Közszolgálati Nemzetközi Képzési Központ

21. századi biztonsági kihívások

Kiberbiztonság - kibervédelem

Csiki Tamás

Tankönyvfejezet alapanyag

Nemzeti Közszolgálati Egyetem 2013.

Nemzeti Közszolgálati Egyetem
Postacím: 1581 Budapest, Pf.: 15.
Cím: 1101 Bp., Hungária krt. 9-11.,
Telefon: +36(1)432-9000
Web: www.uni-nke.hu

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Tartalom

Kiberbiztonság és kibervédelem

A kiberbiztonság kérdései a 21. században eddig a nemzetközi terrorizmus mellett leggyorsabban és legjelentősebb mértékben előtérbe kerülő fenyegetésként jelentek meg mind a nemzetállamok, mind a nemzetközi szervezetek – egyúttal pedig a gazdasági szereplők és a társadalmak napirendjén is. Ez abból a komplexitásból és sokszínűségből ered, amely a digitális kor infokommunikációs társadalmának mindennapjait, az alapvető társadalmi alrendszerek adat- és információ alapú működését jellemzik. Azóta, hogy 1984-ben William Gibson Neuromancer (Neurománc) című tudományos-fantasztikus regényében megalkotta a „kibertér" fogalmát, a modern és posztmodern társadalmak olyan mértékben váltak függővé a digitális technológiáktól, hogy ma már az egyik legkiemelkedőbb fenyegetésként jelenik meg e rendszerek működésének megzavarása, az adatokkal és információval való visszaélések.

1. Kibertér

Amennyiben könnyen kezelhető meghatározást kívánunk adni, akkor ***a kibertér az a környezet, amelyben a digitális információ (adat) technikai eszközökön (számítógépes hálózatokon) keresztül áramlik.*** Mindazonáltal jeleznünk kell, hogy a definíciós kérdések a kibertér, kiberbiztonság, kibervédelem, kiberhadviselés, kiberbűnözés stb. fogalmak esetében nem csupán rendkívül összetettek, hanem jelentős mértékben vitatottak is annak függvényében, hogy ezeket milyen megközelítésben és ki kívánja definiálni. A kibertér használatával és kiberbiztonság kérdéseivel kapcsolatban legalább ***az alábbi, egymással is átfedésben lévő „felhasználói dimenziókat" érdemes szem előtt tartani: a civil és a katonai szféra felhasználói; a magánszféra és a közszféra (állami szféra) felhasználói, valamint a gazdasági szereplők; állami és nem állami szereplők.*** Tehát tisztában kell lennünk azzal, hogy ez az összetett jellemzőkkel bíró környezet számos szereplőjével és eltérő viszonyrendszereiben más-más értelmezést és jelentőséget nyerhet.

Éppen ezért szükséges összetettebb meghatározásokkal is tisztában lennünk, amelyek érzékeltetik e sokszínűséget. Így például Haig Zsolt és Várhegyi István fogalmi kérdéseket tisztázó cikke értelmében „a civil terminológia szerint a kibertér az elektronikus kommunikációs eszközök és rendszerek (számítógép-hálózatok, telefonvonalak, műholdas rendszerek stb.) és a rajtuk található szolgáltatások, információk alkotta virtuális tér vagy világ összefoglaló neve." Ugyanakkor „a kibertér katonai értelmezése ettől eltérő, jóval tágabb. Az USA Nemzeti Katonai Stratégia a Kibertéri Műveletekhez (National Military Strategy for

Cyberspace Operations) c. dokumentuma szerint a kibertér egy olyan tartomány, ahol hálózatos rendszerekben működő elektronikai eszközöket és az elektromágneses spektrumot használják fel az adatok tárolására, cseréjére és módosítására."

Azért kell tudatosan foglalkoznunk a kibertérben tevékenykedő valamennyi szereplővel, mert ***ebben az új „globális közös térben" az egyes szereplők különböző célokkal tevékenykednek, és eltérő lehetőségekkel rendelkeznek***. A fent jelzett „felhasználói dimenziók" önkényesen létrehozott kategóriákat jelentenek, és csupán arra szolgálnak, hogy a kibertérben tevékenykedő szereplők sokszínűségét szemléltessék. E szereplők ugyanis egyszer aktív félként, például szabályozó hatóságként jelenhetnek meg (az állam), máskor viszont passzív félként, például a kormányzati infokommunikációs infrastruktúra elleni támadás alanyaként. Hasonlóképpen: a kibertérben folytatott bármely tevékenység nem egyirányú és abszolút, hanem minden esetben más szereplők felé irányuló (akár szándékosan, akár nem), és mindig relatív, azaz választ és reakciót vált ki, és attól függően képes érvényesülni.

Ha abból indulunk ki, hogy globális jelentőségű közegről van szó – amely e tekintetben hasonlatos a világtengerekhez, melyek szabad használata a világkereskedelem biztonságos áramlása szempontjából nélkülözhetetlen –, logikus lenne feltételezni, hogy a kibertér használatának „alapszabályait" is lefektették. ***Az átfogó és univerzális nemzetközi szabályozás azonban éppúgy hiányzik, mint a pontos definíciók.*** Ez a szabályozatlanság a kibertér sajátos jellemzőivel magyarázható: decentralizált, internet-alapú, nemzetközi infokommunikációs térről beszélünk, amely lehetőséget biztosít a legkülönfélébb tevékenységekre a pénzügyi szolgáltatásoktól a hírszolgáltatásig és a közösségi oldalak működtetéséig, a gazdasági ellátórendszerek irányításától a katonai műveletek támogatásáig.

Az internet létrejöttének és globális elterjedésének alapja a felhasználók bizalma, azaz hogy csatlakoztatják személyi számítógépeiket (vagy más eszközeiket) egy globális hálózathoz, ahol fizikai valójukban nem ismerhetik meg azokat, akikkel interakciókat folytatnak, mégis bíznak abban, hogy nem éri őket sérelem, kár vagy hátrány a másik féllel folytatott interakcióból. Így az infokommunikációs hálózatokra épülő kibertérnek is alapvető jellemzője, hogy a „felhasználók" nem határozhatók meg a hagyományos identitás-fogalmak szerint, és tetteik sem követhetőek nyomon a hagyományos értelemben. Mindennek ellenére az internet globális hálózattá fejlődésének fő mozgatórugója a tevékenységek szabadsága volt az elmúlt évtizedekben, és ezért a szabályozást – legyen az akár globális, akár nemzetállami – a „felhasználók" jelentős része nem tekinti előnyösnek, mert korlátozná az eddig élvezett szabadságot – míg mások csupán a szabályozás jellegéről, mértékéről nem tudnak megegyezni.

