer fejlesztése vagy az ígéretes magas hozzáadott értéket képviselő technológiák (genetika, robotika, biológia, információ, kommunikáció, kognitív technológiák, nanotechnológia és a természethez hasonló konvergens technológiák) kifejlesztése. (Orosz Föderáció 2015)

Mindezek fényében különösen érdekes megvizsgálni, hogy Oroszország miként is tekint a kibertérre, valamint az ott lévő folyamatokra, vagy éppen hogyan igyekszik ezeket a folyamatokat befolyásolni. Ennek oka elsősorban az, hogy Oroszország már többször bizonyította, hogy megfelelően fejlett képességekkel rendelkezik ahhoz, hogy érdekeit különböző kibertéri eszközökkel – legyen az politikai befolyásolás, infrastruktúra működésének akadályozása vagy akár médiaműveletek – nemcsak, hogy meg tudja védeni, hanem ezt nagyon is hatékonyan tudja megvalósítani.

Oroszország viszonya a kibertérhez sokban hasonlít Kínáéhoz. Ez rögtön az orosz fogalmi meghatározások esetében nyilvánvalóvá válik, hiszen az oroszok sokkal inkább információs, semmint kibertéri műveleteknek tekintik azokat az akciókat, amelyek a médiaeszközökkel történő befolyásolástól egészen az elektromágneses spektrum katonai célú felhasználásáig terjednek. Erre utal egy amerikai tanulmány is, amely a Haditengerészeti Elemzési Központ (Center for Naval Analyses, CNA) kiadásában jelent meg: „Az orosz katonai teoretikusok általában nem használják a kiber vagy kiberhadviselés kifejezést. Ehelyett a kiberműveletek fogalmát az információs hadviselés szélesebb keretén belül, egy holisztikus koncepcióval fogalmazzák meg, amely magában foglalja a számítógép-hálózati műveleteket, az elektronikai hadviselést, a pszichológiai műveleteket és az információs műveleteket.” (Connell–Vogler 2017)

Bár nyilvánvalóan az idézett amerikai vélemény is eltér attól a fogalmi rendszertől, amelyet például a NATO is használ, mert a NATO felosztása[45] szerint az információs műveletek részeként értelmezhetők a számítógép-hálózati műveletek, az elektronikai hadviselés és a pszichológiai műveletek is, mégis nagyon jól rávilágít arra, hogy

[45] A NATO vonatkozó doktrínája az információs célok támogatására használt képességek, eszközök és technikák közé sorolja az említett elektronikai hadviselést, pszichológiai műveleteket, illetve a számítógép-hálózati műveleteket. Ugyanakkor ezeket kiegészíti többek között olyan tényezőkkel, mint például a műveleti biztonság, az információbiztonság vagy a megtévesztés. (NATO 2009)

az orosz felfogás inkább az információt és annak eszközként – akár fegyverként – való alkalmazását tekinti fontosnak, semmint a nehezen körül írható kibertér és annak folyamatainak meghatározását.

Mindezekre számos példát is találunk az elmúlt évekből. Erre az egyik legjobb példa az orosz elektronikai hadviselési képességek fejlesztése a közelmúltban, amely eszközöket és rendszereket – elsősorban az ukrajnai, majd a szíriai háborúban – alkalmazták is. Az ezekben a konfliktusokban (bár itt a háború kifejezés is helytálló lehet) alkalmazott új haditechnikai eszközök elemzéséből a következő megállapítások hosszú távon is érvényes következtetések levonását teszik lehetővé: „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)

Az említett következtetés pedig az, hogy a rövid távú célok vezérelte K+F-tevékenység helyett a hosszú távú, a politikai és a stratégiai irányokat is szem előtt tartott képességek kialakítása lehet sikeres. Ugyanakkor az ilyen képességek fejlesztése mellett nem elhanyagolható azok gyakorlatban való alkalmazásának kérdése sem, hiszen a katonai kutatás-fejlesztés egyik legutolsó mozzanata mindig a harctéren, illetve a hadszíntéren való próba, majd az ott szerzett tapasztalatok beépítése – esetlegesen a már megvalósult eszközök és rendszerek módosítása révén is –, amely elengedhetetlen a sikerhez. Amennyiben ebből a gondolatmenetből analóg módon párhuzamot vonunk a kibertérre vonatkozóan, akkor a kiberhadviselés korábban már röviden elemzett elméletéig jutunk el.

3.2.2. Oroszország katonai stratégiája

Oroszország jelen sorok írásakor érvényben lévő katonai stratégiája, amelynek hivatalos címe az *Orosz Föderáció Katonai Doktrínája,* a 2014. év végén jelent meg.

A doktrína a külső veszélyforrások számbavétele során nagyon egyértelműen fogalmaz a kibertérben megjelenő fenyegetésekkel kapcsolatosan, bár hangsúlyozni kell azt a korábban tett megállapításunkat, amely szerint Oroszország sem használja a kiber jelzőt, hanem sokkal inkább az információs kitételt alkalmazza ehelyett. A doktrína az *Orosz Föderáció katonai veszélyei és katonai fenyegetettségei* című részben számos veszélyt sorol fel, köztük fő külső katonai veszélyként állapítja meg a következőt: „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." (Roszijszkaja Gazeta 2014)

Érdemes megjegyezni, hogy a doktrína az információs infrastruktúrák veszélyeztetettségére külön is utal a belső katonai fenyegetések felsorolásakor, amikor megállapítja, hogy az ezen a területen megjelenő egyik veszély: „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." (Roszijszkaja Gazeta 2014)

A doktrína a modern katonai konfliktusok jellemzőjeként utal arra, hogy a hagyományos hadviselési dimenziók – szárazföld, levegő, tenger – mellett globális információs térben is végrehajthatók akciók az ellenségre gyakorolt hatások elérése érdekében. (Roszijszkaja Gazeta 2014)

A doktrína nagyon egyértelműen leszögezi a hadsereg alkalmazásának eseteit és lehetőségeit. Ennek során a dokumentum

megfogalmazza, hogy ha az országot, illetve 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 is. (Roszijszkaja Gazeta 2014)

A doktrína külön kitér arra, hogy szükséges a fegyveres erők információbiztonságának hatékony fenntartására. Ugyanakkor nem részletezi és nem határozza meg, hogy mit kell érteni hatékonyság alatt. (Roszijszkaja Gazeta 2014, idézi: Kovács–Krasznay 2017)

3.2.3. Orosz jelenlét a kibertérben

Az orosz kibertéri jelenlét mibenlétét és mozgatórugóit nagyon jól összefoglalja James R. Clipper, az USA Nemzeti Hírszerzés igazgatójának egyik 2016-os szenátusi meghallgatásán tett nyilatkozata: „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)

11. táblázat

Oroszország internetpenetrációja 2016-ban és 2017-ben

Oroszország			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016[47]	143,4	102,3	71,3%
2017[48]	143,4	109,5	76,4%
Világ			
2017	7519	3885	51,7%

Forrás: www.internetlivestats.com/internet-users/russia/, www.internetworldstats.com/europa2.htm#ru, a szerző szerkesztése

Ezt a fenti megállapítást támasztja alá az elemzés is, amely 2014-ben készült, és amelyet a már említett FireEye nevű kiberbiztonsági cég jegyez. Ebben a jelentésben azonosítottak egy Oroszországhoz köthető, célzott támadásokra szakosodott csoportot, amely az APT28, illetve a Fancy Bear nevet kapta. (FireEye 2014)

A FireEye 2014-es jelentésének címe *APT28: egy ablak Oroszország kiberkémkedési műveleteire?* Ez a címválasztás egyben utalás arra is, hogy a csoport tevékenysége közvetett módon betekintést nyújt az orosz politika kibertéri motivációiba és mozgatórugóiba. (FireEye 2014)

A cég nem is titkolta a jelentés kiadásának célját: „Akárcsak 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)

Meg kell jegyeznünk, hogy a FireEye után az Egyesült Államok hivatalosan is nevesítette Oroszországot, mint az APT28 mögött álló

[46] Forrás: http://www.internetlivestats.com/internet-users/russia/

[47] Forrás: http://www.internetworldstats.com/europa2.htm#ru

állami támogatót a 2016-os amerikai elnökválasztással kapcsolatos kibertámadások vizsgálata után.[48] (US DHS–FBI 2016)

A cég által végzett vizsgálatok összegzett megállapításait, azaz azokat a tényezőket, amelyek az orosz hivatalos kormány támogatására utalnak, egy táblázatban külön is összefoglalták.

12. táblázat

A FireEye által feltárt tényezők, amelyek az APT28 mögött álló hivatalos orosz támogatást bizonyíthatják

Rosszindulatú program	*Célpontok*	*Orosz attribúció*
Eszközök a támadásokhoz és azok hosszú távú fenntartásához: • rosszindulatú szoftverek flexibilis és hosszú távon is alkalmazható platformokkal; • a rosszindulatú programok folyamatos fejlesztése; • a támadóprogramok optimalizálása az áldozat számítógépes környezetére; • a kódfejlesztési környezet fejlesztése. Adatlopási technikák: • hátsó ajtók HTTP protokoll használatával; • hátsó ajtók az áldozat e-mail-szerverének használatával; • helyi kódmásolás a zárt vagy vezetékes hálózatokba.	Grúzia és a Kaukázus: • Belügyminisztérium; • Védelmi Minisztérium; • újságírók, akik a kaukázusi helyzetről tudósítottak; • Kavkaz Központ. Kelet-európai kormányzati és katonai szervezetek: • Lengyel Kormány; • Magyar Kormány; • kelet-európai külügyminisztériumok; • gyakorlatok a Balti-kumban. Biztonsági szervezetek: • NATO; • EBESZ; • védelmi attasék; • védelmi rendezvények és kiállítások.	Orosz nyelvű indikátorok: • orosz nyelv használata a rosszindulatú kódokban 6 éven keresztül; • újságíróknak szánt csalik, amelyek az angol mellett oroszul is értő APT28-ra utalnak. Moszkvai időzóna szerinti munkaidő a rosszindulatú kódokban: • az APT28 kódjaiban 2007 és 2014 között konzisztensen ez jelenik meg; • a legfontosabb orosz városok időzónáira utaló kódtartalmak.

Forrás: FireEye 2014, a szerző szerkesztése

[48] Erre tettünk utalást a kibertér és a politika összefüggéseit bemutató fejezetünkben.

Az elvégzett elemzésekből jól kirajzolódik, hogy az APT28 célterületei geopolitikai alapon három nagy csoportra oszthatók fel: a Kaukázusra, ezen belül is elsősorban Grúziára; Kelet-Európára, amely térségen belül a kelet-európai kormányzatok, kormányzati szervezetek és hadseregek, valamint az olyan biztonsági vagy katonai szervezetek, mint az EBESZ vagy a NATO voltak a célpontok. Természetesen a csoport más földrajzi régiókban is tevékenykedett, hiszen 2016-ban az Egyesült Államokban az amerikai elnökválasztás kapcsán is felbukkant a csoport és annak akciói, de a FireEye olyan helyeken is talált a csoport támadásaira jellemző mintákat, mint Norvégia, Irak vagy éppen Jordánia.

Az APT28 által alkalmazott módszereket a cég 2007 és 2013 között vizsgálta. Ennek során megállapították, hogy az APT28 támadási módszerére a legjellemzőbb a célzott phishinggel kezdődő információszerzés. Ennek során a célpontok olyan e-maileket kaptak, amelyek bár a címzettek számára releváns témákról szóltak, de mégis kompromittáltak voltak. Ezzel a módszerrel a támadók annak az esélyét növelték meg, hogy a célpontok megnyissák a kapott elektronikus leveleket, az azokban lévő linkekre rá is kattintsanak, illetve ezeknek a leveleknek az olyan ártatlannak tűnő csatolmányait is megnyissák, amelyek például .pdf fájlformátumban voltak.

Az egyik legsikeresebb támadási módszer a hamis, de az eredetihez a megtévesztésig hasonló domainnevek alkalmazása volt. Ezeket a domainneveket az említett e-mailekben elhelyezve tovább növekedett annak az esélye, hogy az áldozat ne fogjon gyanút, és közvetlenül az e-mailből megnyissa a linken található weboldalt. Ilyen tartomány volt többek között a magyar kormányzati domainra – a gov.hu-ra – hasonlító quv.hu.info megnevezés is. (FireEye 2014)

Ezeket a célzott phishing támadásokat olyan exploitok futtatására használták, amelyek különböző rosszindulatú programok letöltését segítették elő. Ezeknek a rosszindulatú programoknak az elemzése után a FireEye nagyon sok olyan jellemzőt azonosított, amely egyértelműen az APT28-ra utalt. Ezek az elemzések közvetve arra is utalnak,

hogy ezeket az eszközöket hosszú távú alkalmazásra szánta az APT28. Ugyanakkor ez a tény is mutatja, hogy a hosszú időn keresztül fennálló alkalmazás során szükséges fejlesztések, valamint javítások komoly anyagi támogatást is igényelnek, amelyek szintén a kormányszintű támogatás jeleit viselik magukon. (FireEye 2014)

2017-ben az amerikai elnökválasztás eseményeit elemezve az APT28-cal kapcsolatban számos megállapítást tettünk, amelyek közül az egyik legfontosabb, hogy a csoport valószínűleg az orosz fegyveres erők vezérkarának Felderítő Főcsoportfőnökségéhez (Glavnoje Razvedivatyelnoje Upravlenyije, GRU), azaz az orosz katonai titkosszolgálathoz kapcsolható. Erre utalt az is, hogy a csoport célpontjai sok esetben katonai célpontok, illetve katonai célok támogatásával kapcsolatosak. (Kovács–Krasznay 2017)

Összességében megállapítható, hogy az APT28 tevékenysége alapvetően politikai motivációjú, és nagy valószínűséggel az orosz kormány által támogatott és/vagy megrendelt akciókat hajtott végre. A támadások célja – eltérően a kínai APT1-től – nem a szellemi tulajdon ellopása, hanem politikai döntéstámogató információk megszerzése, illetve sok esetben a politikai befolyásolás volt.

Az ezekhez hasonló – alapvetően Oroszországhoz köthető – támadások 2016-ban az amerikai elnökválasztás során érték el csúcspontjukat. Mint ahogy azt az események egyik első elemzésében – 2017 tavaszán – megállapítottuk: „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 legjobban szervezett és legjobban felügyelt választásához kapcsolódik.” (Kovács–Krasznay 2017)

Ebben az elemzésben az APT28-on kívül egy másik hasonló csoportot, az APT 29-et, más néven Cozy Beart is nevesítettük amerikai

jelentések alapján. Megállapítottuk, hogy „[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)

3.2.4. Oroszország információbiztonsági stratégiája

Ahogy korábban utaltunk rá, Oroszország elsősorban az *információs* kifejezést használja mindazokra a tevékenységekre, illetve a kapcsolódó területekre, amelyekre a nyugati szakmai definíciós készlet a *kiber* szót, illetve jelzőt alkalmazza. Ennek megfelelően az ország kiberbiztonsági stratégiája helyett, de azzal gyakorlatilag egyenértékű dokumentumként hivatalos címén *Az Orosz Föderáció információbiztonsági doktrínájá*t találjuk meg.

A 2016 decemberében kiadott doktrína rögtön a legelején leszögezi, hogy legfontosabb célja, hogy a nemzeti biztonsághoz hozzájáruljon. A dokumentum meghatározza a legfőbb olyan fogalmakat is, amelyek a doktrína által lefedett területeken szükségesek. Ennek megfelelően az információs tér, vagy ahogy a doktrína hivatalos szövege ezt használja, *információs szféra* (oroszul *информационной сферы*) a következőket foglalja magában: „információk, informatikai célú objektumok, információs rendszerek, az internet informatikai és telekommunikációs hálózatain belüli weboldalak összessége, valamint a kommunikációs hálózatok, az információs technológiák, az infor-

máció előállításában és feldolgozásában érintett egységek, a fenti technológiák kifejlesztése és felhasználása, csakúgy, mint az információbiztonság megteremtése, valamint a tömegkommunikáció szabályozása a szférában." (Russian Ministry of Foreign Affairs 2016)

A doktrína a korábban az orosz nemzeti biztonsági stratégiánál már bemutatott felépítéshez hasonló szerkezetű. Először leszögezi mindazokat a nemzeti érdekeket, amelyek az információs térben jelentkeznek. Ezek közül a legfontosabb annak a deklarálása, hogy az információs technológiák az állam és a társadalom integráns részei, így ezek használata a gazdaság növekedésének és az információs társadalomnak az alapját képezi. Mindezeken túl az információs tér elengedhetetlen szerepet játszik a nemzeti stratégiai célok és prioritások elérésében. A doktrína ezek után a következő nemzeti érdekeket azonosítja:

- 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;
- 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. (Russian Ministry of Foreign Affairs 2016)

A stratégia felsorolja és nagyon röviden elemzi is a legfontosabb információs veszélyforrásokat és fenyegetéseket. Itt a következők sorolhatók fel:

- az információtechnológia széles körű alkalmazása, amely során annak határokon átnyúló jellege a nemzetközi biztonságot ne-

gatívan befolyásoló geopolitikai és katonapolitikai célokra történő alkalmazását segíti elő;
- az információs infrastruktúra katonai célokra történő alkalmazása és felhasználása, valamint a műszaki-technikai alapú hírszerzés az orosz kormányszervek, kutatóintézetek 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 a lakosságra, elsősorban az orosz ifjúságon keresztül;
- a különböző terrorista- és szélsőséges szervezetek széles körben használják az információs eszközöket a közvélemény befolyásolására, illetve aktívan fejlesztenek támadóeszközöket 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 kerüljenek, 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 a valódi stratégiai partnerség kialakítása ellen ható tényezőknek. (Russian Ministry of Foreign Affairs 2016)

Mindezek alapján a doktrína felvázolja azokat a legfontosabb stratégiai célokat, amelyeket az Orosz Föderációnak az információbiztonság területén el kell érnie. Ezeket a célokat különböző, úgynevezett kulcsfontosságú területekhez kapcsolja a dokumentum. Nem túl meglepő módon az első ilyen a katonai terület, amelyen belül további olyan fontos tényezőket jelöl meg, amelyek a nemzetbiztonsághoz és így az információbiztonság megteremtéséhez és növeléséhez is hozzájárulnak. Ennek megfelelően az Orosz Föderáció katonai politikája biztosítja:

- a stratégiai elrettentést, és megakadályozza a katonai konfliktusokat, amelyek az információs technológiák alkalmazásával járhatnak;
- a fegyveres erők információbiztonsági rendszereinek és az információs ellentevékenységi eszközeinek korszerűsítését;
- az információs fenyegetések előrejelzését és azonosítását, amelybe beletartozik a fegyveres erők ilyen jellegű fenyegetettsége is;
- az Orosz Föderáció szövetségesei érdekeinek érvényesítését az információs térben;
- a pszichológiai tevékenységek elleni védelmet. (Russian Ministry of Foreign Affairs 2016)

A katonai területet követi az állam és a közbiztonság területeken legfontosabb információbiztonsági irányvonalak rögzítése. Ezek közül kiemelve a lényegesebbeket:

- 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. (Russian Ministry of Foreign Affairs 2016)

A doktrína a gazdaság területén is megfogalmaz stratégiai célokat. Ezek a célok alapvetően az információtechnológiai és az elektronikai szektorok nem megfelelő fejlődéséből következő negatív tényezők hatásainak, mint veszélyeknek az elhárítására, illetve az ezek esetleges hatásainak ellensúlyozására hivatott versenyképes információbiztonsági eszközök kifejlesztésére és előállítására irányulnak. (Russian Ministry of Foreign Affairs 2016)

Ez ugyanígy igaz a tudomány, a technológia és az oktatás területén megjelenő célkitűzésekre is, ahol szintén fontos prioritás a korszerű és versenyképes technológia megteremtése, az ahhoz szükséges kutatás-fejlesztési tevékenység biztosításával. Ez nyilvánvalóan az oktatást is érinti, hiszen a magas szintű információtechnológia előállítása szükségessé teszi a megfelelő mérnöki, műszaki humán erőforrás képzését, de ez egyben az információs rendszerek biztonságtudatosabb

használatának és alkalmazásának a növekedéséhez is hozzájárulhat. (Russian Ministry of Foreign Affairs 2016)

A doktrína nemcsak a veszélyeket és a feladatokat, hanem a veszélyek elhárításához, illetve a kijelölt célkitűzések eléréséhez szükséges szervezeti hátteret is meghatározza. A dokumentum leszögezi, hogy az információbiztonsági szervezeti rendszer az Orosz Föderáció nemzeti biztonsági rendszerének szerves részét kell, hogy alkossa. Mindezt úgy, hogy „[a]z információbiztonságot az önkormányzatokkal, szervezetekkel és állampolgárokkal együttműködésben dolgozó kormányzati szervek jogalkotási, bűnüldözési, igazságügyi, felügyeleti és egyéb tevékenységeinek kombinációja biztosítja." (Russian Ministry of Foreign Affairs 2016)

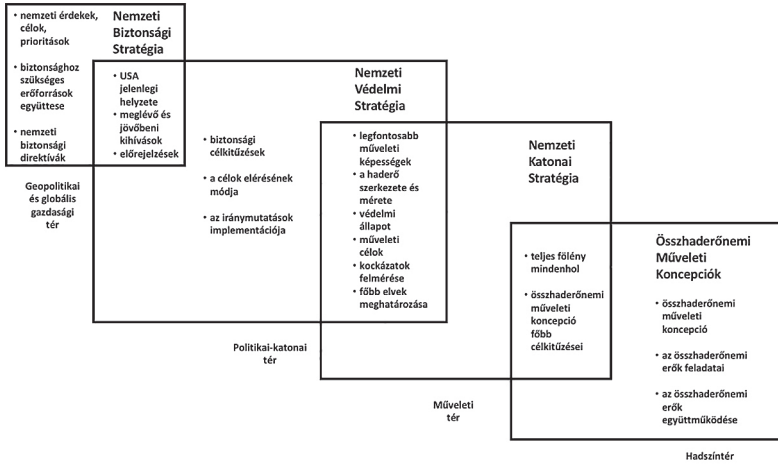
Ennek érdekében a stratégia rögzíti az információbiztonság intézményi kereteit, amelyet a korábban említettek szerint a nemzeti biztonság megteremtésében érintett szervezetek – például az Orosz Föderáció Szövetségi Közgyűlésének Tanácsa, az Állami Duma, az Orosz Föderáció Kormánya, az Orosz Föderáció Központi Bankja, az Orosz Föderáció Katonai-Ipari Bizottsága – alkotják. Az intézményi keretben az információbiztonsági rendszer a következő szereplőket tartalmazza:

- 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. (Russian Ministry of Foreign Affairs 2016)

3.3. Az Amerikai Egyesült Államok és a kiberbiztonság

Az Amerikai Egyesült Államok a világ vezető hatalmaként meghatározó szerepet játszik számos kiberteret érintő kérdésben. Az ország gazdasága immár közel három évtizede nagyban támaszkodik a kibertérre, ami természetszerűleg meghatározza a kiberbiztonságról alkotott véleményét és tevékenységeit is.

Ugyanakkor kisebb magyarázatra szorul az USA stratégiai dokumentumainak rendszere. Ez nagy átfedést mutat a korábban ismertetett általánosan tapasztalható dokumentumok rendszerével, de az USA-ban megjelenik a nemzeti biztonsági stratégia mellett a nemzeti védelmi stratégia is. Ezek összefüggését – kiegészítve a további fontos stratégiai dokumentumokkal – szemlélteti a következő ábra.



5. ábra

Az USA legfontosabb stratégiai dokumentumainak rendszere

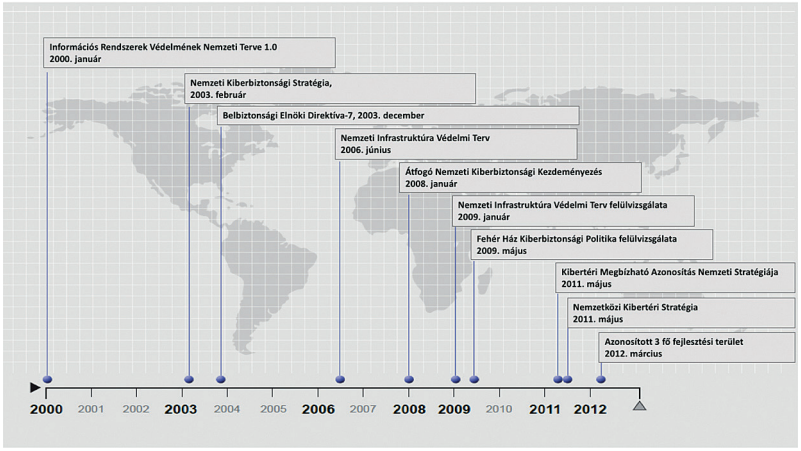
Forrás: HSDL 2018, a szerző szerkesztése

Az USA történelmében a közelmúlt eseményeire való visszatekintésünket az 1990-es évek második feléig tesszük meg, hiszen

a Clinton-adminisztráció már ekkor számos olyan komoly lépést tett, amely a kritikus infrastruktúra, illetve ezen belül a kritikus információs infrastruktúrák védelmének egyes kérdéseit vizsgálta.

1997-re tehető az első olyan, az akkori elnök – Bill Clinton – által létrehozott bizottsági jelentés, amely átfogó módon vizsgálta meg a kritikus infrastruktúrák helyzetét az Egyesült Államokban. Az 1997 októberében kiadott jelentés számba vette az USA számára létfontosságú rendszereket, feltárta az ezekkel szembeni veszélyeket és kihívásokat. A dokumentum a kibertérre, illetve az itt működő létfontosságú rendszerekre is kitért, hangsúlyozva a köz- és magánszektor közötti együttműködés és információmegosztás fontosságát. Ennek az együttműködésnek és információmegosztásnak fontos szerepe van a sérülékenységek felismerésében, valamint az infrastruktúrák egymásrautaltságából eredő problémák kezelésében is. A jelentés nemcsak meghatározta a legfontosabb teendőket, hanem ezt követően a legfontosabb szektorokat kiemelve számos ajánlást fogalmazott meg. Ezen kívül az infokommunikációs, a szállítási, az energia, a bank és pénzügyi, valamint a közműszolgáltatások mint szektorok esetében külön elemezte a veszélyforrásokat és a szektorok sérülékenységeit, az azok bekövetkezése esetén várható következményeket, majd javaslatokat tett az adott szektor védelmének fokozása érdekében. (Critical Foundations 1997)

A 90-es évektől kezdődően egészen 2012-ig számos stratégiai dokumentum és irányelv született az Egyesült Államokban, amelyek nyilvánvalóan – részben vagy egészben – az ország aktuális Nemzeti Biztonsági Stratégiájának főbb célkitűzéseit támogatva a kibertér biztonságának megteremtésére irányultak. Ezeket a dokumentumokat mutatja be időrendi sorrendben 2000 és 2012 között a következő ábra, amelyet 2013-ban az Egyesült Államok Kormányzati Elszámoltatási Hivatala (United States Government Accountability Office, US GAO) készített a Kongresszus számára.



6. ábra

Az USA legfontosabb kiberbiztonsággal kapcsolatos direktívái és stratégiái 2000 és 2012 között

Forrás: GAO 2013, a szerző szerkesztése

Ezeknek a dokumentumoknak a sorából ki kell emelni a Barack Obama hivatalba lépése után azonnal elrendelt kiberbiztonsági felülvizsgálat eredményeit összefoglaló jelentést. A dokumentum többek között egy 10 pontból álló középtávú, de gyakorlatilag azonnal végrehajtandó akciótervet is tartalmazott, amely olyan feladatokat határozott meg, mint például egy megfelelően erős és megfelelő kapacitásokkal, nem utolsósorban megfelelő felhatalmazással rendelkező nemzeti kiberbiztonsági igazgatóság felállítása. A javaslat szerint ez szervezet a nemzeti kiberbiztonsági stratégia kidolgozását és végrehajtásának koordinálását kapta feladatul. Az akciótervek között szerepelt még az is, hogy a kiberbiztonságot olyan prioritássá kell emelni, amely az elnök számára az elsők között szerepel. Mindezeken túl egy, a kiberbiztonság helyzetét reálisan bemutató mérési rendszer kialakítása is szóba került. Az akcióterv a köz- és magánszféra közötti együttműködés erősítésén, valamint a kiberbiztonság jogszabályi hátterének kialakítása

és harmonizációja mellett kiemelt figyelmet szentelt az oktatás, képzés és ezeken keresztül a kiberbiztonsági tudatosság fejlesztése területeknek. (DHS 2009; Kovács 2009b)

13. táblázat

Az Egyesült Államok internetpenetrációja 2016-ban és 2017-ben

Amerikai Egyesült Államok			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	324,1	286,9	88,5%
2017	326,4	286,9	87,9%
Világ			
2017	7519	3885	51,7%

Forrás: www.internetlivestats.com/internet-users/us/, www.internetworldstats.com/america.htm#us, a szerző szerkesztése

3.3.1. Az USA nemzeti biztonsági stratégiája

Az Egyesült Államok legújabb nemzeti biztonsági stratégiáját – Donald J. Trump elnök aláírásával – 2017 decemberében adták ki. (White House 2017)

A dokumentum szerkezeti felépítését tekintve kissé rendhagyó, hiszen négy fő fejezetben, úgynevezett pillérekben mutatja be mindazokat a stratégiai célokat, amelyek az amerikai érdekek és értékek védelme érdekében globálisan vagy regionálisan szükségesek.

A kibertér védelme rögtön az első pillérben, azaz *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 markánsan megjelenik. A stratégia ezen fejezete gyakorlatilag azokat a veszélyforrásokat veszi számba, amelyek közvetlenül vagy közvetett módon veszélyeztetik a fejezet címében is megfogalmazott értékeket. Ebben a felsorolásban kap helyet a kibertér védelme

is. A dokumentum kiemeli a kiberkorszak kihívásaira adandó válaszok, illetve a másik oldalról az abban rejlő lehetőségek kihasználásának fontosságát: „Amerika reakciója a számítógépes kor kihívásaira és lehetőségeire meg fogja határozni a jövőbeni jólétünket és biztonságunkat." (White House 2017)

A kibertérben megjelenő általános veszélyek felsorolása és számbavétele, nevezetesen a határoknélküliség, a globális jelleg, a kritikus infrastruktúrák fontossága, de egyben azok támadhatósága, valamint a kormányzati rendszerek külföldi kormányok általi támadhatósága mellett a stratégia meghatározza azokat a legfontosabb prioritásokat, amelyek feladatként jelentkeznek szövetségi, illetve kormányzati szinten. Ezek a legfőbb feladatok a következők:

- a kockázatok azonosítása és priorizálása, amelyen belül a kritikus infrastruktúrák területén történő kockázatok és veszélyek azonosítása során hat fő kritikusinfrastruktúra-területre kell koncentrálni: a nemzetbiztonságra, az energiaszektorra, a banki és pénzügyi szektorra, az egészségügyre, a kommunikációra, valamint a szállításra;
- 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 elrettenti a potenciális támadókat, és kétséget ébreszt bennük a kritikus infrastruktúrák támadhatóságát illetően;
- 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 azoknak 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)

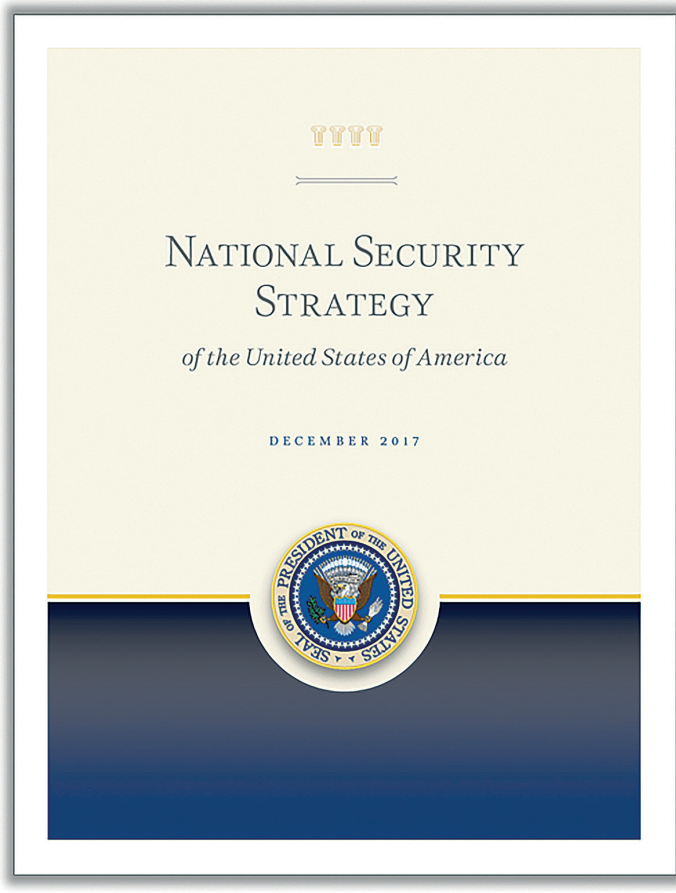
A stratégia harmadik pillére azoknak a képességeknek a kialakítását, illetve újjáépítését tartalmazza, amelyek megfelelő erőt képviselnek a biztonság megteremtéséhez. Ebben komoly szerepet kap a hadsereg, a védelmi ipar, a nukleáris erő, az űr, a hírszerzés, valamint a kibertér.

A kibertérrel kapcsolatban a dokumentum általánosságban leszögezi, hogy akár állami, akár nem állami szereplők olyan rosszindulatú kibertámadásokat képesek végrehajtani a világon bárhol, bárhonnan és bármely célpont ellen, amelyek eredményei alapjaiban ássák alá a kritikus infrastruktúrák működését, veszélyeztetve ezzel nemcsak a megtámadott ország gazdasági és politikai működését, hanem akár a globális demokratikus rendszerek működését, illetve az azokba vetett bizalmat is. Ezzel kapcsolatban a stratégia így fogalmaz: „Számos ország a kiberképességeket mások befolyásolására, és néhányan az autokratikus rezsimek védelmére és azok kiterjesztésére használják. A számítógépes támadások a modern konfliktusok kulcsfontosságú elemévé váltak.” (White House 2017)

Az azonosított kihívásokra és veszélyekre válaszul a dokumentum a kibertérben is olyan képességnövekedést irányoz elő, amely megfelelő válasz lehet, és erősítheti a biztonságot. A kibertérben ennek megfelelően a következő feladatokat kell végrehajtani mint képességnövelő akciókat:
- növelni kell a kibertámadások mögött álló személyek, csoportok vagy országok azonosításának képességét, hozzájárulva a gyors válaszreakciók kialakításához;

- növelni kell a kibervédelem eszközkészletét és szakmai hátterét: ezeket a konfliktusok széles területén javítani kell, és 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 utolsósorban 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 támogatását kéri a stratégia. (White House 2017)

A fentiekben megfogalmazott, a kibertérben jelentkező, de annak számos fizikai kihatásával számoló veszélyeknek és kihívásoknak a felsorolásánál világosan látszik, hogy a stratégia nagyon általános, de ugyanakkor lényegre törő megállapításokat tesz. Ez a tény az egész dokumentumra igaz. A kibertérrel nagyon szoros kapcsolatban lévő információs tevékenységek esetében is ilyen általános érvényű megállapításokat láthatunk a stratégiában, ugyanakkor azok mégis nagyon is reális veszélyre hívják fel a figyelmet. Ilyen veszély többek között, hogy néhány állam a hírszerzési információkat mesterségesen legyártott vagy azokat némileg valós alapokat tartalmazó információkkal vegyítve komoly propagandatevékenységet folytat számos célcsoport befolyásolására: „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)



7. ábra

Az Amerikai Egyesült Államok 2017-es Nemzeti Biztonsági Stratégiája

Forrás: White House 2017

Mindezekben komoly veszélyforrást azonosít a stratégia, mert például a mesterséges intelligenciára alapozott személyes, kereskedelmi és hírszerzési adatok együttes feldolgozása nagyban hozzájárulhat az előbbiekben említett célzott befolyásolás még hatékonyabbá tételéhez, amely

alól a szövetségi szervezetek és intézmények sem lesznek kivételek. A stratégia meg is nevezi Kínát, valamint Oroszországot mint azokat az országokat, akik ezzel a technológiával, illetve ezekkel a módszerekkel élnek. Kína esetében a saját állampolgárai lojalitásának mérésére és ellenőrzésére, míg Oroszország esetében az információs műveletek támadóeszközeként és módszereként utal a dokumentum. (White House 2017)

Ahogy korábban utaltunk rá, erre a fajta befolyásolásra a 2016-os amerikai elnökválasztási kampány során már konkrét példát is láthattunk, hiszen alapvetően orosz állami támogatású csoportok nagyban befolyásolták a választókat, és így nem meglepő módon a választások kimenetelét is. (Kovács–Krasznay 2017)

Természetszerűleg a stratégiában a kibertér nemzetközi jog keretein belüli vezetése, illetve folyamatos alakítása is szóba kerül. Külön kitételben találunk utalást az ingyenes és a nyílt internet védelmének megvalósítására, amelyet az USA az olyan meghatározó nemzetközi szervezetekben való aktív részvételével kíván támogatni, mint például az ICANN (Internet Corporation for Assigned Names and Numbers), az IGF vagy az ITU.