A szabályozatlansággal és szabadsággal szemben a „felhasználók" sebezhetősége áll. Mivel az internet globális hálózata ma már lehetővé teszi, hogy lényegében bárki, szinte bárhol olcsón, előzetes ellenőrzés nélkül kapcsolatot tudjon létesíteni az infokommunikációs hálózatokon keresztül bármilyen informatikai rendszerrel, vagy bármely felhasználóval, afelől sem lehet kétségünk, hogy megfelelő képzettséggel bármilyen az internethez kapcsolódó hálózatba, infokommunikációs eszközbe be lehet hatolni és hozzá lehet férni az ott tárolt adatokhoz, befolyásolni lehet annak alkalmazásait, működését. Ezeknek a sebezhető hálózatoknak a védelme az ellenőrzés és szabályozás fokozásával növelhető, amely által jobban kiszűrhetővé válhatnak a káros tevékenységet kifejtő „felhasználók". Mindez azonban ellentmond az internet alapvető dinamikájának, és a manipuláció, illetve a szabadságjogok (például a véleménynyilvánítás szabadsága, a média területén a sajtószabadság) korlátozásának veszélyérzetét ébreszti a felhasználók egyes köreiben.

2. Kiberbiztonság – kibervédelem

A kibertér fogalmához kapcsolódik, és ugyancsak számos szempontból megközelíthető a ***kiberbiztonság***, amely – ismét könnyen kezelhető meghatározást keresve – definiálható a következőképpen: ***mindazon infokommunikációs eszközök, rendszerek és technológiák biztonságos és zavartalan működése, amelynek révén garantált az ezeken tárolt adatok és információk bizalmassága, sérthetetlensége, megbízhatósága és rendelkezésre állása.*** Mint ahogy a kibertér „felhasználói" között is számtalan állami és nem állami szereplőt találhatunk, a biztonságosan működtetett rendszerek körét sem érdemes kizárólag állami/kormányzati rendszerekre szűkíteni, ugyanis a kiberbiztonság – a kibertér biztonságos használatának – igénye minden gazdasági és magánszereplő részéről is fennáll. Az államok szerepe a fent említett szabályozás kérdésében azonban azért nagyobb, mert a szabályozó joghatóság és a legjelentősebb erőforrások az állami szereplők – esetenként nemzetközi szervezetek, mint például az Európai Unió vagy a NATO – kezében vannak.

A kiberbiztonság fogalmából eredően a kibertámadás és a kibervédelem fogalma is levezethető, miszerint ***a kibertámadás olyan tevékenység, amely meg kívánja zavarni az infokommunikációs eszközök, rendszerek és technológiák biztonságos működését, ezáltal veszélyeztetve az adatok és információk bizalmasságát, sérthetetlenségét, megbízhatóságát és rendelkezésre állását, valamint maguknak a rendszereknek a működőképességét. A kibervédelem pedig mindazoknak az eszközöknek és tevékenységeknek az összessége, amelyek célja, hogy a fenti rendszereket megvédjék a potenciális támadásoktól.*** Ebbe a véde-

lembe beletartozik a támadások korai érzékelése, elhárítása, a rendszerek zavartalan működésének helyreállítása, a hibák elhárítása is.

A kibertér kihívásai és fenyegetései a kibertérben megjelenő szereplők és tevékenységek fent jelzett sokszínűségének megfelelően ugyancsak rendkívül komplexek. Néhány területet és gyakorlati példát kiemelve napjainkban is tanúi vagyunk az alábbi kibervédelmi feladatok nagyarányú jelenlétének (és számolhatunk további fokozódásukkal):

- ***Információvédelem*** (a magánszférában a személyes adatok védelme, üzleti, gazdasági, ipari szférában az ipari kémkedés elleni védelem, közszférában a magánszemélyek személyes adatait rögzítő adatbázisok védelme; a személyiségi, szerzői és gazdasági jogi jogviszonyok tisztázatlansága és szankcionálásának problémái)
- ***Kritikus számítástechnikai és infokommunikációs infrastruktúrák védelme*** (állam- és közigazgatási hálózatok (E-közigazgatás) védelme, alapvető közműszolgáltatásokat és ipari irányítást (például áram- és vízellátást) biztosító rendszerek védelme, pénzügyi és bankhálózatok védelme, közlekedési irányító rendszerek, valamint közszolgálati kommunikációs csatornák védelme)
- ***Kiberbűnözés*** (internet alapú csalások, magánszemélyek és vállalkozások érzékeny (személyes, gazdasági-pénzügyi) adataival elkövetett visszaélések (például bankkártya-csalások))
- ***Katonai hálózatok védelme és kiberháború*** (katonai rendszerek és haditechnikai eszközök informatikai üzemeltetése, információvédelme, rejtjeltevékenység, vezetés-irányítási rendszerek védelme, illetve ezek bénítása)

E fenyegetések tárgyalása további definíciós problémákat, valamint a kibertérből érkező fenyegetések elleni fellépés kérdéseit – Ki, milyen alapon, milyen eszközökkel léphet fel egy támadás esetén? – is felveti.

3. Kiberbűnözés

A *kiberbűnözés általános értelemben olyan bűncselekmények elkövetését jelenti, amelyeket interneten keresztül számítógép segítségével, vagy számítógépek ellenében követnek el.* Előbbi esetben a kiberbűntény (informatikailag általában kevésbé képzett) elkövetője számítógépe segítségével olyan kárt okoz, amely a fizikai világban testesül meg: csalásokat (identitás-lopás), személyes adatokkal történő visszaéléseket (adathalászat, banki csalás) követ el, általában egy áldozat kárára egyszer – például egy E-mailben küldött rosszindulatú program,

illetve annak linkje (malware vagy trójai vírus) vagy kéretlen hirdetések (spam) küldésével. Utóbbi esetben a számítógépeket és azok hálózatait képzettebb kiberbűnözők képesek feltörni, és több, vagy ismétlődő támadások eredményeképpen megszerzett adatokkal visszaélve vagy magát az informatikai rendszert manipulálva, károsítva súlyosabb kárt okoznak – például zaklatás, zsarolás, tőzsdei és banki csalások, ipari kémkedés által.

Természetesen ezek nem élesen elhatárolható cselekmények, és ezek sorát hosszasan lehet folytatni az intenzitás és az okozott kár mértéke szerint egészen a kormányzati rendszerek támadásáig, melyek azonban már szervezett, összehangolt, komoly kapacitást igénylő támadásokat jelentenek, amelyek mögött akár állami szereplők is állhatnak és már nem a kiberbűnözés kategóriájába tartoznak.

4. Tisztázatlan kérdések

A kiberbiztonság és kibervédelem homályos és definiálatlan határterületét jelentik azok a nagyarányú és nagy hatású támadások, amelyek kritikus infokommunikációs infrastruktúrák, kormányzati közigazgatási rendszerek ellen irányulnak, és ezáltal egy állami szereplő biztonságát fenyegetik. Ugyanakkor éppen ez az a terület, amely az egyes államoktól válaszlépéseket követel meg (pontosabban védelmi, elhárítási, helyreállítási képességek létrehozását – egyes szereplők szerint pedig támadó képességekét is). ***E határterületen számos problémával kell számolnunk***:

- Az egyes államok eltérően határozzák meg azt, ***hogyan minősítik a támadásokat és hogyan kívánnak reagálni azokra***: például katonai támadásnak értékelik-e, és ha igen, milyen nagyságrendű támadás esetén, valamint hogyan kívánnak reagálni rá – a kibertéren keresztül végrehajtott ellenakcióval, vagy hagyományos (esetleg elméleti opcióként tömegpusztító) fegyverek bevetésével? ***Milyen nagyságrendű az arányos válaszadás egy kibertámadás esetében, és ki ellen irányuljon?*** Jelenleg a hadijog valamenynyi vonatkozó fogalma (például az „agresszió”) definiálatlan a kibertér incidenseire.
- Egyáltalán ***nem tisztázott a felelősség kérdése*** – sem a nemzetközi jogi szabályozás, sem egy nemzetközi vitában eljárni képes hatóság vonatkozásában; de sok esetben a nemzeti szabályozások sem tudják kezelni azt, hogy akár állami, akár nem állami szereplőkkel (hackerek, hackercsoportok) szemben hogyan lehet fellépni? A kibertér nem ismeri a nemzeti szuverenitás fogalmát és nem területi alapon szerveződik – viszont akkor kinek a fennhatósága alá tartoznak a kibertámadást végrehajtók?

- Alapvető technológiai hiányosság, hogy ***az elkövetett támadások a kibertérben igen nehezen visszakövethetőek***, adott esetben közvetett állomásokon keresztül valósulnak meg (például túlterheléses (DDos) támadás esetén „harmadik fél", egyes magánszemélyek személyi számítógépére telepített rosszindulatú programokon keresztül) – hogyan azonosítható egy támadás kezdeményezője és hogyan bizonyítható a támadás?

5. Kiberhadviselés

Végül a kibertér incidensei közül a legmagasabb intenzitású tevékenységek közül is kiemelkednek a katonai vonatkozásúak. A kiberhadviselés – mint arra Haig Zsolt és Várhegyi István is rámutatnak – az információs műveletek részeként jelenik meg, melyek célja az információs fölény kivívása és megtartása. Ezen műveletek – akárcsak a hadszínterek – tovább bonthatóak. Ennek értelmében az információs műveletek kereteibe tartozik a kinetikus energián alapuló hadviselés (kritikus infrastruktúrák és infokommunikációs rendszerek fizikai pusztítása); a kognitív hadviselés (például pszichológiai műveletek) és a hálózati hadviselés (például elektronikai hadviselés). ***A kiberhadviselés pedig a kibertérben, azaz információs dimenzióban végrehajtott hálózati hadviselés és az ott zajló műveletek összessége, melyek célja a saját elektronikus, információszerző és hálózatközpontú rendszerek védelme és az ellenség ugyanilyen típusú rendszereinek zavarása, blokkolása és leállítása***. A kibertérben folytatott katonai műveletek közül példaként említhető a távközlési hálózatok lehallgatása vagy zavarása, a navigációs rendszerek elleni elektronikai ellentevékenység különböző formái, a számítógép-hálózatok feltérképezése, az azokba való bejutás és az adatbázisok tönkretétele, valamint a szerverek túlterhelése és számos egyéb tevékenység. A kiberhadviselés célpontjai között az ellenséges országok integrált légvédelmi rendszere, felderítő rendszerei, távközlési hálózatai és más hálózatalapú katonai vezetési rendszerei, kritikus információs infrastruktúrái, ezen belül kiemelten az internet hálózat, a cellás rendszerű mobiltelefon hálózatok és az energiaellátás irányító rendszerei szerepelhetnek.

6. A kiberbiztonság fennmaradó problémái

Mindezek alapján látható, hogy a kibertér mindennapi működése és incidensei kapcsán számos kérdés megoldás még előttünk áll:

- ***Szükség van az átfogó nemzetközi szabályozásra***, melynek lehetőleg a nemzetközi közösség minél több országa a tagja, és képes megteremteni a szabad internet és az el-

lenőrzött hálózatok olyan kiegyensúlyozott modelljét, amely a lehető legkisebb szabályozás mellett a lehető legnagyobb biztonságot garantálja és átláthatóságot teremt a kibertér szereplői között.

- A nemzetközi szabályozástól függetlenül ***fokozni kell az állami kibervédelmi képességeket***, mert jelenleg is rohamosan nő mind az állami, mind a nem állami szereplők részéről végrehajtott kibertámadások száma más országok rendszerei ellen.
- Ezzel összhangban ***célszerű fokozni az olyan nemzetközi együttműködéseket***, amelyek az információ, a tapasztalatok és a védelmi képességek megosztása révén fokozni tudja az egyes államok reagálási képességeit is – mint az Európai Unióban és a NATO-ban zajló közös kibervédelmi törekvések.
- Az is egyértelmű, hogy ***a kibervédelem nem lehet csupán állami feladat***, ugyanis a kibertér „felhasználói" között a gazdasági és magánszektor szereplői is igen nagy számban és jelentős érdekekkel képviseltetik magukat, így bevonásuk a hatékony védelmi mechanizmusok kialakításába célszerű. Emellett tagadhatatlan, hogy a legújabb infokommunikációs fejlesztések sem az állami szférában jelennek meg, hanem azoknál a piaci szereplőknél, amelyek a gazdasági érdekeik miatt nem tekinthetnek el saját adataik és rendszereik védelmétől.
- A társadalmat, azaz ***az internet-felhasználók széles tömegeit szintén be kell vonni a kiberbiztonság fenntartását célzó tevékenységekbe***, mert az információbiztonsági tudatosság fokozása a lakosság körében jelentős mértékben csökkenthetné a magánszféra sebezhetőségét a kiberbűnözőkkel szemben.