3.3.2. Az USA nemzetvédelmi stratégiája

A 2018. év elején jelent meg az Egyesült Államok új Nemzetvédelmi Stratégiája, amelynek fő célja az USA versenyképes katonai előnyének helyreállítása. Ez kiterjed arra is, hogy megakadályozza Oroszországot és Kínát abban, hogy akár az Egyesült Államokat, akár szövetségeseit támadva megpróbálja felborítani a második világháború óta fennálló nemzetközi rendet. (Garamone 2018)

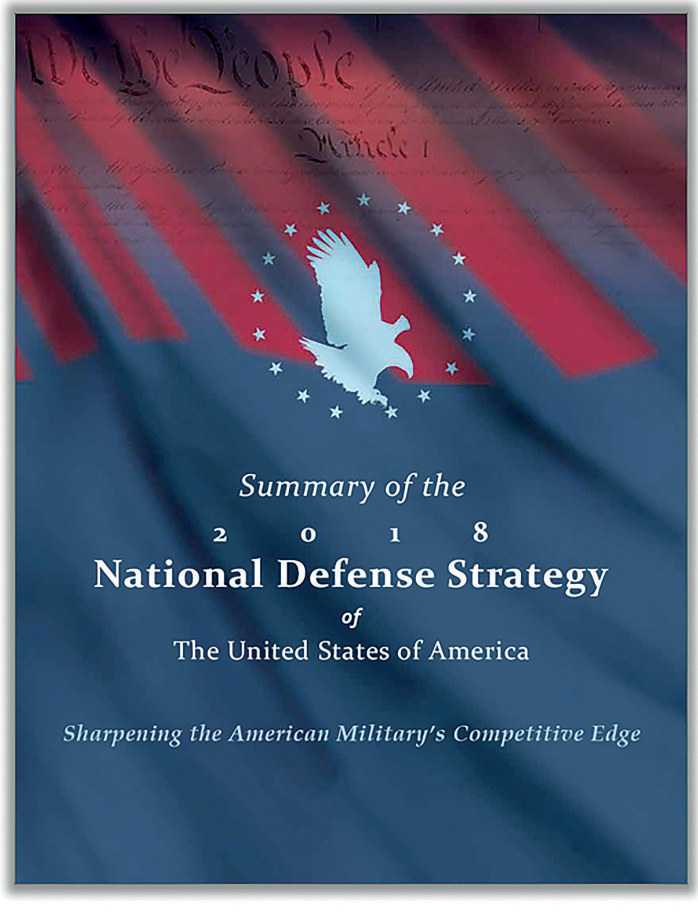
A Jim Mattis[49] tábornok által jegyzett stratégia címéből adódóan is a katonai erő felépítésére, modernizálására – mind technikai, mind alkalmazott eljárásai fejlesztésének tekintetében – ad stratégiai elképzeléseket és jelöli ki a legfontosabb irányokat. A dokumentum – bár teljes egészében annak minősített volta miatt nem olvasható, csak egy 14 oldalas nyílt összefoglalás áll rendelkezésünkre – alapvetően a Nemzetbiztonsági Stratégia alapelveire építve az elrettentés politikáját demonstrálja. A stratégia az USA katonai erejének – a Sivatagi Vihar, azaz az öbölháború stratégiájának és alkalmazott eljárásainak – nagyarányú fejlesztését célozza meg. Ennek egyik legfontosabb célja az orosz és kínai haditechnikai potenciál ellensúlyozása, azok felülmúlása, amellyel kialakítható a hatékony elrettentés. (Garamone 2018)

A stratégia a kihívásokat elemezve megállapítja, hogy a hagyományos négy hadviselési dimenzió mellé a kibertér is bekerült, amelyre ugyanolyan figyelmet kell fordítani, mint a tradicionálisan meglévő négyre. (Department of Defense 2018a)

A dokumentum a veszélyforrások bemutatásánál kitér a kibertérben jelentkező veszélyekre is, hangsúlyozva, hogy ebben a tekintetben az Egyesült Államok is célpont, ráadásul, mivel ebben a dimenzióban nincsenek határok, ezért a kibertámadások vagy akár a korábban már említett információs befolyásolás gyakorlatilag bárhonnan bekövetkezhet. A 2019–2023-as időszakra tervezett védelmi költségvetést a stratégia úgy határozza meg, hogy abban nagy szerepet kap a modernizáció. Ez érinti az űrt és a kiberteret is: „A Védelmi Minisztérium priorizálja mindazokat a beruházásokat, amelyek az űrben lévő

[49] James (Jim) Mattis volt tengerészgyalogos tábornok az Obama-adminisztráció idején még a Központi Parancsnokság parancsnokaként (Commander of Central Command) szolgált, de a stratégia megalkotása idején már a Trump-adminisztráció Védelmi Minisztere. Joe Dunford tengerészgyalogos tábornok, az Egyesített Vezérkari Főnökök Bizottságának főnöke nyilatkozta a Mattis vezetésével készített stratégiáról a következőt: „Biztosíthatom önöket, hogy az egyik olyan dolog, amely miatt teljesen biztos vagyok benne, hogy a Nemzetvédelmi 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)

ellenálló képességre és az ott folyó műveletekre irányulnak. A kibervédelemre, a kiberrugalmasságra és -képességek folyamatos integrációjára nagy hangsúlyt fektetünk a katonai műveletek teljes spektrumába." (Department of Defense 2018a)



8. ábra

Az Amerikai Egyesült Államok 2018-as Nemzeti Védelmi Stratégiájának összefoglalója

Forrás: Department of Defense 2018a

Ugyanakkor a katonai vezetésben használt katonai információs rendszerek (Command, Control, Communication, Computer, Intelligence, C4I) területén többször felmerült már korábban – például a Nemzeti Biztonsági Stratégia is utalt rá –, hogy azok korszerűsítése elengedhetetlen. Kiemelt feladat tehát a katonai információs (digitális) ökoszisztéma fejlesztése a harcászati szinttől egészen a stratégiai szintig. Ezeknek a rendszereknek a modernizációja mellett azok kibertámadásokkal szembeni ellenálló képességének növelése szintén fontos feladat. (Department of Defense 2018a)

A Nemzetvédelmi Stratégiáról összességében elmondható, hogy nagyban magán viseli Mattis tábornok elképzeléseit és elgondolásait a hadsereg átalakításáról, hiszen, ha valaki tisztában van az Egyesült Államok haderejének állapotával, felszerelésével, képességeivel, illetve mindazokkal a kihívásokkal és veszélyekkel, amelyekkel a közeli és a távolabbi jövőben az Egyesült Államoknak szembe kell néznie, akkor az a hadsereget és a különböző eddigi katonai műveleteket belülről is ismerő tábornok.

A stratégia alapvetően az elrettentésre épül, amelyben nagy szerepet kap a korszerű technológiai fejlesztés, valamint a kibertéri támadó és védelmi képességek kihasználása. A stratégia számos helyen utal is arra, mint ahogy korábban Kína bemutatásánál mi is említést tettünk róla, hogy Kína és Oroszország az elmúlt három évtizedben árgus szemekkel figyelte és vizsgálta az USA hadi potenciálját, különböző műveletekben való alkalmazását, ami kiterjedt a csapatok vezetésére, annak stratégiai kérdéseitől egészen a harcászati szintig, valamint folyamatosan elemezték a haditechnikai eszközöket, azok képességeit és hozzájárulásukat a műveletek sikeréhez vagy éppen szerepüket egy-egy kudarcban.

Kína és Oroszország tehát megtanulta a leckét az elmúlt évtizedekben, ami az Egyesült Államok részéről nem hagyható válasz nélkül. Ennek megfelelően a stratégia sok elemében kiemelten kezeli ezt a kérdést, kiegészítve az említett két nagyhatalom kibertéri tevékenységére adandó hatékony válaszokkal, legyen szó információs befolyásolásról,

vagy a kritikus infrastruktúrákat, illetve akár a katonai vezetési rendszereket célzó kibertámadásokról.

3.3.3. Az USA kiberbiztonsággal kapcsolatos stratégiái

Ahogy korábban utaltunk rá, és ahogy alfejezetcímünk is mutatja, az Egyesült Államokban az elmúlt másfél évtizedben számos olyan stratégiai szintű dokumentum – stratégia, elnöki rendelet, törvény, kezdeményezés stb. – született, amely a kiberbiztonsággal valamint a kritikus infrastruktúrákkal, illetve kritikus információs infrastruktúrákkal kapcsolatos. Ezeket az Egyesült Államokat bemutató fejezetünk elején a 2009–2012 közötti időszakra vonatkoztatva egy ábrán igyekeztünk bemutatni, de a teljesség érdekében célszerű egy kronológiai sorrendet felvázoló táblázatban bemutatni a dokumentumokat egészen napjainkig.

14. táblázat

Az Egyesült Államok kiberbiztonságra és kritikus infrastruktúrákra vonatkozó fontosabb stratégiái és törvényei 2000–2017

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

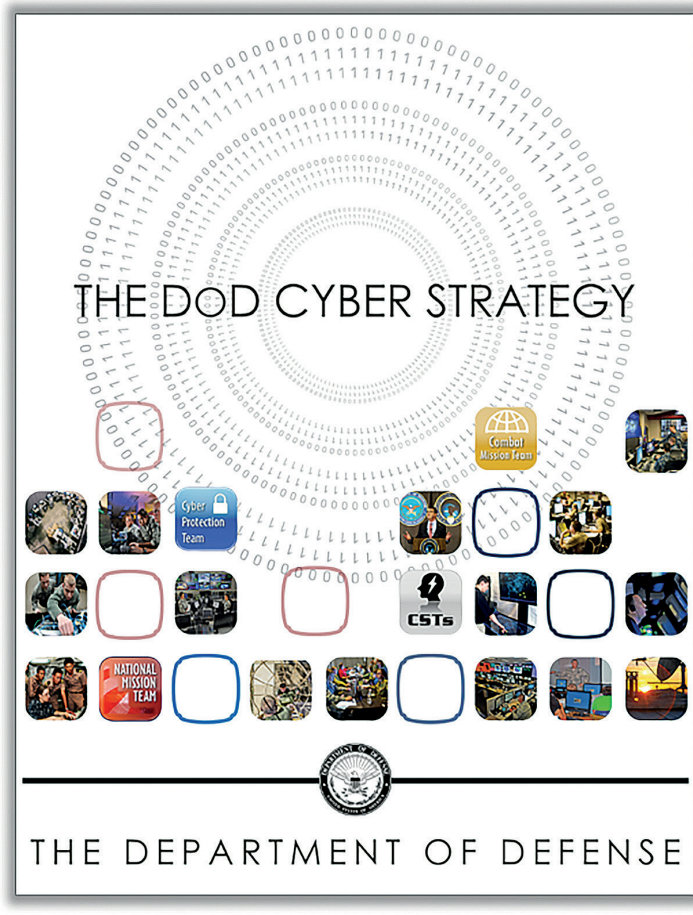
Megjelenés éve	*Eredeti cím*	*Cím*
2013	President's Executive Order on Drawing up a Strategy for Improving Critical Infrastructure Cybersecurity	Elnöki rendelet a kritikus infrastruktúra kiberbiztonságának javítását célzó stratégia kidolgozásáról
2014	Draft Strategy for Improving Critical Infrastructure 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

Forrás: a szerző szerkesztése

A táblázatban lévő felsorolásból jól látszik, hogy az Egyesült Államokban is, hasonlóan több más országhoz, a kiberbiztonság egyrészt szoros kapcsolatban áll a kritikus infrastruktúrák védelmével, másrészt nagyon sok esetben a katonai terület kiemelkedik a kibertérről való gondolkodás során.

Ennek megfelelően érdemes megvizsgálnunk az USA Védelmi Minisztériumának (Department of Defense, DoD) kiberstratégiáját (Department of Defense Cyber Strategy), amely 2015 áprilisában született.

A stratégia arra a három igen markáns területre épül, amely a DoD szempontjából a legfontosabb feladatokat jelenti a kibertérben: a DoD hálózatainak, számítógépeinek és adatainak védelmére; az Egyesült Államok és annak érdekeinek védelmére a súlyos következményekkel járó kibertámadásokkal szemben; valamint a katonai műveletek kibertámogatására. (Department of Defense 2018b)



9. ábra

Az Amerikai Egyesült Államok Védelmi Minisztériumának 2015-ös kiberstratégiája

Forrás: Department of Defense 2015

A dokumentum öt stratégiai célkitűzést határoz meg, amelyek megvalósításának módjai is részletesen bemutatásra kerülnek. Az öt stratégiai célkitűzés a következő:

- a kibertéri műveletek végrehajtásához szükséges készenléti erők és képességek kialakítása, fenntartása: az ehhez szükséges humán erőforrás képzését, a technikai eszközök beszerzési és fejlesztési elképzeléseit a stratégia ötéves 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 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 e rendszerek a támadások következményeként nem vagy csak részben működnek;
- az Egyesült Államok legfontosabb érdekeinek védelme a kibertámadásokkal és azok következményeivel szemben: ki kell építeni olyan felderítő (hírszerzési), figyelmeztető, műveleti és együttműködési képességeket, amelyekkel még azelőtt lehet 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 ter-

> jedése, és amely hozzájárul 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, az ázsiai csendes-óceáni térség, illetve a legfontosabb NATO-szövetségesek. (Department of Defense 2015)

A dokumentum mindegyik stratégiai célhoz és azok implementálására, illetve végrehajtására számos olyan konkrét és mérhető tevékenységet határoz meg, amelyek alapján a célok elérhetők, valamint azok hatásfoka vagy sikeressége mérhető is. Ezeket a stratégiai célokat támogató tevékenységeket a következő táblázatban foglaljuk össze.

15. 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: – képzés, felkészítés, oktatási infrastruktúra – karrierpálya kialakítása – Nemzeti Gárda bevonása – fokozott toborzás – csereprogram a magánszektorral – nemzeti kiberképzési program támogatása • a kiberműveletekhez szükséges technikai képességek kialakítása: – egységes platform kialakítása a kiberműveleti erők számára – gyorsabb kutatás-fejlesztés • pontosított vezetés a kiberműveletek során • kiberszimulációs és modellezési képességek növelése • a kiberműveleti erők értékelése

Stratégiai cél	*A stratégiai célt támogató tevékenység*
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 számítógéphálózat-védelmi szolgáltatója (DoD Computer Network Defense Service Provider, CNDSP) hatékonyságának növelése • terv a hálózatbiztonság és ellenálló képesség növelésére: – a kiber integrálása a műveleti biztonságba – a Kibervédelmi Csoport (Cyber Protection Team, CPT) képességeinek értékelése – a fegyverrendszerek kibervédelmének növelése • saját támadóerők (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

Stratégiai cél	*A stratégiai célt támogató tevékenység*
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, a szerző szerkesztése

A stratégia többször is megnevezi az Egyesült Államok Kiberparancsnokságát (United States Cyber Command, USCYCOM) mint a különböző, a stratégiában kiemelt területek felelős szervezetét.

Az első ilyen feladat, amelyet a stratégiai a USCYCOM-nak delegál, az a legfontosabb kibertéri műveleteknél szerepel. Ez a feladat a szembenálló fél hálózati vagy egyéb, a kibertérben működő rendszerei elleni tevékenységet jelenti. Ugyanakkor rendkívül érdekes annak meghatározása, hogy ez a tevékenység, amely akár támadó tevékenység is lehet, nemcsak a kibertérre korlátozódhat, de kiterjedhet a kibertéren kívüli tartományokra is: „Az 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)

Maga a USCYCOM az Egyesült Államok Stratégiai Parancsnoksága (US Strategic Command, USSTRATCOM) alárendeltségében kezdte meg működését 2009 tavaszán, de 2017. augusztus közepén már önálló műveleti parancsnoksági státuszt kapott.

A Fort Meade-ben található kiberparancsnokság az egyik legfontosabb szervezeti elem az Egyesült Államok olyan katonai szervezetei között, amelyek feladata a kibertér különböző folyamatainak ellenőrzése, illetve irányítása. A parancsnokság legfőbb küldetése: „A műveletek vezetése és a Védelmi Minisztérium hálózatainak védelme érdekében tervezi, koordinálja, integrálja és szinkronizálja 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 szemben álló felet." (Stratcom 2018)

Az USCYBERCOM alárendeltségében látja el feladatait a Hadsereg Kiberparancsnoksága (Army Cyber Command, ARCYBER), a Haditengerészet Kiberparancsnoksága (Fleet Cyber Command, FLTCYBER), a Légierő Kiberparancsnoksága (Air Force Cyber Command, AFCYBER) és a Tengerészgyalogság Kiberparancsnoksága (Marine Forces Cyber Command, MARFORCYBER). A Partiőrség Kiberparancsnoksága (Coast Guard Cyber Command, CGCYBER), bár jogilag a Belbiztonsági Minisztérium alárendeltségébe tartozik, de közvetlen támogatást nyújt az USCYBERCOM-nak. (Stratcom 2018)

Az USCYBERCOM mellett több mint 130 olyan kiberműveleti csoport (Cyber Mission Force, CMF) működik, amelyek az alábbi szervezeti felosztásban látják el feladataikat:

- Nemzeti Műveleti Csoportok (National Mission Teams, NMT), amelyek fő feladata az Egyesült Államok és érdekeinek védelme a súlyos következményekkel járó kibertámadásokkal szemben;
- Kibervédelmi Csoportok (Cyber Protection Teams, CPT), amelyek a DoD kiemelt hálózatainak védelmét látják el a legfontosabb kibertámadásokkal szemben;
- Harci Műveleti Csoportok (Combat Mission Teams, CMT), amelyek a harcoló csapatok parancsnokainak adnak támogatást a kibertér hatékony kihasználása, valamint a saját erők kibertéri védelme érdekében;
- Támogató Csoportok (Support Teams, ST), amelyek elemzői és tervezői munkájukkal járulnak hozzá a Nemzeti Műveleti, illetve a Harci Műveleti Csoportok munkájához. (Department of Defense 2018b)

Természetesen a Védelmi Minisztériumon, illetve a hadseregen kívül a civil terület is kiveszi részét az Egyesült Államok kibervédelmének biztosításából. A már említett Belbiztonsági Minisztérium (Department of Homeland Security, DHS) egyike azoknak a szereplőknek, amelyek a civil rendszerek biztonságát hivatottak biztosítani a kibertérben. Ennek megfelelően a DHS felelős sok esetben 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), amely napi 24 órában, heti 7 napon biztosítja szövetségi szinten az eseménykezelési és irányítási feladatokat. Emellett ez a szervezet kapcsolatot biztosít a szövetségi kormány, a hírszerző közösség és a bűnüldözés hatóságok kiber- és kommunikációs szervezetei között. Az NCCIC a köz- és magánszféra között információmegosztási feladatokat is ellát, amelyek során a sebezhetőségekre, incidensekre, biztonsági eseményekre, illetve azok elhárítására vagy bekövetkezésük esetén azok következményeinek enyhítésére ad tanácsokat, információkat.

Az NCCIC keretei között működik a US-CERT (United States Computer Emergency Readiness Team, US-CERT), amely elemzéseket végez a nemzeti hálózatokat veszélyeztető rosszindulatú támadásokkal kapcsolatban, illetve az Ipari Irányító Rendszerek CERT-je (Industrial Control Systems Cyber Emergency Response Team, ICS-CERT), amely a kritikusinfrastruktúra-ágazatokban és -alágazatokban felelős a kiberbiztonság területén a kockázatok csökkentéséért szövetségi szinttől a legalacsonyabb szintig. (Department of Homeland Security 2018b)

Vákát oldal

4. Az Európai Unió egyes tagországainak kiberbiztonsági politikái és stratégiái

A nagyhatalmak kiberbiztonságot érintő politikai és stratégiai elképzelései után az Európai Unió néhány országának kiberteret érintő elképzeléseit mutatjuk be.

Ahogy korábban már utaltunk rá, a nemzeti szintű kiberstratégiák országonként eltérő módon közelítik meg a kiberteret és annak biztonságát. A különböző megközelítésékben tapasztalható eltéréseknek okait kutatva arra a következtetésre juthatunk, hogy ezek elsősorban abban fedezhetők fel, hogy az adott ország a technika és technológia, az információs társadalom fejlődését és zavartalan működését, illetve a kritikus információs infrastruktúrák védelmét tekintette-e korábban kiindulópontnak.

Ugyanakkor számos közös tényező is jelen van a különböző európai országok kiberbiztonsági stratégiáiban. Az egyik ilyen közös tényező az, hogy kivétel nélkül mindegyik ország a nemzeti biztonság egyik alapösszetevőjét és meghatározó elemét látja a kiberbiztonságban. Ennek megfelelően a nemzeti kiberbiztonsági stratégia nagyban épít a nemzeti biztonsági stratégiában megfogalmazott elvekre, és a kiberbiztonsági célokkal támogatja is az adott ország nemzeti biztonsági stratégiáját. Az Európai Unió egyes országainak nemzeti kiberbiztonsági stratégiáinak bemutatásakor ezért szükségesnek tartjuk kitérni az adott ország nemzeti biztonsági stratégiájára is.

Az Európai Unió jelenleg 28 tagországból áll, hiszen ahogy korábban utaltunk rá, könyvünk írásakor az Egyesült Királyság még tagja az uniónak. Ugyanakkor vállalkozásunk csak a 28 ország mintegy felének, egészen pontosan 13 ország bemutatására terjed ki. Ennek ellenére bízunk benne, hogy az ezen országok kiberbiztonsági stratégiáiból levonható következtetések jól reprezentálják azokat

a kibertér megvalósítására irányuló törekvéseket, amelyek bár nemzeti szinten történnek, de mégis a teljes Európai Unió biztonságához járulnak hozzá.

A következőkben az alábbi európai uniós országok nemzeti kiberbiztonsági stratégiáira fókuszálunk: Ausztria, Cseh Köztársaság, Egyesült Királyság, Észtország, Franciaország, Hollandia, Magyarország, Lettország, Lengyelország, Litvánia, Németország, Szlovénia, Szlovák Köztársaság.

Nemzeti kiberbiztonsági stratégiákat bemutató fejezetünket elsősorban az adott ország nyilvánosan elérhető angol, esetenként német nyelvű stratégiái alapján készítettük el, de például Hollandia esetében, amely könyvünk írásának ideje alatt – 2018 tavaszán – adta ki legújabb kiberteret érintő stratégiáját, amely még nem jelent meg angol nyelven elérhető formában, az eredeti szöveget használtuk, természetesen kisebb fordítói segítséggel. Ugyanakkor ebben a munkában felhasználtuk az ENISA országértékeléseit, valamint a NATO CCDCOE elérhető – nemzeti kiberbiztonsági szervezeteket bemutató – elemzéseit is.

E munka során igyekeztünk az adott ország nemzeti biztonsági stratégiája mellett annak katonai vetületeit is megvizsgálni, amelyek a nemzeti biztonsági stratégiában megfogalmazott célok elérésére valamilyen hatással vannak, és amelyek a kibertérrel kapcsolatosan relevánsak.

4.1. Ausztria

4.1.1. Ausztria nemzeti biztonsági stratégiája

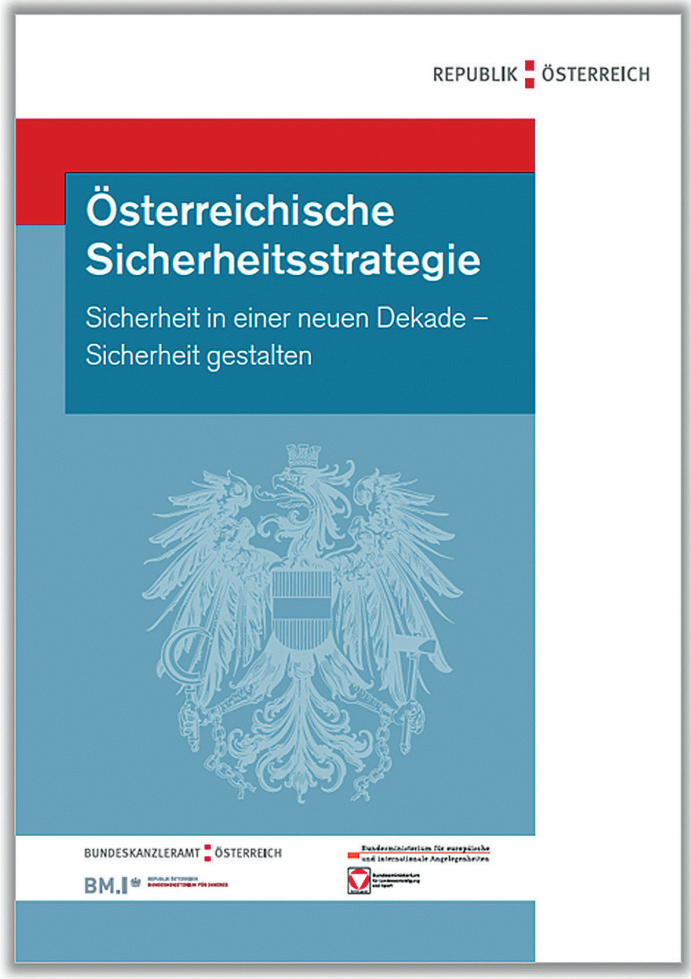
Ausztria nemzeti biztonsági stratégiája, amely a *Biztonság az új évtizedben, a biztonság megteremtése* (németül *Österreichische Sicherheitsstrategie, Sicherheit in einer neuen Dekade – Sicherheit*

gestalten, angolul *Austrian Security Strategy, Security in a new decade – Shaping security*) címet viseli, a 2013. év elején jelent meg.

A stratégia a kihívások, kockázatok és veszélyek felsorolásakor már tartalmaz utalásokat a kibertér árnyoldalaira, megnevezve a kibertámadásokat mint az infokommunikációs rendszerekkel szembeni legfontosabb veszélyeket. (Ausztria 2013a; Ausztria 2013b)

A dokumentum egyik alapvetése a nemzeti szinten megvalósítandó biztonságpolitika, amelynek legfőbb célja a legbiztonságosabb ország megteremtése. A stratégia a belső biztonság esetén kiemelten foglalkozik a kibertérrel: „A kiberbűnözés, a kibertámadások, az internet szélsőséges célokra való alkalmazása és a hálózat biztonsága komoly új kihívások az összes érdekelt fél számára, így széles körű és átfogó együttműködésre van szükség." (Ausztria 2013b)

A stratégia eligazítást ad a védelmi politikára is, beleértve a hadsereget és a kiberteret, illetve az itt jelentkező kibertámadások kezelésének kérdését is. A stratégia explicit módon kijelenti, hogy a kibertámadások jelentette új fenyegetések új megoldásokat várnak a hadseregtől is: „A szubkonvencionális fenyegetések vagy a kibertámadásokból eredő új kockázatok kezelése új katonai tevékenységeket is jelenthetnek." (Ausztria 2013b)



10. ábra

Ausztria nemzeti biztonsági stratégiája

Forrás: Ausztria 2013a

A katonai rendszerek kibervédelme érdekében a stratégia sürgeti minden érdekelt fél bevonását – akár az üzemeltetésben részt vevő civil szereplőkét is –, illetve elrendeli, hogy a hadsereg ilyen jellegű képességeinek fejlesztése érdekében szükséges az osztrák Kiber Krízis Menedzsmenttel való szoros együttműködés. Mindezek mellett a stratégia utal arra is, hogy a hadsereg feladata a kritikus infrastruktúrák és a kibertér védelmében való közreműködés is.

A nemzeti biztonsági stratégia a feltárt és az azonosított veszélyek kezelésére, a kitűzött nemzeti biztonsági, illetve védelmi politikai elveknek megfelelően különböző ajánlásokat fogalmaz meg. Ezek közül az egyik a nemzeti kiberbiztonsági stratégia kiadását és annak – a folyamatosan változó fenyegetések és veszélyek tükrében történő – rendszeres felülvizsgálatát és frissítését irányozza elő. Ezzel párhuzamosan egy másik megfogalmazott ajánlás szerint szükséges létrehozni egy kiberbűnözésre szakosodott kiválósági központot, valamint Ausztriának aktívan hozzá kell járulnia az európai uniós kiberbiztonsági politikák kialakításához, amelyen keresztül az állampolgárok és a vállalkozások kibertérben való hatékonyabb védelme megvalósítható. (Ausztria 2013b)

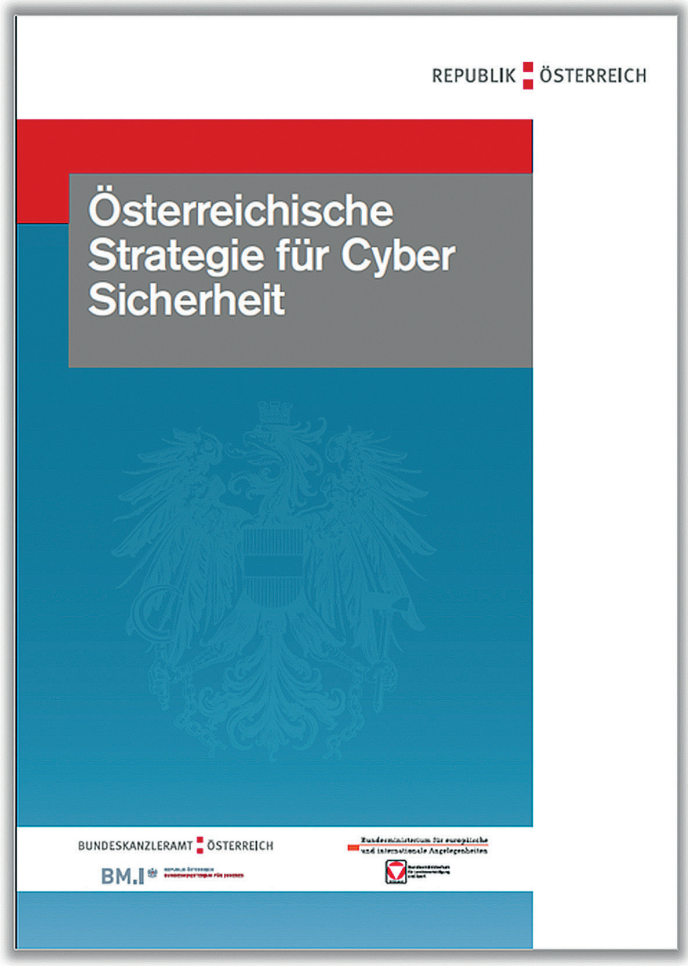
4.1.2. Ausztria nemzeti kiberbiztonsági stratégiája

A nemzeti biztonsági stratégiában megfogalmazottak szerint az ország kiberbiztonsági stratégiáját már 2013 tavaszán kiadták, és német nyelven az *Österreichische Strategie für Cyber Sicherheit,* angolul pedig

az *Austrian Cyber Security Strategy* címet viseli.[50] Ez a stratégia nagyban épít a nemzeti biztonsági stratégiában megfogalmazott alapelvekre. A 25 oldalas dokumentum egy rövid bevezető után a kibertérben jelentkező lehetőségeket és az ott megjelenő veszélyeket veszi sorra. Ugyanakkor a dokumentumban a lehetőségek bemutatása sokkal nagyobb hangsúlyt kap, mint a veszélyek leírása, hiszen a lehetőség felsorolásánál az információs és kommunikációs teret, a társadalmi interakció terét, a gazdaság és kereskedelem terét, a politikai részvétel terét, valamint az irányítást (például az IoT-eszközöket és azok infrastruktúrákban történő alkalmazását) külön-külön is bemutatja és röviden elemzi, míg a kockázatok és veszélyek egyetlen bekezdésbe sűrítve jelennek csak meg.

Ez annak ellenére is szembetűnő, hogy a stratéga egyik melléklete egy kiberkockázati mátrixot mutat be. A mátrix a bekövetkezés valószínűsége függvényében mutatja be a lehetséges következmények nagyságát számos kockázati tényezőt figyelembe véve, bár meg kell jegyeznünk, hogy az elemzés 2011-es datálású. (Ausztria 2013d)

[50] Akár a nemzeti kiberbiztonsági stratégia, akár a nemzeti biztonsági stratégia sok ország esetében az adott ország hivatalos nyelve mellett angol nyelven is publikálásra kerül. Ez több célt szolgál, egyrészt világos képet ad az adott ország biztonsági felfogásáról, másrészt üzenet értékű is, hiszen az abban foglaltak – például a már említett elrettentés – így explicit módon kifejezhetőek a világ számára. Ugyanez igaz a stratégia megjelenésére is – erre utalunk az adott ország egyes stratégiai dokumentumai borítóinak bemutatásával (törekedve az eredeti nyelven kiadott dokumentumok felvillantására) –, hiszen ezek kivitele és megjelenése is hozzájárul annak kommunikálásához, hogy az adott ország mennyire gondolja fontosnak a stratégiában foglaltak széles körű kommunikálását.



11. ábra

Ausztria kiberbiztonsági stratégiája

Forrás: Ausztria 2013c

A stratégia összesen kilenc stratégiai célitűzést fogalmaz meg, amelyek a következők:

- a biztonságos kibertér megteremtése, amelynek a kockázatok és veszélyek kezelése érdekében megfelelően redundánsnak kell lennie;
- Ausztria biztosítja a biztonságos kiberteret, amely során a közés 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, amely 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 szövetségi szinttől kezdődően a közigazgatás minden szintjéig;
- együttműködés szükséges az osztrák vállalatok kiberbiztonsági tevékenységeinek támogatásában;
- a kiberbiztonság tudatosságának állampolgári szinten történő emelése szükséges. (Ausztria 2013d)

16. táblázat

Ausztria internetpenetrációja 2016-ban és 2017-ben

Ausztria			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	8,6	6,9	81,1%
2017	8,6	7,2	84,6%

Forrás: www.internetlivestats.com/internet-users/austria/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

A stratégia a célok után hét akcióterületet fogalmaz meg, amelyek a stratégiai célokat hivatottak támogatni. Ezek az akcióterületek a következők:

- 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. Emellett műveleti szintű koordináló szervezetek felállítása is szükséges, például GovCERT (Government Computer Emergency Response Team, Kormányzati Eseménykezelő Csoport), MiL-CERT (Military Cyber Emergency Readiness Team, Katonai Kibervészhelyzeti Készenléti Csoport), C4 (Cyber Crime Competence Center, Kiberbűnözési Kompetencia-központ). Az állami szereplők mellett szükséges a kritikus infrastruktúra területén is a koordináló szervezetek kialakítása. Fel kell állítani egy krízismenedzsmentet, valamint erősíteni kell a már meglévő kiberbiztonsági struktúrát;
- a kormányzat feladatai: korszerű szabályozási környezetet kell kialakítani, meg kell határozni a minimumkövetelményeket, 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 ösztönzi. Erősíteni kell a kis- és közepes vállalatok kiberbiztonsági támogatását, valamint elő kell készíteni egy kiberbiztonsági kommunikációs stratégiát;
- kritikusinfrastruktúra-védelem: a kritikusinfrastruktúra-szektorokban lévő kiberbiztonság erősítése és hozzájárulás a már meglévő osztrák kritikusinfrastruktúra-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)

4.2. Cseh Köztársaság

4.2.1. A Cseh Köztársaság nemzeti biztonsági stratégiája

A Cseh Köztársaság új nemzeti biztonsági stratégiája 2015-ben jelent meg. A dokumentum számba veszi az ország biztonsági alapelveit, majd ismerteti azokat az értékeket, amelyeket a biztonság területén a legfontosabbnak tart Csehország. A stratégiában ebben a felsorolásban találkozhatunk először a kibertérrel, illetve annak biztonságával, amely többek között az egyik legfontosabb érdekként is jelentkezik. (Cseh Köztársaság 2015b)

A stratégia bemutatja és értékeli az ország biztonsági környezetét. A legfontosabb tényezők és trendek elemzése során a dokumentum fontos megállapításokat tesz a kibertérre vonatkozóan: „Azok a szereplők, akik egyre növekvő ambícióik miatt érdekeik elérése érdekében hajlandók 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)

A stratégia megállapítja, hogy az egyik legfontosabb nem katonai veszélyforrás többek között a kibertámadások jelentette fenyegetés, amelyet külön be is mutat a veszélyek felsorolásakor, illetve azok elemzésekor. Ezzel kapcsolatban a dokumentum kitér a kibertér határoknélküliségére, illetve arra a tényre, hogy ebben a fenyegetések forrása és a fenyegetések célpontjai közötti távolság viszonylagossá, relatívvá válik. Mindezeken túl a stratégia megállapítja, hogy a kibertámadásoknak olyan aszimmetrikus jellege is van, amely lehetővé teszi nemcsak az állami szereplők, hanem az államnál kisebb entitások számára is a támadások indítását a cseh infrastruktúra, illetve maga a cseh állam ellen. Az anyag külön kiemeli a kommunikáció-, az energia-, a közlekedés-, illetve a pénzügyi szektor és az ipar hálózatait mint azokat a legfontosabb infrastruktúrákat, amelyek kitettsége a legnagyobb a kibertámadásokkal szemben. Külön veszélyként értékelik a katonai rendszerek elleni ilyen kibertámadásokat, hiszen ezek működésképtelensége az állam védelmének egyik legfontosabb pillérében

okozhat fennakadásokat. Ezek mellett a kibertérben folyó politikai és gazdasági kémkedés veszélyességét is hangsúlyozza a dokumentum. (Cseh Köztársaság 2015b)

12. ábra

A Cseh Köztársaság nemzeti biztonsági stratégiájának borítója

Forrás: Cseh Köztársaság 2015a

A feltárt veszélyforrások kezelésére, valamint azok csökkentésére a stratégia számos intézkedést határoz meg, amelyek között a kibertámadásokkal szembeni fellépés, valamint a kritikus információs infrastruktúrák védelme is természetszerűleg helyet kapott. Ennek érdekében az anyag meghatározza egy – a 2015–2020 évekre vonatkozó – nemzeti kiberbiztonsági stratégiai elkészítését, illetve hangsúlyozza a kibertámadások elleni fellépés szervezeti hátterének kialakítását, megnevezve a kormányzati CERT-et mint ennek egyik legfontosabb elemét. Ugyanakkor a CERT mint operatív szervezet mellett a stratégia hatósági jogkörökkel ellátva, a nemzeti szintű kiberbiztonsági kérdések koordináló szervezeteként a Nemzeti Biztonsági Hatóságot jelöli meg, valamint ezen a hatóságon belül a Nemzeti Kiberbiztonsági Központ lesz az a szervezeti elem, amely a nemzeti és a nemzetközi kiberbiztonsági korai előrejelzőrendszer részeként, valamint a nemzetközi koordinációban Csehországot képviseli. (Cseh Köztársaság 2015b)

4.2.2. A Cseh Köztársaság nemzeti kiberbiztonsági stratégiája

Mielőtt a Csehország nemzeti biztonsági stratégiájában meghatározott nemzeti kiberbiztonsági stratégiát bemutatnánk, érdemes néhány utalást tenni azokra a korábbi lépésekre, amelyek a kiberbiztonság, illetve az információbiztonság területén Csehországban korábban történtek.