A kiberbiztonság számos tisztázatlan kérdése következtében komoly akadályok állnak nemcsak a nemzetközi szabályozás kialakítása, hanem a nemzetközi együttműködés előtt is. Az Egyesült Nemzetek Szervezetén – vagy más, a kiberbiztonság kérdéseiben illetékes és felhatalmazással bíró, globális fennhatóságú, újonnan létrehozandó szervezeten – belül a nemzetközi közösség valamennyi államának igen sokrétű és sok tekintetben eltérő érdekeit nehéz közös mederbe terelni, és már napjainkban is látszanak bizonyos elkülönülő érdekcsoportok (a „nyugati országok", Kína, Oroszország), akik egyes kulcsfontosságú szabályozási kérdésekben nem értenek egyet. Emellett a kiberbiztonság megteremtése ma még döntően az egyes államok feladatrendszerébe, szuverén fennhatósága alá tartozik, és a regionális együttműködési formák inkább a kivételt, mint a szabályt jelentik. Két regionális kibervédelmi együttműködésről azonban szólnunk kell: a NATO és az Európai Unió keretében kialakított mechanizmusokról. Ezek fejlettsége és a gyakorlatban megjelenő képességei is eltérőek,

azonban kifejezik azt a szándékot, hogy a legfejlettebb – így a kiberbiztonság szempontjából legsebezhetőbb – államok közös nevezőre hozzák és elterjesszék a kiberbiztonság fenntartásához szükséges normákat, és megteremtsék a saját és szövetségeseik védelméhez szükséges képességeket.

7. A NATO kibervédelmi politikája és képességei

Az Észak-atlanti Szerződés Szervezetének biztonságpolitikai napirendjén először 2002-ben, a prágai csúcstalálkozón elfogadott Zárónyilatkozat részeként jelent meg a kiberbiztonság kérdése, mint a szövetségre és tagállamaira irányuló fenyegetések forrása. Négy évvel később a Prágai Képességfejlesztési Csomag részeként már a szövetség vezetés-irányítási és kommunikációs rendszereinek fejlesztését és védelmük erősítését tűzték ki célul, azonban ***a valós lökést a 2007-es észtországi és 2008-as grúziai események adták meg a NATO kibervédelmi politikájának fejlesztéséhez.***

2007 áprilisában és májusában két héten át kibertámadások sora érte Észtország teljes infokommunikációs hálózatát, megbénítva a kormányzati, bank-, és közszolgálati hálózatok jelentős részét – a támadást orosz hackercsoportoknak tulajdonították. 2008 augusztusában pedig a grúz-orosz háború során az orosz fél által végrehajtott információs műveletek – a katonai műveleteket kiegészítő, a grúz kormányszervereket támadó kibertéri műveletek – jelezték a kiberhadviselés gyakorlati, a hagyományos hadviselést kiegészítő jelentőségét. Ezek az esetek – a NATO szövetségi és a tagállamok nemzeti infokommunikációs hálózatait érő egyre növekvő számú támadás mellett – ***stratégiai jelentőségű változást idéztek elő a NATO fenyegetettség-percepciójában, ami a 2010-ben „Aktív Szerepvállalás, Modern Védelem" címmel Lisszabonban elfogadott Stratégiai Koncepcióba is bekerült:*** „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 euró-atlanti prosperitást, biztonságot és stabilitást veszélyezteti. Külföldi haderők és titkosszolgálatok, szervezett bűnözők, terrorista és/vagy szélsőséges csoportok egyaránt lehetnek egy ilyen támadás végrehajtói." ***A Stratégiai Koncepció egyúttal beemelte a kibertámadások kérdését a NATO kollektív védelmi mechanizmusába*** – azaz valamely tagállam ellen elkövetett kibertámadás felveti a kollektív cselekvés lehetőségét. ***Fontos azonban hangsúlyozni, hogy a kollektív fellépés nem automatizmus, hanem a tagállamok egyeztetését követő konszenzusos döntés függvénye, egyúttal pedig az Észak-atlanti Tanácsban eldőlő politikai kérdés, és nem a***

kibervédelmet technikai szinten megvalósító szerveknek vagy a szövetség katonai vezetőinek hatáskörébe tartozó döntés.

A kibervédelmi kérdések megnövekedett súlyának megfelelően az elmúlt években nagyarányú fejlesztésekre került sor:

- **A politikai szinten** elfogadták a tagállamok azokat a stratégiai irányelveket, amelyek „elhelyezik" a kiberbiztonság kérdéseit a szövetség által érzékelt fenyegetések között. 2011-ben a NATO védelmi miniszterei új Kibervédelmi Irányelveket és egy kapcsolódó Cselekvési Tervet fogadtak el, amelyek a szövetségi rendszerek centralizált védelmi képességeinek kiépítését szabták feladatként, és beépítették a kibervédelem kialakításának igényeit a szövetség védelmi tervezési rendszerébe. A 2012-es chicagói csúcstalálkozón a kibervédelem már a szövetség biztonságpolitikai napirendjének egyik kiemelt témája volt. Szintén kialakították azt a mechanizmust, amely révén támadás esetén egyes tagállamok Gyorsreagálású Csoportok (Rapid Reaction Teams) formájában támogatást és segítséget kaphatnak a NATO kibervédelmi szervezeteitől.
- **A szervezetek szintjén** kialakították a kibervédelemmel kapcsolatos döntéshozatali mechanizmust: a politikai döntést valamely támadás esetén az Észak-atlanti Tanács (North Atlantic Council) hozza meg, a kibervédelmet a Kibervédelmi Igazgatóság (Cyber Defence Managemenet Board) irányítja, a védelmet pedig a NATO Kommunikációs és Információs Ügynöksége (NATO Communication and Information Agency) és alárendelt szervezetei (például a NATO Cyber Incidence Response Center) biztosítják.
- **A technikai hátteret és gyakorlatban megvalósuló kibervédelmet illetően** végrehajtották azokat a kritikus hardver- és szoftverfejlesztéseket, amelyek nélkülözhetetlenek voltak ahhoz, hogy létrehozzák, majd 2012 végéig teljesen működési kapacitásra fejlesszék a szövetség kibervédelmi képességét (NATO Computer Incident Response Capability), kialakítva az alkalmazási gyakorlatokat és a központi, valamint tagállamok közötti együttműködésben megvalósuló védelmi eljárásokat. Ugyancsak létrehoztak egy a megelőzést és gyors reagálási képességet biztosító Fenyegetés-értékelő Egységet (Cyber Threat Awareness Cell).
- **A kibervédelmi kutatás-fejlesztés és innováció terén** még 2008-ban létrehozták a Kooperatív Kibervédelmi Kiválósági Központot Tallinban, és az elmúlt években fokozottan törekszenek a NATO szervezetei, a védelmi szféra más szereplői, az in-