A biztonsággal és így – bár csak érintőlegesen, de – a kiberbiztonsággal kapcsolatos stratégiai szintű dokumentum 2008-ban jelent meg a Cseh Köztársaságban, amelynek címe *Nemzeti biztonsági kutatási stratégia* volt. A cseh Belügyminisztérium által kidolgozott anyagban felállított prioritások a kiválóságot, a legjobb gyakorlatok elterjesztését és alkalmazását, valamint a beruházások racionalizálását célozták meg. A biztonság tekintetében a stratégia három fő területen határozott meg elsődleges feladatokat, ezek a következők:

- a polgárok biztonsága (beleértve a terrorizmus elleni tevékenységet, a szervezett bűnözést, a polgári védelmet, a környezeti biztonságot stb.);
- a létfontosságú infrastruktúrák (beleértve az energia-, víz-, élelmiszer-, a közlekedés-, banki és pénzügyi, az IKT-szektorokat stb.);
- a válságkezelés (beleértve a korai figyelmeztetést és a felkészülést). (Kovács 2012)

A stratégia meghatározott olyan, horizontális értelemben vett prioritásokat is, mint például az incidens-előrejelzés, a készenlét (tudatosítása), az innováció, a felhasználók és eszközök azonosítása, valamint az EU-val történő koordináció.

Ezt követően 2011 januárjában elfogadták a Digitális Cseh Köztársaság stratégiát, amely alapvetően a nagy sebességű hálózati hozzáférés fejlesztését tűzte ki célul. Ennek megfelelően a dokumentumban megfogalmazott legfőbb cél a Cseh Köztársaság polgárai és a vállalatai nagysebességűinternet-hozzáférésének és az elektronikus kommunikációs technológiák használatának a legszélesebb társadalmi kör számára történő biztosítása. A stratégia támogatása érdekében a cseh Ipari és Kereskedelmi Minisztérium elindította a www.digitalnicesko.cz információs portált, amely az említett területeken megjelenő legfontosabb hírek, jogszabályok, valamint az ajánlott technológiai megoldások információs portálja kívánt lenni. A stratégia a feladatok pénzügyi támogatásához az Európai Beruházási Bank, valamint a Vidékfejlesztési Alap és a strukturális alapok bevonását is szorgalmazta. (Kovács 2012)

2011-ben készült el és jelent meg a Cseh Köztársaság első kiberbiztonsági stratégiája, amely akkor a 2011–2015 közötti időszakra vonatkozott, és amely alapvetően a Cseh Köztársaság korábbi Nemzeti Biztonsági Stratégiáján alapult. Ennek a stratégiának a fő célja az volt, hogy a Cseh Köztársaság területén a számítógépes biztonság megszilárduljon, és létrejöjjön egy jogi alapokkal rendelkező hiteles,

szilárd információs társadalom. A dokumentum elkötelezett volt a biztonságos információtovábbítás és -feldolgozás iránt, valamint az információáramlás – az élet valamennyi területén történő – szabad és biztonságos megvalósítása mellett. Ebben a stratégiában a következő legfontosabb célok fogalmazódtak meg:

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

17. táblázat

A Cseh Köztársaság internetpenetrációja 2016-ban és 2017-ben

Cseh Köztársaság			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	10,5	9,3	88,4%
2017	10,5	9,3	88,4%

Forrás: www.internetlivestats.com/internet-users/czech-republic/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

Ezt a 2011-es stratégiát váltotta le a 2015-ben megjelent új, *Nemzeti Kiberbiztonsági Stratégia 2015–2020* című dokumentum, amelyet az említett Nemzeti Kiberbiztonsági Központ jegyez.

A stratégia mintegy bevezetőként számos célt fogalmaz meg. E célkitűzések között szerepel az olyan képességek nemzeti szintű megteremtése, amelyek a legújabb kiberfenyegetettségeknek is ellenállnak, vagy a nemzetközi együttműködés rendszerében való aktív és hatékony együttműködés, legyen szó akár a NATO, akár az Európai Unió keretében, akár bilaterális együttműködésben megvalósuló együttműködésről.

13. ábra

A Cseh Köztársaság Nemzeti Kiberbiztonsági Stratégiája a 2015–2020 időszakra.

Forrás: Cseh Köztársaság 2015c

A kritikus információs infrastruktúrák területén a stratégia külön hangsúlyozza, hogy nem elegendő az egyes elemek védelmére kon-

centrálni, hanem szükséges a hálózatok egységes, az egész kibertérre – ebbe beleértve a teljes lakosságot is – kiterjedő, komplex biztonságának a megteremtése. A stratégia ezen a területen vezető szerepet szán a kormányzati CERT-nek, azaz a GovCERT.CZ-nek, amely szervezet feladata lehet többek között az ágazati CERT-ek vagy CSIRT-ek közötti koordináció is. (Cseh Köztársaság 2015d)

A stratégia megadja azokat az alapelveket is, amelyek mentén a kiberbiztonság területén elengedhetetlen feladatokat, illetve az azok végrehajtásához szükséges szervezetrendszert meghatározza. 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)

A dokumentum értékeli a kihívásokat és a veszélyeket is. Itt 19 olyan kihívást azonosít a stratégia, amelyek negatívan befolyásolják az ország kiberbiztonsági helyzetét. Ezek a 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;
- a 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 és a kritikus technológiai hibák számának növekedése;
- a mobil eszközöket használók számának, illetve ezzel párhuzamosan a mobil eszközökön megjelenő kártékony kódok növekvő száma;
- a hardveres hátsó ajtókon keresztül történő 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;
- a big data és az új adattárolási módszerek kihívásai;
- az ipari irányító rendszerek védelme és az egészségügy információs rendszerei;
- okoshálózatok: az alapvetően a jövő energiaellátásában kulcsszerepet játszó olyan eszközök biztonsága, amelyek a hatékony energiatermelésben és -elosztásban működnek közre;
- a védelmi szektor növekvő függősége az infokommunikációs eszközökkel és rendszerekkel szemben;
- a fejlett rosszindulatú szoftverek számának növekedése;
- botnetek, DoS- és DDoS-támadások;
- növekvő kiberbűnözés;
- a közösségi médiumok biztonsági kihívásai;
- a felhasználók alacsony szintű digitális tudása;
- a kiberbiztonsági szakértők alacsony száma, valamint a képzésük reformjának szükségessége. (Cseh Köztársaság 2015d)

A stratégia a kihívások felsorolása és rövid bemutatása után nyolc fő feladatcsoportot határoz meg. Ezek a következők:

- 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, a NATO, az ENSZ és az EBESZ különböző programjaiban való részvétel, valamint a közép-európai térségben a kiberbiztonság területén szükséges

országok közötti párbeszéd elősegítése,[51] nemzetközi kibergyakorlatok és képzések szervezése, valamint a nemzetközi jogi szabályozás és jogi keretek kialakításának felgyorsítása;

- a nemzeti kritikus információs infrastruktúrák és kiemelt információs rendszerek[52] védelme: világos eljárásrend kialakítása a kritikus infrastruktúrákat fenyegető veszélyek folyamatos elemzése, az infrastruktúrák ellenálló képessége, megbízhatósága növelése érdekében, valamint a Nemzeti Kiberbiztonsági Központ és a govcert.cz technikai képességeinek, illetve humán erőforrásának 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, 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;
- az oktatás és a biztonságtudatosság növelése, valamint 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;

[51] Erre az egyik legjobb példa a cseh és osztrák kezdeményezésre létrejött Közép-Európai Kiberbiztonsági Platform létrehozása, amelyben a két említett országon kívül hazánk, Lengyelország és Szlovákia is részt vesz.

[52] A stratégia külön említi a kiemelt információs rendszereket (Important Information Systems, IIS).

- a cseh rendőrség kiberbűnözés elleni képességeinek fejlesztése: humán és technológiai erőforrásfejlesztés szükséges, valamint fokozni kell a nemzetközi együttműködést e területen;
- a 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)

4.3. Egyesült Királyság

4.3.1. Az Egyesült Királyság nemzeti biztonsági stratégiája

Az Egyesült Királyság nemzeti biztonsági stratégiáját, amelynek hivatalos címe *Erős Nagy-Britannia a bizonytalanság korában: A Nemzeti Biztonsági Stratégia* (a stratégia eredeti angol címe: *A Strong Britain in an Age of Uncertainty: The National Security Strategy*) 2010-ben adták ki. Ez az ország második nemzeti biztonsági stratégiája a hidegháború vége óta. Ugyanakkor ez a stratégia maga is több módosításon, illetve aktualizáláson esett át, többek között 2012-ben, valamint 2015 novemberében. A 2015-ös módosítás, amely egy lényeges, sok elemre kiterjedő felülvizsgálat eredménye, az eredeti dokumentumhoz képest több mint kétszeres terjedelműre nőtt, és szerkezetében is teljesen új dokumentum. (Egyesült Királyság 2015)

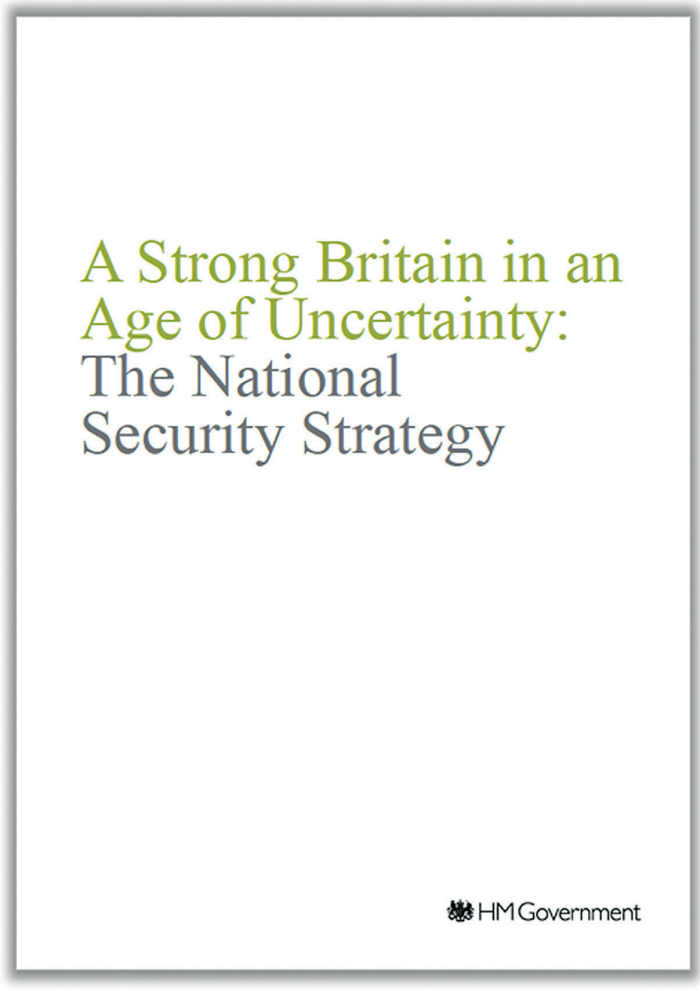
A 2010-es eredeti stratégiában a kibertámadások jelentette veszélyek rögtön a dokumentum előszavában[53] megjelennek, együtt a többi

[53] A stratégia előszavát az akkori brit miniszterelnök, David Cameron, valamint a miniszterelnök helyettese, Nick Clegg jegyzi.

nem hagyományos veszélyforrásra történő utalással. A stratégia már a bevezetőben számba veszi és felsorolja a Nemzeti Biztonsági Tanács által kiemelt, a brit nemzet biztonságát leginkább fenyegető veszélyforrásokat, amelyek a következők:

- 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)

A stratégia ezt követően nemcsak a veszélyforrásokat, hanem azoknak az Egyesült Királyságra gyakorolt hatásait is elemzi, amely során a kibertérben megjelenő veszélyek esetében kiemeli: „Az ellenfelek, akikkel szembenézünk, 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)



14. ábra

Az Egyesült Királyság 2010-es Nemzeti Biztonsági Stratégiája

Forrás: Egyesült Királyság 2010

A 2010-es stratégiával szemben az annak 2015-ös felülvizsgálata során létrejött dokumentum már lényegesen nagyobb teret szentel a kibertérnek, az ott megjelenő technológiának és az arra épülő gazdaságnak, illetve a kibertér veszélyeinek.

A *Nemzeti biztonsági stratégia és védelmi stratégiai és biztonsági felülvizsgálat 2015: Biztonságos és prosperáló Egyesült Királyság (National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom)* című dokumentum természetesen szintén kiemelt veszélyforrásként értékeli a kibertámadásokat, de a legfontosabb stratégiai célkitűzések bemutatásánál már az is megjelenik, hogy a brit polgárok védelme érdekében szükséges olyan kemény és innovatív intézkedések meghozatala és bevezetése, amelyek a kiberbiztonság területén az Egyesült Királyságot a világ vezető hatalmai közé emelik. (Egyesült Királyság 2015)

Mindezeken túl a stratégia külön fejezetben elemzi a technológia és ezen belül a kiberteret alkotó hálózati és információtechnológia szerepét, ahol – hasonlóan a 2010-es stratégiában megfogalmazottakhoz, de azt némileg bővítve – a kibertérben megjelenő veszélyekkel is számot vet: „Az 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. A nem állami szereplők, ideértve a terroristákat és a kiberbűnözőket is, könnyen elérhető számítógépes eszközöket és technológiát használhatnak fel destruktív célokra.” (Egyesült Királyság 2015)

A stratégia címében is megjelenő védelmi politika felülvizsgálatának eredményét rögzítve a dokumentum a fegyveres erők vonatkozásában is meghatároz számos stratégiai alapelvet. Ezek közé tartozik az Egyesített Fegyveres Erő 2025 (Joint Force 2025) koncepció

alapjainak lefektetése is. Ebben a koncepcióban külön szerepet kap a kiberképességek fejlesztése, amely többek között egy, a legmagasabb vezetési szinten létrehozandó kibercsoport felállítását is előirányozza mindamellett, hogy az Egyesült Királyság elkötelezett az új technológia katonai célú alkalmazása, valamint a kibertérben történő, lehető legnagyobb előnyöket jelentő használata mellett.

A stratégia az elrettentésre épül, amelyet többször is hangsúlyoz a dokumentum, többek között akkor is, amikor kijelenti, hogy a polgárok védelme érdekében az elrettentés fenntartása érdekében képességeinek teljes spektrumát használni fogja, beleértve a katonai erőt és a kibertámadásokat is.

A dokumentum leszögezi, hogy az akkor még csak tervezett 2016-os NATO varsói csúcstalálkozó során a kibertér és az ott megvalósítandó biztonság kiemelt szerepet kell, hogy kapjon. (Egyesült Királyság 2015)

Hasonlóan a technológia szerepének elemzéséhez, a kibertér és annak összetevői külön fejezetet kaptak a stratégiában. A dokumentum megállapítja, hogy az Egyesült Királyság kibernagyhatalom, amelyhez az üzleti, a kormányzati szektor, beleértve a nemzetbiztonsági szolgálatokat és a védelmi szféra is nagyban hozzájárul. 2011-ben külön stratégia készült a nemzeti kiberbiztonság megteremtésére, és ezt követően a terület hatalmas anyagi erőforrásokat is kapott, valamint a kiberbiztonsághoz szükséges szervezeti rendszer kialakítása is megkezdődött, hiszen többek között felállt a Kiber Értékelési Központ (Centre for Cyber Assessment), illetve az Egyesült Királyság CERT-je (UK's Computer Emergency Response Team, CERT-UK). A következő ötéves időszakra a nemzeti biztonsági stratégia további anyagi erőforrásokat irányozott elő, amelyeket a 2016-ban megjelent új Nemzeti Kiberbiztonsági Stratégiában meghatározott biztonsági programokra kellett felhasználni. (Egyesült Királyság 2015)

Ahogy a fentiekből is kitűnik, a dokumentum a nemzeti biztonsági stratégiákhoz képest szokatlan részletességgel elemzi a kibertér egyes elemeit, illetve mindazokat a tevékenységeket, amelyeket a biz-

tonság megteremtése érdekében a kibertérben is szükséges megtenni. Ennek során meghatározta, hogy a kibertámadások detektálása és az ellenük való védekezés, valamint a válaszreakciók milyen feladatokat igényelnek. Ugyanígy külön bemutatta a kiberbűnözés elleni fellépést – például meghatározta a Nemzeti Kiberbűnözés Elleni Egység (National Cyber Crime Unit, NCU) felállítását és fejlesztését –, valamint előírta a nemzetközi téren szükséges teendőket. (Egyesült Királyság 2015)

A stratégia külön kitér a kritikus infrastruktúrák területére, illetve a kiberbiztonság és az infrastruktúrák védelmének kérdéseire is. Itt a dokumentum leszögezi annak szükségességét, hogy a kritikus-infrastruktúra-tulajdonosok és -üzemeltetők számára szükséges kiberbiztonsági képzések kialakítása érdekében, valamint a terület szabályozásához el kell készíteni azokat az ajánlásokat, amelyek alapján a kibervédelem ezen a területen is hatékonyabbá tehető.

A stratégia utolsó fejezete, amely a társadalmi és gazdasági jólétet irányozza elő, a gazdasági biztonság, az innováció, valamint a védelmi és biztonsági ipar területein szintén számos helyen utal a kibertérre, illetve annak fontosságára. A gazdasággal kapcsolatosan a dokumentum kiemeli a kiberbűnözés elleni fellépés fontosságát, az innovációs tevékenységek és feladatok bemutatásakor pedig megjegyzi, hogy a brit kiberbiztonsági vállalatok a világ élmezőnyébe tartoznak, de ezen a területen is szükséges a magánvállalkozások innovációs tevékenységének ösztönzése. Ehhez a már működő védelmi ipari együttműködéseket is fel kell használni. Emellett a stratégia külön kiemeli a kiberbiztonsági szektor növekedésének elősegítését: „Ösztönözni fogjuk egy élénk kiberbiztonsági ágazat létrehozását és növekedését, beleértve két innovációs központ kialakítását; a legkorszerűbb kiber kkv-k támogatását; és hozzá kívánunk járulni az egyetemeken folyó kutatások eredményeinek kereskedelmi forgalomba hozatalához.” (Egyesült Királyság 2015)

4.3.2. Az Egyesült Királyság nemzeti kiberbiztonsági stratégiája

15. ábra

Az Egyesült Királyság első, 2011-ben megjelent nemzeti kiberbiztonsági stratégiája

Forrás: Egyesült Királyság 2011

Ahogy a Nemzeti Biztonsági Stratégia is utalt rá, az Egyesült Királyság első kiberbiztonsági stratégiája 2011 novemberében látott napvilágot. Ez a stratégia, amely *Az Egyesült Királyság védelme és támogatása a digitális világban (The UK Cyber Security Strategy Protecting and promoting the UK in a digital world)* címet kapta, akkor még csak a 2015-ig terjedő időszakra határozott meg kiberbiztonsági kiemelt célokat.

A stratégia legfontosabb céljai a következők voltak:

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

18. táblázat

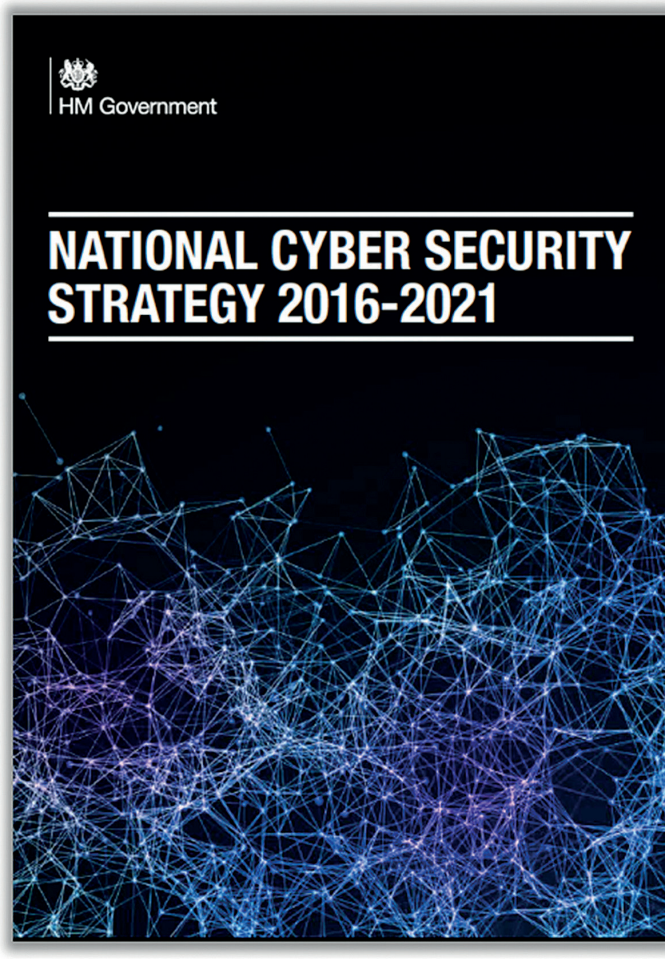
Az Egyesült Királyság internetpenetrációja 2016-ban és 2017-ben

Egyesült Királyság			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	65,1	60,2	92,6%
2017	65,5	62,1	94,8%

Forrás: www.internetlivestats.com/internet-users/uk/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

A kissé általános, ugyanakkor a megjelenésekor nagyon is ambiciózus célokat tartalmazó stratégiát 2016-ban egy új nemzeti kiberbiztonsági stratégia követte *Nemzeti Kiberbiztonsági Stratégia 2016–2021 (National Cyber Security Strategy 2016–2021)* címmel.

A 2015-ös *Nemzeti Biztonsági Stratégiá*hoz hasonlóan meglehetősen hosszú, mintegy 80 oldalas dokumentum a stratégiai környezet bemutatásával kezdődik, amely a kibertérben megjelenő veszélyek és sebezhetőségek elemzését foglalja magában.



16. ábra

Az Egyesült Királyság második kiberbiztonsági stratégiája

Forrás: Egyesült Királyság 2016

A stratégia által feltárt, majd röviden elemzett legfontosabb veszélyek a következők:

- kiberbűnözés;
- állami és állami támogatású veszélyek, beleértve a kiberkémkedést, illetve a kritikus infrastruktúrákat fenyegető kibertámadásokat is;
- terrorizmus;
- hacktivizmus;
- script kiddies, azaz igazi számítógépes tudással nem rendelkező, de a különböző támadóeszközök felhasználásával károkat okozó fiatalok. (Egyesült Királyság 2016)

Ebből a felsorolásból is látszik, hogy nem teljesen egyenszilárd a veszélyek megítélése, hiszen például az állami támogatású kibertámadások nagy valószínűséggel nem ugyanolyan szintű veszélyt jelentenek, mint például a script kiddie-k, azaz az igazi programozási tudással nem rendelkező, de lelkes, fiatal felhasználók jelentette veszélyek.

A veszélyek elemzése után a stratégia a sérülékenységeket veszi számba. A feltárt sérülékenységek a következők:

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

Mindezekre a veszélyekre és kihívásokra, valamint a sérülékenységekre a stratégia a védelem–elrettentés–fejlesztés (defend–deter–develop) hármas filozófiai meghatározással kíván válaszokat adni. Ezek közül a védelem nyilvánvalóan nem igényel sok magyarázatot, hiszen ezen a területen a stratégia kijelenti, hogy az állam a kibertámadásokkal szemben megvédi mind az állampolgárokat, mind a gazdasági szereplőket és a közigazgatást is. Ebbe a védelembe beletartozik az is, hogy a felhasználókat olyan tudás birtokába juttassák, amelyek alapján képesek felismerni és bizonyos szintig kezelni is a támadásokat.

Az elrettentés azonban már nem ennyire egyszerű terület. Ennek kapcsán a stratégia kijelenti, hogy természetszerűleg a támadások detektálására, azok forrásainak felderítésére, valamint az azok elleni jogi és technikai lépések megtételére is késznek kell lenni, de mindezeken kívül a támadókkal szembeni offenzív lépés, azaz az ellentámadás vagy akár a megelőző támadás sem elképzelhetetlen. (Egyesült Királyság 2016)

Ez egy nagyon fontos kijelentés, hiszen a támadóval szembeni – álljon a támadó mögött gazdasági érdekcsoport vagy akár, ahogy a stratégia a veszélyforrásoknál említi, egy állam – potenciális offenzív tevékenység, azaz kibertámadások kivitelezése valóban lehet olyan elrettentő erő, amely visszatarthatja az adott elkövetőt – vagy az amögött álló erőket – a támadástól. Ebben az értelemben a kiberelrettentés nagy valószínűséggel működhet. Azért csak nagy valószínűséggel, mert ehhez az ellentevékenységhez, azaz a kibertámadó képességekhez megfelelő jogi, szervezeti és technikai háttér kiépítése és megléte is szükséges.

A harmadik terület, azaz a fejlesztés pedig nyilvánvalóan a védelemhez és az elrettentéshez szükséges innovatív megoldásokat jelenti, amelyek során a tudományos alapokon nyugvó kutatás-fejlesztésre, majd ennek az ipari gyártásban és alkalmazásban való megjelenésére is komoly hangsúlyt helyeznek.

A stratégia előremutató módon a kiberbiztonság különböző szereplői között szétosztja a feladatokat és a felelősségi köröket. Külön meghatározza az egyéni felhasználók, azaz az individuumok, a gazdasági élet szereplőinek, valamint a kormányzat szereplőinek a feladatát és felelősségét.

A kormányzat általános érvényű feladatai, mint például az állampolgárok kibertámadásokkal szembeni védelme, az információs rendszerek és az adatvagyon védelme, együttműködés kialakítása és az érdekelt felek közötti koordináció biztosítása stb. meghatározása mellett a stratégia elrendeli egy Nemzeti Kiberbiztonsági Köz-

pont (National Cyber Security Centre, NCSC) felállítását is. (Egyesült Királyság 2016)

Az NCSC 2016 októberében meg is kezdte működését azzal a legfontosabb feladattal, hogy hatékony koordináló partner legyen a kormányzat, a közigazgatás szereplői, az ipar, illetve a társadalom között. A központ egyfajta kiberbiztonsági tanácsadó szerepet is betölt a kormányzat számára, de emellett egy, a társadalom számára jól látható entitás is, amely egyrészt professzionalizmusa révén garancia a kiberbiztonság megteremtésére és fenntartására, másrészt valóban hatékonyan képes megvédeni az Egyesült Királyság szervezeteit és állampolgárait a kibertámadásokkal szemben. Mindezek mellett a központ képes a már meglévő olyan képességeket szintetizálni, amelyek többek között a Nemzeti Technikai Információbiztonsági Hatóságnál (jelenlegi megnevezése: National Technical Authority for Information Assurance, korábban: Communications-Electronic Security Group, CESG), a Nemzeti Infrastruktúra Védelmi Központnál (Centre for the Portection of National Infrastructure, CPNI), a CERT-UK-nél vagy a Nemzeti Kiberbiztonsági Elemző Központnál (Centre for Cyber Assessment, CCA) állnak rendelkezésre.

Az NCSC legfontosabb feladatait a stratégia a következőkben állapította meg:

- 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;
- 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)

A stratégia a megfogalmazott célok eléréséhez szükséges feladatok végrehajtására tartalmaz egy implementációs tervet is. Ez az implementációs terv a már említett védelem–elrettentés–fejlesztés hármas mellett határozza meg mindazokat a tevékenységeket, amelyek szükségesek az Egyesült Királyság számára a kiberbiztonság eléréséhez.

A védelem vonatkozásában az aktív kibervédelmi megoldásokat, a biztonságos internet kialakítását, a kormányzat és a közigazgatás, a kritikus infrastruktúrák védelmét – mindezek során a hatékony incidenskezelést is hangsúlyozva –, valamint a társadalom kiberbiztonsággal kapcsolatos felfogásának – benne a biztonságtudatosság alapvető átalakítását és fejlesztését – jelöli meg legfontosabb feladatként. Ugyanakkor a feladatok mellett az azok végrehajtásához szükséges tevékenységeket is meghatározza az azokkal elérendő legfontosabb célokkal egyetemben.

Az elrettentés feladatai során a stratégia először magyarázatot ad arra, hogy a kibertérben ez hasonlóan kell, hogy működjön, mint a fizikai térben, majd meghatározza az ehhez szükséges feladatokat. Ezek a kiberbűnözés elleni fellépés, illetve annak radikális csökkentése, az ellenséges külföldi szereplők elleni tevékenység, a terrorizmus elleni védelem, a támadó kiberképességek kiépítése, valamint az erősebb titkosítási eljárások kidolgozása. Természetszerűleg itt is minden tevékenységhez célokat, illetve megoldási módokat, valamint a célok elérésének hatékonyságát (sikerességét) mérhetővé tevő megoldásokat ír le a dokumentum. Mindezek közül önkényesen emeljük ki a kibertámadó képességeket. Ezekhez a támadó képességekhez a stratégia megnevez (de nem részletez) egy Nemzeti Kibertámadási Programot (National Offensive Cyber Programme, NOCP). A támadóképességekhez a stratégia a következő célt társítja: „Biztosítani 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)

A megfelelő kibertámadó-képességekhez – ahogy korábban említettük – megfelelő technikai és szervezeti háttér is szükséges a megfelelő humán erőforrással együtt. Ennek tesz eleget a stratégiában megfogalmazott feladategyüttes, amely a kibertámadást egyrészt a hadsereg kompetenciájába utalja, hiszen meghatározza, hogy a Védelmi Minisztérium az NOCP-ben meghatározottak szerint, illetve természetesen együttműködve a Nemzeti Kommunikációs Központtal[54] (Government Communications Headquarters, GCHQ) kell, hogy a támadóképességeket és -eszközöket kifejlessze, másrészt a fegyveres erőknél olyan képességeket kell kialakítani, amelyek a katonai műveletek részét képezik, és azokkal együtt alkalmazhatók. (Egyesült Királyság 2016)

A fejlesztési feladatokkal kapcsolatban a stratégia a következő feladatokat határozza meg:

- 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)

A stratégia külön fejezetben tér ki a nemzetközi együttműködés feladataira és lehetőségeire, amelyben hangsúlyozza az ENSZ, a G20, az EU, a NATO, az EBESZ, illetve a Brit Nemzetközösség kereteiben végzett olyan feladatokat, amelyek egyrészt a bizalomerősítést, másrészt a kevésbé fejlett országok felzárkóztatását és segítését jelentik.

A stratégia egy nagyon rövid következtetéslevonással zárul, amely a 2021 utáni évekre vonatkozó vízióval fejeződik be. A dokumentum ebben továbbra is hangsúlyozza, hogy a gyors technológiai változás olyan stratégiát igényel, amely alapján a kihívásokra és veszélyekre

[54] Ennek része a kormányzati rádióelektronikai felderítő- és a kibertértechnikai felderítőszervezet is.

gyors, megfelelő és hatékony válasz adható. A következő évtizedre pedig egy olyan technológiai robbanást prognosztizál, amelyben a kibertéri veszélyek is robbanásszerű fejlődésen mennek keresztül, mind azok számát, mind azok volumenét tekintve. Ugyanakkor – teszi hozzá a stratégia –, ha sikerül a mindennapi biztonság és a biztonságról való gondolkodás részévé tenni a kiberbiztonságot, akkor sokkal kevésbé lesz a nemzet kitéve ezeknek a veszélyeknek a jövőben, mint ma. Ebben az esetben még az is elképzelhető, hogy maga a társadalom, a piaci szereplők és szolgáltatók lesznek azok a meghatározó entitások, amelyek hatékonyan fel tudnak lépni – a piac diktálta szabályok alapján – a kibertérben megjelenő kihívásokkal szemben, és így az állam szerepe ezen a területen lényegesen kisebb lehet. (Egyesült Királyság 2016)

4.4. Észtország

4.4.1. Észtország nemzeti biztonsági stratégiája

Észtország geopolitikai helyzete rendkívül érzékennyé teszi az észt kormányzatot és nem mellesleg az észt embereket is a biztonság iránt. Ennek oka egyrészt a történelemben, másrészt a 2007-es tavaszi eseményekben keresendő. Az észt politikai döntéshozók, de az egyszerű mindennapi emberek is nagyon jól emlékeznek arra az eseménysorozatra, amely során alapvetően túlterheléses támadásokkal a támadók gyakorlatilag egész Észtország működését tették lehetetlenné néhány óráig, esetenként néhány napig 2007 áprilisában és májusában. (Kovács 2014)

Ezt a tapasztalaton alapuló biztonságfelfogást tükrözi az észt stratégiai dokumentumok rendszere is. Észtország ugyanis rendelkezik egy nemzeti biztonsági koncepcióval, amelyet 2010-ben adtak ki, de emellett egy nemzeti védelmi stratégiát is alkotott, amely az első – 2005-ös kiadása után – 2011-ben frissített és átdolgozott formában jelent meg.

A nemzeti biztonsági koncepció célja természetesen az ország függetlenségének, területi integritásának, valamint az állampolgárok védelmének biztosítása és garantálása. A dokumentum ezeket a célokat olyan általános érvényű alapelvekkel támogatja, mint a veszélyek és kihívások kezelésének szükségessége, valamint a nemzetközi együttműködési rendszerben – elsősorban a NATO keretében – történő biztonsági garanciák és az ezekhez szükséges tevékenységek végzése. (Észtország 2010)

A biztonsági környezet értékelése során a koncepció utal arra a sok esetben az információtechnológia fejlettsége miatt keletkező veszélyre, amely a kibertérben érhető tetten: „Az országok ellenálló képessége 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 terroristacsoportokat és a szervezett bűnözést, egyre növekszik." (Észtország 2010)

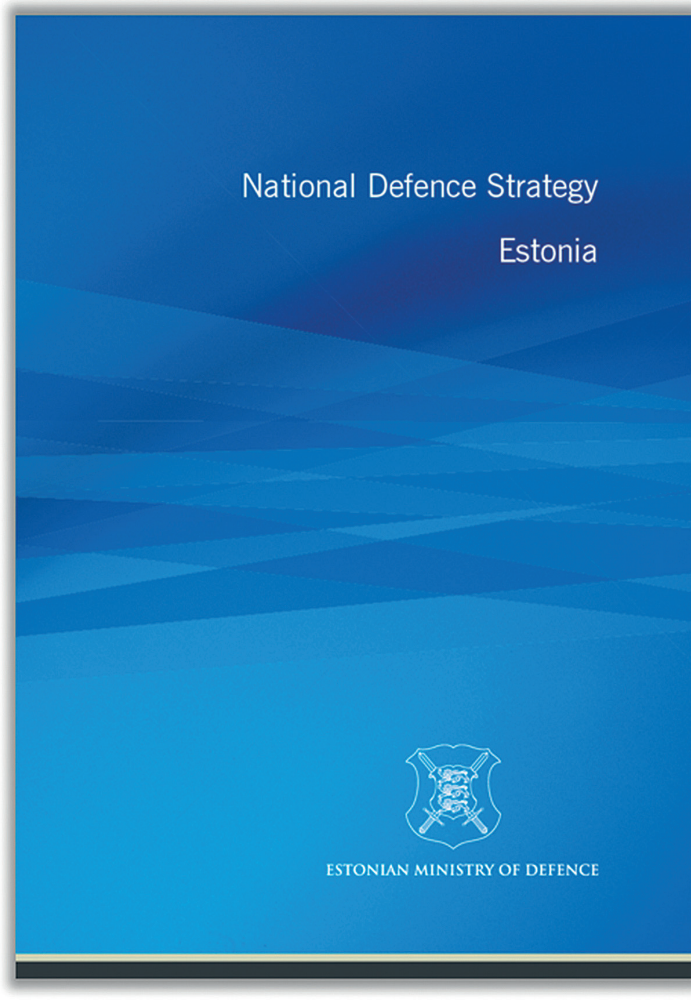
A koncepció a kibertér jellegzetességei, illetve az infokommunikációs rendszerek egymásra hatásában, az azoktól való – a fenti idézetben is jól nyomon követhető – egyre nagyobb társadalmi és gazdasági függőségben, valamint a kibertérben megjelenő veszélyekre adott elégtelen válaszokban komoly kihívásokat azonosít.

Ezeken kívül a dokumentum kiemeli a kiberbűnözés elleni tevékenységet, amely során az IKT-rendszerek működőképességének biztosítását jelöli meg célként. A kiberbűnözés során az együttműködés és a jogszabályi keretrendszer fontosságát is hangsúlyozza, majd nem utolsósorban a koncepció rögzíti, hogy az e feladathoz szükséges technikai és tudásbeli erőforrásokat a kormány biztosítja: „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 fenntarthatóságot a szükséges technikai eszközök és a know-how rendelkezésre állásának biztosításával." (Észtország 2010)

A fentiekből is jól érzékelhető, hogy a kiberbiztonság kiemelt szerepet kap Észtország nemzeti biztonsági koncepciójában. A kiberbiztonságot a társadalmi ellenálló képesség és a társadalmi kohézió megteremtésének eszközeként mutatja be a dokumentum. Itt az olyan tényezőkre kerül a hangsúly, mint az IKT-rendszerekben meglévő sérülékenységek csökkentése, a kibertérben megjelenő veszélyekre való hatékony reagálóképesség megteremtése (ez nyilvánvaló utalás az általunk is említett 2007-es események során tapasztalt elégtelen védekező- és reagálóképességekre), a hatékony jogszabályi keretek kialakítása, valamint a szoros nemzetközi kapcsolatok kiépítése.

A társadalmi ellenálló képesség és kohézió megteremtésében tehát a kiberbiztonság alapvető szerepet játszik, különösen egy olyan fejlett információs infrastruktúrával rendelkező ország esetében, mint Észtország, így a dokumentum nagyon előremutató módon (ne felejtsük el: 2010-et írunk a koncepció megjelenésekor, és az európai országok zömében még nem is kezdődött meg a kiberbiztonságról való stratégiai gondolkodás) a szükséges feladatok meghatározására egy kiberbiztonsági akciótervet irányoz elő. (Észtország 2010)

A 2010-es nemzeti biztonsági koncepció után 2011-ben jelent meg a nemzeti védelmi stratégia, amely a 2005-ös első ilyen stratégia átdolgozott verziója. Az új stratégia meg is indokolja a sűrű biztonsági stratégiaalkotás okát: a gyorsan változó biztonságpolitikai helyzet, az újonnan megjelenő veszélyek és kihívások megjelenése miatt szükséges a stratégia ilyen ütemű frissítése.



17. ábra

Észtország 2011-es Nemzeti Védelmi Stratégiája

Forrás: Észtország 2011

Az új dokumentum rögtön az első gondolatok között leszögezi, hogy a nemzet védelme ma már átfogó megközelítést igényel, amely során a katonai erőt és a katonai megoldásokat kell ötvözni más, nem katonai eszközökkel. (Észtország 2011)

A stratégia itt is a biztonsági környezet elemzésével kezdődik, amelyben a dokumentum Észtország NATO- és európai uniós tagságából eredően megállapítja, hogy az ország sosem volt ekkora biztonságban. Ugyanakkor a dokumentum a Balti-tenger térségének biztonságára kitérve hangsúlyozza, hogy Észtország biztonsága nagyban függ a balti országok biztonsági helyzetétől, illetve az ezt befolyásoló tevékenységétől, de ez természetesen fordítva is igaz. A dokumentum nagyon röviden elemzi az olyan alacsony szintű konfliktusok gyors eszkalálódásának a veszélyét is, amelyeket nem a megfelelő időben és nem a megfelelő eszközökkel kezelnek. A stratégia megállapítja, hogy az országgal szembeni közvetlen katonai támadás valószínűsége kicsi, ugyanakkor nem zárható ki teljes egészében, bár a NATO-tagság bizonyos garanciákat nyújt ezzel szemben. A nem katonai támadásoknak azonban nagyobb a veszélye, főleg, ha azok az energia- vagy más kritikusinfrastruktúra-rendszereket célozzák. (Észtország 2011)

A dokumentum külön kitér és nevesíti is Oroszországot, hiszen ennek mind belpolitikai, mind külpolitikai tevékenysége hatással van Észtországra: „Az észt biztonsági környezetet is befolyásolja az Orosz Föderáció bel- és a külpolitikája. Az Orosz Föderáció fokozott érdeklődést mutat a befolyásának visszaállítása, valamint az európai biztonsági környezetre gyakorolt hatásának megerősítése iránt. Az Orosz Föderáció katonai erőinek jelenléte az észt határ közelében növekedett." (Észtország 2011)

A stratégia következő része az észt védelmi politika bemutatása. A 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 – tevékenységben látja a védelem stratégiai pontjait.

A katonai erő fejlesztése során a stratégia a védelmi minisztérium feladatai közé besorolja a kibervédelem koordinálását is. E feladat mellett a Nemzeti Védelmi Liga – azaz a hadsereg támogatására hivatott önkéntes civil szerveződés – számára meghatározza a kibervédelmi képességek fejlesztését.[55]

4.4.2. Észtország nemzeti kiberbiztonsági stratégiája

Észtország első nemzeti kiberbiztonsági stratégiáját a 2008–2013-as időszakra 2008-ban adták ki. Az ország ezzel történelmet írt, mert Észtország volt az első, amely nemzeti kiberbiztonsági stratégiát adott ki. A dokumentumot a Védelmi Minisztérium dolgozta ki, amely mellé egy implementációs tervet is készítettek. Maga a stratégia – a 2007-es eseményeket gyakorlatilag azonnal feldolgozva – az átfogó megközelítés elvét alkalmazva született. Olyan kérdésekre koncentrált, amelyek nyilvánvalóan az előző években még nem voltak ennyire hangsúlyosak, és amelyekről csak a 2007-es incidenst követően kezdődött egyáltalán valamilyen gondolkodás. Ilyen kérdés volt például az információbiztonsági tudatosság nemzeti szintű növelése, a hatékony és működő jogszabályi környezet meghatározása vagy a nemzetközi együttműködés rendszerének a kiberbiztonság területén is megvalósuló kiépítése. (Osula 2015)

[55] Ezzel kapcsolatban meg kell jegyezni azt a magyar kezdeményezést, amely filozófiájában nagyban hasonlít a fenti észt elgondolásra. Ez a Magyarországon Önkéntes Kibervédelmi Összefogás (KIBEV) néven létrejött szervezet, amelynek célja, 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)

Ezt a stratégiát 2014-ben egy új dokumentum követte *Nemzeti Kiberbiztonsági Stratégia 2014–2017 (Küberjulgeoleku strateegia 2014–2017)* címmel. (Észtország 2014a)

19. táblázat

Észtország internetpenetrációja 2016-ban és 2017-ben

Észtország			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	1,3	1,2	91,4%
2017	1,3	1,27	97,7%

Forrás: www.internetlivestats.com/internet-users/estonia/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

Az új stratégia a kiberbiztonsági helyzet elemzésével kezdődik. Ebben az előző időszak változásait bemutatva a stratégia kiemeli, hogy 2009-ben felállt a Kiberbiztonsági Tanács, amely a Kormány Biztonsági Bizottságának is része lett. Mindezeken túl átnevezték és megerősítették a korábbi észt informatikai központot, amelynek az új neve Észt Információs Rendszer Hatóság (Riigi Infosüsteemi Amet, RIA) lett. A hatóság nemcsak új nevet kapott, de feladatai is kibővültek. Feladatkörébe bekerült a kritikus infrastruktúrák védelmén belül az azokban meglévő információs rendszerek biztonságáról való gondoskodás is. Ennek érdekében a RAI-n belül egy Kritikus Információs Infrastruktúra Védelmi Osztályt is felállítottak. (Észtország 2014b)

18. ábra

Észtország Nemzeti Kiberbiztonsági Stratégiája a 2014–2017-es időszakra

Forrás: Észtország 2014a

A stratégia természetesen számba veszi azokat a kihívásokat is, amelyek Észtország esetében ebben az időszakban relevánsak lehetnek. A dokumentum kihívásként értékeli az IKT-eszközök, rendszerek és szolgáltatások gyors fejlődési ütemeből eredő kihívásokat, amelyek a következő területeken jelentkeznek a leginkább:

- alapvető közműszolgáltatások: a határokon átnyúló technológiai függőség azt eredményezi, hogy már nemcsak 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;
- nemzetvédelem: 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 emberierőforrás-fejlesztés is szükséges a jövőben várhatóan megjelenő veszélyek hatékony kezelése érdekében. (Észtország 2014b)

A stratégia egy általános célkitűzést és ezen belül számos részcélt fogalmazott meg. A legfontosabb cél a következő: „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)

Ez a cél összefoglalja mindazokat a tényezőket, amelyekről említést tettünk korábban, és amelyek a 2007-es orosz–észt válsággal kerültek a felszínre, nemcsak Észtországban, hanem fejlett nyugati világunk összes – állampolgárainak biztonságáról gondoskodni akaró és tudó – országában egyaránt. Amennyiben össze kellene foglalni azt, hogy miért kell egy országban stratégiai szinten gondolkodni és gon-

doskodni a kiberbiztonság megteremtéséről, akkor keresve sem találnánk meggyőzőbb érvelést a fenti stratégiai célban megfogalmazottnál.

A stratégiai cél elérése érdekében meghatározott részcélok a következők:

- a fontos szolgáltatások alapját képező információs rendszerek védelme:
  - alternatív megoldások biztosítása fontos szolgáltatások számára;
  - a kritikus 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;
  - a 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;

- a nemzetközi együttműködés fokozása:
  - nemzetközi kiberbiztonsági politika kialakítása;
  - szorosabb együttműködés a partnerekkel és a szövetségesekkel;
  - az Európai Unió kiberbiztonsági képességeinek növelése. (Észtország 2014b)

4.5. Franciaország

4.5.1. Franciaország nemzeti biztonsági stratégiája

Franciaország új nemzeti biztonsági stratégiájának elkészítéséről, amelynek hivatalosan *Fehér könyv: Védelmi és nemzeti biztonság 2013 (Livre blanc: Défense et sécurité nationale 2013)* a címe, a francia köztársasági elnök 2012 júliusában döntött.[56] (Franciaország 2013a)

A 2013 áprilisában megjelent, szokatlanul hosszú – mintegy 160 oldal terjedelmű – stratégia bevezető gondolatait az akkori köztársasági elnök, François Hollande jegyzi.

A stratégia három prioritásra épül: a védelemre, az elrettentésre és az intervencióra, amelyek a legfontosabb célkitűzések hátterét is jelentik. E prioritások mindegyikében markánsan megjelenik a kibertér és az abban rejlő veszélyek, valamint az ellenük való védekezés szükségessége.

A stratégia elején megtörténik az ország értékeinek és érdekeinek megfelelően a biztonsági környezet feltérképezése és elemzése. Ebben a kibertérrel kapcsolatban a dokumentum olyan kérdéseket mutat be, mint a nem állami szereplők által indított kibertámadások, illetve az ellenük való védekezés lehetőségei, de az ázsiai térség elemzése során külön teret szentel a kibertéri tevékenységek mögött álló állami szereplőknek, nevezetesen Kínának és a kínai kiberképességeknek: „Kína

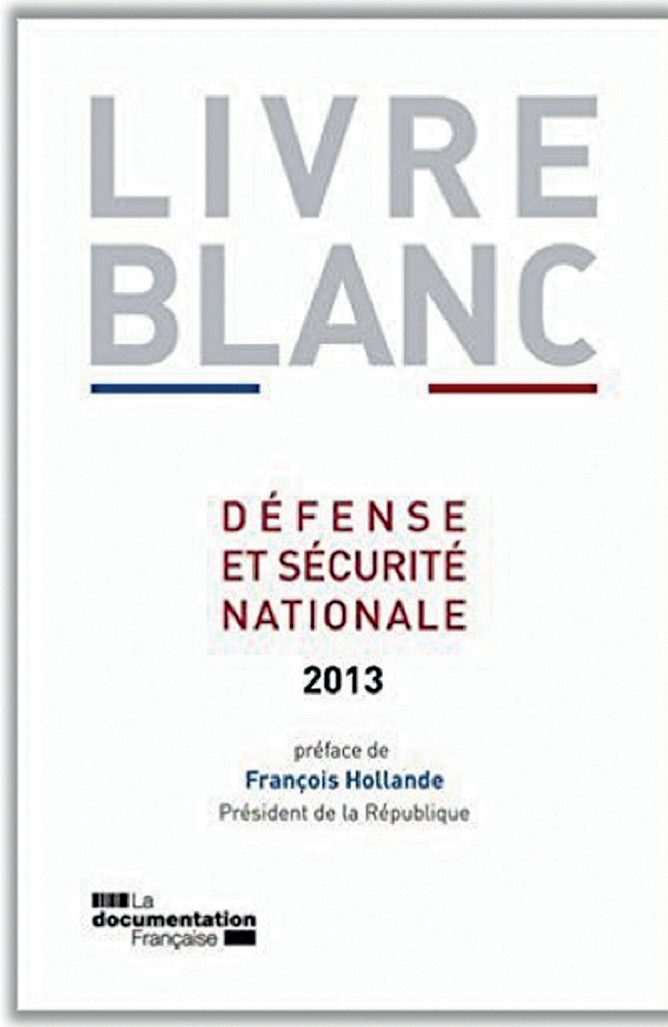
[56] A korábbi Fehér könyv Franciaország biztonságáról 2009-ben jelent meg.

a védelmi korszerűsítés terén rendkívül gyors ütemben haladt előre, különösen a nukleáris arzenálja fejlesztése, korszerűsítése, valamint annak erőkivetítése és a kibertámadások képességének terén." (Franciaország 2013b)

A biztonsági környezet elemzése során a stratégia a 2009 óta bekövetkezett alapvető változások közé sorolja azt a tényt, hogy az internet és az információtechnológia segítségével a robbanóanyagokhoz való hozzáférés, illetve az azok előállításához szükséges információ könnyen elérhetővé vált, ami komoly veszélyt jelent az ország számára.

A stratégia leszögezi, hogy az információs rendszerek olyan szinten szövik át a társadalmat, hogy a rendszerek sérülékenysége révén bekövetkező rendszerkiesések a társadalom működésére is komoly kihatással lehetnek. A stratégia azt is megjegyzi, hogy a digitális technológia fejlődése nem szükségszerűen járt együtt azok biztonságának megteremtésével. Ráadásul ezen rendszerek támadása mögött sokszor nehéz azonosítani a támadókat, akik lehetnek nem állami szereplők, de akár államok is, ahogy ezt korábban Kína esetében már láthattuk, amely országot nevesíti is a stratégia. A kibertérben megjelenő veszélyeket a dokumentum különböző szinteken látja megvalósulni. A legalsó szinten a kiberbűnözés és a hozzákapcsolható támadások – például a személyiséglopások, zsarolások, személyes adatok eltulajdonítása –, a legmagasabb szinten pedig azok a kibertámadások állnak, amelyek a kritikus információs infrastruktúrákat vagy a stratégiai katonai információs rendszereket és képességeket veszik célba. (Franciaország 2013b)

Mindezek alapján a kibertérrel kapcsolatban a stratégia levonja azt a következtetést, hogy az itt bekövetkezett támadások a kiberhadviselést is előrejelezhetik: „A kibertér így a konfrontáció terévé vált. Ahogy azt az előző 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)



19. ábra

Franciaország 2013-as Fehér könyve a nemzeti biztonsági stratégiáról

Forrás: Franciaország 2013a

Az említett prioritások közül az első a védelem, amellyel kapcsolatosan a stratégia a következő fő veszélyforrásokat azonosítja:

- az ország területével szembeni, másik ország által elkövetett agresszió;
- terroristatámadások;
- 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)

A felsorolásból világosan látszik, hogy Franciaország – számos más országhoz hasonlóan – a nemzeti biztonságra komoly fenyegetést jelentő veszélyforrásként értékeli a kibertámadásokat.

Nyilvánvalóan a fenti fenyegetések és veszélyek kezelésére a stratégia számos olyan tevékenység implementációját határozza meg, amelyekkel ezek a kihívások kezelhetők. A kibertámadások, illetve a kibertér egyéb veszélyforrásainak kezelésére egyrészt a hírszerzés aktivitásának fokozását, másrészt a technikai és a humán erőforrások fejlesztését irányozza elő a dokumentum, majd ezeken túl a kibertámadó képességek kialakításában jelöli meg azt az eszközt, amellyel hatékony válasz adható ezekre a kihívásokra.

Nagyon figyelemreméltó, hogy a stratégia a fenti általános kibertéri feladatokon kívül egy külön alfejezetben részletesen meghatározza azokat a feladatokat, amelyekkel a kibertéri veszélyek ellen fel kell lépni. A dokumentum méltatja a 2009-ben kiadott előző stratégiában meghatározott és azóta megvalósult kibervédelmi lépéseket, de hozzáteszi, hogy a kiberfenyegetettségek gyors növekedése megköveteli, hogy Franciaország egy szinttel feljebb lépjen ezen a területen. Az előző stratégia megalkotása óta megjelent új kibertéri veszélyek megkövetelik az országtól, hogy olyan nagyarányú humánerőforrás-fejlesztésbe kezdjen a kibervédelem területén, mint Németország vagy

az Egyesült Királyság. A stratégia hangsúlyozza, hogy a kibertéri veszélyek azonosítása és felismerése egyenesen a nemzeti szuverenitás alapjává vált. A kibervédelemre, illetve azt igénylő beruházásokra elkülönített éves költségvetési keretet kell biztosítani. Ezzel összefüggésben kiemelt célkitűzés a hatékony nemzeti és európai információtechnológiai ipar megőrzése. Mindezeken túl elengedhetetlenül fontos a megfelelő jogalkotási és szabályozási eljárások kialakítása, valamint a kiberfenyegetésekkel szemben támasztott biztonsági követelmények meghatározása. Olyan eljárásokat kell kialakítani, amelyben világosan szabályozhatók az állami és magánszereplők jogai és kötelezettségei. Ezeknek a feladat- és hatásköri leosztásoknak ki kell terjedniük az ellenőrzések, valamint a kiberbiztonsági incidensek és események bejelentésére. Az infokommunikációs rendszerek biztonságáért felelős Nemzeti Információbiztonsági Ügynökség (Agence nationale de la sécurité des systèmes d'information, ANSSI)[57] kapacitását úgy kell kialakítani, hogy komoly válság esetén más állami ügynökséggel közösen hatékonyan be tudjon avatkozni az incidensek kezelésébe. (Franciaország 2013b)

A stratégia a súlyos kibertámadásokra adandó válaszokat két egymásra épülő tényező mentén határozza meg:

- 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

[57] Az ANSSI 2009-ben került megalakításra a Védelmi Minisztérium (Secrétaire général de la défense et de la sécurité nationale, SGDSN) alárendeltségében. A szervezet nemzeti hatóságként a kiberbiztonságért és a hálózatbiztonságért felelős, szakértői és technikai támogatást nyújt a kormányzati és a gazdasági szféra szereplőinek, valamint tanúsítási feladatokat is ellát az informatikai eszközök és szolgáltatások területén. Nemzetközi tevékenységei sorában a CERT-ek közösségében az ANSSI képviseli Franciaországot. (ANSSI 2018)

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 2013a)

Mindezeken túl a dokumentum hangsúlyozza a szoros nemzetközi kapcsolatok kialakítását és fejlesztését. Ezen a területen a stratégia alapvetően a Németországgal és az Egyesült Királysággal való szoros együttműködést irányozza elő, de fontosnak tartja az európai szintű kritikus infrastruktúrák védelmében való aktív szerepvállalást és az infokommunikációs rendszerek védelmét célzó közös európai szabályozás kialakítását is. (Franciaország 2013b)

A stratégia címéből eredően a hadsereg stratégiai feladatait is meghatározza. Ezen a téren a dokumentum kitér azokra a tényezőkre, amelyek a francia hadsereg külföldi misszióiban – például Maliban, Líbiában, illetve Elefántcsontparton történt alkalmazása során szerzett tapasztalatokra épülhetnek. A dokumentum a feladatok mellett a finanszírozási hátteret is meghatározza mindehhez.

A kibertéri feladatokkal kapcsolatban stratégia a katonai kibervédelmi képességek fejlesztését jelöli meg prioritásként, amely során az ezt a feladatot ellátó szervezeteket integrálni kell a hadsereg hagyományos alakulataiba. A kibervédelmi képességek mellett a hadseregnek kibertámadó kapacitásokat is ki kell építenie, amelyekkel a katonai tevékenységeket kell támogatnia. (Franciaország 2013b)

Emmanuel Macron elnöksége azonban új politikai gondolkodást is hozott Franciaországban. 2017 őszére elkészült a 2013-as Fehér könyv felülvizsgálata, amely eredménye gyakorlatilag egy új stratégia. Bár az új stratégia épít a korábbi Fehér könyv megállapításaira, mégis rövidebb és tömörebb formában határozza meg az ország ambícióit. (Nádudvari 2018)

A védelem területén Macron elnök a dokumentum előszavában ezeknek az ambícióknak a támogatására a hadsereget nevezi meg a legfontosabb tényezőként. Az új stratégiai dokumentum a kibertéri veszélyeket a 2013-as stratégiához hasonló módon kiemelten kezeli, ugyanakkor a technológiai fejlődés elmúlt években tapasztalt hatalmas ütemű fejlődését a stratégiai környezet bemutatásakor külön alfejezetben is elemzi. A technológiai fejlődés kibertérben megjelenő árnyoldalait elemezve megállapítja, hogy a kibertéri támadások akár fegyveres támadásnak is minősülhetnek: „A kibertérben bizonyos támadások fegyveres agressziónak tekinthetők nagyságuk és súlyosságuk okán. Nagyobb kibertámadások az általuk okozott esetleges károkra tekintettel az ENSZ Alapokmánya 51. cikke szerinti jogos védelmi intézkedéseket is életre hívhatnak." (Franciaország 2017)

Nagyon figyelemreméltó a dokumentumban az, hogy Oroszország tevékenységét a legnagyobb regionális veszélyként és így fenyegetésként értékeli, Kína esetében viszont nem használja a fenyegetés szót. A *kínai fenyegetés* helyett a *Kína globális ambíciói* megfogalmazást használja a stratégia, amely ambíciók a kibertérben és az információtechnológiai fejlesztésekben is megjelennek. (Nádudvari 2018)

Bár ez nem teljesen meglepő a 2015-ös francia nemzeti kiberbiztonsági stratégia után, de mindenképp előremutató az új stratégiában a kibertámadó képesség kiépítésének meghatározása. Ez a támadóképesség a műveleti képességeknek szerves részét kell, hogy képezze. (Franciaország 2017)

4.5.2. Franciaország nemzeti kiberbiztonsági stratégiája

Franciaország nemzeti kiberbiztonsági stratégiáját *Francia Nemzeti Digitális Biztonság Stratégia (Stratégie nationale pour la sécurité du numérique)* címmel 2015-ben adták ki. Ez a 2011-ben napvilágot látott korábbi stratégia után már a második stratégiai szintű dokumentum,

amely a kiberbiztonságot, illetve, ahogy címéből is kitűnik, a digitális biztonságot célozza Franciaországban.

20. ábra

Franciaország digitális stratégiája

Forrás: Franciaország 2015a

A jelenlegi stratégia rögtön a dokumentum elején – mintegy a kor szellemét meghatározó hashtagekkel bevezetett kulcsszavak együttesével – meghatározza azt az öt stratégiai célkitűzést, amelyek mentén a kiberbiztonságot megvalósíthatónak látja. Ezek a legfontosabb kulcsszavak, illetve kifejezések, amelyek a legfontosabb célkitűzések meghatározására is szolgálnak, a következők:

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

A stratégia mindezek után részletesen végigveszi az öt stratégiai célkitűzést, amely során mindegyik esetében értékeli a jelenlegi helyzetet, kifejti magát a célkitűzést, valamint megadja azokat a feladatokat, amelyekkel ezek a célkitűzések elérhetők.

20. táblázat

Franciaország internetpenetrációja 2016-ban és 2017-ben

Franciaország			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	64,7	55,9	86,4%
2017	64,9	56,4	86,8%

Szerkesztette: www.internetlivestats.com/internet-users/france/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

Az első stratégiai cél, amelyet az „alapvető érdekek, az állami információs rendszerek biztonsága és védelme; súlyos kiberbiztonsági vál-

ságok" szavakkal jellemeztek, nem jelent mást, mint Franciaország elkötelezettségét amellett, hogy az ország a kibertérben is érvényesíti érdekeit, megerősíti a digitális biztonságot, valamint biztosítja az ország gazdasága számára alapvető kritikus infrastruktúrák védelmét.

Ennek érdekében a következő feladatokat jelöli ki a stratégia:

- 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 panelt is fel kell állítani, valamint az információbiztonságért felelős hatóság mellett számos minisztérium, civil szervezet, ipari és tudományos testület bevonása is szükséges;
- 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 mint arra a szervezetre, amely ezt a monitorozást folyamatosan végzi, és veszély esetén a különböző minisztériumokat értesíti;
- fel kell gyorsítani az állami információs rendszerek kiberbiztonságára vonatkozó fejlesztéseket: 2010 óta ezen a területen számos fejlesztés már megvalósult, és többek között 2014-ben kiadták a Nemzeti Információs Rendszerek Biztonsági Politikáját (Politique de sécurité des systèmes d'information, PSSIE), de a digitális technika hatalmas ütemű fejlődése megköveteli azok biztonsági megoldásainak újragondolását és folyamatos fejlesztését; (Franciaország 2014)
- Franciaország és a hozzá kapcsolódó multilaterális szervezetek felkészítése egy esetleges súlyos kiberkonfliktusra: a 2013-as nemzeti biztonsági stratégia azokat a szereplőket már felszólította, akik a francia létfontosságú rendszereket üzemeltetik, és ők 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 a CERT-EU munkáját ebben a feladatban. Katonai oldalról ugyanezt a NATO NCIRC esetében is hangsúlyozza a dokumentum. (Franciaország 2015b)

A második stratégiai cél, azaz „a digitális bizalom, adatvédelem, személyes adatok, kiberrosszindulat" szavak mögött Franciaország azon elkötelezettsége áll, miszerint a kibertérben is megvédi az állampolgárait, azok jogait, és határozottan fellép a kiberbűnözéssel szemben. E cél eléréséhez a következő feladatokat rendeli hozzá a stratégia:

- 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 állampolgárok figyelmét a kibertéri veszélyekre, az információval történő befolyásolásra és a rosszindulatú propagandatevékenységekre;[58]
- 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 egy olyan nemzeti rendszer kiépítését kezdte meg 2016-ban, amelynek fő feladata a segítségnyújtás a kiberbűnözés áldozatainak;
- a kiberbűnözéssel szembeni hatékony fellépés: ezen a téren az egyik legfontosabb feladat egy megbízható nyilvántartási rendszer felállítása, amely mind ez idáig hiányzott ezen a területen. Ennek kialakítására a Belügyminisztérium és az ANSSI kapott megbízást;

[58] Ennek a feladatnak a végrehajtása során a francia kormány a 2015-ös terrortámadások után egy információmegosztó portált hozott létre, amelynek URL-címe is nagyon sokat elárul annak céljáról: stop-djihadisme.gouv.fr (Franciaország 2015).

- 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;
- az állampolgárok és a vállalkozások számára olyan műszaki megoldások ajánlása, 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)

A harmadik stratégiai cél, azaz a tudatosság növelése, az alapvető felkészítés és a folyamatos képzés területén a stratégia a következő feladatokat sorolja fel:

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

A negyedik stratégiai cél, azaz a „digitális technológia üzleti környezete, iparpolitika, export és nemzetköziesítés" kifejezésekkel meghatározott területeken a legfontosabb cél olyan környezet kialakítása, amely megfelelő versenyképességi feltételeket nyújt a kiberbiztonsági kutatás-fejlesztéssel foglalkozó francia vállalatoknak. Ennek érdekében a stratégia a következő feladatokat határozza meg:

- támogatni kell a (digitális) biztonsági termékeket és szolgáltatásokat gyártók nemzeti és európai kínálatát, amihez 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 2015)

Az ötödik stratégiai céllal, azaz az Európában megvalósítandó digitális stratégiai autonómiával és a kibertér stabilitásával kapcsolatban a legfontosabb megvalósítandó cél, hogy az Európai Unió tagországai között – önkéntes alapon – a kiberbiztonság területén, a biztonságos, stabil és nyílt kibertér megteremtése és fenntartása érdekében minden országnak stratégiai önállósága legyen. Ennek kialakításában Franciaország vezető szerepre törekszik. Mindezt a következő stratégiai feladatokkal látja elérhetőnek a dokumentum:

- az önkéntes tagországok között egy stratégiai ütemtervet kell készíteni, amelyben meghatározhatóak mindazok a kulcsterületek, amelyek rövid távon is biztosítják a stratégiai autonómia kialakítását úgy, hogy a részt vevő 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)

4.6. Hollandia

4.6.1. Hollandia nemzeti biztonsági stratégiája

Hollandia legújabb 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 áprilisában jelent meg.

A megelőzés, védelem és megerősítés filozófiája mentén született stratégiának már a címe is nagyon jól tükrözi azt a gondolkodásmódot, amelyet Hollandia a nemzetközi biztonságból levezetve a nemzet biztonságáról gondol. Erre a gondolkodásra a stratégia bevezetője is utal, amely Hollandiát egy nagyon stabil és biztonságos országként értékeli, ugyanakkor utalásokat találunk arra is, hogy ez a világ többi régiójáról nem feltétlenül mondható el. A nemzetközi biztonsági helyzet negatív változásai pedig nyilvánvalóan kihatással vannak Hollandia nemzeti biztonságára is. (Hollandia 2018a)

A dokumentum mindezeknek megfelelően elsőként a stratégiai biztonsági környezetet és biztonsági viszonyokat vázolja, röviden elemezve azokat. Így bemutatja azokat az instabiltást és veszélyt okozó tényezőket, amelyek Európában, illetve a Holland Királyság karibi érdekeltségei esetében láthatók. Ezen kívül a stratégia kitér a technológia gyors ütemű fejlődéséből és a hibrid konfliktusokból eredő veszélyek bemutatására is. A gyors technológiai fejlődéssel – például az önvezető járművekkel, a robotizációval, a szintetikus biológiával vagy a mesterséges intelligenciával – kapcsolatban a stratégia kiemeli annak pozitív hatásait a gazdaságra és a társadalmi fejlődésre, valamint a nemzetközi együttműködés hatékonyabbá tételére, ugyanakkor annak könnyű hozzáférhetősége és olcsósága miatt az ilyen új technológia rossz kezekbe kerülhet, ezért a stratégia a veszélyek növekedésére figyelmeztet: „Az 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)

21. ábra

Hollandia 2018-as, új nemzeti biztonsági stratégiája

Forrás: Hollandia 2018a

A stratégia részben a technológiai fejlődés gyors üteméből, valamint a fenti megállapításokból vezeti le a hibrid konfliktusok megjelenését. Ezzel kapcsolatban a dokumentum hozzáteszi, hogy vannak olyan államok, amelyek a hagyományos katonai, politikai, diplomáciai és gazdasági eszközökkel kombinálják az új technológia által elérhetővé vált különböző megoldásokat, amivel céljuk a befolyásolás, valamint a stratégiai céljaik elérése. Ezért a stratégia ezt az egyik olyan veszélyforrásként értékeli, amelynek megoldása, illetve kezelése az egyik legsürgetőbb feladat. (Hollandia 2018a)

Ezt követően a stratégia felsorolja és elemzi a legfontosabb – a dokumentum szóhasználatával élve legsürgetőbb – veszélyeket. Ezek a következők:

- terroristatámadások;
- kiberveszélyek;
- nemkívánatos külföldi beavatkozások és zavarkeltések;
- katonai veszélyek;
- gazdasági folyamatokra negatív hatást gyakorló veszélyek;
- a vegyi, biológiai, radiológiai és nukleáris fegyverek jelentette veszélyek. (Hollandia 2018)

A kiberveszélyekkel kapcsolatban a stratégia kiemeli a kiberbűnözést, a más állam(ok) által támogatott kiberkémkedést mint olyan veszélyforrásokat, amelyek az állam működésére, illetve a szociális biztonságra is közvetlenül negatív hatással lehetnek. A stratégia itt utal arra a korábbi – 2017-ben született –, a holland nemzeti kiberbiztonságot bemutató elemzésre, amely megállapította, hogy az ország kiberfenyegetések elleni felkészültsége messze le van maradva a gyors ütemben fejlődő veszélyek mögött. (Hollandia 2018a)

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

Ezeknek a feladatoknak az általános felvezetése már utal a kiberveszélyek elleni hatékony fellépés szükségességére, csakúgy, mint a létfontosságú infrastruktúrák, az energia vagy a legfontosabb erőforrások védelmére. (Hollandia 2018a) Mindezeket a stratégia nemzetközi kontextusban és együttműködési keretek között látja hatékonyan kivitelezhetőnek. Ehhez számos egyéb stratégiai területet jelöl meg a dokumentum:

- a fegyveres erők fejlesztése és modernizációja (amelyet az erről szóló Fehér könyvben rögzítettek);
- a külkereskedelemre és a fejlesztési együttműködésekre vonatkozó politika (amely kidolgozása a közeljövőben várható);
- a diplomácia fejlesztése;
- integrált migrációkezelési terv;
- tematikus regionális és bilaterális kerettervek;
- a gazdasági biztonság növelésének akcióterve;
- nemzeti politika a nemzetbiztonsági szolgálatokkal;
- Nemzeti Kiberbiztonsági Stratégia;
- Digitalizációs Program;
- nemzetközi politikai stratégia;
- Nemzeti Terrorizmus Elleni Stratégia. (Hollandia 2018a)

A megelőzés mint stratégiai pillér érdekében a dokumentum számos célkitűzést határoz meg, amelyek a következők:

- a konfliktusok megelőzése Európában és Hollandia környezetében;
- a terrorizmus eredetének megszüntetése;
- leszerelés, fegyverkorlátozás és a tömegpusztító fegyverek korlátozása;
- világos nemzetközi normák meghatározása a kibertevékenységekre. (Hollandia 2018a)

Ez utóbbival, azaz a nemzetközi kibernormák meghatározásával kapcsolatban a stratégia hangsúlyozza, hogy a növekvő kiberveszélyek jel-

legükből adódóan csak nemzetközi együttműködés keretében kezelhetők. Ennek megfelelően egy hatékony kiberdiplomáciára van szükség, amelyben Hollandia kész szerepet vállalni. Ennek egyik első feladata a kibertérre vonatkozó nemzetközi jogi szabályozás kialakítása kell, hogy legyen. Ezzel kapcsolatban a dokumentum hangsúlyozza, hogy a jelenlegi nemzetközi humanitárius jog Hollandia számára kiindulópont, amelynek alkalmazását a kibertérre is érvényesíteni kell. Nagyon előremutató a stratégia azon megállapítása, amely a kiberfegyverek exportja szabályozásának szükségességét szorgalmazza: „Az exportszabályozás hasznos és szükséges ahhoz, hogy megakadályozza az olyan katonai és egyéb kiberképességek elterjedését, amelyek kiberfegyverkezési versenyhez vezetnének." (Hollandia 2018a)

Ezt az exportszabályozást a kibertéri megfigyelő- és ellenőrzőrendszerekre is kiterjesztené a stratégia, hiszen a dokumentum szerint az autokratikus rendszerek gyakran ezeknek a rendszereknek a használatával korlátozzák saját állampolgáraik jogait. (Hollandia 2018a)

A második pillér, azaz a védelem vonatkozásában az alábbi célkitűzések szerepelnek a stratégiában:

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

Kissé meglepő módon ezen célok között találjuk a kiberelrettentés kialakítását is, amely nyilvánvalóan a védelem tekintetében inkább a közvetett eredményeivel képes hatást gyakorolni. Ugyanakkor ennek a célnak a bemutatásánál a stratégia nem részletezi, hogy milyen olyan képességek kiépítése szükséges az olyan elrettentéshez, amelyek valóban hatékonyak lehetnek. Csak általánosságban utal arra, hogy az olyan országok ellen, amelyek agresszív politikai és katonai célú

kibertámadásokkal operálnak – többek között a létfontosságú infrastruktúra támadásával, hamis vagy álhírek terjesztésével –, és amely támadások nemcsak fizikai és gazdasági károkat okozhatnak, hanem a demokratikus értékrendre is kihatással vannak, alkalmazható a már kialakult terrorizmus elleni diplomáciai hálózat. Ennek segítségével egyensúly teremthető a preventív és a represszív akciók között. Ehhez azonban szükséges a magán- és a civil szféra bevonása is. (Hollandia 2018a)

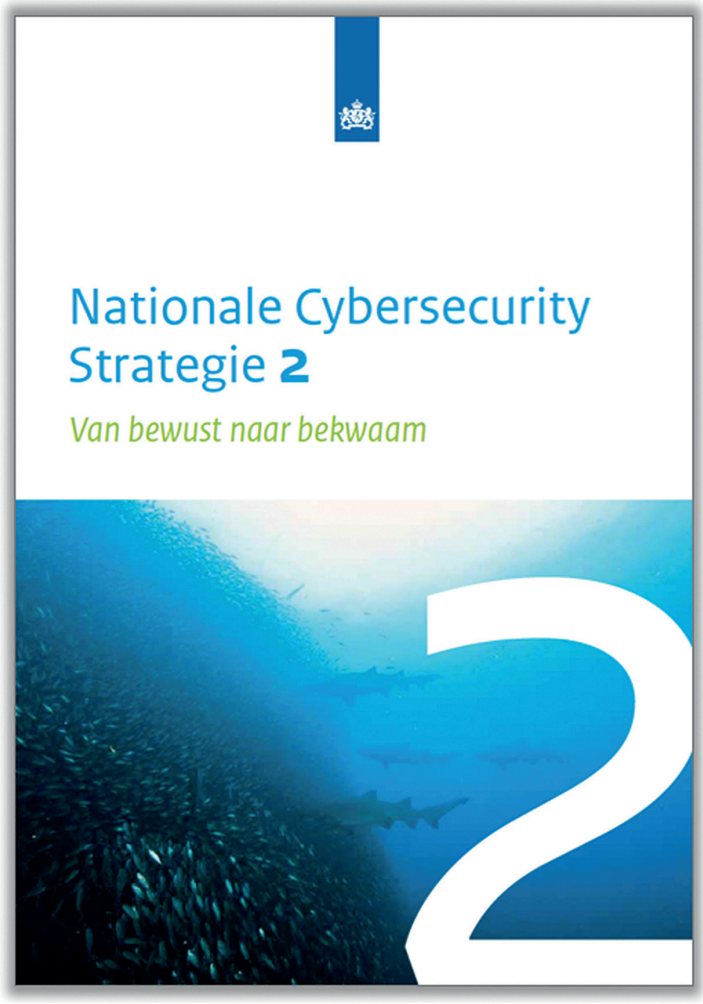
A stratégia a harmadik pillérben, azaz a megerősítésben a következő feladatokat vázolja fel:

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

4.6.2. Hollandia nemzeti kiberbiztonsági stratégiája

Hollandia 2013-ban frissítette a nemzeti kiberbiztonsági stratégiáját. Ugyanakkor fontos megemlíteni a korábbi, 2011-ben megjelent holland *Nemzeti Kiberbiztonsági Stratégiát* is, hiszen számos olyan intézkedést tartalmazott, amelynek máig tartó szervezeti kihatásai is vannak. A korábbi stratégia azon kívül, hogy meghatározta a legfontosabb célokat – például a biztonságos és megbízható IKT-rendszerekre épülő digitális társadalom fejlesztését – létrehozta a Nemzeti Kiberbiztonsági Tanácsot, valamint a Nemzeti Kiberbiztonsági Központot. (Hollandia 2011)

A nemzeti Kiberbiztonsági Tanács mint a kormány nemzeti és független tanácsadó testülete egyik legfontosabb feladata, hogy a kormány számára stratégiai szinten adjon kiberbiztonsággal kapcsolatos tanácsokat és megoldási javaslatokat. A tanács tagjai állami és magánszervezetek, valamint a tudomány magas szintű képviselői. (Hollandia 2018b)



22. ábra

Hollandia 2013-as Nemzeti Kiberbiztonsági Stratégiája

Forrás: Hollandia 2013a

A nemzeti Kiberbiztonsági Központ a holland Igazságügyi Minisztérium alárendeltségében a kiberbiztonság nemzeti szintű koordinációjáért, a kiberbiztonsággal kapcsolatos információmegosztásért, valamint többek között a 24 órás incidenskezelésért felelős. (Hollandia 2018c)

Hollandia 2013-as Nemzeti Kiberbiztonsági Stratégiája számba veszi az országot fenyegető kibertéri veszélyeket és kihívásokat. Mindezt a 2013-ban elvégzett Nemzeti Kiberbiztonsági Értékelésre alapozva teszi meg.