formáció-technológiai szektor és a civil társadalom közötti kapcsolatok és együttműködés erősítésére.

Ezekre alapozva a szövetség kibervédelmi törekvéseit a következő években az határozza meg, hogy minden tagállamot segítsenek annak az alapvető kibervédelmi képességnek a kialakításában, amelyekkel a NATO feladatainak ellátásában résztvevő rendszereket biztosítani tudják. Emellett segítik a tagállamokat abban is, hogy saját nemzeti infokommunikációs kritikus infrastruktúrájuk védelmét ki tudják alakítani. Az egyes tagállamoknak lehetősége nyílik arra, hogy a szövetségesi szolidaritás és kollektív védelem jegyében felajánlják saját képességeiket más tagállamok vagy a szövetség számára valamely kibertámadás elhárítása során.

Annak érdekében, hogy a szövetségi rendszerek védelme a jövőben is biztosított legyen, a további beszerzések során szigorú, a kiberbiztonság szempontjait, a megbízhatóságot is figyelembe vevő szempontokat dolgoznak ki és érvényesítenek, és ezeket az ellátási lánc kockázatkezelési folyamatába is beépítik. Bizonyos alapvető kibervédelmi követelmények betartását a NATO-val együttműködő államoktól is el fogják várni.

A megfelelő források biztosítása céljával a kibervédelem forrásigényét teljes mértékben integrálják a szövetségi tervezési folyamatokba, és a fennálló sebezhetőségek kiküszöbölése érdekében a következő években prioritásként kezelik. Hasonlóképpen, a katonai szervek értékelni fogják, hogy a kialakított kibervédelmi képességek hogyan járulnak hozzá a NATO alapfeladatainak ellátásához, műveleteinek tervezésének és végrehajtásának biztosításához.

A fenti intézkedések célja egyértelműen az, hogy erősítse a szövetség megelőzési, észlelési, kezelési, válaszadási és helyreállítási képességeit, valamint bővítse a támadások értékelésének, elemzésének eszköztárát és a tagállamok körében is meghonosítsa a legjobban működő gyakorlatokat. A gyakorlati megvalósítást az egyre gyakoribb és átfogóbb többnemzeti és szövetségi kibervédelmi gyakorlatok biztosítják.

8. Az Európai Unió kibervédelmi törekvései

Míg a NATO politikai-katonai szövetségként a tagállamok biztonságát érintő kiberbiztonsági kérdéseket a katonai konfliktusok, terrorizmus, kritikus infrastruktúrák védelme kapcsán közelíti meg, addig ***az Európai Unió a „civil megközelítésből" eredő kihívásokra és fenyegetésekre – szerzői jogi és adatvédelmi kérdések, biztonságos internethasználat, kiberbűnözés – is koncentrál, és a szabad és nyílt internet megőrzését lehetővé tevő nemzetközi normákra és együttműködési formákra is hangsúlyt helyez.*** Az ezredfordulót követően, amikor a kritikus

infrastruktúraelemek és infokommunikációs hálózatok védelme az Európai Unió – és annak tagállamai – napirendjére került, elsősorban a nemzetközi terrorizmus fenyegetése lebegett a döntéshozók előtt.

Ennek megfelelően a 2003-ban elfogadott EU Biztonsági Stratégia is a nemzetközi terrorizmust és a modern társadalmak sebezhetőségét nevesítette, érintve ezzel a kritikus infrastruktúraelemeket – azonban a kiberbiztonság kérdései még nem jelentek meg a dokumentumban. Az első, kifejezetten az informatikai infrastruktúrák védelmét célzó bizottsági közlemény 2009-ben született „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása" (Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience) címmel – négy évvel az után, hogy az Unió elfogadta a kritikus infrastruktúrák védelméről szóló ún. „Zöld Könyvet", és két évvel az Észtországot ért kibertámadás után. Ezen túlmenően a kibertér biztonságos felhasználására – egyúttal a tagállamok lakosai infokommunikációs technológiákhoz (internethez) való hozzáférésének bővítésére – szolgált a Digitális Menetrend (A Digital Agenda for Europe) 2020-ig tartó fejlesztési programja.

Végül az EU-ra jellemző lassabb döntéshozatali mechanizmusok miatt ***az Európai Parlament 2012 novemberében fogadott el a tagállamok felé megfogalmazott ajánlást „A kiberbiztonságról és -védelemről"***, amelyben a következő javaslatokat rögzítette:

- alakítsák ki saját nemzeti kiberbiztonsági és –védelmi stratégiáikat, megteremtve a szükséges jogi szabályozást, szervezeteket és kormányzati koordinációs képességet a kockázatkezeléshez és a kibervédelem feladatainak ellátásához;
- hozzák létre nemzeti kibervédelmi veszélyhelyzeti terveiket és a válságkezeléshez szükséges képességeket;
- hozzák létre a kibervédelem szervezeteit nemzeti haderejükön belül, felkészítve azokat az Európai Unió hasonló szervezeteivel való együttműködésre;
- építsék be jogrendjükbe a kiberbiztonság fenntartásához szükséges, a kiberbűnözés elleni fellépést lehetővé tevő jogszabályokat és hozzák létre az ilyen ügyekben eljárni képes bíróságokat;
- tegyék a kutatás-fejlesztési tevékenységet a kiberbiztonság megteremtésére irányuló tevékenységek egyik alappillérévé, és támogassák az ez irányú szakemberképzést.

2013 februárjában pedig elfogadták ez EU átfogó Kiberbiztonsági Stratégiáját. **A *„Nyílt, biztonságos és megbízható kibertér – Az Európai Unió Kibrebiztonsági Stratégiája" (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace)***

című dokumentum öt stratégiai prioritást határoz meg az EU közösségi szervei és a tagállamok számára:

- Rugalmas reagálási képesség kialakítása a kibervédelemben;
- A kiberbűnözés drasztikus csökkentése;
- A Közös Biztonság- és Védelempolitikához (KBVP) kapcsolódó kibervédelmi politika és képességek kialakítása;
- A kiberbiztonság szavatolásához szükséges ipari és technológiai erőforrások létrehozása;
- EU-szintű koherens nemzetközi kibertér-politika kialakítása és az Unió alapvető normáinak terjesztése a kiberbiztonság terén.

Fontos megjegyezni, hogy a kibervédelem beágyazása a Közös Biztonság- és Védelempolitikába ugyanazokat a kérdéseket veti fel a Lisszaboni Szerződés szolidaritási záradékával kapcsolatban, mint a NATO esetében a kollektív védelem értelmezése: hogyan reagáljon a közösség, ha egyik tagállamát kibertámadás éri; milyen súlyú válaszlépéseket fogalmazzon meg, stb.?

A Stratégiához kapcsolódik az Európai Parlament és a Tanács közös ajánlása (Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure the high common level of network and information security across the Union) egy közösségi szintű, a hálózati és információs biztonság megteremtését lehetővé tévő Irányelv elfogadására.

Abból eredően, hogy az EU kiberbiztonsággal kapcsolatos közösségi politikája csak most formálódik, a kibervédelmi szabályozás és képességek fejlesztése döntően a tagállamok szuverén fennhatósága alá tartozik még ma is. Az infokommunikációs rendszerek terén legfejlettebb – így leginkább sebezhető – államok azonban már az 1990-es évektől állandó szervezetek létrehozásával igyekeztek biztosítani maguknak a hatékony védelem lehetőségét és a reagálás képességét. Erre a célra jöttek létre az ún. ***Hálózatbiztonsági Reagáló Csoportok, vagy CERT-ek*** (Computer Emergency Response Team), amelyek olyan információ- és hálózatbiztonsági szakembereket tömörítő csoportok, amelyek felügyelik a kritikus rendszereket, támadás esetén pedig a lehető leggyorsabban (valós időben) reagálnak. Ilyen CERT-ek ma már minden EU tagállamban működnek tagállami/kormányzati szinten (legalább egy), amelyeket további nemzeti, nem kormányzati CERT-ek egészíthetnek ki (Nagy-Britanniában például 20 különböző szervezet) – és a bevált gyakorlatnak megfelelően 2010 óta az Európai Unió intézményei mellé is kialakították azok saját CERT-jeit (összesen több mint 50-et) a biztonságos működés fenntartása érdekében. Végül 2012 szeptemberében elérte teljes műkö-

dési képességét az EU legfőbb intézményeinek – az Európai Bizottság, az Európai Unió Tanácsának Főtitkársága, a Parlament, a Régiók Bizottsága, stb. – közös CERT-je (CERT-EU), így összességében ***az Európai Unióban ma már több mint 250 különböző területre – kormányzati, pénzügyi, ipari, kereskedelmi, szolgáltatási szektor, kutatás-fejlesztési, közszolgáltatásokért felelős, stb. – szakosodott Hálózatbiztonsági Csoport alkot egymással is kapcsolatban lévő hálózatot annak érdekében, hogy biztosítani tudják a tagállami és közösségi kibertér védelmét.***

Az Unió szervei és tagállamai közötti együttműködésért a 2004-ben létrehozott és a következő évtől működő ***Európai Hálózat- és Információbiztonsági Ügynökség*** (European Network and Information Security Agency – ENISA) felel, segítve a koordinációt, jogszabályalkotást, információcserét, valamint fokozva a tagállamok lakosságának tájékozottságát és a biztonságos internet-felhasználás tudatosságát.

9. Magyarország kibervédelmi politikája

Magyarország elköteleződése a kiberbiztonság kérdései mellett nem új keletű: ***az első nemzetközi, a kiberbűnözés elleni összehangolt fellépést elősegítő egyezményt, a Kiberbűnözésről szóló Konvenciót (Convention on Cybercrime) Budapesten fogadták el 2001-ben***, és Magyarország napjainkig fontos szerepet szán a nemzetközi kiberbiztonsággal foglalkozó kezdeményezések, tárgyalások támogatásának. Az Európai Tanács által előkészített Budapesti Konvenció célja az volt, hogy a számítógépes és internetes bűnözés elleni nemzeti jogi szabályozás nemzetközi szintű egységesítésével hatékonyabbá tegye a fellépés lehetőségét, azaz: a nemzeti jogszabályokba bekerüljenek a kiberbűnözés különböző formái (szerzői jogi jogsértések, számítógépes csalások, gyermekpornográfia, gyűlöletkeltő internetes tartalmak megjelentetése, stb.); kialakítsák a szükséges nyomozó hatóságokat és büntetőjogi fórumokat, eljárásokat; megteremtsék az eljárások átlátható rendszerét és a határokon átnyúló kiberbűnözés elleni fellépéshez szükséges nemzetközi együttműködést.

Az elmúlt évek magyar szerepvállalását a nemzetközi együttműködés elősegítése terén a 2012. októberi ***Budapesti Kibertér Konferencia*** foglalta keretbe, melynek kiemelt célja volt, hogy ráirányítsa a politika, a szakemberek, a közigazgatás, az üzleti és a tudományos szféra figyelmét az együttműködés és az információmegosztás fontosságára, a megelőzés kiemelt szerepére és az elektronikus védelem kialakításának szükségességére. Az elmúlt tíz évben ugyanis a nemzetközi gyakorlatnak és erősödő együttműködésnek megfelelően Magyarország

is megteremtette a kibertérből érkező sokszínű fenyegetések elleni védelemhez és fellépéshez szükséges képesség alapjait.