A legfontosabb veszélyként az olyan információlopást, illetve digitális kémkedést jelöli meg a dokumentum, amely a nemzeti szintű – stratégiai – információkat érinti. Emellett azokat a kiberbűnözés eszköztárában megjelenő támadásokat sorolja fel veszélyként, amelyekkel az állampolgárok és a vállalkozások nap mint nap találkozhatnak. Ilyenek például a botnetek és a zsarolóvírusok. A stratégia megjegyzi, hogy a kiberbűnözés olyan súlyos problémává vált, amelyet a szolgáltatásként árult kiberbűnözői módszerek jellemeznek a legjobban. (Hollandia 2013)

Mindezek annak ellenére okoznak komoly károkat az országnak, hogy számos fontos kiberbiztonsági kezdeményezés született Hollandiában az elmúlt időben, de ezek ellenére mind a lakosság, mind a vállalkozások digitális tudatossága, illetve a kibertámadásokkal szembeni felkészültsége alacsony szinten maradt. (Hollandia 2013b)

21. táblázat

Hollandia internetpenetrációja 2016-ban és 2017-ben

Hollandia			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	17,0	15,9	93,7%
2017	17,0	16,1	94,8%

Forrás: www.internetlivestats.com/internet-users/netherlands/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

Ezek alapján, kiegészítve a technikai jellegű veszélyekkel, a stratégia a következő olyan kibertéri kihívásokat azonosítja, amelyekkel Hollandia szembe kell, hogy nézzen:

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

Így nem meglepő a stratégia azon kijelentése, miszerint „[a] kiberbiztonság nem képzelhető el elszigetelten, így olyan témákkal együtt kell megközelíteni, mint az alapvető jogok, az értékek és a társadalmi-gazdasági előnyök.” (Hollandia 2013b)

A stratégia új megközelítést és új megoldásokat is felvet a korábbi stratégiához képest. A legfontosabb különbség az új és a korábbi stratégia között az, hogy amíg a régi stratégia a kiberbiztonság struktúrájára fókuszált, addig az új stratégia a hálózatokra és a stratégiai együttműködésre helyezi a hangsúlyt. Emellett az új stratégia a kockázatalapú megközelítést alkalmazza, amely során a védelem és az érdekek között egyensúly teremthető, ellentétben a korábbi stratégia általános alapú megközelítésével, amely során a szervezetek kiberbiztonsági képességeinek kiépítése volt fontos.

A stratégia a biztonság megteremtését a szabadság és a szociális-gazdasági előnyök szem előtt tartásával kívánta elérni. Mindezt úgy, hogy ezekben a feladatokban a kormányzat facilitátor és irányító szerepet tölt be. A stratégia szerint a kormány felelős a biztonság megteremtéséért, és ez nincs másként a kibertérben sem, de

ezt a személyiségi jogok védelmének figyelembevételével, átlátható módon kell megtennie. Természetesen ehhez szükséges az állampolgárok közreműködése is, amelynek érdekében növelni kell a kiberhigiéniát és a személyes felelősségvállalást is. Ugyanez igaz a vállalkozások esetében is, ezek részéről is biztosítani kell a felelős magatartást és az elszámoltathatóságot.

Mindezek nemcsak nemzeti, hanem nemzetközi feladatokat is jelentenek, hiszen csak az integrált és más országokkal közös együttműködés hozhat eredményeket. A stratégia hangsúlyozza, hogy Hollandia ennek érdekében meghatározó szerepet kíván játszani egyrészt abban, hogy nemzetközi együttműködési koalíciót hozzon létre, másrészt abban, hogy nemzetközileg elfogadható szabályozás jöjjön létre a kiberbiztonságra vonatkozóan. (Hollandia 2013b)

A stratégia kitér a hadsereg szerepére is, de hangsúlyozza a civil–katonai együttműködés kialakításának szükségességét a kibertérben is, hiszen ebben a komplex környezetben a polgári hírszerző, rendőrségi vagy kiberbiztonsági szervezetek információi és nem utolsósorban kiberbiztonsági képességei elengedhetetlenül szükségesek ahhoz, hogy a hadsereg a feladatait el tudja látni. A dokumentum ezen kívül a hadsereg kibervédelmi képességeinek fejlesztését is szorgalmazza. Ebben a feladatban a NATO fontos szerepet kaphat, hiszen a nemzeti szintű képességépítéshez is hozzájárul a magán- és közszféra együttműködésének, illetve az interoperabilitás szem előtt tartásának hangsúlyozásával. A védelmi képességek fejlesztése során a stratégia az EU-szintű gyakorlatok és a hatékony kiberbűnözés elleni nyomozati tevékenységeket is bemutatja. Ebben a feladatban Hollandia támogatja a Budapest Konvenció szélesebb körű, még több országra kiterjedő ratifikációját.

23. ábra

Hollandia 2018 áprilisában megjelent új kiberbiztonsági menetrendje

Forrás: Hollandia 2018d

A stratégia legfontosabb célkitűzései és ambíciói a következők:

- 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)

Ezekhez a stratégiai célokhoz akcióterveket kell készíteni – az első ilyen a 2014–2016 évekre készült (a stratégia első melléklete tartalmazza ezt a tervet) –, és az abban foglaltak végrehajtásának hatékonyságát évente meg kell vizsgálni, valamint annak eredményétől függően változtatni kell a feladatokon. (Hollandia 2013b)

A 2013-ban megjelent Nemzeti Kiberbiztonsági Stratégia után 2018 áprilisában a holland kormány elfogadta a *Hollandia Kiberbiztonsági Menetrendje: Hollandia digitálisan biztonságos (Nederlandse Cybersecurity Agenda Nederland digitaal veilig)* című dokumentumot, amely a 2011-es és az általunk is bemutatott 2013-as Nemzeti Kiberbiztonsági Stratégia alapvető megállapításaira és célkitűzéseire épít.

Az új dokumentum hangsúlyozza, hogy a kiberbiztonság a nemzeti biztonság része kell, hogy legyen. A kiberbiztonság megteremtése érdekében a korábbi stratégiák már lefektették a megfelelő alapot, de a biztonsági szintet emelni kell, mert újabb és újabb kiberveszélyek és -fenyegetések jelennek meg. Mindezt csak úgy lehet eredményesen megtenni, ha a kormányzat és a magánszektor között szoros összefogás alakul ki. Mindezt a holland Igazságügyi és Védelmi Miniszter – Ferd Grapperhau –, aki a stratégia előszavát is jegyzi, így fogalmazta meg egyik nyilatkozatában: „A kiberbiztonság elválaszt-

hatatlanul kapcsolódik a nemzeti biztonsághoz 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)

Az új dokumentum nagyon hasonló ambíciókat fogalmaz meg, mint a korábbi stratégia. Ezek az ambícióként megjelenített célok a következők:

- 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)

Az új dokumentum mindezeknek megfelelően a kiberbiztonság területén szükséges feladatokat – és természetszerűleg a veszélyeket és kihívásokat is – nagyon hasonló módon határozza meg, mint a korábbi anyag, de azok intenzitásának növelését szorgalmazza.

Ilyen feladatok például a kiberbűnözés elleni törvény elkészítése és várhatóan 2020-ban történő hatálybaléptetése, az ágazati CERT-ek (például az egészségügy, biztosítási szektor) felállítása, illetve egy nemzeti kibertámadás-detektáló hálózat felállítása a következő években. Ezeken kívül fejleszteni kell az NCSC-t és a Digitális Megbízhatósági

Központot (Digital Trust Center, DTC). A nemzetközi együttműködési területen a Globális Bizottság a Kibertér Stabilitásáért (Global Commission on the Stability of Cyberspace, GCSC)[59] munkájának támogatását hangsúlyozza a menetrend. (Hollandia 2018d)

4.7. Magyarország

4.7.1. Magyarország nemzeti biztonsági stratégiája

Hazánk jelenlegi Nemzeti Biztonsági Stratégiája 2012-ben született, és a kibertér biztonságáról való gondolkodásban is alapvető változásokat hozott azzal az egyszerű ténnyel, hogy a Magyarország biztonságát meghatározó tényezők, illetve veszélyforrások közé bekerült a kiberbiztonság, illetve a kibertérben jelentkező veszélyek bemutatása is: „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 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 katasztrófavé-

[59] A Bizottságot a Hágai Stratégiai Tanulmányok Központ (The Hague Centre for Strategic Studies, HCSS) és a Kelet-Nyugat Intézet (EastWest Institute, EWI) hívta éltre. Jelenleg olyan támogatói vannak, mint a holland és azt észt kormány vagy a francia külügyminisztérium. Legfontosabb feladata a kibertér biztonsága érdekében szükséges nemzetközi együttműködések kialakítása, illetve azok támogatása. (GCSC 2018)

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

A fentiekből nagyon jól látszik, hogy a stratégia a kiberbiztonság területén az átfogó megközelítés elvét alkalmazta, amelyben 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. A stratégia ennek megfelelően azt is deklarálja, hogy a kibertérben jelentkező fenyegetéseket és veszélyeket, valamint az így jelentkező kockázatokat az államnak kell kezelnie. Ennek érdekében a Nemzeti Biztonsági Stratégia feladatokat is megfogalmaz: „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." [1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról]

Bár 2016. év végén létrejött egy munkacsoport a Nemzeti Biztonsági Stratégia felülvizsgálatára, s ennek munkája jelenleg is zajlik, az bizonyosra vehető, hogy a kibertéri veszélyek még markánsabban fognak megjelenni az új nemzeti biztonságról szóló, stratégiai szintű dokumentumban. [57/2016. (XI. 24.) HM–MvM–BM–KKM együttes utasítás a Nemzeti Biztonsági Stratégia felülvizsgálatára létrehozott munkacsoportról]

A Nemzeti Biztonsági Stratégia mellett szükséges szót ejtenünk hazánk katonai stratégiájáról is, hiszen hazánk Nemzeti Katonai Stratégiája, amely szintén 2012-ben született, nagyon előremutató módon számos, a kiberbiztonságra utaló kitételt tartalmaz.

A stratégia a biztonság és stabilitás ellen ható folyamatok elemzésekor a kiberbiztonsággal kapcsolatosan megállapítja, hogy „[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.” [1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról 33. pont]

A fenti idézetből is világosan látszik, hogy a jogalkotó, illetve a stratégia készítői milyen előremutató módon értelmezték a kiberteret, a kiberbiztonságot, illetve annak katonai vetületeit, hiszen ezen egyszerű félmondat, miszerint mindezek „szükségessé teszik a háborúval kapcsolatos fogalmaink átfogó felülvizsgálatát és adott esetben módosítását”, előrevetíti a kiberhadviselésről való gondolkodást, amely még a Nemzeti Biztonsági Stratégiában is rejtve maradt. Mindezeken túl a hadviselés újraértelmezésének szükségessége annál is inkább előremutató, mert a NATO majd csak 2016-ban, a varsói csúcsértekezleten teszi a hivatalos gondolkodás részévé a kiberhadviselést, akkor, amikor a kiberteret a katonai műveletek ugyanolyan dimenziójaként ismeri el, mint a három másik hagyományos dimenziót.

A stratégia a haderő várható alkalmazása jellemzőinek elemzésekor szintén utal a kiberhadviselésre, amikor az aszimmetrikus kihívások miatt kibővülő háború és támadás fogalmát mutatja be: „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 fogal-

mainak 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." [1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról 52. pont]

Természetesen a dokumentum meghatározza a magyar haderő kibertérrel kapcsolatos feladatait 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." [1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról 82. pont]

Mindezekkel kapcsolatban azonban meg kell jegyezni, hogy ahogy a későbbiekben utalni fogunk erre, a Magyar Honvédség kibervédelmének megerősítése mind a szervezeti, a jogszabályi és a képességfejlesztési területeken elkezdődött, de a kiberhadviselésnek egyelőre sem a jogszabályi, sem a szervezeti keretei nincsenek kidolgozva.

4.7.2. Magyarország nemzeti kiberbiztonsági stratégiája

A katonai terület után visszakanyarodva a kiberbiztonság békésebb területei felé, meg kell állapítanunk, hogy az információs korszak, illetve annak egyes fejlesztési kérdései már jóval a jelenleg érvényben lévő Nemzeti Biztonsági Stratégia kiadása, azaz 2012 előtt megjelentek stratégiai szinten is Magyarországon.

Hazánk a 2000-es évek elejétől kezdődően az információs társadalom fejlesztését tartotta szem előtt, és az volt a prioritás. 2000

és 2014 között négy olyan stratégia is született,[60] amely az információs társadalom, illetve ennek egyes területeinek fejlesztését célozták. Ezek kronologikusan a következők voltak:

2001: Nemzeti Információs Társadalom Stratégia, amely egy az akkori korszakban európai összehasonlításban is előremutató irányelv-gyűjteménynek számított, hiszen az európai trendekkel közel egy időben született. Tartalmazta a kibertérre (az akkori szóhasználattal élve az infokommunikációs eszközökre és rendszerekre) épülő technológiai háttér kialakításának nagybani elképzeléseit is. A stratégia fő célkitűzései a következők voltak:

- a gazdaság információtechnológiára alapozott fejlesztése;
- az oktatás és kultúra, a társadalompolitika fejlesztése;
- az elektronikus kormányzati és önkormányzati rendszerek fejlesztése;
- a célokhoz szükséges infrastrukturális rendszerek kialakítása és fejlesztése. (NITS 2001)

- 2003: Magyar Információs Társadalom Stratégia, amelynek céljai nagyban megegyeztek a korábbi stratégia céljaival. Az elképzelés fő célja egy olyan tudásalapú gazdaság létrehozása volt, amely hozzájárul az állampolgárok életminőségének és életkörülményének növeléséhez. (MITS 2003)
- 2010: Digitális megújulás cselekvési terv 2010–2014, amely az infokommunikációs ágazatra vonatkozó cselekvési terv volt. Ez a stratégiai elképzelés már az EU 2020 digitális menetrendjébe illeszkedett, és tartalmazta azokat az elemzéseket, illetve az azokra épülő fejlesztési irányokat, amelyek az oktatástól kezdődően a gazdaság különböző szektorainak versenyképességéhez járulhatnak hozzá. Ki kell emelnünk e stratégia

[60] Meg kell jegyezni, hogy a 2000-es éveket megelőzően is születtek olyan elképzelések, amelyek az információs társadalom kialakulását, valamint annak fejlesztését célozták. Ilyen elképzelés volt többek között a *Magyar válasz az Információs Társadalom kihívásaira* (Havass–Lengyel 1999) vagy a *Tézisek az információs társadalomról* című tanulmánykötet. (Talyigás é. n.)

vonatkozásában, hogy ez az első olyan stratégia, amely már tartalmaz utalásokat a kiberbiztonságra, és teret szentel az információbiztonsági jogszabályok átdolgozása témakörnek. (DMCST 2010)

- 2014: A Nemzeti Infokommunikációs Stratégia 2014–2020, amely bár alapvetően az infokommunikációs szektor fejlesztését célozta, de ez volt az első olyan stratégia, amelyben a biztonság és az infokommunikációs rendszerek zavartalan működésének biztosítása kiemelt helyen szerepel. Maga a stratégia leírja azokat a pilléreket, amelyek a legfontosabb fejlesztendő területek: például a digitális infrastruktúra, a digitális kompetenciák, a digitális gazdaság, a digitális állam. Ezekhez több, úgynevezett horizontális tényezőt is hozzárendel a stratégia: az e-befogadást, amely a digitális ökoszisztémából eddig kimaradó emberek digitális térbe való bevonását célozza, a K+F+I területet, illetve a biztonságot. A biztonsággal kapcsolatosan a stratégia a kritikus információs infrastruktúráknak, a közigazgatás rendszereinek, illetve a felhasználók adatainak védelmét hangsúlyozza, de ezek mellett kitér a felhasználók folyamatos – a kockázatokról és ezek kezelésének mikéntjéről szóló – tájékoztatására is. (Nemzeti Infokommunikációs Stratégia 2014)

22. táblázat

Magyarország internetpenetrációja 2016-ban és 2017-ben

Magyarország			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	9,8	7,9	80,2%
2017	9,8	7,9	80,2%

Forrás: www.internetlivestats.com/internet-users/hungary/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

Mindezek után a 2013. év elején jelent meg hazánk történelmének első olyan stratégiai dokumentuma, amely valóban és egyedüliként a kiberbiztonságot célozza. Ez pedig nem más, mint a Nemzeti Kiberbiztonsági Stratégia.

Ez a stratégia nyugodtan nevezhető mérföldkőnek hazánkban, hiszen meghatározó jelentőséggel bír a magyar kiberbiztonság területén. A stratégia legfőbb célja, összhangban Magyarország Alaptörvényével és építve a Nemzeti Biztonsági Stratégiában meghatározott célkitűzésekre, a következő megfogalmazásban szerepel a dokumentumban: „Jelen 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]

Az idézetben is találunk utalást az úgynevezett magyar kibertérre, amely terminológiát e stratégia vezette be, és amelynek értelmezéséhez segítségül kell hívnunk magát a stratégiát: „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]

Magáról a stratégiáról el kell mondani, hogy egy nagyon rövid – összesen hatoldalnyi terjedelmű – dokumentumról beszélhetünk. Ugyanakkor ez egy valódi stratégia, hiszen iránymutatást ad, feladatokat szab, de azok nem túl részletesek, nem túlszabályozottak. Ez a stratégia egy valódi keretrendszer, egy világos irányvonalat adó dokumentum, amely rögzíti azokat a jogszabályokat, stratégiákat

és legmagasabb szintű elképzeléseket, amelyek meghatározók hazánk kiberbiztonságának szempontjából.

A stratégia felvázolja Magyarország kiberbiztonsági környezetét, benne a már említett magyar kibertérrel, utal a kibertérben lévő veszélyek és kihívások komplexitására, azok egymásra hatására, valamint definiálja a kiberbiztonságot is: „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 stratégia világos, bár kissé általános feladatokat határoz meg a kiberbiztonság kialakítása és fenntartása érdekében. Ugyanakkor ezek a célok is egymásra épülnek, és a nemzetbiztonság és a válságkezelés érdekében történő, illetve a felhasználók, vagyis a magyar állampolgárok és szervezetek kibertérben való biztonságos tevékenységeinek védelmét szolgálják. Ezek a 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]

A célok meghatározása mellett a stratégia az azok végrehajtásához szükséges feladatokat is meghatározta, és ezeket már lényegesen részletesebben mutatja be. Ezek a feladatok – röviden azok tartalmi elemeivel – a következők:

- olyan kormányzati koordinációt kell megvalósítani, amely során a Miniszterelnökség vezetésével az összkormányzati koordináció erősödik, valamint a kormányzati és ágazati erőforrásokat koordináltan és lehetőleg koncentráltan használják fel és alkalmazzák;
- 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, ami 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 is ki 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]

Ezeknek a feladatoknak az ellátásához a stratégia számba veszi mindazokat a kormányzati eszközöket, amelyek jelentős része már ekkor rendelkezésre állt, de amelyek erősítése és további fejlesztése szükséges volt. Ilyen eszközök a kormányzati szervezetek, a magánszektorban meglévő szervezetek vagy éppen azok a tudományos szereplők – egyetemek, kutatóintézetek –, amelyek intézményes keretet adhatnak a feladatok között felvázolt és elvárt együttműködéseknek. Mindezeken túl a stratégia utal arra is, hogy a kritikus infrastruktúrák területén a védelem szervezeti és jogszabályi keretrendszerének kialakítása már

elkezdődött, illetve a kiberbiztonság szakosodott intézményei kialakultak. [1139/2013. (III. 21.) Korm. határozat]

Ugyanakkor, bár valóban működött már ebben az időben egyfajta szervezeti keretrendszer, de ennek fejlesztése és bizonyos szintű újragondolása mindenképpen szükséges volt. Az első eseménykezelési csoportok is működtek már, hiszen például már 2002-ben megalakult a CERT-Hungary[61] a Puskás Tivadar Közalapítvány keretében, és szintén működött a SZTAKI CERT-je is, de a stratégia által elvárt koordinációs és együttműködési feladatok ellátására egy magasabb – stratégiai – szintű testület, nevezetesen a Nemzeti Kiberbiztonsági Koordinációs Tanács felállítására is szükség volt. (Kovács–Szentgáli 2015)

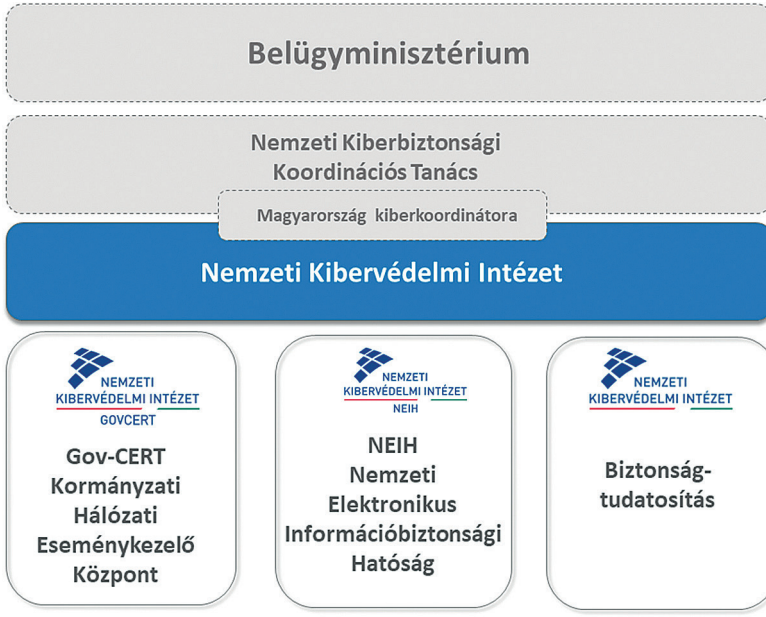
A Nemzeti Kiberbiztonsági Stratégia alapján elkészült az információbiztonsági törvény, amely a *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról* címet kapta.

A stratégia, illetve az említett információbiztonsági törvény hatására létrejött szervezeti keretrendszer azonban nagyon heterogén volt, a szervezeti elemek gyakran egymás feladatait is jelentős mértékben átfedték. Mindezek következményeként 2014-ben elkezdődött a szervezeti keretrendszer átszervezése, majd a Parlament 2015 júliusi, az információbiztonsági törvényt módosító döntésével[62] egy új szervezeti elemekből álló, új feladatstruktúrával felálló hazai kiberbiz-

[61] A CERT-Hungary 2002 és 2010. január 1. között működött ezen a néven, amikor is *Az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendelet* alapján a Nemzeti Hálózatbiztonsági Központ nevet kapta kiterjesztett feladatokkal (Kormányzati Eseménykezelő Központ 2009). Ezt követően a 2013. évi L. törvény alapján (2013. július 1-jével) létrejött a Kormányzati Eseménykezelő Központ (GovCERT-Hungary), így a CERT-Hungary, illetve a Nemzeti Hálózatbiztonsági Központ megszűnt.

[62] A 2013. évi L. törvény vonatkozásában nagyon sok alapvető szervezeti és hatásköri változást is hozott ez a törvénymódosítás, amelynek címe: *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.*

tonsági szervezetrendszer kezdte meg működését. A törvény módosításával 2015. október 1-jével létrejött a Nemzeti Kibervédelmi Intézet (NKI). Az NKI működtetését a BM felügyelete alatt lévő Nemzetbiztonsági Szakszolgálat (NBSZ) látja el. Az NKI egyik pillére a GovCERT-Hungary, másik pillére a Nemzeti Elektronikus Információbiztonsági Hivatal (NEIH), harmadik pillére pedig az információbiztonsági tudatosítás és annak minden feladata és tevékenysége. E tevékenység kiterjed többek között az állami és önkormányzati szervezetek munkatársainak felkészítésére, amely során az internet, valamint az infokommunikációs eszközök és rendszerek biztonságtudatos használatára készítik fel őket. (Kormányzati Eseménykezelő Központ 2017)

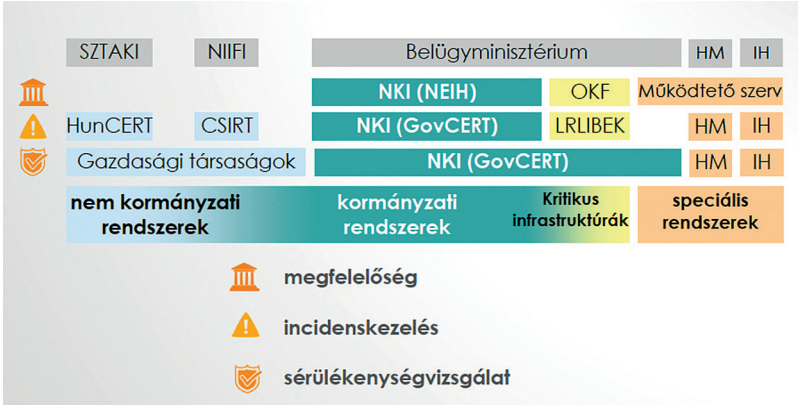


24. ábra

A Nemzeti Kibervédelmi Intézet pillérei és kapcsolódásai

Forrás: Bencsik 2015, a szerző szerkesztése

Az információbiztonsági törvény módosítása, illetve a többek között ennek hatására bekövetkezett szervezeti változások új szervezeti keretrendszert jelentettek a hazai kibervédelemben. A már említett Nemzeti Kibervédelmi Intézet mellett, amelynek fő feladata az állami és önkormányzati szereplők, illetve azok rendszereinek védelme, létrejött a kritikus infrastruktúrák védelméért is felelős Országos Katasztrófavédelmi Főigazgatóság (OKF) alárendeltségében működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (LRLIBEK), valamint később a Honvédelmi Minisztérium (HM) irányítása mellett a Katonai Nemzetbiztonsági Szolgálatnál (KNBSZ) felállt katonai CERT (HÁEIEK, azaz Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ).



25. ábra

A 2015 óta működő hazai állami kibervédelmi szervezetek

Forrás: Bencsik 2015

Meg kell jegyezni, hogy a bemutatott, 2013-ban született Nemzeti Kiberbiztonsági Stratégia jelen sorok papírra vetésekor felülvizsgálat alatt áll. Az új stratégia szövege elkészült, annak közigazgatási és szakmai egyeztetése megtörtént. A felülvizsgálat egyik komoly oka az első stratégia megalkotása óta eltelt közel 5 esztendő alatt bekövetkezett

változások (például új biztonsági kihívások, új technológiai trendek, új biztonsági megoldások), illetve a NIS irányelvekben foglaltak nemzeti stratégiába való átültetésének szükségessége.

4.8. Lengyelország

4.8.1. Lengyelország nemzeti biztonsági stratégiája

Lengyelország jelenlegi nemzeti biztonsági stratégiája 2014-ben született. A stratégia négy fő fejezetből áll, amelyből az első Lengyelország értékeinek és érdekeinek a számbavétele, majd ezt követi a második fejezetben az ország biztonsági környezetének felmérése és bemutatása globális, regionális és nemzeti dimenzióban. A harmadik rész azokat a stratégiai tevékenységeket mutatja be, amelyeket célokként határoz meg az ország értékeinek és érdekeinek védelme érdekében. A negyedik fejezet pedig a mindezekhez a tevékenységekhez szükséges szervezeti keretrendszert írja le mint védelmi, szociális és gazdasági alrendszereket. (Lengyelország 2014b)

A dokumentum már rögtön a nemzeti érdekek és az ezekkel összefüggő stratégiai célok meghatározásánál említi a kiberteret. Itt rögzíti, hogy Lengyelország biztonságos működését a kibertérben is biztosítani kell. Ezt követően a stratégia meghatározza, hogy a nemzeti biztonság garantálása érdekében milyen védelmi képességekkel kell rendelkeznie az országnak, és ebben kiemeli a kibervédelem területén szükséges kapacitások meglétét is.

Természetszerűleg a biztonsági környezet elemzésekor, illetve a globális veszélyek és kihívások számbavételekor is utal a stratégia a kibertérre, valamint az ott megjelenő kihívásokra: „Az 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)

A dokumentum a regionális biztonsági környezet esetén is hangsúlyozza a kibertér védelmének egyre növekvő fontosságát, amelynél rögtön megemlíti, hogy ez nemzetközi együttműködést igényel, amely bilaterális alapon, illetve a NATO és EU szövetséges keretek között valósítható meg. A nemzeti szintű biztonsági környezet bemutatásakor a stratégia kitér a nemzeti infokommunikációs rendszerek zavartalan működésének biztosítására, de megemlíti a felhasználók kiberbiztonsági tudatosságának alacsony fokában rejlő kihívásokat is. (Lengyelország 2014b)

26. ábra

Lengyelország Nemzeti Biztonsági Stratégiája

Forrás: Lengyelország 2014a

Nagyon előremutató a stratégia azon része, amelyben a védelmi tevékenységeket veszi számba. Itt a hadsereg kibertéri tevékenységével,

illetve az ehhez szükséges képességek tekintetében a következőképpen fogalmaz: „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)

A stratégiából származó idézetből is látható, hogy Lengyelország explicit módon kijelenti a kibertéri támadóképességek szükségességét mind a kiberelrettentés megvalósításához, mind a valós kiberműveletek vagy esetlegesen a kiberháborúk megvívásához.

A dokumentum a nemzeti biztonság szervezeti keretrendszerének meghatározása során is hangsúlyosan utal a kibertérre, illetve a kiberbiztonságra, amely során meghatározza a Nemzeti Kiberincidens-kezelési Rendszer fejlesztését, valamint egy nemzeti kiberkoordinációs központ felállítását. Ennek a szervezeti rendszernek kompatibilisnek kell lennie más országok hasonló rendszereivel, támogatnia kell a közés magánszféra együttműködését, kiemelten a PPP-konstrukciók megvalósítását, és hozzá kell járulnia a kiberbiztonság-tudatosság emeléséhez Lengyelországban. (Lengyelország 2014b)

4.8.2. Lengyelország nemzeti kiberbiztonsági stratégiája

2007-ben Lengyelország – hasonlóan sok más régióbéli országhoz – az információs társadalom fejlesztését határozta meg stratégiai szinten, amelyhez egy fejlesztési stratégiát készített a 2013-ig terjedő időszakra. Ez a stratégiai dokumentum előirányozta egy olyan társadalom kialakítását, ahol az állampolgárok és a vállalkozások tudatosan használják az IKT nyújtotta lehetőségeket a gazdasági, társadalmi és kulturális fejlődés érdekében. Ennek hatékony támogatásával egy korszerű és felhasználóbarát közigazgatás létrehozása is cél volt.

Ez az információs társadalom fejlesztését célzó stratégia választ kívánt adni a sajátos lengyel kihívásokra, ugyanakkor összhangba kívánta hozni mindezeket az európai kezdeményezésre létrejött európai digitális menetrenddel. A stratégia a következő attribútumokat határozza meg az ország információs társadalmának kialakításához:

- hozzáférhetőség, biztonság bizalom: hozzáférés biztosítása a megbízható információkhoz vagy biztonságos szolgáltatásokhoz, amelyek elengedhetetlenek a polgárok és a vállalkozások számára;
- nyitottság és sokszínűség: nincs preferencia az információhoz való hozzáférés, különösen a lakosság tájékoztatásának kérdésében;
- egyetemesség és elfogadhatóság: olyan erőfeszítéseket kell tenni annak biztosítása érdekében, hogy minél több szereplő aktívan részt vegyen az információs társadalom kiépítésében, amelyek alapján az a lehető legnagyobb mértékben megvalósítható, és az információs társadalom termékei és szolgáltatásai minél szélesebb körben hozzáférhetővé válnak;
- kommunikáció és interoperabilitás: az információ keresése és hozzáférése a biztonságos, gyors és egyszerű legyen. (Kovács 2012)

Lengyelország kiberbiztonságra vonatkozó stratégiai szintű dokumentumainak kidolgozása 2010-ben kezdődött meg a *Kormányzati kiberbiztonság 2011–2016 cselekvési terv* elkészítésével (Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011–2016, RPOC). Az RPOC meghatározta a nemzeti információbiztonságban szerepet játszó minden szereplő feladatát és azok felelősségi körét, illetve rögzítette az elérendő célokat a 2011 és 2016 közötti időszakra vonatkozóan. (Kovács 2012)

23. táblázat

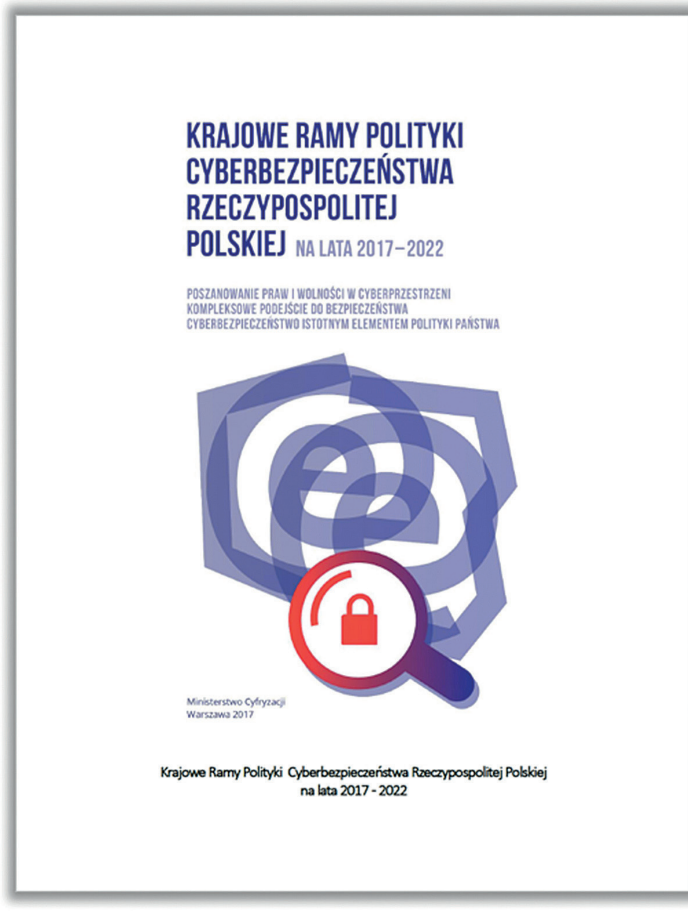
Lengyelország internetpenetrációja 2016-ban és 2017-ben

Lengyelország			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	38,6	27,9	72,4%
2017	38,6	28,3	73,3%

Forrás: www.internetlivestats.com/internet-users/poland/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

Ebben az időszakban a kiberbiztonság szervezeti háttere a CERT közösségre épült, amely kulcsfontosságú szerepet játszott a stratégiában megfogalmazott célkitűzések megvalósításában. A cert.gov.pl csapat működési keretein belül létrehozott Belső Biztonsági Ügynökség (ABW) aktív szerepet töltött be a kormányzati CERT feladatainak megvalósulása során. Együttműködve a CERT Polskával, amely a legrégebbi nemzeti CERT, egy saját fejlesztésű korai előrejelző rendszert, az ARAKIS-GOV működtetését kezdte meg annak érdekében, hogy valamennyi kormányzati hálózat esetében biztosítani tudják azok malware-ekkel és más új biztonsági fenyegetésekkel szembeni védelmét.

A 2017. év eleje azonban új stratégiát hozott Lengyelországban, amelynek címe *Lengyelország Kiberbiztonsági Politikájának Keretrendszere 2017–2020.* Az új stratégia legfontosabb célja a közés magánszektor biztonságának garantálása az alapvető digitális szolgáltatások használata során. (Lengyelország 2017b)



27. ábra

Lengyelország 2017–2022-es időszakra vonatkozó nemzeti kiberbiztonsági stratégiája

Forrás: Lengyelország 2017a

E legfontosabb cél elérése érdekében négy részcélt fogalmaz 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 magában 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[63] tevékenykedni; nemzeti szintű kiberfenyegetettség-értékelő képességet kell kiépíteni; a nemzetbiztonság számára biztonságos kommunikációs rendszert kell felállítani; biztonságos audit- és tesztképességekkel 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, aminek ki kell terjednie az állampolgárok ilyen képességeire is;

[63] A stratégia itt utal arra, hogy a NATO a 2016-os varsói csúcstalálkozón a kiberteret hadviselési dimenzióként elismerte. (NATO 2016a; Lengyelország 2017b)

- erős nemzetközi pozíció kiépítése Lengyelország számára a kiberbiztonság területén mind stratégiai, mind politikai szinten. (Lengyelország 2017b)

A stratégia kitejed mindezen feladatok anyagi hátterének előrevetítésére is, hiszen meghatározza, hogy egy akciótervet (Action Plan for Implementation of the National Framework of Cybersecurity Policy) kell készíteni a stratégia megvalósítására. Az ebben az akciótervben lefektetendő különböző projektek finanszírozásával kapcsolatban az akcióterv alapján kell intézkedni, és fel kell használni a Nemzeti Kutatás és Fejlesztési Központ, valamint az Európai Unió rendelkezésre álló forrásait. (Lengyelország 2017b)

4.9. Lettország

4.9.1. Lettország nemzeti biztonsági stratégiája

Lettország nemzeti biztonsági koncepcióját 2015-ben fogadta el a lett parlament (Saeima). A koncepciót 3-4 évente felülvizsgálják, így ez már a negyedik stratégiai szintű biztonsági dokumentum. (Lettország 2018)

A koncepció utal arra, hogy az állam rendszeresen végzi a kockázatok és fenyegetések értékelését, amely alapján az országra nézve legfontosabb veszélyforrások alapján pontosítják, illetve frissítik a dokumentumot.