A 2012. februárjában elfogadott Nemzeti Biztonsági Stratégia (1035/2012 Kormányhatározat, 31. pont) a kiberbiztonság szerepéről a következőt írja: „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 katasztrófavédelmi vonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelem feladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására Magyarországnak is készen kell állnia.***

a) Elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális fenyegetések és kockázatok rendszeres felmérése és priorizálása, a kormányzati koordináció erősítése, a társadalmi tudatosság fokozása, valamint a nemzetközi együttműködési lehetőségek kiaknázása.
b) A nemzeti kritikus információs infrastruktúra védelmének erősítése mellett szövetségeseinkkel és EU-partnereinkkel együtt arra törekszünk, hogy az információs rendszerek biztonsága erősödjön, valamint részt vegyünk a megfelelő szintű kibervédelem kialakításában.

A stratégiába foglaltaknak megfelelően készült el 2013. márciusában az NBS-re épülő ágazati stratégia, Magyarország Nemzeti Kiberbiztonsági Stratégiája (1139/2013. Kormányhatározat), amely rögzíti, hogy a megelőzésre épülő hatékony védelmi intézkedések útján elsődleges cél a kibertérben jelentkező és a kibertérből érkező fenyegetések és az ezzel járó kockázatok kezelése, az ehhez szükséges kormányzati koordináció és eszköztár erősítése, illetve annak a döntéshozó politikai és szakmai figyelemnek és képességnek a kiépítése, mely rugalmasan reagálva lehetővé teszi a belátható jövőben a technológiai fejlődésből fakadó új kiberbiztonsági problémák kezelését.

A Kiberbiztonsági Stratégia összhangban áll az ország közvetlen nemzetközi partnereinek – a NATO és az Európai Unió fent bemutatott – kibervédelmi dokumentumaival, irányelveivel és az Európai Biztonsági és Együttműködési Szervezet (EBESZ), az ENSZ, az Európa Tanács és más nemzetközi szervezetek tagságán keresztül törekszik a globális kibertér szabad és biztonságos használatának szavatolására.

A Stratégiához kapcsolódó további jogszabályok és gyakorlati intézkedések célja, hogy Magyarország rendelkezzen hatékony megelőzési, észlelési, kezelési (reagálási), válaszadási és helyreállítási képességekkel a magyar kiberteret érintő rossz szándékú kibertevékenység, fenyegetés, támadás, illetve vészhelyzet, valamint a vétlen információszivárgás ellen; illetve nemzeti adatvagyona megfelelő szintű védelemben részesüljön, létfontosságú rendszereinek és létesítményeinek kibertérhez kapcsolódó működése üzembiztos legyen, valamint rendelkezésre álljon kompromittálás esetén a megfelelően gyors, hatékony és a veszteséget minimalizáló, különleges jogrend idején is alkalmazható helyreállítási képesség.

A Kiberbiztonsági Stratégiában foglaltakat röviddel a Stratégia után elfogadott, ***Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény rendelkezései ültetik át a gyakorlatba több – korábban ki nem alakított – területen.*** Így a törvény nyomán hozzák létre kormányzati szinten a Nemzeti Kiberbiztonsági Koordinációs Tanácsot, szaktárca szinten pedig Nemzeti Elektronikus Információvédelmi Hatóságot. További, az ország információs biztonságát alapvetően meghatározó jogszabályok Az elektronikus hírközlésről szóló 2003. évi C. törvény, A médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. Törvény, valamint **A létfontosságú rendszerek** és létesítmények azonosításáról, kijelöléséről és **védelméről szóló** 2012. évi CLXVI. törvény, illetve végrehajtási rendelete (65/2013. Kormányrendelet).

10. Magyarország kibervédelmi képességei

A kibervédelem gyakorlati megvalósítását Magyarország – a kiberbiztonság szerteágazó fenyegetéseit leképezve és a nemzetközi gyakorlatnak megfelelően – magas szintű kormányzati koordináció mellett az együttműködés javításával és a hatékony információcsere fokozásával, a kormányzati oldal mellett a civil, a gazdasági és a tudományos területek képviselőinek operatív együttműködési fórumokon fenntartott részvételével és szakosított intézmények működtetésével, a már létező szervezetek bevonásával kívánja biztosítani. E tekintetben – az adatvédelem, hírközlés és média területén kapcsolódó feladatokat ellátó szervezeteket külön nem kiemelve – a legfontosabb állami szereplők a következők:

- A ***Miniszterelnökség*** keretében valósul meg az összkormányzati koordináció, és 2013 nyarán a Miniszterelnökséget vezető államtitkár tesz javaslatot a ***Nemzeti Kiberbiztonsági Koordinációs Tanács*** kialakítására. A Tanács a kormány javaslattevő, véleményező szerveként működik a Miniszterelnökséget vezető államtitkár vezetésével és a Miniszterelnökség által delegált kiberkoordinátor támogatásával. A kormányzat ágazati koordinációs tevékenysége mellett a Tanács fontos feladata, hogy támogassa a nem-kormányzati szereplőkkel való együttműködésnek keretet biztosító Nemzeti Kiberbiztonsági Fórum munkáját.
- ***Nemzeti Fejlesztési Minisztérium az Infokommunikációért Felelős Államtitkárság***on keresztül számos, a kibervédelemhez kapcsolódó terület biztonságos és zavartalan működtetéséért felelős. Így az infokommunikációs területen feladata az e- közigazgatás fejlesztése és a digitális szolgáltatások minél szélesebb körben történő elérhetővé tétele; a kormányzati informatika területén a közigazgatási informatikai és infokommunikációs infrastruktúra működtetése és fejlesztése – például a kormányzati gerinchálózat üzemeltetése és a közigazgatási intézmények, illetve állami vagy részben állami tulajdonban lévő gazdasági társaságok hírközlési, informatikai tevékenységének biztosítása –, az elektronikus hírközlés terültén pedig az egyetemes elektronikus hírközlési szolgáltatás ellátásának felügyelete.
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény értelmében a Nemzeti Fejlesztési Minisztérium alárendeltségében a ***Nemzeti Elektronikus Információvédelmi Hatóság*** feladata – többek között – a releváns szervezetek esetében az elektronikus információs rendszerek információbiztonsági vizsgálata, értékelése és minősítési osztályba sorolása (ún. biztonsági auditja). Emellett a Hatóság éves és egyedi jelentéseket készít a kormány részére az elektronikus információs rendszerek biztonságával, a létfontosságú információs rendszerelemek védelmével, illetve a kibervédelem helyzetével kapcsolatban.
- Míg a Nemzeti Elektronikus Információvédelmi Hatóság feladata az infokommunikációs rendszerek bevizsgálása és minősítése, addig a létfontosságú információs infrastruktúrák és vagyonelemek támadhatóságának vizsgálatát és részben védelmét a ***Nemzeti Hálózatbiztonsági Központ*** (PTA CERT Hungary) **biztosítja. A nemzetközi – korábban az Európai Unió kibervédelmi képességeinél ismertetett – gyakorlathoz teljes mértékben illeszkedő nemzeti/kormányzati CERT szerepet Magyarországon 2004 óta a Puskás Tivadar Közalapítványon belül működő CERT-Hungary Központ** a Nemzeti Fejlesztési Minisztérium felügyelete alatt, az