Az ország biztonságpolitikai alapelvei nagyban hasonlítanak a balti országokéhoz, hiszen a legfontosabb biztonsági tényezőket egyrészt Lettország geopolitikai helyzete, másrészt a NATO és az európai uniós tagság határozza meg. (Lettország 2015)

A nemzeti biztonsági koncepció megvizsgálja azokat a biztonsági kihívásokban bekövetkezett változásokat, amelyek az előző – 2011-es – biztonsági koncepció kiadása óta jelentek meg a térségben, illetve

Lettország tágabb értelemben vett nemzetközi környezetében. A dokumentum itt kiemeli a Krím félsziget orosz annektálását, valamint az ezzel járó nemzetközi biztonságpolitikai problémákat mint a legnagyobb veszélyforrást a második világháború óta. Oroszország euroatlanti biztonságra, valamint a közvetlen környezetére gyakorolt hatásait elemezve a dokumentum megállapítja, hogy a hibrid veszélyek és a katonai erő agresszív demonstrálása olyan veszélyek, amelyek csak hosszú távon kezelhetők.

A koncepció a veszélyek kezelésére prioritásokat állít fel, amelyek a következők:

- belső biztonságot fenyegető veszélyek, amelyek kezelésére a határőrizeti szervek, a belső rendfenntartó erők, a kríziskezelés és kommunikáció fejlesztését, a migráció kezelését és a radikalizációból eredő kockázatok csökkentését irányozza elő;
- más országok titkosszolgálati tevékenységéből eredő veszélyek, amelyben a hagyományos felderítő és hírszerző módszerektől kezdve a kibertérben megjelenő információszerzés, valamint a hamis hírekkel történő befolyásolás a legkiemelkedőbb kihívás;
- katonai veszélyek, amelyek kapcsán a koncepció kiemeli, hogy ezek a veszélyek szignifikánsan nőttek az elmúlt időszakban. Ennek kezelése érdekében szükséges az ország önvédelmi erői képességeinek növelése, valamint a hosszú távú szövetségből adódó kollektív védelem fenntartása;
- az információs térben megjelenő veszélyek, amelyek elsősorban a külső forrásokból származó – hamis híreken és információkon alapuló – befolyásolásban érhetők tetten. A dokumentum itt nevesíti Oroszországot, mint azt az állami szereplőt, amely hatalmas erőt képvisel a lett belső folyamatok és politika befolyásolására irányuló tevékenységek során. A koncepció abban látja az ezzel szembeni védelem egyik módszerét, hogy több kereskedelmi és kábeltelevíziós csatornát kell támogatni, mert így a la-

> kosságnak lesz alternatívája ezek közül kiválasztani a számára megfelelő információs csatornát. (Lettország 2015)

A koncepció külön értékeli a kiberveszélyeket is, amelyekkel kapcsolatban kiemeli, hogy azok szintén jelentősen nőttek az elmúlt időszakban, de nem lehet őket különválasztani az egyéb – például geopolitikai – kihívásoktól és veszélyektől. A kiberveszélyek elemzésekor a dokumentum utal az IKT-eszközök és -rendszerek növekvő számából és szerepéből eredő függőségre, amely komoly veszélyforrás, de kitér arra is, hogy az ezekkel szembeni támadások mögött álló erők sok esetben államok: „Az elmúlt néhány évben nőtt azoknak az országoknak a száma, amelyek képesek a kiberfelderítésre, információs műveletek, valamint a kibertérben pusztító tevékenységek (a szolgáltatások blokkolása, az információs technológia vagy a fizikai infrastruktúra károsítása) végrehajtására. Számos ország, például az Orosz Föderáció készen áll arra, hogy ilyen módszereket alkalmazzon." (Lettország 2015)

Mindezek alapján a koncepció a kiberveszélyek elleni védekezés során a következő prioritásokat állította fel:

- a kiberbiztonsági politika hatékony implementációja szükséges: Lettország – ahogy a következőkben bemutatjuk – rendelkezik nemzeti kiberbiztonsági stratégiával, valamint az információs társadalom fejlesztését célzó stratégiával is, de az ezekben foglalt intézkedések hatékony végrehajtása elengedhetetlen a kiberbiztonság megvalósításához;
- a kiberfenyegetések azonosításának és kezelésének erősítése;
- az információs infrastruktúra biztonságának növelése, amely munkát a cert.lv-vel közösen állami szinten kell koordinálni;
- a kiberbiztonság megvalósítása érdekében erősíteni kell a nemzeti és a nemzetközi együttműködést. (Lettország 2015)

4.9.2. Lettország nemzeti kiberbiztonsági stratégiája

A *Lettország Nemzeti Kiberbiztonsági Stratégiája 2014–2018* című dokumentum 2014-ben jelent meg. A fejlesztés, együttműködés, felelősség és nyitottság alapelvekkel jellemzett stratégia öt kiemelt cselekvési területet határoz meg, amelyek stratégiai célokként is értékelhetők:

- a kiberbiztonság irányításának és erőforrásainak meghatározása és fejlesztése;
- a kibertér jogi kereteinek meghatározása és a kiberbűnözés csökkentése;
- válságkezelés;
- tudatosság növelése, oktatás és kutatás fejlesztése;
- nemzetközi együttműködés fejlesztése. (Lettország 2014)

24. táblázat

Lettország internetpenetrációja 2016-ban és 2017-ben

Lettország			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	1,95	1,49	76,3%
2017	1,92	1,66	86,2%

Forrás: www.internetlivestats.com/internet-users/latvia/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

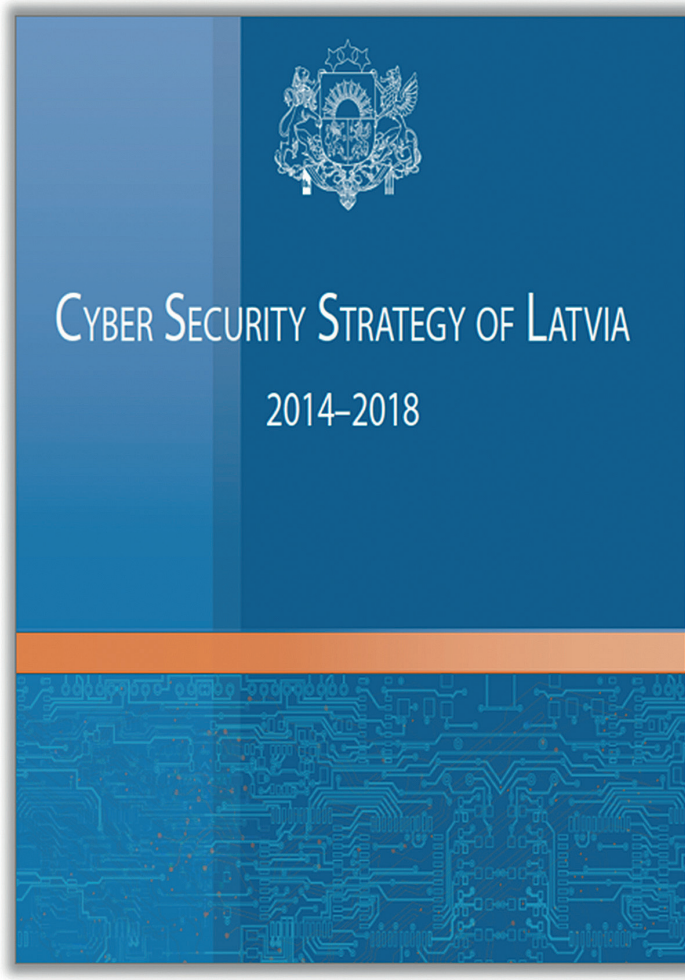
Az első prioritással kapcsolatosan a stratégia bemutatja azt a három dimenzióra – infrastruktúrára, szolgáltatásokra és folyamatokra – osztható kiberbiztonságot, amelynek irányítása részben centralizáltan működik Lettországban. A kiberbiztonság kölcsönös együttműködéseken alapul, amelyben az állami hatóságok közvetlenül vagy közvetett módon a Nemzeti Információtechnológiai Biztonsági Tanácson keresztül végzik tevékenységüket. A tanács mint legfelsőbb hatóság koordinálja a kiberbiztonsági szervezetek és egyéb hatóságok tevékenységét, valamint végzi a kiberbiztonsági a célok eléréséhez

szükséges tevékenységek tervezését, és ellenőrzi azok végrehajtását. Ezen kívül a tanács egyik legfontosabb feladata a nemzeti információcsere biztosítása, valamint az állami és a magánszektor közötti együttműködés koordinálása és erősítése.

A stratégia egyik nagyon előremutató megoldása az, hogy a nemzeti kiberbiztonságban valamilyen szerepet is kapó szervezeteket felméri, és erről egy olyan felelősségi köröket és kapcsolati hálót is bemutató térképet készít, amely egyértelműsíti a koordinációt és a feladatokat. (Lettország 2014)

A dokumentum következő stratégiai prioritása a kibertér jogi kereteinek meghatározása és a kiberbűnözés csökkentése. Ezeken a területeken a dokumentum hangsúlyozza, hogy a kibertérben zajló tevékenységek ugyanolyan elbírálás alá kell, hogy essenek, mint a fizikai térben történők. A kiberbűnözés elleni tevékenységet két dimenzióra osztja a stratégia, amelyben az első a prevenció, a második pedig a hatékony kiberbűnözés elleni fellépés. Mindezek érdekében számos olyan tevékenység végrehajtása szükséges, mint például a területre érvényes törvények és jogszabályok megalkotása, az információbiztonsági és kiberbiztonsági lett nyelvű terminológia kialakítása vagy a kiberbűncselekmények során alkalmazott nyomozási technika fejlesztése. (Lettország 2014)

A válságkezeléshez szükséges képességek növelése területén a stratégia megjegyzi, hogy ennek szervezeti keretei már kialakultak, de jelenlegi képességei nem teszik lehetővé a gyors és hatékony fellépést a kibertérben megjelenő incidensekkel és krízisekkel szemben. Mindezek érdekében a hadsereg (National Armed Forces) egy Kibervédelmi Egységet (Cyber Defence Unit) hozott létre, amely együttműködésben a cert.lv-vel támogatja az incidens- és krízisekezelést. Ez az egység az állami és a közszféra önkénteseiből áll, akik jogilag a Nemzeti Gárdához tartoznak a hadseregen belül. Így szükséges a hadsereg információs eszközeinek és rendszereinek fejlesztése, a rendszeres képzés és kiképzés, de ugyanígy szükséges a nemzetközi együttműködés fejlesztése is a területen. (Lettország 2014)



28. ábra

Lettország Nemzeti Kiberbiztonsági Stratégiája

Forrás: Lettország 2014

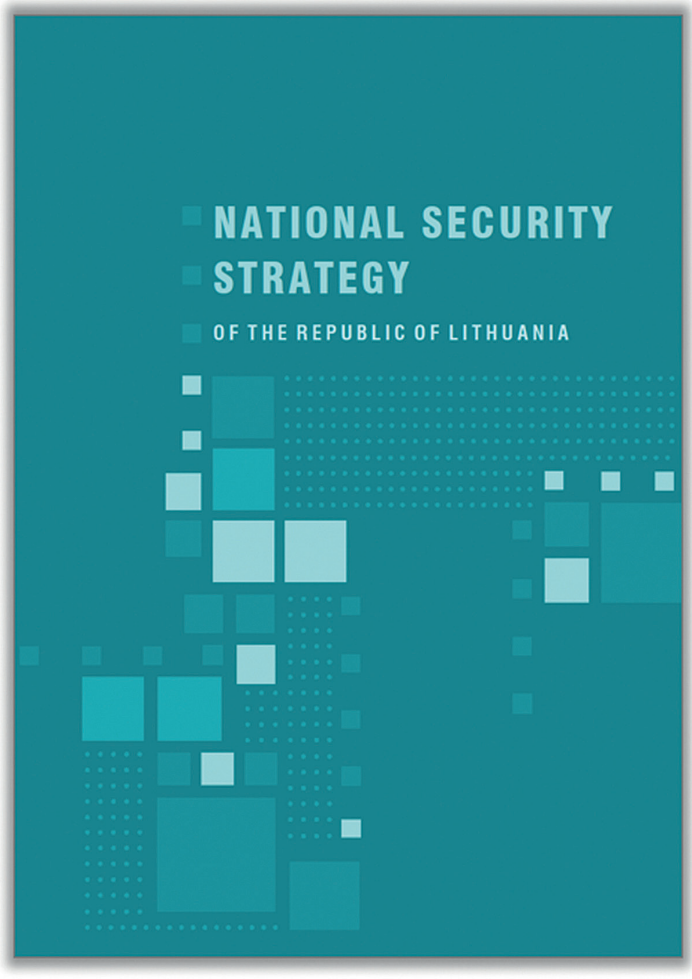
A tudatosság növelése, valamint az oktatás és kutatás fejlesztése terén a stratégia kiemeli, hogy a lakosság kiberbiztonsági tudatossága, képzettsége és általános ismeretei alacsony szinten vannak. Ezért ezeken a területeken komplex megoldás szükséges, amely során elsőként az oktatási intézmények tanári és oktatói állományának kiberbiztonsági képzésére van szükség, majd olyan képzési tematikák és anyagok elkészítését kell megvalósítani, amelyek hatékonyan tudják növelni az állampolgárok biztonsággal kapcsolatos ismereteit. Mindezekhez kiberbiztonsági laborokra, konferenciákra és biztonságtudatosító kampányokra is szükség van. A stratégia itt kiemeli az általunk is említett európai kiberbiztonsági hónap rendezvénysorozathoz való kapcsolódás szükségességét. (Lettország 2014)

A nemzetközi együttműködés fejlesztésének területén a NATO-, az EU-, valamint az EBESZ-szervezetekben való munka folytatása szükséges, amely hozzájárul a bizalomerősítéshez. A dokumentum ezen kívül egy olyan közös balti egyetem létrehozására tesz javaslatot, amely egyetemi oktatással és regionális képzésekkel tud hozzájárulni egy új kiberbiztonsági szakértői generáció kineveléséhez. (Lettország 2014)

4.10. Litvánia

4.10.1. Litvánia nemzeti biztonsági stratégiája

Litvánia nemzeti biztonsági stratégiáját 2002-ben hagyta jóvá a litván parlament, de ez a dokumentum 2017-ben egy frissítésen esett át, amely egy újabb parlamenti döntéssel Litvánia jelenlegi nemzeti biztonsági stratégiáját jelenti. (Litvánia 2017)



29. ábra

Litvánia Nemzeti Biztonsági Stratégiája

Forrás: Litvánia 2017

A stratégia általános bevezetővel és a nemzeti biztonsági politika ismertetésével kezdődik. Ezt követően az ország érdekeinek a bemutatása következik, amelyek az általános biztonságpolitikai elvekre épülnek. Ezeknek az érdekeknek a bemutatása során találkozhatunk első alkalommal a *kiber* kifejezés használatával, amely az állam fejlődésének fenntarthatóságában szerepel az olyan fontos területek mellett, mint a gazdaság, az energia, a környezet, valamint a szociális biztonság. Meg kell jegyezni, hogy a stratégia, hasonlóan a Lettországi hasonló dokumentumhoz, különválasztja a kiberteret és az információs teret. Ez utóbbi nyilvánvalóan az olyan tömegtájékoztatási, valamint elektronikus médiumok és eszközök által lefedett teret jelöli, ahol a külföldi befolyásolás nagyon aktív, és nem utolsósorban annak hatékonysága miatt különösen nagy nemzetbiztonsági kockázatot hordoz magában.

A stratégia következő része a veszélyek és kockázati tényezők feltárása, illetve azok bemutatása. Ezek a veszélyek közül a legfontosabbak a következők:

- hagyományos katonai veszélyek, amelyek esetében a stratégia nevesíti az Orosz Föderáció jelentette veszélyt;
- fedett katonai és hírszerzési műveletek jelentette veszélyek;
- az euroatlanti egységet fenyegető veszélyek;
- regionális és globális instabilitás;
- terrorizmus, extrémizmus, radikalizáció,
- információs veszélyek: az állami és nem állami szereplők által terjesztett hamis és megtévesztő információk, amelyek aláássák az állampolgárok bizalmát, és amelyek célja a megosztottság elérése és a zavarkeltés;
- kiberveszélyek, amelyek a kritikus információs rendszereket támadva, azokat befolyásolva negatív hatást gyakorolnak a gazdaságra, így közvetve a nemzeti biztonságra is;
- gazdasági és energiafüggőség, gazdasági sérülékenység;
- nem biztonságos nukleáris beruházások Litvánia közelében. (Litvánia 2017)

A stratégia a veszélyek bemutatása után prioritásokat és stratégiai célokat fogalmaz meg. Ezek közül a legfontosabbak a következők:

a nemzeti védelmi képességek növelése;

- a NATO kollektív védelmének fejlesztése;
- a NATO kríziskezelésének növelése, a partnerség erősítése;
- az Európai Unió egységének és szolidaritásának erősítése;
- a bi- és multilaterális kapcsolatok erősítése;
- a nemzetközi biztonság és stabilitás erősítésében való aktív részvétel;
- a nemzeti biztonságot fenyegető veszélyek előrejelzésére, értékelésére és kezelésére alkalmas rendszerek fejlesztése;
- a hírszerzési képességek fejlesztése;
- a nemzeti krízismegelőzési és -kezelési képességek fejlesztése;
- az információbiztonság és a litván politikai rendszer biztonságának fejlesztése;
- a terrorizmus elleni védelem fejlesztése;
- a gazdasági és az energiabiztonság növelése;
- a kiberbiztonság erősítése: ezen belül olyan nemzeti kiberbiztonsági rendszer kiépítése szükséges, amely kiemelt figyelmet fordít a kritikus információs infrastruktúrák és az állami intézmények kiberbiztonságára, valamint ezen belül megerősített kibertéri incidenskezelő képességek és az állampolgárok kiberbiztonsági tudatosságának magasabb szintjének elérése szükséges.

4.10.2. Litvánia nemzeti kiberbiztonsági stratégiája

Litvánia nem rendelkezik nemzeti kiberbiztonsági stratégiával. Ennek okairól nagyon keveset lehet tudni,[64] ugyanakkor ezt a stratégiát gyakran a litván kormány 2011-ben született, az elektronikus információbiztonság (kiberbiztonság) területére vonatkozó rendeletével helyettesítik. A kormányrendelet, amelynek hivatalos címe *796. számú Kormányrendelet (2011. június 29.) az elektronikus információs rendszerek 2011–2019 között történő fejlesztésére vonatkozó program elfogadásáról,* angolul *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,* nyilvánvalóan tartalmaz utalásokat a kiberbiztonságra, ráadásul a 2011–2019 közötti időszakra vonatkozó olyan feladatokat is megfogalmaz, amelyek valóban stratégiai jelentőségűek. (Litvánia 2011; Butrimas 2015)

[64] Ezeket az okokat több tényezővel magyarázzák. Az egyik ilyen ok az, hogy a litván parlament 1996-ban fogadta el a nemzeti biztonság alapjairól szóló törvényt, amely felsorolja legfontosabb nemzetgazdasági ágazatokat. Ebben már helyet kapott az információtechnológiai és telekommunikációs szektor is. Ezen kívül egy másik ok lehet az, hogy az általunk is bemutatott litván Nemzeti Biztonsági Stratégia külön is nevesíti a kiberveszélyeket, és számos feladatot határoz meg az ezekkel szembeni védelem kialakítására. (Butrimas 2015)

25. táblázat

Litvánia internetpenetrációja 2016-ban és 2017-ben

Lettország			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	2,85	2,19	77,2%
2017	2,87	2,59	90,4%

Forrás: www.internetlivestats.com/internet-users/lithuania/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

A kormányrendelet három fő programelemet határoz meg, amelyek az előbbiekből következően stratégiai célokként is értelmezhetők. Ez a három fő feladat:

- az állami tulajdonú információforrások biztonságának növelése;
- a kritikus információs infrastruktúrák hatékony működésének biztosítása;
- a litván állampolgárok és a Litvániában tartózkodók kiberbiztonságának növelése. (Litvánia 2011; Butrimas 2015)

Ezeknek a céloknak a megvalósítása érdekében a rendelet számos feladatot határoz meg. Ezek a feladatok a kiberbiztonság koordinálására és felügyeletére, a kiberbiztonság jogszabályi kereteinek kidolgozására, a nemzeti információs infrastruktúra biztonságának növelésére és a nemzetközi együttműködés fokozására adnak eligazítást. (Litvánia 2011)

A kormányrendelet a benne megfogalmazott programpontok végrehajtásának ellenőrzését egy, a rendelet mellékletében megadott kritériumrendszer szerint határozza meg. A kritériumokhoz indikátorokat rendel hozzá, amelyeket a 2011-es kiinduló adatokhoz képest 2015-ben és 2019-ben kell felmérni. (Litvánia 2011)

4.11. Németország

4.11.1. Németország nemzeti biztonsági stratégiája

Németország Európa és a világ egyik legfontosabb és nem mellesleg egyik legnagyobb gazdasága. Magának az országnak és gazdaságának kibertérrel való számtalan kapcsolódási pontja ma már igazi függőséget is jelent nemcsak Németország, hanem közvetett módon a világgazdaság számára is, hiszen az információtechnológia jelentette kibertér nélkül nehéz elképzelni a gazdaság fejlődését, de egyáltalán annak fenntartható működését is. Abban az esetben, ha a német gazdaság például kibertámadások miatt alacsonyabb szinten teljesít, akkor az kihatással van az egész Európai Unió, de nyugodtan mondhatjuk, egész Európa és a világ egészének gazdaságára is.

Németország 2016 júliusában új nemzeti biztonsági stratégiát fogadott el, amelynek címe *Fehér könyv 2016: Biztonságpolitika és a Bundeswehr jövője*, eredeti, német címe pedig *Weissbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr.*

A dokumentum előszavát Angela Merkel kancellár jegyzi, aki utal arra, hogy a gyorsan fejlődő kibertér ma már nemcsak előnyöket hordoz magában, hanem a gyűlölet és az erőszak ideológiáinak terjesztésére is felhasználható eszköz. (Németország 2016a)

A stratégia, amely meglehetősen hosszúra sikerült – terjedelme, több mint 140 oldal –, a német biztonságpolitika legfontosabb tényezőinek számbavételével kezdődik. Itt bemutatja és elemzi Németország szerepét a világban és annak biztonságában, valamint felsorolja az ország értékeit és érdekeit. A nemzeti érdekek esetében az ország alkotmányát, az alapvető emberi jogokat, a demokráciát és a jogállamiságot, valamint a béke megőrzését sorolja fel a stratégia. Ezekkel az érdekekkel párhuzamosan jelennek meg Németország és szövetségesei biztonsági érdekei, amelyek az állampolgárok, az ország függetlenségét és területi integritásának védelmét jelentik, valamint a kialakult nemzetközi rend és a nemzetközi jog megőrzését, az európai

integráció elmélyítését és a transzatlanti partnerség fenntartását. (Németország 2016a)

30. ábra

Németország 2016-os nemzeti biztonsági stratégiájának borítója

Forrás: Németország 2016a

A stratégia értékeli Németország biztonsági környezetét, amely során számba veszi a legfontosabb biztonsági kihívásokat. Ezek a következők:

- 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 a szállítást, a nyersanyagok biztosítását és az energiaszektort fenyegető veszélyek;
- a klímaváltozás;
- az ellenőrizetlen migráció;
- epidémia és pandémia. (Németország 2016a)

A felsorolásból kitűnik, hogy a német biztonsági stratégia külön tárgyalja a kibertérben jelentkező, valamint az információs és kommunikációs rendszereket fenyegető veszélyeket. A kibertérrel kapcsolatosan a stratégia megállapítja, hogy az itt bekövetkező konfliktusok egyenlőek lehetnek a fizikai térben bekövetkező fegyveres konfliktusokkal: „A kibertámadások hatásai megegyezhetnek a fegyveres konfliktusok hatásaival, és a fizikai dimenzióra is kiterjedhetnek." (Németország 2016a)

Ugyanakkor az információs és kommunikációs rendszereket fenyegető veszélyeket – együtt az ellátási láncokkal, a szállítással, illetve az energiával – nem teljesen különíti el a kibertértől, sokkal inkább azt a függőséget kívánja bemutatni, amely ezekkel a rendszerekkel szemben alakult ki a 21. század gazdasága és társadalma oldaláról: „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)

A veszélyek számbavétele után a dokumentum meghatározza Németország biztonsággal összefüggő stratégiai céljait, amelyek a következők:

- 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)

Az ezekkel a prioritásokkal kapcsolatos tevékenységek meghatározása során a stratégia hangsúlyozza, hogy Németország biztonsági politikája globális, amely kiterjed az űrre és a kibertérre is.

Mindezeken túl a dokumentum kijelenti azt is, hogy a biztonság megteremtése nemcsak az állam feladata, mert abban részt kell vállalnia az iparnak, a tudományos közösségeknek és a társadalomnak is. Ennek megfelelően a kiberbiztonság megvalósításához is nemzeti és nemzetközi szintű együttműködés szükséges. A nemzetközi együttműködési keretek adottak, de akár a NATO-n, akár az EU-n belüli együttműködést – holisztikus megközelítéssel – kell tükröznie Németország készülő új Nemzeti Kiberbiztonsági Stratégiájának is.

A stratégia nemcsak a biztonsági környezetet és az ezzel kapcsolatos német feladatokat mutatja be, hanem a német haderő – a Bundeswehr – jövőjét és feladatait is számba veszi.

A Bundeswehr feladatai között a stratégia meghatározza a kiberfenyegetések elleni fellépés szükségességét is, ugyanakkor ezt alapvetően csak a védelem oldaláról közelíti meg. Ennek megfelelően a német

haderőnek képesnek kell lennie és részt kell vennie a német kibervédelemben, valamint természetszerűleg a saját hálózatainak védelmét is el kell látnia. Mindezen feladatok megvalósításához a stratégia előirányozza mind a hadsereg technológiai fejlesztését, mind a megfelelő személyzet kiválasztását, felvételét és azok képzését, továbbképzését. (Németország 2016a)

4.11.2. Németország nemzeti kiberbiztonsági stratégiája

Németország első kiberbiztonsági stratégiája 2011-ben született, *Kiberbiztonsági Stratégia Németország számára (Cyber-Sicherheitsstrategie für Deutschland)* címmel. A dokumentum összesen tíz stratégiai célt és az ezekhez kapcsolódó feladatokat határozza meg. A kiemelt célok a következők:

- a kritikus információs infrastruktúrák védelme;
- biztonságos IKT-rendszerek alkalmazása az állampolgárok és a kkv-k részéről;
- a közigazgatás információbiztonságának erősítése;
- 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)

26. táblázat

Németország internetpenetrációja 2016-ban és 2017-ben

Németország			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	80,7	71,0	88,0%
2017	80,7	72,2	89,6%

Forrás: www.internetlivestats.com/internet-users/germany/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

A fenti célok között szerepel a közigazgatás információbiztonságának növelése, amellyel kapcsolatban fontos megjegyezni, hogy Németország már 2010-ben elfogadta az E-Kormányzat Stratégiáját (Nationale E-Government-Strategie, NEGS). Ennek 2015-ben megtörtént a felülvizsgálata, amelynek eredményei 2015 októberében egy dokumentumban jelentek meg *E-Kormányzat Stratégiai Felülvizsgálat 2015 (Nationale E-Government-Strategie Fortschreibung 2015)* címmel. Ebben az e-kormányzattal kapcsolatos egyik fontos stratégiai célkitűzés, hogy szövetségi szinten olyan magas szintű, elektronikus közigazgatási szolgáltatásokat nyújtsanak az állampolgároknak, amelyekben az információbiztonság és az adatok védelme során a korábban már említett információbiztonsági alapelvek – nevezetesen a bizalmasság, sértetlenség és rendelkezésre állás – teljesülnek. Ennek a célnak a megvalósulása érdekében a stratégia tartalmazza a közigazgatásban dolgozók rendszeres és magas szintű információbiztonsági képzéseit és továbbképzéseit. (Németország 2015)

31. ábra

Németország 2011-es Nemzeti Kiberbiztonsági Stratégiája

Forrás: Németország 2011

A kiberbiztonsági stratégia ezt követően a felsorolt célokat elérendő, fenntartható implementációs leírást is körvonalaz, ugyanakkor abban nem fogalmaz meg részletes akciótervet vagy feladatokat.

Németország első nemzeti kiberbiztonsági stratégiáját 2016-ban egy új stratégia követte, amely nem túl meglepő módon a *Kiberbiztonsági Stratégia Németország számára 2016 (Cyber-Sicherheitsstrategie für Deutschland 2016)* címet kapta.

Az új stratégia terjedelmében és szerkezetében sem tér el lényegesen a korábbi stratégiától, ugyanakkor négy nagy tevékenységi körben határoz meg akciókat a kiberbiztonság fokozása érdekében. Ez a négy tevékenységi kör a következő:

- 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)

A stratégia az első akcióterületen, azaz a biztonságos és önálló tevékenység a digitális környezetben, számos olyan feladatot határoz meg, amelyek hozzájárulnak a stratégia legfontosabb célkitűzéseinek eléréséhez. Ezek a feladatok többek között kiterjednek digitális írástudás fejlesztésére, amely során a kiberbiztonság-tudatosság is fejleszthető; a biztonságos elektronikus kommunikáció és internetes szolgáltatások feltételeinek a kialakítására; az állampolgárok biztonságos elektronikus azonosítására, amely magában foglalja egy elektronikus személyi igazolvány bevezetését is; az információbiztonsági tanúsítványok iránti igény növelésére, amely egy információbiztonsági tanúsítvány bevezetését is jelentheti; valamint a kiberbiztonsági kutatások támogatására. (Németország 2016b; Rothenpieler 2016)

32. ábra

Németország 2016-os Nemzeti Kiberbiztonsági Stratégiája

Forrás: Németország 2016b

A második akcióterület, azaz az állam és az üzleti élet közös erőfeszítései és kiberbiztonságra irányuló tevékenységei esetében a stratégia meghatározza a kritikus infrastruktúrák védelmét,[65] a németországi vállalatok és vállalkozások védelmének biztosítását, a hazai informatikai ipari ágazatok megerősítését, a szolgáltatókkal történő szoros együttműködést, illetve ezen szolgáltatók bevonását a kiberbiztonság megteremtésébe és fenntartásába, valamint egy olyan platform létrehozását, amely segítséget nyújt a gyors és hatékony információcseréhez a sérülékenységek, veszélyek, kibertámadások és a védelem terén. (Németország 2016b; Rothenpieler 2016)

A stratégia harmadik akcióterülete – a hatékony és fenntartható állami kiberinfrastruktúra létrehozása – vonatkozásában számos további feladatot határozott meg, amelyek közül a legfontosabbak a következők:

- a Nemzeti Kiberreagáló Központ további fejlesztése;
- a helyszíni kiberelemzési és -reagálási képességek/lehetőségek növelése;[66]
- 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;

[65] A kritikus infrastruktúrák védelme esetében meg kell jegyezni, hogy 2009-ben született meg Németország első nemzeti kritikus infrastruktúra védelmi stratégiája, amely egyrészt meghatározta a kritikus infrastruktúra fogalmát, másrészt fel is osztotta technikai alapú infrastruktúrákra és társadalmi-gazdasági szolgáltató infrastruktúrákra. (Németország 2009) Ezt követően a 2015-ben megjelent német információbiztonsági törvény számos kiegészítést tett a kritikusinfrastruktúra-védelemmel kapcsolatban is, amely alapján a kritikus ágazatok és alágazatok, illetve az abban megvalósítandó kibervédelem hatékonysága növekedhet, hiszen a törvény többek között az incidensek jelentésére, azok kezelésére, a kommunikációra és az együttműködésre egyaránt számos új szabályt hozott. (BMI 2018)

[66] Ennek érdekében létrejöttek mobil incidenskezelő csoportok (Mobile Incident Response Team, MIRT).

- egy informatikai biztonsági központi szervezet[67] 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 2016b; Rothenpieler 2016)

A negyedik akcióterületen, azaz az európai és nemzetközi kiberbiztonság politikájának alakításában való aktív német részvétellel kapcsolatosan a stratégia olyan, kissé általános feladatokat határoz meg, mint a hatékony európai kiberbiztonsági politika kialakításában, a NATO kibervédelmi politikájának megerősítésében való részvétel, valamint a kétoldalú és regionális együttműködés szorgalmazása, illetve a nemzetközi (kiber)bűnüldözés megerősítése. (Németország 2016b; Rothenpieler 2016)

Bár nem kapcsolódik szorosan a stratégiához, de fontos említést tennünk a kiberbiztonság szervezeti hátteréről Németországban. A kiberbiztonság, illetve az információbiztonság szervezeti rendszerében az egyik legfontosabb szereplő a Szövetségi Információs Biztonsági Hivatal (Bundesamt für Sicherheit in der Informationstechnik,

[67] Ez a központi informatikai biztonsági szervezet ZITiS (Zentral Stelle für Informationstechnik im Sicherheitsbereich, azaz a biztonsági szektor információtechnológiai központja) néven létre is jött. A szervezet saját meghatározása szerint: „A ZITiS a számítógépes technikai megoldások kutatási és fejlesztési testülete. Németország biztonsági hatóságainak nyújtunk szolgáltatásokat, és technikai know-how-nk egyesítésével támogatjuk őket. Szakértelmünk révén olyan eszközöket és megoldásokat hozunk létre, amelyek elengedhetetlenek a biztonsági hatóságok tevékenységeihez.” (ZITiS 2018)

BSI).[68] A szervezet szolgáltatásain túlmenően – információbiztonsági tanácsadás, elemzések készítése –, amelyeket különböző célcsoportok számára nyújt, az 1991-es magalapítása óta Németország információbiztonságának legmagasabb szintű szervezeti felelőse. A BSI öt osztályban, egy központi és négy szakosodott szervezeti egységben működik. A központi osztály – hivatalos nevén „Z" osztály – a központi feladatok ellátásért (mint például a humán, gazdasági ügyek), a négy szakosodott osztály közül az úgynevezett „CK" osztály a kiberbiztonságért és a kritikus infrastruktúrák területéért, a „B" osztály a kormányzat és a magánszektor közötti együttműködésért, a „KT" osztály a kriptotechnológiáért és a kiemelt biztonsági követelményekért, a „D" osztály a kiberbiztonság tanúsításához és szabványosításához szükséges feladatokért felelős. (BSI 2018a; BSI 2018b)

4.12. Szlovén Köztársaság

4.12.1. A Szlovén Köztársaság nemzeti biztonsági stratégiája

Szlovénia nemzeti biztonsági stratégiáját 2010. április elején tették közzé. A stratégia, amely hivatalosan a szlovén országgyűlés határozataként jelent meg,[69] párhuzamosan tartalmazza a szlovén és az angol nyelvű változatot.

A dokumentum legfontosabb célja – hasonlóan az eddig bemutatott nemzeti biztonságot meghatározó stratégiai dokumentu-

[68] A BSI-ről, illetve annak tevékenységéről és feladatairól külön törvény rendelkezik. A BSI megalapítását elrendelő 1991-es 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. (BSI-Gesetz 2009) E törvény mellett a már említett 2015-ös információbiztonsági törvény számos jogkört és feladatot – például a kritikusinfrastruktúra-védelem nemzeti koordináló feladatait – ruházott a BSI-re.

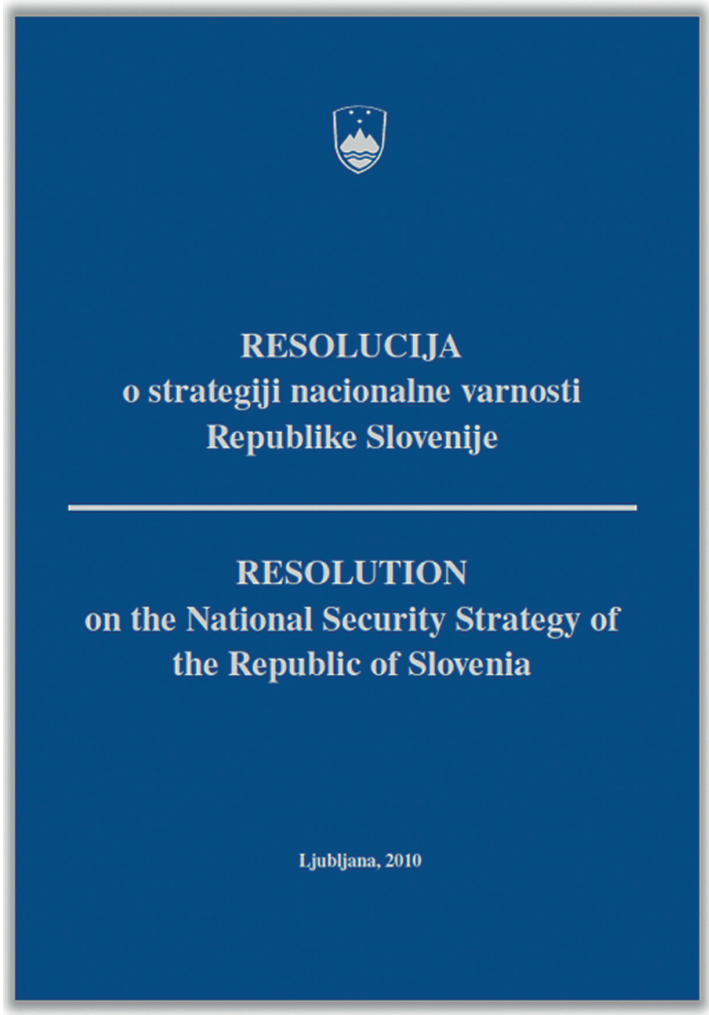
[69] Ez hasonló hazánk nemzeti biztonsági, illetve nemzeti kiberbiztonsági stratégiájához, amely stratégiákat kormányhatározatként adták ki.

mokhoz –, hogy a nemzeti biztonság területén legalapvetőbb fejlesztésekhez adjon iránymutatást. A stratégia számba veszi a Szlovén Köztársaság nemzeti érdekeit és ezek alapján azokat a célkitűzéseket, amelyek mindezen érdekek védelme során a nemzeti biztonsággal kapcsolatosak.

A stratégia Szlovénia nemzeti érdekei bemutatásakor az általánosságokon nem megy túl. Az ország függetlensége, területi integritása, valamint állampolgárainak védelme azok a legfontosabb tényezők, amelyeket a dokumentum felsorol mint az ország legfőbb érdekei. Mindezek védelme érdekében a határozat egyetlen stratégiai célt tűzött ki, amely nem más, mint ezek átfogó védelme a meghatározott jogrend keretei között, illetve az ehhez szükséges megfelelő védelmi megelőzés és olyan szervezeti rendszer kialakítása, amely megfelelő képességekkel rendelkezik a veszélyek időbeni felismerésére és azok kezelésére. Mindezek mellett a környezetvédelem és a nemzeti erőforrások megfelelő kezelése szintén kiemelt jelentőségű az ország szempontjából.

A stratégia értékeli az ország geopolitikai és geostratégiai helyzetét, bemutatja a nemzetközi biztonsági helyzetet, majd kitér azokra a veszélyforrásokra, amelyek Szlovénia nemzeti biztonságát fenyegetik.

A stratégia a kihívásokat és veszélyeket több nagyobb kategóriába, illetve több szintre osztva mutatja be. Ez a bemutatás azonban alapvetően csak felsorolás, nagyon kevés és nagyon rövid értékelést tartalmaz. A dokumentum három szinten különíti el a veszélyeket: a globális, a transznacionális és a nemzeti veszélyek szintjén. (Szlovénia 2010)



33. ábra

Szlovénia nemzeti biztonsági stratégiája

Forrás: Szlovénia 2010

E három szinten a következő kihívásokat azonosítja a stratégia:

- globális veszélyek és kockázatok:
  - klímaváltozás;
  - globális pénzügyi, gazdasági és szociális kockázatok;
  - válságövezetek;
- transznacionális veszélyek és kockázatok:
  - terrorizmus;
  - a hagyományos, a tömegpusztító és a nukleáris fegyverek proliferációja;
  - szervezett bűnözés;
  - illegális migráció;
  - kiberfenyegetések, valamint az információs technológia és rendszerek nem megfelelő használata;
  - külföldi hírszerző szervezetek tevékenysége;
  - katonai veszélyek;
- nemzeti veszélyek és kockázatok:
  - a közbiztonságot fenyegető veszélyek, amelyek alapvetően az előbbi felsorolásból eredő veszélyek közvetett és közvetlen hatásaiként jelentkeznek;
  - természeti és egyéb katasztrófák;
  - a természeti erőforrások kimerülése és a környezet degradációja;
  - egészségügyi és epidemiológiai veszélyek;
  - a bizonytalanságból eredő tényezők, amelybe többek között a kritikus infrastruktúrák elleni esetleges terror- vagy egyéb támadások következményei is beletartozhatnak. (Szlovénia 2010)

Természetesen a stratégia mindezekre a kihívásokra megadja a lehetséges válaszokat, azaz bemutatja az elvárt védelmi megoldásokat is. Ennek első lépése a nemzeti biztonsági politika meghatározása, amely összefoglalja mindazokat az ágazati politikák szempontjából legfontosabb irányelveket, amelyeket többek között a külpolitikában, a védelmi

politikában, a belső biztonságot meghatározó politikában vagy éppen a természeti és egyéb katasztrófák kezelése érdekében meghirdetett politikában szükséges követni.

A felsorolt veszélyek kezelése érdekében azok mindegyikére nagyon rövid, de határozott, elvárt válaszokat mutat be a stratégia. Ebben helyet kap a kiberfenyegetések és az információs technológia és rendszerek nem megfelelő használatából eredő veszélyekre adandó válaszok bemutatása is. Ennek egyik fő gondolatát a dokumentum így fogalmazza meg: „A kiberbiztonság tekintetében a Szlovén Köztársaság nemzeti stratégiát fog kialakítani a kiberfenyegetésekre és az információs technológiákkal való visszaélésre adott válaszként, és meghozza mindazokat a szükséges intézkedéseket, amelyek a hatékony kibervédelem biztosításához szükségesek, és amelyek magukban foglalják az állami és magánágazatot egyaránt." (Szlovénia 2010)

Ez mindenképpen előremutató, hiszen egyrészt a stratégiának az ország nemzeti biztonságról való gondolkodása tartalmazza a kibertér és az információs rendszerek jelentette veszélyeket, másrészt nagyon korán – hiszen még csak 2010-ben járunk – született ez az elhatározás, amikor még az európai országokban nem volt jellemző nemzeti szinten a kiberbiztonsági stratégia megléte.

4.12.2. A Szlovén Köztársaság nemzeti kiberbiztonsági stratégiája

A 2010-ben kiadott szlovén nemzeti biztonsági stratégia – ahogy a fentiekben bemutattuk – már egyértelmű utalást tartalmazott arra vonatkozólag, hogy el kell készíteni egy nemzeti kiberbiztonsági stratégiai dokumentumot. Erre azonban csak 2016-ban került sor.

27. táblázat

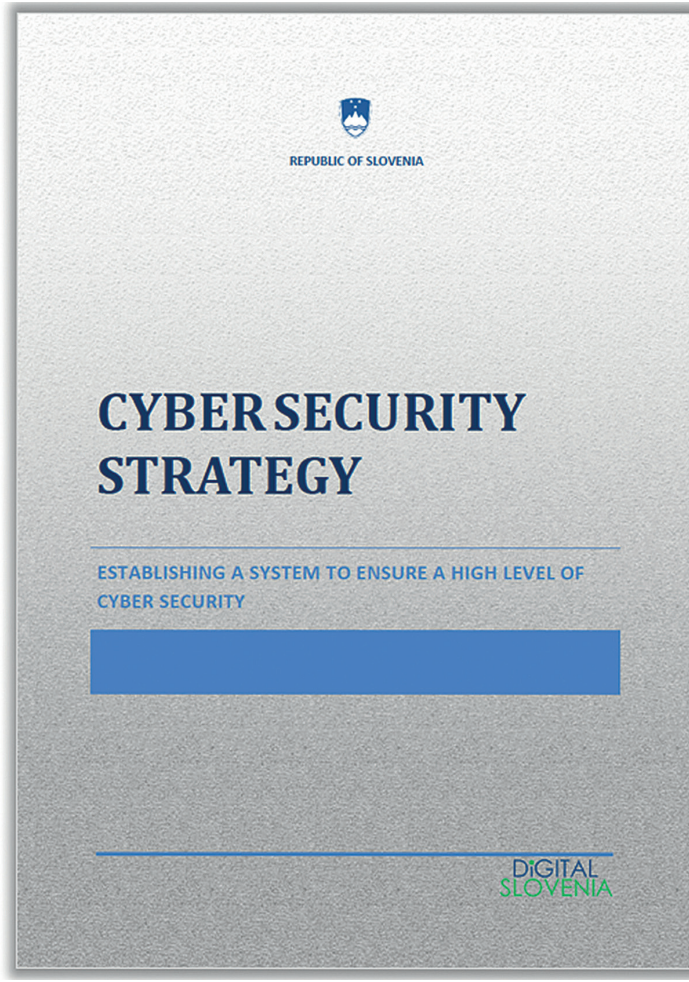
A Szlovén Köztársaság internetpenetrációja 2016-ban és 2017-ben

Szlovén Köztársaság			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	2,07	1,49	72,0%
2017	2,081	1,66	79,9%

Forrás: www.internetlivestats.com/internet-users/slovenia/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

A *Kiberbiztonsági Stratégia: egy rendszer kialakítása a kiberbiztonság magas szintjének biztosítására* című dokumentumra a nemzeti biztonsági stratégiát követően közel 5 évet kellett várnia Szlovéniának. A dokumentum elkészítésében több mint 15 minisztérium, illetve kormányzati szerv vett részt, ami talán magyarázatként szolgálhat arra, hogy miért volt szükség 5 évre az elkészítéséhez.

A dokumentum összesen 20 oldalban foglalja össze mindazokat a tényezőket, amelyek meghatározzák Szlovénia kiberbiztonságát. A stratégia a készítés időpontjára vonatkozó kiberbiztonsági helyzet elemzésével kezdődik. Ebben a részben a dokumentum megállapítja, hogy az ország incidenskezelési képességei, illetve az ezt biztosító szervezeti rendszer nagyon széttagolt. Számos olyan intézménynyel rendelkezik Szlovénia, amelyek feladata részben vagy egészben a kiberincidensek kezelése. Ilyen szervezet többek között a SI-CERT (Slovenian Computer Incident Response Team, azaz szlovén számítógép-vészhelyzeti incidenskezelő csoport), a Közigazgatási Minisztérium IT Igazgatósága, a Védelmi Minisztérium, a Szlovén Hírszerzési és Biztonsági Ügynökség (Slovenska obveščevalno-varnostna agencija, SOVA) vagy a Szlovén Rendőrség IT és Kommunikációs Irodája. Mindezek ellenére azonban stratégiai szinten nincs meg az a képesség, illetve az ehhez szükséges intézmény, amely koordinálná az említett szervezetek közötti együttműködést. (Szlovénia 2016)



34. ábra

Szlovénia kiberbiztonsági stratégiája

Forrás: Szlovénia 2016

A helyzetértékelés után – nyilvánvalóan alapozva annak megállapításaira – a dokumentum meghatározza azokat a stratégiai célokat, ame-

lyek a nemzeti biztonsághoz a nyitott és biztonságos kibertér[70] megteremtésével járulnak hozzá. A stratégia legfontosabb célja, hogy 2020-ra egy olyan hatékony nemzeti kiberbiztonsági rendszert hozzon létre, amely hatékony védelmet biztosít a kiberincidensekkel szemben, illetve amely megfelelően képes ezek esetleges bekövetkezése esetén a következmények felszámolására. Ezt a célt nyolc részcél megvalósításával kívánja a stratégia elérni:

- a nemzeti kiberbiztonsági rendszer megerősítése és szisztematikus szabályozása;
- a polgárok biztonságának megteremtése a kibertérben;
- a kiberbiztonság megteremtése a gazdaságban;
- a kritikus infrastruktúrák működésének biztosítása azok információs rendszereinek támogatásán keresztül;
- a kiberbiztonság megteremtése a közbiztonság területén, valamint a kiberbűnözés elleni küzdelem fokozása;
- a kibervédelmi képességek fejlesztése;
- a kulcsfontosságú IKT-rendszerek biztonságos üzemeltetésének és rendelkezésre állásának biztosítása a legfontosabb természeti és egyéb katasztrófák esetén;
- a kiberbiztonság növelése a nemzetközi együttműködés révén. (Szlovénia 2016)

A stratégia ezt követően bemutatja a legfontosabb kibertéri kockázatokat. Ez azonban nem egy részletes elemzés, hanem valójában egy rövid felsorolás és az adott veszély rövid bemutatása csak, amely a SI-CERT korábbi éves jelentésein, illetve azok összefoglalásain alapul. Ezek alapján a stratégia a legfontosabb kockázatok közé a gyors technológiai fejlődésben – például az IoT technológiában vagy a nagy mennyiségű adatokban – rejlő veszélyeket, a kiberbűnözést, a külföldi országok által végzett hírszerző tevékenységet, a személyes adatokhoz való

[70] A stratégia angol nyelvű fordításában ez nyilvánvaló utalás az Európai Unió kiberbiztonsági stratégiájára, amely ezzel a címmel jelent meg 2013-ban.

illetéktelen hozzáférést, illetve azok engedély nélküli felhasználását sorolja. (Szlovénia 2016)

A dokumentum a stratégiai cél és a részcélok eléréséhez számos tevékenységet rendel hozzá. Ezek intézkedések formájában a következők:

- a nemzeti kiberbiztonsági rendszer megerősítése és szisztematikus szabályozása cél érdekében:
  - központi koordináció kialakítása;
  - a szükséges humán erőforrás és technikai kapacitás megerősítése és egy kormányzati CERT (SIGOV-CERT) megalapítása;
  - rendszeres részvétel nemzetközi gyakorlatokon és rendszeres nemzeti gyakorlatok szervezése;
  - biztonságos kommunikációs rendszerek kialakítása a szlovén hatóságok számára;
- a polgárok biztonságának megteremtése a kibertérben cél érdekében:
  - rendszeres kiberbiztonság-tudatossági kampányok szervezése;
  - kiberbiztonsági elemek megjelenítése az oktatásban;
- a kiberbiztonság megteremtése a gazdaságban cél érdekében:
  - új kiberbiztonsági, technológiai és technikai megoldások bevezetése, illetve azok ösztönzése;
  - rendszeres kiberbiztonság-tudatossági kampányok szervezése a pénzügyi szervezetek számára;
- a kritikus infrastruktúrák működésének biztosítása azok információs rendszereinek támogatásán keresztül cél érdekében:
  - rendszeres kockázatelemzés a kritikus infrastruktúrák működéséhez nélkülözhetetlen IKT-rendszerek körében;
- a kiberbiztonság megteremtése a közbiztonság területén, valamint a kiberbűnözés elleni küzdelem fokozása cél érdekében:
  - a rendőrségi rendszerek kiberbiztonságának növelése;
  - rendszeres kiberbiztonsági képzések a rendőrség állományának;

  - az IKT-rendszerek fejlődését követni képes jogszabályi rendszer kialakítása és folyamatos fejlesztése;
- a kibervédelmi képességek fejlesztése cél érdekében:
  - a védelmi szektor működéséhez szükséges IKT-rendszerek kiberbiztonságának növelése;
- a kulcsfontosságú IKT-rendszerek biztonságos üzemeltetésének és rendelkezésre állásának biztosítása a legfontosabb természeti és egyéb katasztrófák esetén cél érdekében:
  - a természeti és/vagy egyéb katasztrófák kezelése érdekében szükséges IKT-rendszerek kiberbiztonságának növelése;
- a kiberbiztonság növelése a nemzetközi együttműködés révén cél érdekében:
  - meg kell teremteni annak a lehetőségét, hogy szlovén szakértők nagyobb számban és hatékonyabban tudjanak részt venni a kiberbiztonsággal kapcsolatos nemzetközi szervezetek munkájában. (Szlovénia 2016)

A stratégia egy SWOT-analízist is elvégez, amelyben elemzi mindazokat a kihívásokat is, amelyek a stratégiában megadott tevékenységek bevezetésében, illetve végrehajtásában jelentkezhetnek. Ilyen kihívás, vagy ahogy a SWOT analízisben a stratégia megadja, gyengeségek lehetnek a pénzügyi, a technikai és humán erőforrás területeken jelentkező hiányok, az érdekelt felek közötti nem megfelelő együttműködés vagy a szabályozási környezet kialakításának hiánya. A stratégia bevezetése során kockázatként azonosították a kiberincidensekkel kapcsolatos elégtelen veszély-előrejelzést vagy az olyan rendszerkiesések bekövetkezését, amelyek még azelőtt történnek, hogy a rendszer elérte volna a működőképességét. (Szlovénia 2016)

4.13. Szlovák Köztársaság

4.13.1. A Szlovák Köztársaság nemzeti biztonsági stratégiája

2016-ban jelent meg a Szlovákia nemzeti védelméről szóló Fehér könyv, amelyet a 2013-as előző dokumentum után egy aktualizált, az új biztonságpolitikai környezetben – például Oroszország Krím félszigetet érintő annektálása miatt – bekövetkezett változásokra válaszul adtak ki. Az alapvetően a katonai területet érintő, valamint a hadsereg fejlesztését célzó dokumentumot mintegy az ország nemzeti biztonsági stratégiájaként is értékelhetjük.

A könyv az ország külső biztonsági környezetének értékelése során utal először a kibertérre. A dokumentum hangsúlyozza, hogy a katonai tevékenységek súlypontja egyre inkább a nem konvencionális területekre helyeződik át, amelyek magukban foglalják az információs-, elektromágneses- és kiberteret, valamint az űrt is. Az ezeken a területeken tapasztalható technológiai fejlődés sebességétől függően, illetve az olyan új területen, mint a nanotechnológia tapasztalható forradalmi fejlődésnek köszönhetően a biztonságról alkotott elképzeléseink is alapjaiban változnak meg.

A kibertérrel kapcsolatban a dokumentum 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)

35. ábra

A Szlovák Köztársaság 2016-os Fehér könyve

Forrás: Szlovákia 2016a

Figyelemre méltó, hogy a dokumentum a Szlovák Köztársaságot fenyegető legfontosabb globális katonai és nem katonai, szimmetrikus és aszimmetrikus biztonsági fenyegetések, illetve veszélyforrások

számbavételekor – a terrorizmus, illetve a szervezett terrorcsoportok után – a második helyen a kibertámadásokat említi. (Szlovákia 2016b)

4.13.2. A Szlovák Köztársaság nemzeti kiberbiztonsági stratégiája

2009 októberében jelent meg a *Szlovákia Információs Társadalom Stratégia 2009–2013* című dokumentum, amely felváltotta a még 2004-ben született korábbi információstársadalom-stratégiát és cselekvési tervet. Időközben számos stratégia született az információs technológia, illetve a digitális társadalom egyes területeire vonatkozóan. Ugyanakkor a 2009-ben megszületett dokumentum egységesen igyekezett lefedni az addigi részstratégiák által kezelt területeket. Az átdolgozott stratégia meghatározta azokat a legfontosabb fejlesztendő területeket, amelyek a Szlovák Köztársaság információs társadalmának építése során elengedhetetlenek. Ezek a következők voltak:

- széles sávú hozzáférés növelése;
- információbiztonsági szabványok kidolgozása;
- e-kormányzat és e-egészségügy fejlesztése;
- digitális írástudás fejlesztése, e-oktatás kialakítása;
- az energiafogyasztás csökkentése és az energiahatékonyság növelése. (Kovács 2012)

Szlovákia első nemzeti informatikai biztonsági stratégiája 2008-ban jelent meg. Ez a dokumentum három szinten fogalmazott meg feladatokat az információbiztonság területén. Az első szint a hosszú távú információbiztonsági stratégiai célokat, a második szint a stratégiai prioritásokat, a harmadik szint pedig a legfontosabb problémákat, valamint az ezek kezelésével kapcsolatos feladatokat mutatta be. A dokumentum világosan szétválasztotta a hatásköröket, meghatározta a prioritásokat és a legfontosabb intézkedéseket. (Kovács 2012)

Az informatikai biztonságot meghatározó 2008-as stratégia után a szlovák kormány 2015 júniusában fogadta el a *Szlovák Köztársaság kiberbiztonsági koncepciója 2015–2020 évekre* című dokumentumot. A koncepció legfontosabb célja a kiberbiztonság új intézményi keretének megteremtése a Szlovák Köztársaságban. Maga a dokumentum az EU NIS-irányelv – akkor még csak tervezetének – legfontosabb kérdéseinek figyelembevételével készült. (Szlovákia 2015b)

25. táblázat

A Szlovák Köztársaság internetpenetrációja 2016-ban és 2017-ben

Szlovák Köztársaság			
	Teljes népesség (millió fő)	*Internethasználók száma (millió fő)*	*Internetpenetráció (a teljes lakosság százalékos arányában)*
2016	5,4	4,5	82,5%
2017	5,4	4,6	85,2%

Forrás: www.internetlivestats.com/internet-users/slovakia/, www.internetworldstats.com/stats4.htm#europe, a szerző szerkesztése

A kiberbiztonsági koncepció nagyon előremutató módon megfogalmazza mindazokat az alapelveket, amelyeket már jelen könyvünkben is többször említettünk, például a nemzetközi szervezetek kiberbiztonsági stratégiákra vonatkozó ajánlásainak bemutatásakor. Ilyen alapelv többek között a nemzetközi együttműködés szükségessége, valamint a komplex, rendszerszintű problémakezelés, amely során a lehető legtöbb érdekelt fél bevonása szükséges, legyen szó akár a magán-, akár az állami szereplőkről.

Maga a koncepció deklaráltan az Európai Unió kiberbiztonsági stratégiájára, valamint a NATO kibervédelmi politikájára épül. (Szlovákia 2015b)

36. ábra

A Szlovák Köztársaság 2015–2020-as időszakra vonatkozó kiberbiztonsági stratégiája

Forrás: Szlovákia 2015a

A dokumentum legfontosabb célkitűzése mindazoknak a kockázatoknak a csökkentése, amelyek a kibertérből érkeznek, anélkül, hogy

a kibertér használatát csökkentenék vagy azt korlátoznák. Ennek a célnak az elérése érdekében a következő feladatokat tűzte ki a szlovák kormány:

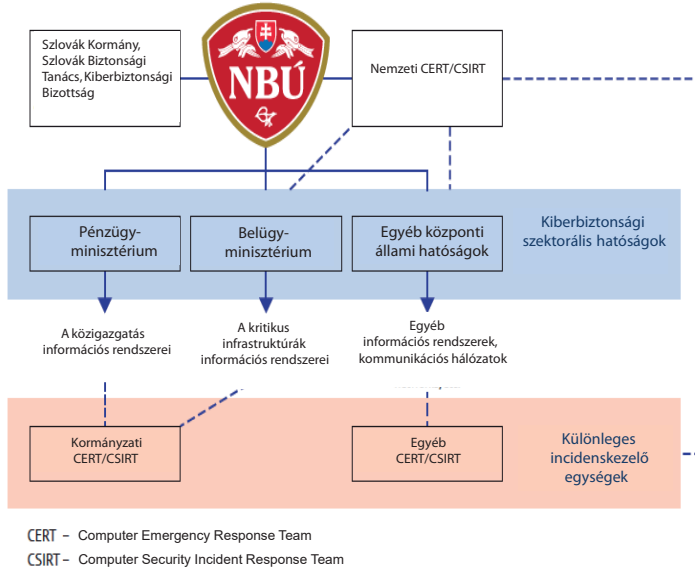
- a kiberbiztonság irányítási rendszerének és annak jogi hátterének a megteremtése (intézményi, szabályozási és módszertani keretrendszer), beleértve ebbe a szakosított intézményeket és a terminológiát is;
- a magán- és az állami szektor közötti információcsere növelése és hatékonyabbá tétele, amely együtt kell, hogy járjon a kiberbiztonsági szereplők tudásának növelésével, valamint a magasabb szintű kockázatkezelési 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)

Ezeknek a feladatoknak a végrehajtása érdekében a koncepció hét úgynevezett kulcsintézkedést fogalmaz meg:

- a kiberbiztonsági igazgatás intézményi kereteinek kiépítése, amelyhez a 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 törvényt);
- 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, amely 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 2015)

A szlovák kiberbiztonság szervezeti struktúrájának stratégiában tervezett kialakítását a következő ábra mutatja be.



37. ábra

A szlovák kiberbiztonsági szerezetek kapcsolatai

Forrás: Szlovákia 2015b, a szerző szerkesztése

Ezt követően a szlovák kormány 2016-ban a kiberbiztonsági koncepcióban meghatározott módon, az ott rögzített – és a fentiekben bemutatott – legfontosabb teendők és célkitűzések biztosítására, illetve azok implementációjára egy cselekvési tervet fogadott el.

A cselekvési terv tartalmazza mindazokat 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)

A cselekvési terv Szlovákia egyik legfontosabb olyan, a kibertérre vonatkozó dokumentuma, amely a 2016 és 2020 közötti időszakra meghatározott feladatokat megszabja. Ezek a feladatok a jogalkotás, a szabványok és szabályzók, a különböző kiberbiztonsági módszertanok, valamint a biztonsági politikák kialakítását foglalják magukban. Mindezeken túl a nemzetközi együttműködésre, a tudatosság növelésére és a kiberbiztonsági kapacitások növelésére is tartalmaz olyan utalásokat, amelyek alapján a kiberbiztonság magasabb szintje érhető el Szlovákiában. (Szlovákia 2016c)

A cselekvési terv a kiberbiztonsági koncepcióban megfogalmazott hét legfontosabb feladat analógiájára hét területet nevez meg, amelyek mindegyikén több részletesen kifejtett feladategyüttes végrehajtásával biztosíthatóak az eredetileg kitűzött célok. A területek és az azokon meghatározott feladategyüttesek mindegyikéhez felelős szervezetet, illetve a végrehajtásukhoz időintervallumokat is hozzárendel a dokumentum. (Szlovákia 2016c)

Vákát oldal

Összefoglaló
a könyvben bemutatott országok kiberbiztonsági stratégiáinak legfontosabb elemeiről

Amerikai Egyesült Államok	
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Department of Defense Cyber Strategy
Kiadás ideje:	2015
Kiberbiztonsági stratégiai célok:	• a kibertéri műveletek végrehajtásához szükséges készenléti erők és képességek kialakítása és fenntartása; • a védelmi minisztérium hálózatainak és adatainak védelme, valamint a műveletek során jelentkező kockázatok csökkentése; • olyan felderítő (hírszerzési), figyelmeztető, műveleti és együttműködési képességek kiépítése, amelyekkel még azelőtt lehet 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; • széles nemzetközi együttműködés és partnerség kialakítása.
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen
Kibertámadó képesség meghatározásra kerül-e:	Igen

Kína	
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

Oroszország	
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Az Orosz Föderáció információbiztonsági doktrínája
Kiadás ideje:	2016
Kiberbiztonsági stratégiai célok:	Katonai terület: • stratégiai elrettentés; • a fegyveres erők információbiztonsági rendszereinek és információs ellentevékenységi eszközeinek 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; • a külföldi nemzetbiztonsági szervezetekkel szembeni védelem növelése; • a 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; • az ország lakosságának erkölcsi és morális állapotának gyengítésére és aláásására irányuló információs tevékenységek hatásainak kivédése. Gazdasági terület: • 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	
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Osztrák Kiberbiztonsági Stratégia
Kiadás ideje:	2013
Kiberbiztonsági stratégiai célok:	• a biztonságos kibertér megteremtése, amelynek a kockázatok és veszélyek kezelése miatt megfelelően redundánsnak 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; • Ausztria kiberbiztonsági kultúra építésébe kezd; • a kiberbiztonság területén meglévő magán- és közszféra közötti párbeszédnek, valamint az új kezdeményezéseknek a digitális társadalom területén olyan pozitív hatásai vannak, amelyek többek között az üzleti befektetéseket is ösztönzik, így ezeket folytatni szükséges; • Ausztria folytatja a kiberbiztonság területén folytatott 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	
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, a NATO, az ENSZ és az 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; • a 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	
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; • a kibertámadásokat a hagyományos támadásokkal egyenértékűként kezeli; • a nemzetközi egyezményeket és szerződéseket betartja; • az ország alapértékeit – a demokráciát, a jogrendet, a szabadságot, az emberi jogokat és a szabadságot – 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	
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; • a nemzetközi együttműködés fokozása.
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen
Kibertámadó képesség meghatározásra kerül-e:	Nem

Franciaország	
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Francia Nemzeti Digitális Biztonság Stratégia
Kiadás ideje:	2015
Kiberbiztonsági stratégiai célok:	• alapvető érdek 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 környezete az ehhez szükségese iparpolitika támogatása, az export és a 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	
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Hollandia Kiberbiztonsági Menetrendje: Hollandia digitálisan biztonságos
Kiadás ideje:	2018
Kiberbiztonsági stratégiai célok:	A stratégia ambíciókat fogalmaz meg, amelyek 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

[71] A könyv megírásakor – 2018. január–október – a stratégia felülvizsgálata zajlott. Az új stratégia egyeztetés és szövegezés alatt állt.

Magyarország	
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Nemzeti Kiberbiztonsági Stratégia
Kiadás ideje:	2013[72]
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	
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 gyakorlatoknak a 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 tesztképességekkel kell rendelkezni; • a nemzeti potenciál és kompetencia növelése a kibertér biztonsága érdekében, amely magában 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, aminek 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

Lettország	
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Lettország Nemzeti Kiberbiztonsági Stratégiája 2014–2018
Kiadás ideje:	2014
Kiberbiztonsági stratégiai célok:	• a kiberbiztonság irányításának és erőforrásainak meghatározása és fejlesztése; • a kibertér jogi kereteinek meghatározása és a kiberbűnözés csökkentése; • válságkezelés; • tudatosság növelése, oktatás és kutatás fejlesztése; • nemzetközi együttműködés fejlesztése; • a kibertámadások megakadályozhatók, vagy azok bekövetkezése esetén a helyzet kezelhető; • széles nemzetközi együttműködés és partnerség kialakítása.
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen
Kibertámadó képesség meghatározásra kerül-e:	Nem

Litvánia	
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	796. számú Kormányrendelet (2011. június 29.) az elektronikus információs rendszerek 2011–2019 között történő fejlesztésére vonatkozó program elfogadásáról
Kiadás ideje:	2011
Kiberbiztonsági stratégiai célok:	A stratégiaként értelmezhető kormányrendelet három fő programpontja: az állami tulajdonú információforrások biztonságának növelése; • a kritikus információs infrastruktúrák hatékony működésének biztosítása; • a litván állampolgárok és a Litvániában tartózkodók kiberbiztonságának növelése.
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen
Kibertámadó képesség meghatározásra kerül-e:	Nem

Németország	
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: a digitális írástudás fejlesztése, amely során a kiberbiztonság tudatosság is fejleszthető; a biztonságos elektronikus kommunikáció és internetes szolgáltatások feltételeinek kialakítása; biztonságos elektronikus azonosítás az állampolgárok részére, amely magában foglalja egy elektronikus személyi igazolvány bevezetését is; információbiztonsági tanúsítványok iránti igény növelése; a kiberbiztonsági kutatások támogatása; • 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 együttműködés és ezen szolgáltatók bevonása a kiberbiztonság megteremtésébe; platform létrehozása a hatékony információcsere, sérülékenységek, veszélyek, kibertámadások és a védelem gyors biztosítására; • hatékony és fenntartható állami kiber-infrastruktúra: a Nemzeti Kiberreagáló 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

Szlovén Köztársaság	
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	Kiberbiztonsági Stratégia: egy rendszer kialakítása a kiberbiztonság magas szintjének biztosítására
Kiadás ideje:	2016
Kiberbiztonsági stratégiai célok:	A stratégia legfontosabb stratégiai célja 2020-ra egy olyan hatékony nemzeti kiberbiztonsági rendszer létrehozása, amely védelmet biztosít a kiberincidensekkel szemben. Ehhez nyolc részcélt rendel hozzá: • a nemzeti kiberbiztonsági rendszer megerősítése és szisztematikus szabályozása; • a polgárok biztonságának megteremtése a kibertérben; • a kiberbiztonság megteremtése a gazdaságban; • a kritikus infrastruktúrák működésének biztosítása azok információs rendszereinek támogatásán keresztül; • a kiberbiztonság megteremtése az állampolgárok tevékenysége során, valamint a kiberbűnözés elleni küzdelem fokozása; • a kibervédelmi képességek fejlesztése; • a kulcsfontosságú IKT-rendszerek biztonságos üzemeltetésének és rendelkezésre állásának biztosítása a legfontosabb természeti és egyéb katasztrófák esetén; • a kiberbiztonság növelése a nemzetközi együttműködés révén.
Kiberbiztonság megjelenik-e a nemzeti biztonsági stratégiában:	Igen
Kibertámadó képesség meghatározásra kerül-e:	Nem

Szlovák Köztársaság	
Jelenlegi nemzeti kiberbiztonsági stratégia címe:	A Szlovák Köztársaság kiberbiztonsági koncepciója 2015–2020
Kiadás ideje:	2015
Kiberbiztonsági stratégiai célok:	A legfontosabb célkitűzés mindazon kockázatok csökkentése, amelyek a kibertérből érkeznek, anélkül, hogy a kibertér 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 a magasabb szintű kockázatok kezelési kultúrájával 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

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	Kritikusinfrastruktúra-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	Kiberbűnözési 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 reagálócsoport

Rövidítés	Idegen nyelvű kifejtés	Magyar nyelvű kifejtés
CERT.LV	Computer Emergency Response Team Latvia	Lett számítógép-vészhelyzeti reagálócsoport
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 hálózat
CMF	Cyber Mission Force	Kiberműveleti csoport
CNA	Center for Naval Analyses	Haditengerészeti Kutatások Központja
CNDSP	Computer Network Defense Service Provider	Védelmi Minisztérium számítógéphálózat-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

Rövidítés	Idegen nyelvű kifejtés	Magyar nyelvű kifejtés
DNS	Domain Name Service	Domainnév-szolgáltatás
DoD	Department of Defense	USA Védelmi Minisztériuma
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 Központot
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

Rövidítés	Idegen nyelvű kifejtés	Magyar nyelvű kifejtés
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	Fájlátviteli protokoll
GCA	Global Cybersecurity Agenda	Globális Kiberbiztonsági Program
GCHQ	Government Communications Headquarters	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	Hypertext 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

Rövidítés	Idegen nyelvű kifejtés	Magyar nyelvű kifejtés
ICS	Industrial Command System	Ipari vezérlőrendszer
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team	Ipari Irányító Rendszerek Kibervészhelyzeti Reagáló Csoport
IDS	Intrusion Detection System	Behatolásdetektáló rendszer
IEC	International Electrotechnical Commission	Nemzetközi Elektrotechnikai Tanács
IG	Internet Governance	Internetirányítás
IGF	Internet Governance Forum	Internetirányítási 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 Távközlési Szervezet
ITU-D	ITU Development Sector	A Nemzetközi Távközlési Szervezet fejlesztésekért felelős ágazata
ITU-R	ITU Radiocommunication Sector	A Nemzetközi Távközlési Szervezet rádiókommunikációs ágazata
ITU-T	Telecommunication Standardisation Sector	A Nemzetközi Távközlési Szervezet telekommunikáció-egységesítésért és -szabványosításért felelős ágazata
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

Rövidítés	Idegen nyelvű kifejtés	Magyar nyelvű kifejtés
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
LRL IBEK	–	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 reagálócsoport
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 kiberincidens-reagáló képesség
NCP	National Cybercontingency Plan	Nemzeti kiberkészenléti terv
NCU	National Cyber Crime Unit	Nemzeti Kiberbűnözés Elleni Egység
NCSC	National Cyber Security Centre	Nemzeti Kiberbiztonsági Központ
NEGS	Nationalen E-Government-Strategie	Nemzeti E-Kormányzati Stratégia
NEIH	–	Nemzeti Elektronikus Információbiztonsági Hatóság

Rövidítés	Idegen nyelvű kifejtés	Magyar nyelvű kifejtés
NHS	National Health Service	Nemzeti Egészségügyi Szolgálat (brit)
NHTCU	National High Tech Crime Unit	Számítástechnikai Bűncselekmények Elleni Egység (holland)
NIPRNet	Nonsecure Internet Protocol Router Network	Nem Biztonságos Internetprotokoll-hálózat
NIS	Network and Information Systems	Hálózati és információs rendszer
NIST	National Institute of Standards and Technology	Nemzeti Szabványügyi és Technológiai Intézet
NKI	–	Nemzeti Kibervédelmi Intézet
NMT	National Mission Teams	Nemzeti Műveleti Csoportok
NOCP	National Offensive Cyber Programme	Nemzeti Kibertámadási Program
NSA	National Security Agency	Nemzetbiztonsági Ügynökség
NTG	–	Nemzeti Távközlési Gerinchálózat
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
PDSA	Plan-Do-Study-Act	Tervezés-cselekvés-tanulmányozás-beavatkozás
PLA	People's Liberation Army	Kínai 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 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 Committee	Republikánus Nemzeti (Választási) Tanács

Rövidítés	Idegen nyelvű kifejtés	Magyar nyelvű kifejtés
RPOC	Rządowy Program Ochrony Cyberprzestrzeni	Kormányzati kiberbiztonsági cselekvési terv
RSA	Rivest–Shamir–Adleman	Aszimmetrikus titkosító algoritmus (a megalkotók neveinek kezdőbetűiből alkotott rövidítés)
RTU	Remote Terminal Unit	Távoli elérést biztosító terminálok
SCADA	Supervisory Control and Data Acquisition	Felügyeleti, irányítás és ellenőrzés
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 Főparancsnoksága
SIGINT	Signals Intelligence	Rádióelektronikai felderítés
SI-CERT	Slovenian Computer Incident Response Team	Szlovén számítógép-vészhelyzeti incidenskezelő csoport
SIGOV-CERT	Sloven Governmental Computer Incident Response Team	Szlovén kormányzati számítógép-vészhelyzeti incidenskezelő csoport
SIPRNet	Secret Internet Protocol Router Network	Titkosított Internetprotokoll-hálózat
SOA	Service-Oriented Architecture	Szolgáltatásorientált architektúra
SOCTA	Serious and Organised Crime Threat Assessment	Súlyos és szervezett bűnözéssel kapcsolatos fenyegetésértékelés
SOVA	Slovenska obveščevalno-varnostna agencija	Szlovén Hírszerzési és Biztonsági Ügynökség
SPU	Strategy and Policy Unit	(Az ITU) Stratégiai és Politikai Egység(e)
SQL	Structured Query Language	Strukturált lekérdezőnyelv
SSH	Secure SHell	Nyilvános titkosítású protokollcsalád
SSL	Secure Sockets Layer	Biztonságos protokoll (szállítási réteg és alkalmazási réteg között)
ST	Support Team	Támogató Csoport

Rövidítés	Idegen nyelvű kifejtés	Magyar nyelvű kifejtés
SZTAKI	–	Számítástechnikai Automatizálási Kutatóintézet
SZVR	Szluzsba Vnyesnyej Razvedki	Külső Hírszerző Szolgálat
TLS	Transport Layer Security	Szállításiréteg-biztonság
UNDP	United Nations Development Programme	ENSZ Fejlesztési Programja
UK NISCC	United Kingdom National Infrastructure Co-ordination Center	Egyesült Királyság Nemzeti Infrastrukturális Biztonsági Koordinációs Központja
UNCTAD	United Nations Conference on Trade and Development	ENSZ Kereskedelmi és Fejlesztési Konferenciája
UNESCO	United Nations Educational, Scientific and Cultural Organization	ENSZ Nevelésügyi, Tudományos és Kulturális Szervezete
UPU	Universal Postal Union	ENSZ Egyetemes Postaegyesülete
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
WGIG	Working Group on Internet Governance	Internetirányítási Munkacsoport
WHO	World Health Organisation	ENSZ Nemzetközi Egészségügyi Szervezete
WSIS	World Summit on Information Society	Információs Társadalom Világ-csúcstalálkozó
ZITiS	Zentral Stelle für Informationstechnik im Sicherheitsbereich	Biztonsági szektor információtechnológiai központja

Vákát oldal

Illusztrációk jegyzéke

Vákát oldal

Táblázatok jegyzéke

Vákát oldal

Irodalomjegyzék

1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

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

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

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

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

39/2016. (XII. 21.) EMMI rendelet az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról

57/2016. (XI. 24.) HM–MvM–BM–KKM együttes utasítás a Nemzeti Biztonsági Stratégia felülvizsgálatára létrehozott munkacsoportról

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról

Annan, Kofi (2018): *Has information technology become a threat to democracy?* Forrás: www.kofiannanfoundation.org/supporting-democracy-and-elections-with-integrity/msc-technology-democracy/ (Letöltés ideje: 2018. 06. 11.)

ANSSI (2018): *Our Audiences and Our Activities*. Forrás: www.ssi.gouv.fr/en/mission/audiences-and-activities/ (Letöltés ideje: 2018. 06. 11.)

Ausztria (2013a): *Österreichische Sicherheitsstrategie. Sicherheit in einer neuen Dekade – Sicherheit gestalten.* Forrás: www.bmi.gv.at/502/files/130717_Sicherheitsstrategie_Kern_A4_WEB_barrierefrei.pdf (Letöltés ideje: 2018. 06. 11.)

Ausztria (2013b): *Austrian Security Strategy. Security in a New Decade – Shaping Decurity.* Forrás: www.bundesheer.at/pdf_pool/publikationen/sicherheitsstrategie_engl.pdf (Letöltés ideje: 2018. 06. 11.)

Ausztria (2013c): *Österreichische Strategie für Cyber Sicherheit.* Forrás: www.bmi.gv.at/504/files/130416_strategie_cybersicherheit_WEB.pdf (Letöltés ideje: 2018. 06. 11.)

Ausztria (2013d): *Austrian Cyber Security Strategy.* Forrás: www.digitales.oesterreich.gv.at/documents/22124/30428/AustrianCyberSecurityStrategy.pdf/35f1c891-ca99-4185-9c8b-422cae8c8f21 (Letöltés ideje: 2018. 06. 11.)

Az Európai Parlament és a Tanács 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

Az Európai Tanács határozata 2008/114/EC (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint a védelem javításának fokozásáról

Az Európai Tanács kerethatározata 2001/413/IB (2001. május 28.) a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről

Bencsik Balázs (2015): *GovCERT-Hungary bemutatása*. Előadás, Budapest, Nemzeti Kibervédelmi Intézet.

Biztonságpolitikai Szakkollégium (2010): *NATO stratégiai koncepciója 2010 a Biztonságpolitikai szakkollégium fordításában*. Forrás: www. o.biztonsagpolitika.hu/documents/1291766875_NATO_Strat_Koncepcio_2010_hun_BSZK.pdf (Letöltés ideje: 2018. 06. 11.)

BMI (2018): *Critical infrastructure protection*. Forrás: 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: jnslp.com/wp-content/uploads/2014/02/Easier-Said-than-Done.pdf (Letöltés ideje: 2018. 06. 11.)

Brzezinski, Zbigniew (1999): *A nagy sakktábla*. Budapest, Európa.

BSI (2018a): *Organisationsübersicht des BSI.* Forrás: www.bsi.bund.de/DE/DasBSI/Aufgaben/aufgaben_node.html (Letöltés ideje: 2018. 06. 11.)

BSI (2018b): *Organisational Chart*. Forrás: www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/org_chart_IFG_pdf.pdf?__blob=publicationFile&v=7 (Letöltés ideje: 2018. 06. 11.)

BSI-Gesetz (2009): *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG).* Forrás: www.gesetze-im-internet.de/bsig_2009/BSIG.pdf (Letöltés ideje: 2018. 06. 11.)

Burton, Joe (2018): *Cyber Deterrence: A Comprehensive Approach?* Forrás: ccdcoe.org/sites/default/files/multimedia/pdf/BURTON_Cyber_Deterrence_paper_April2018.pdf (Letöltés ideje: 2018. 06. 11.)

Butrimas, Vytautas (2015): *National Cyber Security Organisation: Lithuania.* CCDCOE, Tallinn. Forrás: ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_LITHUANIA_092015.pdf

Carr, Jefrrey (2011): *Inside Cyber Warfare: Mapping the Cyber Underworld.* 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: ccdcoe.org/history.html (Letöltés ideje: 2018. 06. 11.)

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. 06. 11.)

CERT (2017): *Authorized Users of "CERT".* Forrás: www.cert.org/incident-management/csirt-development/cert-authorized.cfm? (Letöltés ideje: 2018. 06. 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. 06. 11.)

China Law Translate (2015): *National Security Law.* Forrás: www.chinalawtranslate.com/2015nsl/?lang=en#_Toc423592311 (Letöltés ideje: 2018. 06. 11.)

CIA (2018): *The World Factbook: Central Asia: Russia.* Forrás: www.cia.gov/library/publications/the-world-factbook/geos/rs.html (Letöltés ideje: 2018. 06. 11.)

Clapper, James R. (2016): *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community. Senate Armed Services Committee*. Forrás: www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf (Letöltés ideje: 2018. 06. 11.)

CNN (2008): CNN Web site targeted. *CNN,* 2008. 04. 18. Forrás: edition.cnn.com/2008/TECH/04/18/cnn.websites/ (Letöltés ideje: 2018. 06. 11.)

Connell, Michael – Vogler, Sarah (2017): *Russia's Approach to Cyber Warfare.* CNA. Forrás: www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf (Letöltés ideje: 2018. 06. 11.)

Council of Europe (2001): *Concention on Cybercrime.* Forrás: www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (Letöltés ideje: 2017. 08. 25.)

Council of Europe (2017): *Chart of Signatures and Ratifications of Treaty 185.* Forrás: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (Letöltés ideje: 2017. 08. 25.)

Critical Foundations (1997): *Critical Foundations. Protecting America's Infrasctructures, The Report of the President's Commission on Critical Infrastructure Protection.* Forrás: www.nist.gov/sites/default/files/documents/2017/04/26/keyes_part2_032613.pdf (Letöltés ideje: 2018. 06. 11.)

Cseh Köztársaság (2015a): *Bezpečnostní strategie České republiky.* Forrás: www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf (Letöltés ideje: 2018. 06. 11.)

Cseh Köztársaság (2015b): *National Security Strategy of Czech Republic.* Forrás: www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf (Letöltés ideje: 2018. 06. 11.)

Cseh Köztársaság (2015c): *Národní strategie kybernetické bezpečnosti České republiky pro období od roku 2015 do roku 2020.* Forrás: www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf (Letöltés ideje: 2018. 06. 11.)

Cseh Köztársaság (2015d): *National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020.* Forrás: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (Letöltés ideje: 2018. 06. 11.)

Csiki Tamás (2008): A stratégiai dokumentumok rendszere. *Nemzet és Biztonság,* 1. évf. 8. sz. 76–81. Forrás: www.nemzetesbiztonsag.hu/cikkek/csiki_tamas-a_strategiai_dokumentumok_rendszere.pdf (Letöltés ideje: 2018. 06. 11.)

Denning, Dorothy E. (2001): *Is Cyber Terror Next?* Forrás: essays.ssrc.org/sept11/essays/denning.htm (Letöltés ideje: 2018. 06. 11.)

Department of Defense (2015): *The Department of Defense Cyber Strategy.* Forrás: www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (Letöltés ideje: 2018. 06. 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: nssarchive.us/wp-content/uploads/2018/01/2018-National-Defense-Strategy-Summary.pdf (Letöltés ideje: 2018. 06. 11.)

Department of Defense (2018b): *The Department of Defense Cyber Strategy.* Forrás: www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/ (Letöltés ideje: 2018. 06. 11.)

Department of Homeland Security (2018a): *Cybersecurity.* Forrás: www.dhs.gov/topic/cybersecurity (Letöltés ideje: 2018. 06. 11.)

Department of Homeland Security (2018b): *Cyber Incident Response.* Forrás: www.dhs.gov/cyber-incident-response (Letöltés ideje: 2018. 06. 11.)

DHS (2009): *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*. Forrás: https://www.energy.gov/sites/prod/files/cioprod/documents/Cyberspace_Policy_Review_final.pdf (Letöltés ideje: 2018. 06. 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. 06. 11.)

Egyesült Királyság (2010): *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* Forrás: assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf (Letöltés ideje: 2018. 06. 11.)

Egyesült Királyság (2011): *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world.* Forrás: assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (Letöltés ideje: 2018. 06. 11.)

Egyesült Királyság (2015): *National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom.* Forrás: 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. 06. 11.)

Egyesült Királyság (2016): *National Cyber Security Strategy 2016–2021.* Forrás: assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (Letöltés ideje: 2018. 06. 11.)

ENISA (2012): *National Cyber Security Strategies Practical Guide on Development and Execution*. Forrás: www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport (Letöltés ideje: 2018. 06. 11.)

ENISA (2014): *An Evaluation Framework for National Cyber Security Strategies.* Forrás: www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport (Letöltés ideje: 2018. 06. 11.)

ENISA (2016): *NCSS Good Practice Guide. Designing and Implementing National Cyber Security Strategies.* Forrás: www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport (Letöltés ideje: 2018. 06. 11.)

ENISA (2017a): *About Enisa.* Forrás: www.enisa.europa.eu/about-enisa (Letöltés ideje: 2018. 06. 11.)

ENISA (2017b): *Cyber Europe.* Forrás: www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme (Letöltés ideje: 2018. 06. 11.)

ENISA (2017c): *Enisa Strategy 2016–2020.* Forrás www.enisa.europa.eu/publications/corporate/enisa-strategy (Letöltés ideje: 2018. 06. 11.)

ENISA (2018): *National/governmental CERTs Baseline Capabilities.* Forrás: www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/baseline-capabilities (Letöltés ideje: 2018. 06. 11.)

Észtország (2010): *National Security Concept of Estonia.* Forrás: www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf (Letöltés ideje: 2018. 06. 11.)

Észtország (2011): *National Defence Strategy Estonia.* Forrás: www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf (Letöltés ideje: 2018. 06. 11.)

Észtország (2014a): *Küberjulgeoleku strateegia 2014–2017.* Forrás: www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf (Letöltés ideje: 2018. 06. 11.)

Észtország (2014b): *Cyber Security Strategy 2014–2017.* Forrás: www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf (Letöltés ideje: 2018. 06. 11.)

Europe 2020 Strategy (2010): *Europe 2020 – A European Strategy for Smart, Sustainable and Inclusive Growth.* Forrás: ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf (Letöltés ideje: 2018. 06. 11.)

European Commission (2013): *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.* Forrás: eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52013JC0001&from=HU (Letöltés ideje: 2018. 06. 11.)

European Commission (2015a): *A Digital Single Market for Europe*. Forrás: ec.europa.eu/commission/sites/beta-political/files/2-years-on-dsm_en_0.pdf (Letöltés ideje: 2018. 06. 11.)

European Commission (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: eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:52015DC0192 (Letöltés ideje: 2018. 06. 11.)

European Commission (2015c): *The European Agenda on Security.* Forrás: ec.europa.eu/anti-trafficking/sites/antitrafficking/files/eu_agenda_on_security_en.pdf (Letöltés ideje: 2018. 06. 11.)

European Commission (2017a): *Az Unió helyzetéről szóló 2017. évi beszéd – Kiberbiztonság: a Bizottság megerősíti a kibertámadásokkal szembeni uniós reagálási képességet.* Forrás: europa.eu/rapid/press-release_IP-17-3193_hu.htm (Letöltés ideje: 2018. 06. 11.)

European Commission (2017b): *Kiberbiztonsági reform Európában 2017.* Forrás: www.consilium.europa.eu/hu/policies/cyber-security (Letöltés ideje: 2018. 06. 11.)

European Commission (2017c): *Az európai digitális menetrend.* Forrás: europa.eu/european-union/file/1515/download_hu?token=BR0rWYPW (Letöltés ideje: 2018. 06. 11.)

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. 06. 11.)

Europol (2017b): *Strategic Analysis. Complementing Operational Analysis.* Forrás: www.europol.europa.eu/activities-services/services-support/strategic-analysis (Letöltés ideje: 2018. 06. 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. 06. 11.)

FireEye (2016): *Red Line Drawn: China Recalculates its Use of Cyber Espionage*. Forrás: www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf (Letöltés ideje: 2018. 06. 11.)

FireEye (2017): *Mandiant Consulting Services. Responding to the Most Critical Breaches and Empowering Companies to Protect their Key Assets.* Forrás: www.fireeye.com/content/dam/fireeye-www/global/en/services/pdfs/ds-mandiant-consulting-services.pdf (Letöltés ideje: 2018. 06. 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. 06. 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,* Vol. 2. No. 3. Forrás: cyberdefensereview.army.mil/Portals/6/Documents/CDR-FALL2017.pdf?ver=2017-11-21-092725-887 (Letöltés ideje: 2018. 06. 11.)

Franciaország (2013a): Livre blanc: Défense et sécurité nationale 2013. Forrás: www.defense.gouv.fr/content/download/206186/2286591/file/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf (Letöltés ideje: 2018. 06. 11.)

Franciaország (2013b): *French White Paper. Defence and National Security 2013.* Forrás: www.defense.gouv.fr/content/download/215253/2394121/file/White%20paper%20on%20defense%20%202013.pdf (Letöltés ideje: 2018. 06. 11.)

Franciaország (2014): *La politique de sécurité des systèmes d'information de l'État (PSSIE).* Forrás: www.ssi.gouv.fr/entreprise/reglementation/protection-des-systemes-dinformations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/ (Letöltés ideje: 2018. 06. 11.)

Franciaország (2015a): *Stratégie nationale pour la sécurité du numérique.* Forrás: www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf (Letöltés ideje: 2018. 06. 11.)

Franciaország (2015b): *French National Digital Security Strategy.* Forrás: www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf (Letöltés ideje: 2018. 06. 11.)

Franciaország (2017): *Defence and National Security Strategic Review 2017.* Forrás: 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. 06. 11.)

GAO (2013): *Report to Congressional Addressees. Cybersecurity. National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented.* Forrás: www.gao.gov/assets/660/652170.pdf (Letöltés ideje: 2018. 06. 11.)

Garamone, Jim (2018): *DoD Official: National Defense Strategy Will Enhance Deterrence.* Forrás: 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: cyberstability.org/about/ (Letöltés ideje: 2018. 06. 11.)

Google (2018): *Az Egyesült Államok, Kína, Oroszország, valamint Németország, Franciaország és az Egyesült Királyság nemzeti összterméke közötti alakulása 1990 és 2015 között.* Forrás: https://www.google.com/publicdata/explore?ds=d5bncppjof8f9_&met_y=ny_gdp_mktp_cd&hl=hu&dl=-hu#!ctype=l&strail=false&bcs=d&nselm=h&met_y=ny_gdp_mktp_cd&scale_y=lin&ind_y=false&rdim=region&idim=country:USA:CHN:-DEU:GBR:FRA:RUS&ifdim=region&hl=hu&dl=hu&ind=false (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.* London, Routledge.

Harold, Scott W. (2016): The U.S.-China Cyber Agreement: A Good First Step. *RAND Blog.* Forrás: www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html (Letöltés ideje: 2018. 06. 11.)

Havass Miklós – Lengyel Veronika szerk. (1999): *Magyar válasz az Információs Társadalom kihívásaira. Szakértői anyag.* Forrás: members.iif.hu/lengyel/valasz (Letöltés ideje: 2017. 08. 25.)

Heath, Timothy R. – Gunness, Kristen – Coope, Cortez A. (2016): *The PLA and China's Rejuvenation. National Security and Military Strategies, Deterrence Concepts, and Combat Capabilities.* RAND Corporation. Forrás, www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1402/RAND_RR1402.pdf (Letöltés ideje: 2018. 06. 11.)

Hollandia (2011): *The National Cyber Security Strategy (NCSS).* Forrás: english.nctv.nl/binaries/cyber-security-strategy-uk_tcm32-83648.pdf (Letöltés ideje: 2018. 06. 11.)

Hollandia (2013a): *Nationale Cybersecurity Strategie. Van bewust naar bekwaam.* Forrás: www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2/rapport-nationale-cybersecurity-strategie-2-2.pdf (Letöltés ideje: 2018. 06. 11.)

Hollandia (2013b): *National Cyber Security Strategy 2. From awareness to capability.* Forrás: Forrás: english.nctv.nl/binaries/national-cyber-security-strategy-2_tcm32-84265.pdf (Letöltés ideje: 2018. 06. 11.)

Hollandia (2018a): *Wereldwijd voor een veilig Nederland. Geïntegreerde Buitenland- en Veiligheidsstrategie 2018–2022.* Forrás: www.eerstekamer.nl/overig/20180327/_wereldwijd_voor_een_veilig/document3/f=/vkn0m270yrz6.pdf (Letöltés ideje: 2018. 06. 11.)

Hollandia (2018b): *Cyber Security Raad: Over de CSR.* Forrás: www.cybersecurityraad.nl/005_OverdeCSR/index.aspx (Letöltés ideje: 2018. 06. 11.)

Hollandia (2018c): *National Cyber Security Centrum: Incident Response.* Forrás: www.ncsc.nl/english/Incident+Response/24-hour-support.html (Letöltés ideje: 2018. 06. 11.)

Hollandia (2018d): *Nederlandse Cybersecurity Agenda. Nederland digitaal veilig.* Forrás: www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig/CSAgenda_def_web.pdf (Letöltés ideje: 2018. 06. 11.)

HSD Foundation (2018): *Minister Grapperhaus Launched the Dutch Cyber Security Agenda*. Forrás: www.thehaguesecuritydelta.com/news/newsitem/1072-minister-grapperhaus-launched-the-dutch-cyber-security-agenda (Letöltés ideje: 2018. 06. 11.)

HSDL (2018): *National Strategy Documents*. Forrás: www.hsdl.org/?collection&id=4 (Letöltés ideje: 2018. 06. 11.)

ICANN (2018): *The IANA Functions. An Introduction to the Internet Assigned Numbers Authority (IANA) Functions.* Forrás: www.icann.org/en/system/files/files/iana-functions-18dec15-en.pdf (Letöltés ideje: 2018. 06. 11.)

ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements.

ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements.

ITU (2003a): *World Summit on the Information Society (WSIS).* Forrás: www.itu.int/net/wsis/basic/about.html (Letöltés ideje: 2018. 06. 11.)

ITU (2003b): *Declaration of Principles. Building the Information Society: a global challenge in the new Millennium.* Forrás: www.itu.int/net/wsis/docs/geneva/official/dop.html (Letöltés ideje: 2018. 06. 11.)

ITU (2003c): *Plan of Action.* Forrás: www.itu.int/net/wsis/docs/geneva/official/poa.html (Letöltés ideje: 2018. 06. 11.)

ITU (2005): *Tunis Agenda for the Information Society.* Forrás: www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (Letöltés ideje: 2018. 06. 11.)

ITU (2017a): *About International Telecommunication Union (ITU).* Forrás: www.itu.int/en/about/Pages/default.aspx (Letöltés ideje: 2018. 06. 11.)

ITU (2017b): *Definition of Cybersecurity.* Forrás: www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (Letöltés ideje: 2018. 06. 11.)

ITU (2018): *Global Cybersecurity Agenda (GCA).* Forrás: www.itu.int/en/action/cybersecurity/Pages/gca.aspx (Letöltés ideje: 2018. 06. 11.)

Ivanov, Anton – Mamedov, Orkhan (2017): *In ExPetr/Petya's shadow, FakeCry ransomware wave hits Ukraine.* Forrás: securelist.com/in-expetrpetyas-shadow-fakecry-ransomware-wave-hits-ukraine/78973 (Letöltés ideje: 2018. 06. 25.)

Jacobs, Andrew (2009): China Fears Ethnic Strife Could Agitate Uighur Oasis. *New York Times,* 2009. 06. 22. Forrás: www.nytimes.com/2009/07/23/world/asia/23kashgar.html?scp=1&sq=Uighur%20internet%20&st=cse (Letöltés ideje: 2018. 06. 11.)

KIBEV (2018): *Célok és alapvetések.* Forrás: www.kibev.hu/ (Letöltés ideje: 2018. 06. 11.)

Klimburg, Alexander ed. (2012): *National Cyber Security. Framwork Manual.* Tallin, NATO CCDCOE. Forrás: ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (Letöltés ideje: 2018. 06. 11.)

Kormányzati Eseménykezelő Központ (2009): *PTA CERT-Hungary Központ, mint Nemzeti Hálózatbiztonsági Központ.* Forrás: www.cert-hungary.hu/node/65 (Letöltés ideje: 2018. 06. 11.)

Kormányzati Eseménykezelő Központ (2017): *Magunkról.* Forrás: www.cert-hungary.hu/node/1 (Letöltés ideje: 2018. 06. 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. 06. 11.)

Kovács László (2009a): Információs hadviselés kínai módra. *Nemzet és Biztonság,* 2. évfolyam 7. szám (Letöltés ideje: 2018. 06. 11.)

Kovács László (2009b): Obama's New Cybersecurity Policy. *Hadtudományi Szemle,* 2. évf. 3. sz. Forrás: archiv.uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2009/2009_3/2009_3_hm_kovacs_laszlo_15_20.pdf (Letöltés ideje: 2018. 06. 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 évf. 1. sz. Forrás: www.hadmernok.hu/171_17_kovacs.pdf (Letöltés ideje: 2018. 06. 11.)

Lengyelország (2014a): S*trategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Forrás*: www.bbn.gov.pl/ftp/SBN%20RP.pdf (Letöltés ideje: 2018. 06. 11.)

Lengyelország (2014b): *National Security Strategy of the Republic Of Poland.* Forrás: www.bbn.gov.pl/ftp/dok/NSS_RP.pdf (Letöltés ideje: 2018. 06. 11.)

Lengyelország (2017a): K*rajowe ramy polityki bezpieczeństwa cybernetycznego Rzeczypospolitej Polskiej na lata 2017–2022.* Forrás: 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. 06. 11.)

Lengyelország (2017b): *National Framework of Cybersecurity Policy of the Republic Of Poland for 2017–2022.* Forrás: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf (Letöltés ideje: 2018. 06. 11.)

Lettország (2014): *Cyber Security Strategy of Latvia 2014–2018.* Forrás: 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. 06. 11.)

Lettország (2015): *The National Security Concept (informative section).* Forrás: www.mod.gov.lv/~/media/AM/Par_aizsardzibas_nozari/Plani,%20koncepcijas/NDK/NDK_ENG_final.ashx (Letöltés ideje: 2018. 06. 11.)

Lettország (2018): *Ministry of Defence of Republic of Latvia. The National Security Concept of the Republic of Latvia.* Forrás: www.mod.gov.lv/Par_aizsardzibas_nozari/Politikas_planosana/Koncepcijas/Nac_dros.aspx (Letöltés ideje: 2018. 06. 11.)

Liang, Qiao – Xiangsui, Wang (2002): *Unrestricted Warfare: China's Masterplan to Destroy America.* Panamy City, Pan American Publishing Company.

Lindsay, Jon R. – Ming, Cheung Tai – Reveron, Derek S. (eds.) (2015): *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain.* Oxford, 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: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (Letöltés ideje: 2018. 06. 11.)

Litvánia (2017): *National Security Strategy of the Republic of Lithuania*. Forrás: kam.lt/download/57457/2017-nacsaugstrategijaen.pdf (Letöltés ideje: 2018. 06. 11.)

Magyar Információs Társadalom Stratégia – MITS (2003) Forrás: itf.njszt.hu/23r4r23r/uploads/2013/08/MITS-magyar.pdf (Letöltés ideje: 2018. 06. 11.)

Microsoft (2018): A Digital Geneva Convention to protect cyberspace. *Microsoft Policy Papers*. Forrás: query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH (Letöltés ideje: 2018. 06. 11.)

Military Balance (2018): *The Military Balance 2018: Chapter 5. Russia-Eurasia.* Forrás: www.iiss.org/en/publications/military%20balance/issues/the-military-balance-2018-545f/mb2018-05-russia-eurasia-dcce (Letöltés ideje: 2018. 06. 11.)

Miller, Alice (é. n.): The CCP Central Committee's Leading Small Groups. *China Leadership Monitor,* No. 26. Forrás: www.hoover.org/sites/default/files/uploads/documents/CLM26AM.pdf (Letöltés ideje: 2018. 06. 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. 06. 11.)

MOD PRC (2015): *National Security Law of the People's Republic of China (2015).* Forrás: eng.mod.gov.cn/publications/2017-03/03/content_4774229.htm (Letöltés ideje: 2018. 06. 11.)

MOD PRC (2018): *Central Military Commission.* Forrás: eng.mod.gov.cn/leadership/index.htm (Letöltés ideje: 2018. 06. 11.)

Moen, Ronald (é. n.): *Foundation and History of the PDSA Cycle*. Forrás: deming.org/uploads/paper/PDSA_History_Ron_Moen.pdf (Letöltés ideje: 2018. 06. 11.)

MTI – Origó (2009): Kína ideiglenesen letiltotta a Hotmailt, a BBC-t és a CNN-t is. *Origó,* 2009. 06. 3. Forrás: www.origo.hu/nagyvilag/20090603-internet-es-tevekorlatozas-kinaban-a-tienanmen-teri-verengzes-evfordulojan.html (Letöltés ideje: 2018. 06. 11.)

Munk Sándor (2018): A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* 28. évf. 1. sz. 113–131.

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: 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. 06. 11.)

Nádudvari Anna (2018): A 2017-es francia stratégiai felülvizsgálat eredménye. *Stratégiai Védelmi Kutatóközpont Elemzések,* 2018/12.

NATO (2002): *Prague Summit Declaration.* Forrás: www.nato.int/cps/en/natohq/official_texts_19552.htm (Letöltés ideje: 2018. 06. 11.)

NATO (2009): *Allied Joint Doctrine for Information Operations.* AJP-3.10. Forrás: info.publicintelligence.net/NATO-IO.pdf (Letöltés ideje: 2018. 06. 11.)

NATO (2010): *A NATO-tagállamok állam- és kormányfői által Lisszabonban elfogadott Stratégiai Koncepció az Észak-atlanti Szerződés Szervezete tagállamainak védelméért és biztonságáért. Aktív szerepvállalás, modern védelem.* Forrás: 2010-2014.kormany.hu/download/b/52/20000/nato_strategiai_koncepcio.pdf (Letöltés ideje: 2018. 06. 11.)

NATO (2012): *Chicago Summit Declaration.* Forrás: www.nato.int/cps/en/SID-D95FAE1D-99C8ECE1/natolive/official_texts_87593.htm (Letöltés ideje: 2018. 06. 11.)

NATO (2016a): *Warsaw Summit Communiqué.* Forrás: www.nato.int/cps/en/natohq/official_texts_133169.htm (Letöltés ideje: 2018. 06. 11.)

NATO (2016b): *Cyber Defence Pledge.* Forrás: www.nato.int/cps/su/natohq/official_texts_133177.htm (Letöltés ideje: 2018. 06. 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: www.nato.int/cps/en/natohq/opinions_148417.htm (Letöltés ideje: 2018. 06. 11.)

NATO (2018): *Cyber Defence.* Forrás: www.nato.int/cps/en/natolive/topics_78170.htm (Letöltés ideje: 2018. 06. 11.)

Németország (2009): *National Strategy for Critical Infrastructure Protection (CIP Strategy).* Forrás: www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1 (Letöltés ideje: 2018. 06. 11.)

Németország (2011): *Cyber Security Strategy for Germany.* Forrás: www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile (Letöltés ideje: 2018. 06. 11.)

Németország (2015): *Nationale E-Government-Strategie Fortschreibung 2015.* Forrás: 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: www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf (Letöltés ideje: 2018. 06. 11.)

Németország (2016b): *Cyber-Sicherheitsstrategie für Deutschland 2016. Forrás:* www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (Letöltés ideje: 2018. 06. 11.)

Nemzeti Infokommunikációs Stratégia (2014): *Az infokommunikációs szektor fejlesztési stratégiája (2014–2020) v7.0.* Forrás: 2010-2014.kormany.hu/down-

load/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf (Letöltés ideje: 2018. 06. 11.)

Nemzeti Információs Társadalom Stratégia NITS (2001). Forrás: itf.njszt.hu/23r4r23r/uploads/2013/08/nits_kesz.doc (Letöltés ideje: 2018. 06. 11.)

NIS Directive (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,* No. 10. CCDCOE. Forrás: ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper_10_2018.pdf (Letöltés ideje: 2018. 06. 11.)

Orosz Föderáció (2015): *Стратегия национальной безопасности Российской Федерации.* Forrás: static.kremlin.ru/media/events/files/ru/l8iXkR8XLAtxeilX7JK3XXy6Y0AsHD5v.pdf (Letöltés ideje: 2018. 06. 11.)

Osula, Anna-Maria (2015): *National Cyber Security Organisation: Estonia.* CCDCOE. Forrás: ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ESTONIA_032015_1.pdf (Letöltés ideje: 2018. 06. 11.)

Pagliery, Jose (2015): Sniper attack on California power grid may have been ‚an insider,' DHS says. *CCN Tech,* 2015. 10. 17. Forrás: money.cnn.com/2015/10/16/technology/sniper-power-grid/index.html (Letöltés ideje: 2018. 06. 11.)

Raud, Mikk (2016): *China and Cyber: Attitudes, Strategies, Organisation.* Tallinn, CCDCOE. Forrás: ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf (Letöltés ideje: 2018. 06. 11.)

Roszijszakaja Gazeta (2014): *Военная доктрина Российской Федерации.* Forrás: rg.ru/2014/12/30/doktrina-dok.html (Letöltés ideje: 2018. 06. 11.)

Rothenpieler, Samuel (2016): *National Cyber Security Strategy 2016.* Forrás: www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/april-2017/170426-bsi-enisa-nlo-presentation-v2.pdf (Letöltés ideje: 2018. 06. 11.)

Russian Ministry of Foreign Affairs (2016): *Doctrine of Information Security of the Russian Federation*. Forrás: www.mid.ru/en/foreign_policy/official_

documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 (Letöltés ideje: 2018. 06. 11.)

Sanger, David E. – Perlroth, Nicole (2014): N.S.A. Breached Chinese Servers Seen as Security Threat. *New York Times,* 2014. 03. 22. Forrás: www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=0 (Letöltés ideje: 2018. 06. 11.)

SANS (2016): *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Forrás: ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (Letöltés ideje: 2017. 08. 25.)

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: www.schneier.com/blog/archives/2012/06/cyberwar_treati.html (Letöltés ideje: 2018. 06. 11.)

Der Spiegel (2007): Innenministerium bestreitet Schäden durch Hackerangriffe. *Der Spiegel,* 2007. 08. 25. Forrás: www.spiegel.de/netzwelt/tech/infizierte-regierungscomputer-innenministerium-bestreitet-schaeden-durch-hackerangriffe-a-502008.html (Letöltés ideje: 2018. 06. 11.)

Der Spiegel (2013): Cyber-Spionage Chinesische Hacker greifen EADS und ThyssenKrupp an. *Der Spiegel,* 2013. 02. 24. Forrás: www.spiegel.de/netzwelt/web/it-sicherheit-chinesische-hacker-greifen-eads-und-thyssenkrupp-an-a-885189.html (Letöltés ideje: 2018. 06. 11.)

Stratcom (2018): *United States Cyber Command.* Forrás: www.stratcom.mil/Portals/8/Documents/CYBERCOM_Fact_Sheet.pdf (Letöltés ideje: 2018. 06. 11.)

Szlovákia (2015a): *Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015–2020.* Forrás: www.nbusr.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf (Letöltés ideje: 2018. 06. 11.)

Szlovákia (2015b): *Cyber Security Concept of the Slovak Republic for 2015–2020.* Forrás: www.nbusr.sk/wp-content/uploads/cyber-security/Cyber-Security-

Concept-of-the-Slovak-Republic-for-2015-2020.pdf (Letöltés ideje: 2018. 06. 11.)

Szlovákia (2016a): *Biela kniha o obrane Slovenskej republiky*. Forrás: www.mod.gov.sk/data/BKO2016_LQ.pdf (Letöltés ideje: 2018. 06. 11.)

Szlovákia (2016b): *White Paper on Defence of the Slovak Republic*. Forrás: www.mosr.sk/data/WPDSR2016_LQ.pdf (Letöltés ideje: 2018. 06. 11.)

Szlovákia (2016c): *Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015–2020.* Forrás: 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. 06. 11.)

Szlovénia (2010): *Resolucija o strategiji nacionalne varnosti Republike Slovenije – Resolution ont he National Security Strategy of the Republic of Slovenia*. Forrás: www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/ministrstvo/RSNV2010_slo_en.pdf (Letöltés ideje: 2018. 06. 11.)

Szlovénia (2016): *Cyber Security Strategy. Establishing a System to Ensure a Highl Level of Cyber security.* Forrás: www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (Letöltés ideje: 2018. 06. 11.)

Takács, Dávid (2017): Ukraine's deterrence failure: Lessons for the Baltic States. *Journal on Baltic Security,* Vol. 3. No. 1. 1–10.

Talyigás Judit szerk. (2000): *Tézisek az információs társadalomról.* Budapest, Miniszterelnöki Hivatal. Forrás: www.artefaktum.hu/kozgaz/tezisek.html (Letöltés ideje: 2018. 06. 11.)

United Nations (2013): *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* Forrás: www.un.org/ga/search/view_doc.asp?symbol=A/68/98 (Letöltés ideje: 2018. 06. 11.)

United Nations (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: repository.un.org/bitstream/handle/11176/158448/A_69_723-EN.pdf?sequence=3&isAllowed=y (Letöltés ideje: 2018. 06. 11.)

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: 2017. 08. 25.)

US DoD Cybersecurity Strategy (2015): *The DoD Cyber Strategy*. Forrás: www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (Letöltés ideje: 2018. 06. 11.)

USCC (2008): *2008 Report to Congress of the U.S.-China Economic and Security Review Commission One Hundred Tenth Congress Second Session.* Washington, U.S. Government Printing Office. Forrás: www.uscc.gov/sites/default/files/annual_reports/2008-Report-to-Congress-_0.pdf (Letöltés ideje: 2018. 06. 11.)

USCC (2015): *2015 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: www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF (Letöltés ideje: 2018. 06. 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: www.uscc.gov/sites/default/files/annual_reports/2017_Annual_Report_to_Congress.pdf (Letöltés ideje: 2018. 06. 11.)

Valeriano, Brandon – Jensen, Benjamin – Maness, Ryan C. (2018): *Cbyer Strategy: The Evolving Charachter of Power and Coercion*. Oxford, Oxford University Press.

Wamala, Frederick (2011): *The ITU National Cybersecurity Strategy Guide.* Forrás: www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf (Letöltés ideje: 2018. 06. 11.)

White House (2017): *National Security Strategy of the United States of America*. Forrás: www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (Letöltés ideje: 2018. 06. 11.)

Wong, Edward (2015): China Approves Sweeping Security Law, Bolstering Communist Rule. *New York Times,* 2015. 07. 01. Forrás: www.nytimes.com/2015/07/02/world/asia/china-approves-sweeping-security-law-bolstering-communist-rule.html (Letöltés ideje: 2018. 06. 11.)

ZITiS (2018): *Über Uns.* Forrás: www.zitis.bund.de/DE/ZITiS/Ueber_Uns/ueber_uns_node.html;jsessionid=96BB2385345B065ED4537A388F651F6F.2_cid377 (Letöltés ideje: 2018. 06. 11.)

Vákát oldal

A Dialóg Campus Kiadó
a Nemzeti Közszolgálati Egyetem könyvkiadója.

Nordex Nonprofit Kft. – Dialóg Campus Kiadó
www.dialogcampus.hu
www.uni-nke.hu
1083 Budapest, Ludovika tér 2.
Telefon: (30) 426 6116
E-mail: kiado@uni-nke.hu
A kiadásért felel: Petró Ildikó ügyvezető

Felelős szerkesztő: Kilián Zsolt
Olvasószerkesztő: Tóth Anikó
Korrektor: Sós Dóra Gabriella
Tördelőszerkesztő: Stubnya Tibor
Nyomdai kivitelezés: Pátria Nyomda Zrt.
Felelős vezető: Simon László vezérigazgató

ISBN 978-615-5920-92-9 (nyomtatott)
ISBN 978-615-5920-93-6 (elektronikus)

A fejlett országok stratégiai szinten keresik a választ a kibertérben megjelenő kihívásokra és veszélyekre, hiszen a digitális rendszerek és szolgáltatások zavartalan működési környezetének garantálása mára egyre inkább állami feladattá vált. A kiberbiztonsági stratégiák kialakítása során a klasszikus információbiztonság mellett ma már olyan tényezőket is figyelembe kell venni, mint például a kiberhadviselés, vagy akár a kiberelrettentés. Könyvünk megvizsgálja három nagyhatalom – az Egyesült Államok, Kína és Oroszország – viszonyát a kibertérhez, de kitér az olyan nemzetközi politikai, illetve katonai szövetségek, mint az Európai Unió és a NATO, valamint számos európai kis, közepes és nagy ország kiberbiztonságról alkotott stratégiai elképzeléseire is. Ezek bemutatását az adott ország nemzeti biztonsági stratégiájának kontextusába helyezve úgy elemzi, hogy eközben a kiberbiztonságot megvalósítani hivatott egyes szervezetek működésébe is bepillantást enged.

A kiadvány
a KÖFOP-2.1.2-VEKOP-15-2016-00001
„A jó kormányzást megalapozó
közszolgálat-fejlesztés” című projekt
keretében került kiadásra.