Informatikai Biztonsági Felügyelő irányításával **látja el,** mint N**emzeti Hálózatbiztonsági Központ. A Központ a nemzeti/kormányzati CERT tevékenység ellátása keretében, mint a magyar kormányzat információ-megosztó és incidenskezelő szervezete, illetve nemzeti kapcsolati pontja** részt vesz a Nemzeti Fejlesztési Minisztérium által létrehozott **Kormányzati információ-megosztó és incidenskezelő munkacsoport munkájában.** Kiemelt feladata, hogy hálózatbiztonsági szolgáltatásokat nyújtson a támogatott közigazgatási és kritikus információs infrastruktúrákat üzemeltető szervek részére, valamint további f**eladata az** incidenskezelés optimalizálása, illetve az internetes hálózatbiztonsági incidensek időzóna függetlensége miatt **24 órás ügyeleti rendszer működtetése**. Tevékenysége során a magyar és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezetek felé, mint az **országon belüli koordinációs szervezet** végzi az internetet támadási csatornaként felhasználó incidensek kezelését és elhárításának koordinálását, továbbá közzéteszi a felismert és publikált szoftver sérülékenységeket.

- A fenti szervezetek munkáját kiegészítve a közigazgatási és igazságügyi miniszter irányítása alatt álló ***Nemzeti Biztonsági Felügyelet*** a nemzeti adatvagyon számbavétele és védelmének biztosítása terén végez szerteágazó tevékenységet. A Nemzeti Biztonsági Felügyelet feladatai közé tartozik a minősített adat – beleértve a nemzeti és a külföldi (NATO/EU) – védelmének hatósági felügyelete, a minősített adatok kezelésének hatósági engedélyezése és felügyelete, valamint a nemzeti iparbiztonsági hatósági feladatok ellátása.
- **A létfontosságú rendszerek** és létesítmények azonosításáról, kijelöléséről és **védelméről szóló** 2012. évi CLXVI. törvény végrehajtási rendelete értelmében 2013. márciusában hozták létre a Belügyminisztérium felügyelete alá sorolt ***Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központját***. A Központ feladata a hivatásos katasztrófavédelem központi szervének (azaz BM Országos Katasztrófavédelmi Főigazgatóságnak) feladatkörébe tartozó, a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenység ellátása.
- A kibervédelem szerteágazó feladataiból adódóan további feladatokat látnak el a nemzetbiztonsági szolgálatok, a Nemzeti Adatvédelmi és Információszabadság Hatóság és a Nemzeti Média- és Hírközlési Hatóság, melyek tevékenységének bemutatásától jelenleg eltekintünk.

A kormányzati kibervédelmi szervezetek mellett meg kell említeni a civil szféra kibervédelmi kezdeményezéseit, amelyek ugyancsak jól illeszkednek a nemzetközi gyakorlatban tapasztalt modellbe, hiszen a civil társadalom tagjai, gazdasági szervezetek és kutatóhelyek, szakosított intézmények munkatársai ezeken a szervezeteken keresztül járulhatnak hozzá szakértelmükkel egy ország – esetünkben Magyarország – kibervédelmi képességeihez.

- A ***CrySyS Adat- és Rendszerbiztonság Laboratórium (CRYSYSLAB)***, a Budapesti Műszaki és Gazdaságtudományi Egyetem Híradástechnikai Tanszékének munkatársaira alapozva jött létre azzal a céllal, hogy nemzetközileg elismert, minősített kutatási bázist teremtsen a hálózati és rendszerbiztonság, a kriptográfia és adatvédelem területén.
- Az ***Önkéntes Kibervédelmi Összefogás (KIBEV)*** az ország kiberbiztonságáért tenni akaró, megrendelő oldali rendszerüzemeltetőket és biztonsági szakembereket, auditorokat tagjai között tudó független civil tömörülés, melynek tagjai felajánlják az állam számára szaktudásukat és tettrekészségüket abból a célból, hogy szükség esetén részt vegyenek Magyarország kiberterének védelmében. Az Összefogás felvállalja az a fontos feladatot is, hogy más civil szervezetekkel együttműködve felhívja a figyelmet a kibertér fenyegetettségeire, és fejlessze a magyar állampolgárok biztonságtudatosságát.

Felhasznált és ajánlott források:

„A Digital Agenda for Europe”

„Aktív Szerepvállalás, Modern Védelem” – Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója (2010)

„A Secure Europe in a Better World” – European Security Strategy (2003)

Budapest Convention on Cybercrime

Cybersecurity Strategy of the European Union: „An Open, Safe and Secure Cyberspace”

Defending the Networks – The NATO Policy on Cyber Defence

Digitális Megújulás Cselekvési Terv

Haig Zsolt – Várhegyi István: A cybertér és a cyberhadviselés értelmezése. In: Hadtudomány, 2008/2. pp. 1-22.

Norton 2012 Cybercrime Report

Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure the high common level of network and information security across the Union

The Tallin Manual on the International Law Applicable to Cyber Warfare

US National Military Strategy for Cyberspace Operations

1035/2012 Kormányhatározat Magyarország Nemzeti Biztonsági Stratégiájáról

1139/2013 Kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

Az elektronikus hírközlésről szóló 2003. évi C. törvény

A médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtási rendelete (65/2013 Kormányrendelet)

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény