16. Kiberbiztonság

Berzsenyi Dániel

Biztonság – kibertér – kiberbűnözés – magánszféra – internet – rosszindulatú szoftver – aszimmetrikus hadviselés – EBESZ – ENSZ – Európai Unió – NATO

Az államokat és a nemzetközi rendszert fenyegető 21. századi biztonsági kihívások számbavétele során különös figyelmet kell fordítanunk az információs társadalom kialakulásának és fejlődésének biztonsági vetületeire. Bár a könyvben tárgyalt jelenségek között történeti szempontból a kibertérből érkező kihívások és fenyegetések valószínűleg a legfiatalabbak közé sorolhatók, mégis komoly szakirodalommal rendelkező területről van szó. A kiberbiztonság történetével foglalkozó írások alapján az 1970-es évekre tehető azoknak a kártékony számítógépes programoknak a megjelenése, amelyek képesek voltak saját magukat reprodukálni, és a ma ismert internet elődjeként számon tartott ARPANET számítógépei között terjedni. A működési alapok tekintetében azonban egészen az 1940-es évekig kell visszamennünk az időben, ugyanis Neumann János matematikus ekkor fektette le az önmaga reprodukálására képes automata elméleti alapjait. (Chen–Robert 2004, 3.) Mindez önmagában még nem igényelne kitüntetett figyelmet, azonban a kibertérből érkező kihívások dinamikája, a rendkívüli mértékű technológiai fejlődés és tudástranszfer, a felhasználói tudatosság alacsony szintje és az okozott károk nagysága már olyan kombinációt eredményez, ami a kibertér biztonságos működését és használatát a 21. század egyik leginkább összetett kihívásává teszi.

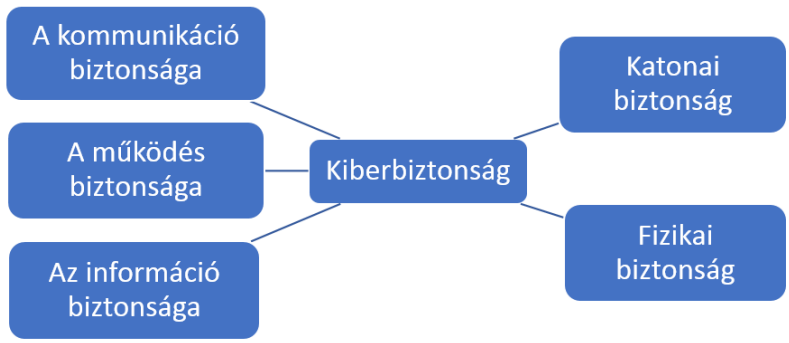
16.1. A kiberbiztonság fogalma és helye a biztonsági kihívások között

Általános és leegyszerűsített megközelítést alkalmazva elmondható, hogy a kiberbiztonság a biztonsági kihívásoknak azon területe, amely a kibertér működésének és használatának biztonsági dimenzióival foglalkozik. Azonban a kiberbiztonság meghatározásakor a biztonsági tanulmányokból ismert terminológiai problémákba ütközünk. Ahogy a biztonságnak nincs egységesen elfogadott definíciója, a kiberbiztonság kapcsán sem található olyan meghatározás, amelyet a nemzetközi szervezetek és az államok egyformán használnának. Sokkal inkább jellemző, hogy minden kiberbiztonsággal foglalkozó kiadvány – legyen szó stratégiai dokumentumról, jogszabályról vagy katonai doktrínáról – saját megközelítést alkalmaz, és ennek megfelelően definiálja a kiberbiztonságot. A kiberbiztonság definiálására már csak azért is szükség van, mert ezen a téren egyre intenzívebbek a nemzetközi elvárások, és a terminológia következetes alkalmazásának szerepe is fokozatosan növekszik, ahogy egyre több együttműködés alakul ki a kibertér használatával és védelmével kapcsolatban. A kiberbiztonság

https://doi.org/10.36250/00797_16

(cybersecurity) kifejezés alapvetően a kibertér (cyberspace) és a biztonság (security) közötti összefüggések meghatározására alakult ki, amelyet nemcsak az informatikai szakemberek használnak, hanem stratégiai tanácsadók és elemzők éppúgy, mint az iparági lobbisták vagy a politikai szereplők. Ezen a ponton számtalan kérdés merülhet fel a kifejezés tartalma és használata kapcsán, vagy akár az érintett folyamatok, eszközök és felhasználók tekintetében. A kiberbiztonság fogalmi kereteinek megállapítását tovább bonyolítja a média egyre erősödő figyelme, amelynek köszönhetően számos kifejezés helytelenül terjed el a köztudatban. Ez alól a kiberbiztonság sem képez kivételt, a tömegtájékoztatásban túl általános és sokszor leegyszerűsített formában használják az olyan eseményekkel kapcsolatban, amelyek a számítógépek működését megzavarják. (Beláz–Berzsenyi 2017, 2.) A kiberbiztonság meghatározását illetően az egyik leginkább kézenfekvő segítséget a kiberbiztonsággal foglalkozó stratégiai dokumentumok jelentik, amelyek közül a Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat a következőt rögzíti. Az 5. pont szerint: „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." Tekintettel arra, hogy az ehhez hasonló nemzeti meghatározások sehol máshol a világon nincsenek használatban teljesen azonos formában, a kiberbiztonság ügyét zászlóikra tűző nemzetközi szervezetek az utóbbi években inkább arra fókuszálnak, hogy legalább azokat az alapvető tartalmi komponenseket meghatározzák, amelyek a fogalom definiálásához szükségesek. Az Európai Unió területén a kiberbiztonság egyik legfőbb letéteményese az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (a továbbiakban: ENISA), amely 5 pontban foglalta össze azokat a területeket, amelyeket a kiberbiztonság meghatározásakor figyelembe kell venni (ENISA 2015, 11–12.):

1. A kommunikáció biztonsága: a technikai infrastruktúra védelme olyan fenyegetésekkel szemben, amelyek az infrastruktúra sajátosságainak megváltoztatásával a tulajdonosok, a tervezők vagy a felhasználók szándékaitól eltérő tevékenységre használhatók.
2. A működés biztonsága: védelem az eljárások és munkafolyamatok szándékos megzavarásával szemben.
3. Az információ biztonsága: védelem az információs rendszerben tárolt vagy továbbított adat lopásával, törlésével vagy megváltoztatásával szemben.
4. A fizikai biztonság: védelem a fizikai fenyegetésekkel szemben, amelyek befolyásolhatják az információs rendszert (például: fertőzött hardver telepítése a számítógéphez vagy számítógépes hálózathoz történő hozzáférés révén).
5. Közbiztonság/nemzetbiztonság: védelem az olyan kibertérből érkező fenyegetésekkel szemben, amelyek a kibertérben vagy fizikailag bekövetkezett károkozással képesek politikai, katonai vagy stratégiai előnyt szerezni a támadó számára (például: a 2010-ben felfedezett Stuxnet, vagy a kritikus információs infrastruktúrák elleni nagy méretű szolgáltatásmegtagadással [Denial of Service] járó támadások).



16.1. ábra

A kiberbiztonság fogalmába tartozó különböző területek az ENISA meghatározása alapján

Forrás: ENISA 2015, 11.

Kiberbiztonsági definíciók és alapfogalmak

Kibertér: a kibertérnek számos definíciója létezik, amelyek közül érdemes kiemelni a szabványosításért felelős nemzetközi szervezet meghatározását, amely szerint a kibertér egy komplex környezet, amely ember, szoftver és szolgáltatások interakciója nyomán az internetre csatlakoztatott technikai eszközök és hálózatok révén jön létre, és fizikai formában nem létezik. (Maurer–Morgus 2014)

Kiberbiztonság (+2): a kiberbiztonság tekintetében a magyar stratégia meghatározásán túl érdemes ismerni még néhány definíciót, például az ISO/IEC szerint a kiberbiztonság nem más, mint az információ bizalmasságának, integritásának és rendelkezésre állásának megőrzése a kibertérben. (ISO/IEC 2012) A NIST szintén nem túl terjedelmes meghatározása pedig így szól: a kiberbiztonság nem más, mint a kibertér kibertámadásoktól történő védelmének képessége. (Kissel 2013)

Kibertámadás: a Tallin Manual szerint a kibertámadás olyan kibertérben végrehajtott offenzív vagy defenzív művelet, amelytől indokkal várható, hogy személyi sérülést vagy halált, illetve anyagi kárt és megsemmisülést okoz. (Schmitt 2017)

Kiberháború: a kiberháború amerikai–orosz meghatározás szerint olyan eszkalált állapot egy államok között fennálló kiberkonfliktusban, amely során kiber-infrastruktúrák ellen katonai művelet részeként kibertámadásokat hajtanak végre állami szereplők. A kiberháború lehet deklarált és de facto.

Kiberhigiénia/tudatosság: a kiberhigiénia azoknak az általános érvényű szabályoknak az összeségére utal, amelyek a kibertérben, illetve a kibertér használata közben tudatosan és célirányosan követendők a biztonságunk megőrzése érdekében. A biztonságtudatosság szorosan kapcsolódó fogalom, amelynek szintén kevés meghatározása van, de az alábbiak szerint lehet leírni: a biztonságtudatosság „feltételezi, hogy az érdekelt összefüggéseiben ismerje, hogy a számára fontos érdek, tárgy, viszonyrendszer milyen értéket képvisel, és legyen tisztában azzal, hogy mit jelenthet ez az ellenérdekelt fél részére”. (Biztonságpiac 2010)

A kiberbiztonság helyének meghatározása a biztonsági kihívások között a definiáláshoz szükséges összetett szemléletmódot és átfogó megközelítést igényel. A legtöbb biztonsági kihívást nem lehet steril módon elkülöníteni egymástól, így minden esetben maradnak bizonyos mértékű átfedések egy vagy több területtel, amelyek így kölcsönösen hatást gyakorolnak egymásra. Az ilyen típusú összefüggések kapcsán kiváló példa a fegyveres konfliktusokból fakadó megannyi kihívás a migráció, a környezetbiztonság vagy éppen a gazdasági biztonság területén. Azonban a kiberbiztonság egyedülálló helyet foglal el a biztonsági kihívások halmazában, mert szinte minden más kihívással van közös metszete, vagy ha a gondolatot megfordítjuk, akkor minden biztonsági kihívásnak van kiberbiztonsági szegmense. A kiberbiztonsági kihívások egyre jelentősebb tényezőként tűnnek fel a fegyveres konfliktusokban vagy a nemzetbiztonság szintjén. Eközben az ipari folyamatirányító rendszerek által részben vagy egészben automatizált nyersanyag-kitermelő és energiaellátó rendszerek informatikai sebezhetőségei soha nem látott mértékben befolyásolhatják egy ország vagy egy egész régió energiabiztonságát és erőforrásokhoz való hozzáférését. A robotizálás, illetve a navigációs és nyomkövető rendszerekhez használt informatikai eszközök hasonló helyzetet eredményeznek a tengeri biztonság terén, míg az egészségügyi nyilvántartások és ellátás digitalizálása a szociális biztonságra és az emberi életre is közvetlen veszélyt jelent. A kiberbiztonsági kihívásoknak számos formája van, azonban a rendkívül gyors anyagi haszonszerzés lehetősége, a visszakövethetetlenség vagy éppen a teljes titokban történő működés potenciálja a digitalizációt az olyan illegális tevékenységekre is kiterjeszti, mint a fegyver-, a kábítószer- vagy az emberkereskedelem. A szervezett bűnözés klasszikus formái mára már szinte kivétel nélkül léteznek digitalizált változatban, ezért egyre több szervezett bűnözői csoport terjeszti ki működését a kibertérre, ami jelentős kihívások elé állítja a szervezett bűnözés ellen küzdő szervezeteket nemzeti és nemzetközi szinten egyaránt. Ha a leírtakat anyagi megvilágításba helyezzük, nyilvánvalóvá válik, hogy a kiberbiztonsági kihívásokból fakadó károk olyan többletköltséget, illetve pénzügyi vagy reputációs veszteséget jelentenek, amelyek direkt és indirekt módon egyaránt képesek veszélyeztetni a gazdasági biztonságot. A fentieken túl megjegyzendő, hogy a kiberbiztonsági kihívások folyamatos és dinamikus növekedést mutatnak, aminek elsődleges oka az, hogy a mindennapi életünket egyre inkább átszövi a digitalizáció, és a társadalmi folyamatok egyre nagyobb arányban zajlanak a kibertérben, vagy annak felhasználásával. Többek között ennek a dinamikus növekedésnek is köszönhető, hogy a kibertérből érkező kihívásokkal és a kibertér biztonságos használatának különböző dimenzióival egyre több nemzetközi szervezet egyre magasabb szinten foglalkozik. Azonban a nemzetközi szervezetek szerepvállalásának áttekintése előtt vessünk egy pillantást a kibertérből érkező kihívások kategorizálására.

16.2. Kiberbiztonsági kihívások

A kiberbiztonsági kihívások többféle módon csoportosíthatók, ezért a definícióhoz hasonlóan nem található olyan felosztás, amit mindenki egyöntetűen alkalmazna. Ennek hátterében az áll, hogy a kiberbiztonsági kihívások számos eltérő szempontrendszer alapján vizsgálhatók. A kiberbiztonsági kihívások kapcsán az átlagember a médiában leggyakrabban előforduló kibertámadásokra asszociál, azonban a kibertér biztonsága és védelme túl-

mutat a támadások egyszerű felsorolásán és megkülönböztetésén. Tágabb értelemben véve a kiberbiztonsági kihívások magukban foglalják a támadások megelőzése, a felhasználók tudatossága vagy a technológiai fejlődés kapcsán felmerülő problémákat is, de egy olyan entitás számára, ahol korábban nem foglalkoztak kiberbiztonsággal, a hatékony kiberbiztonsági szabályozás és szervezeti struktúra kialakítása szintén kihívást jelenthet. A terjedelem korlátozottsága miatt nincs lehetőség minden egyes kiberbiztonsági kihívás részletes bemutatására, így azok számára, akik fokozott érdeklődést tanúsítanak a kiberbiztonság iránt, ajánlott a speciális szakmai kurzusok és tréningek elvégzése. Ha a kiberbiztonsági kihívásokat pusztán a támadásokra szűkítjük le, még mindig többféle megközelítést alkalmazhatunk. A kiberbiztonsági támadások motivációjukat tekintve szinte kivétel nélkül besorolhatók valamelyik kategóriába az alábbiak közül:

- politikai/ideológiai;
- pénzügyi/gazdasági;
- hírszerzési/kémkedési;
- hacktivista;
- vagy destruktív indíttatású.

Ha a kibertámadásokat a motiváció szempontjából közelítjük meg, akkor a lista élén a pénzügyi, illetve gazdasági haszonszerzés okán elkövetett támadásokat találjuk, miközben egyre jelentősebb arányt képviselnek a hírszerzési, illetve kémkedési céllal indított, leginkább állami szereplők által vagy állami szereplő támogatásával megvalósuló támadások. Sorrendben a politikai és ideológiai motiváció következik, ahova a gyakran külön kezelt terrorizmus ténylegesen tartozik, hiszen a terroristák végső célja a saját politikai, ideológiai vagy vallási akaratuk másokra történő rákényszerítése. A motivációk között az utolsó előtti helyre került hacktivizmus kapcsán fontos kiemelni, hogy a legismertebb hacktivista mozgalmak (Anonymous, LulzSec) általában valamilyen politikai vagy ideológiai cél köré szerveződnek, így ezek támadásai – akárcsak a terrorizmus – a végső cél tekintetében a politikailag, illetve ideológiailag motivált támadások közé sorolhatók. A hacktivizmusnak mára kevésbé domináns ága, amikor valaki csak azért hajt végre egy kibertámadást, hogy a képességeit bizonyítsa saját maga, a megtámadott vagy egy harmadik fél számára. Miközben a kvázi kedvtelési célú támadások eltűnőfélben vannak, feltűntek olyan kibertámadások, amelyeknek egyetlen célja a rombolás és pusztítás, elsősorban a kibertér működését és használatát biztosító eszközök tönkretételével. A kibertámadások trendjei folyamatosan változnak, így könnyen találhatunk olyan csoportosítást, ahol a destruktív és a politikai, illetve ideológiai támadásokat a kiberhadviselés címszó alatt gyűjtik össze. Minden esetben érdemes arra ügyelni, hogy az adott kategorizálást milyen metodika mentén alakították ki, és milyen céllal. A kibertérből érkező kihívások egy másik módon történő csoportosítása, amit sokszor ötvöznek a motivációval, az a támadó és a megtámadott szervezet között fennálló kapcsolatra utal. A kibertámadások kapcsán sokakban él az a téves prekoncepció, hogy a támadások az adott rendszeren vagy szervezeten kívülről érkeznek, és a szervezet számára ismeretlenek az elkövetők. Azonban a valóság az, hogy a kibertámadások jelentős része köthető valamilyen belsős közreműködéshez, mint például jelenlegi vagy korábbi munkavállaló szándékos vagy nem szándékos tevékenysége. Látható, hogy a belülről érkező fenyegetések rögtön tovább bonthatók két újabb kategóriára. Az információs rendszerek auditálásával és biztonságával foglalkozó szakembereket tömörítő nemzetközi szervezet

(Information Systems Audit and Control Association – ISACA) felmérése alapján 2016-ban a 3 legjelentősebb kiberbiztonsági kihívás között negyven százalékkal a második helyen voltak a belülről érkező fenyegetések. (DIMITRIADIS 2016) Tekintettel arra, hogy a kiberbiztonság nemcsak technológiai, hanem jelentős mértékben humán kihívás is, minden esetben kiemelt figyelmet kell fordítani az emberi tényezőre, a végfelhasználóra. A kibertérből érkező kihívások tovább elemezhetők a támadások típusának meghatározásával, azonban fontos megjegyezni, hogy napjainkban a különböző technikákat és eljárásokat a támadók legtöbbször kombináltan alkalmazzák, aminek számos oka lehet. Az úgynevezett elosztott szolgáltatásmegtagadással járó (Distributed Denial of Service – DDoS) támadásokat például gyakran alkalmazzák önmagukban egy-egy nagyobb rendszer megbénítására és elérhetetlenné tételére, de nem ritka, hogy csak elterelésként vetik be azért, hogy egy szofisztikáltabb műveletet leplezzenek vele. Napjainkban gyakoriak az úgynevezett „phishing", illetve „social engineering" támadások, amelyek a felhasználók megtévesztésén alapulnak, és elsősorban információ megszerzésére irányulnak (például személyes adatok, online banki bejelentkezéshez szükséges adatok, vállalati belső információ stb.). Egy-egy ilyen támadást jellemzően valamilyen rosszindulatú szoftver, úgynevezett „malware" bevetése követ, amelyek számtalan funkciót és feladatot képesek ellátni az áldozat számítógépén vagy okostelefonján anélkül, hogy tudomást szerezne róla. Ezen a ponton válik érdekessé a támadó motivációja, hiszen ha valaki kémkedni akar, attól nagy valószínűséggel nem kell féltenünk a pénzügyi hozzáféréseinket, annál inkább a vállalati kommunikációt (például: azonnali üzenetküldők, elektronikus levelezés stb.) és a céges dokumentumokat. Ez többnyire fordítva is igaz, ha egy anyagi haszonszerzési céllal indított kibertámadás áldozatává válunk, akkor elsősorban a bankszámlánk megcsapolása, illetve az ismeretlen tranzakciók miatt érdemes aggódni, ettől még a személyes fotó- vagy videógyűjteményünk nem kerül veszélybe. Más a helyzet az úgynevezett zsarolóvírusok esetében, amelyek az áldozat eszközére települve titkosítanak minden adatot, amelyekhez csak váltságdíj megfizetése után férhetünk hozzá újra, ha szerencsénk van, és megkapjuk a feloldókulcsot a támadótól. A kibertér bizonyos szegmensei kimondottan veszélyesek az átlagfelhasználó számára, ezért is fontos az általános kiberbiztonsági tudatosság növelése, a kiberhigiénia megteremtése már a legfiatalabb generáció esetében is. Sajnos ezen a téren nem áll túl jól társadalmunk, nem véletlen, hogy a legtöbb nemzetközi szervezet kiberbiztonságot érintő napirendjén kiemelt helyen szerepel a képzés, oktatás és a tudatosság növelése.

Kiberbiztonsági kihívások és támadások (DDoS, vírus, féreg, phishing stb.)

Rosszindulatú szoftver: olyan szoftver, amelyet szándékosan arra terveztek, hogy kárt okozzon egy számítógépben, szerverben vagy számítógépes hálózatban.

Vírus: olyan számítógépes kód, amely képes önmagát másolni és hátrányos hatást kiváltani a rendszer elrontásával vagy adat megsemmisítésével.

Féreg: a számítógépes féreg olyan önálló rosszindulatú számítógépes program, amely képes önmagát sokszorozni annak érdekében, hogy más számítógépekre átterjedjen. Gyakran a megtámadott rendszer hibáját kihasználva számítógépes hálózatot használ a terjedéshez.

Trójai: az informatika világában a trójai faló olyan rosszindulatú számítógépes program, amely megtéveszti a felhasználót a valódi céljai, illetve funkciói tekinte-

tében. Jellemzően valamilyen „social engineering" támadással kerülnek az áldozat számítógépére, például egy e-mail-csatolmány megnyitásával, és bár számos modern formájuk megtalálható, jellemzően valamilyen hátsó ajtót nyitnak a támadók számára a megtámadott rendszeren.
Phishing/adathalászat: olyan eljárás, amelynek keretében csalók egy jól ismert szervezet nevében hamis oldalt hoznak létre az eredetire megszólalásig hasonló formában, és így személyes adatokat, azonosítókat, jelszavakat, bankkártyaszámot és más információkat próbálnak illetéktelenül megszerezni. Azt, hogy az oldalt minél többen meglátogassák, a csalók általában e-mailben, illetve azonnali üzenetküldőben népszerűsítve próbálják meg elérni.
Social Engineering: vagyis pszichológiai manipuláció, amikor egy megtévesztés nyomán egy jogosult személy adatokat ad át vagy hozzáférést biztosít egy jogosulatlan személynek. Az emberi természet két aspektusát, a segítőkészséget és a konfliktuskerülést célzó nem technológiai jellegű behatolás, amely az emberi interakciókon alapul. Napjainkban a legtöbb kibertámadás kezdeti szakaszában jut szerephez a pszichológiai manipuláció és az így megszerzett információ.
DDoS: az elosztott szolgáltatásmegtagadással járó vagy más néven elosztott túlterheléses támadás a számítógépes rendszer, illetve informatikai szolgáltatás teljes vagy részleges megbénítását, elérhetetlenségét eredményezi. Jellemzően egy ismert gyengeséget vagy sérülékenységet használnak ki a támadók, amivel az információ rendelkezésre állását veszélyeztetik elsősorban.
Zsarolószoftver (zsarolóvírus): olyan kártékony szoftver, amely fenyegetés révén próbál anyagi hasznot szerezni a támadónak. Általában ez azt jelenti, hogy a szoftver használhatatlanná teszi a számítógépet, vagy elérhetetlenné az azon tárolt adatokat, és csak pénz (váltságdíj) kifizetése után állítható vissza az eredeti állapot.

16.3. Az ENSZ fellépése a kiberbiztonsági kihívásokkal szemben

A 193 tagországot tömörítő Egyesült Nemzetek Szervezete a legnagyobb nemzetközi fórum a világon, amelynek keretén belül különböző kormányközi testületekben és szervezeti platformokon folyik a kiberbiztonsági kihívásokkal kapcsolatos munka. Bár számos entitás hozhat határozatot kiberbiztonsági kérdések kapcsán, a legtöbbet az ENSZ Közgyűlésének (UN General Assembly – UNGA) vagy az ENSZ Biztonsági Tanácsnak (UN Security Council – UNSC) el kell fogadnia. Utóbbi kivételével az ENSZ kiberbiztonsági határozatai jogilag nem kötelező érvényűek a tagországok számára, az ENSZ BT azonban még nem fogadott el kiberbiztonsági kérdésekkel kapcsolatos határozatot. Az egyik legfontosabb kiberbiztonsági ügyekkel foglalkozó ENSZ-testület a Leszerelési és Nemzetközi Biztonsági Kérdések Főbizottsága, amely a kibertér olyan kulcsfontosságú nemzetállami szereplőit ülteti egy asztalhoz a legmagasabb diplomáciai szinteken, mint Kína, Oroszország és az Amerikai Egyesült Államok. 1998 óta az orosz kormány kezdeményezésére a bizottság minden évben határozati javaslatot készít az ENSZ Közgyűlés számára az információs és telekommunikációs fejlesztések biztonsági vetületeiről. 2001-ben szintén orosz kezdeményezésre létrejött egy kormányzati szakértőkből álló csoport (Group of Governmental Experts – GGE) 15 ország részvételével annak

érdekében, hogy felmérjék a potenciális fenyegetéseket és a lehetséges együttműködési lehetőségeket az információbiztonság terén. Három évvel később a csoport első gyűlésén nem sikerült konszenzuson alapuló jelentést kiadni a nemzetközi információbiztonsághoz kapcsolódó jelentősen eltérő kulcsfontosságú nézőpontok miatt. A sikertelen munkát 2009-ben egy újabb csoport létrehozása követte, amelynek már sikerült konszenzusos jelentést elfogadnia, 2011-ben pedig egy harmadik csoportot is alakítottak. A harmadik csoport által készített jelentés a nemzetközi kiberbiztonsági normák fejlesztésével foglalkozott elsősorban, és megerősítette a nemzetközi jog – ezen belül is az ENSZ Alapokmány – alkalmazhatóságát a kibertérrel összefüggésben. Bár 2014 és 2015 között egy negyedik GGE is eredményesnek bizonyult, a konszenzus csak látszólagos, nincs egyetértés azzal kapcsolatban, hogy a jelenlegi nemzetközi joganyag pontosan miként alkalmazható a kibertérben. Ezt erősíti a 2016 és 2017 folyamán létrehozott GGE sikertelensége, amelynek egyik fő feladata volt tanulmányozni az információbiztonság terén meglévő és potenciális fenyegetéseket, valamint felmérni a kapcsolódó normákat, szabályokat és alapelveket az államok felelős viselkedésével, a bizalomerősítő intézkedésekkel és a kapacitások kiépítésével összefüggésben. A német képviselő elnökségével 25 tagállami szakértő bevonásával működő csoport másik fontos feladata volt tanulmányozni a nemzetközi jog alkalmazhatóságát az információs és telekommunikációs technológia állami felhasználása során. A jelek szerint a nemzetközi jog és annak alkalmazhatósága volt az a kritikus pont, amely végül a csoport eredménytelenségéhez vezetett. Ezzel kapcsolatban az amerikai képviselő, Michele Markoff nyilatkozatot adott ki, amelyben úgy fogalmaz (Korzak 2017), hogy a konszenzusos jelentés elkészítését alapvetően gátolta néhány résztvevő ellenállása, a nemzetközi jogi kérdésekben való komoly elköteleződéssel szemben. Válaszként a kubai képviselő azzal érvelt, hogy az egyoldalú büntető szankciók és a katonai erő alkalmazásának legitimizálása a kibertér militarizálásához vezet, miközben a csoportnak éppen a kibertér békés használatára és a konfliktusmegelőzésre kellene koncentrálnia. Bár az elérhető források alapján csak a kubai nyilatkozat publikus, valószínűsíthető, hogy az orosz és kínai álláspont a kubaihoz nagyon hasonló volt. A 2016–2017-es GGE sikertelensége megoldatlanul hagyta az egyik legfontosabb nemzetközi jogi vitát, és bizonytalanná tette a szélesebb nemzetközi párbeszéd folytatását is a kiberbiztonság és a nemzetközi jog határterületén.

Az ENSZ 2. számú (Gazdasági és Pénzügyi Főbizottság) bizottsága a 2000-es évek eleje óta három kibertérhez kapcsolódó határozatot is a Közgyűlés elé terjesztett (2002, 2003, 2009), amelyek a kiberbiztonság globális kultúrájának létrehozására fókuszáltak. A Szociális, Humanitárius és Kulturális Főbizottság alapvetően a kiberbűnözéssel és a magánélethez való jogokkal kapcsolatos kérdésekkel foglalkozik, aminek eredményeként 2000-ben és 2001-ben két határozatot készített az információs technológia bűnözői célú felhasználása és a visszaélések elleni fellépésről. Szintén foglalkozik a kiberbűnözés elleni fellépéssel az ENSZ Gazdasági és Szociális Tanácsa (ECOSOC), valamint annak funkcionális bizottságai. 2013-ban – részben az Edward Snowdenhez kötődő leleplezések nyomán – a Közgyűlés elfogadta a „Magánélethez való jog a digitális korban" című határozatot. A dokumentum kihangsúlyozza az államok felelősségét a magánszféra tiszteletben tartása és védelme kapcsán, és elsőként erősíti meg, hogy az emberek jogait az online és offline világban egyformán védeni kell. A határozat

nyomán az ENSZ emberi jogi főbiztosa jelentést készített a témában, illetve 2015-ben a magánszférához való jogért felelős rendkívüli megbízottat is kineveztek.

Az ENSZ kiberbiztonság terén folytatott tevékenysége kapcsán fontos megemlíteni a szakosított szervek közül a Nemzetközi Távközlési Egyesületet (International Telecommunication Unit – ITU), illetve a 2006-ban az ENSZ főtitkára által létrehozott Internet Irányító Fórumot, amely az online világ szabályozásának kialakítása terén játszik szerepet. Az ITU-val összefüggésben a 2003-as és 2005-ös Információs Társadalom Világcsúcstalálkozót (World Summit on the Information Society – WSIS) érdemes megjegyezni, amelyek nyomán 2007-ben létrejött egy globális kiberbiztonsági fórum (Global Cybersecurity Agenda – GCA) a bizalom és biztonság erősítésére az információs társadalomban. A fórum együttműködik a kiberfenyegetések elleni multilaterális szövetséggel (International Multilateral Partnership Against Cyber Threats – IMPACT), amely a közszereplők és a magánszektor bevonásával foglalkozik a korai előrejelző rendszerek, az incidenskezelés és az ezeket elősegítő globális platform létrehozásával. Az ITU felelős az ENSZ Globális Kiberbiztonsági Indexért (Global Cybersecurity Index – GCI), amely a világ kiberbiztonsági helyzetét vizsgálja azzal a céllal, hogy segítse a fejlődő országokat a biztonsági hiányosságok kezelésében, és globális szinten ösztönözze a kiberbiztonsági erőfeszítéseket. Az IGF tevékenységének fókuszában internethez kötődő közpolitikai kérdések és kulcsfontosságú témakörök állnak, úgymint az internet fenntarthatósága, biztonsága, stabilitása és szilárdsága, valamint a fejlődése. A fórum további feladata a párbeszéd és információcsere serkentése, valamint a jó gyakorlatok megosztása és tanácsadás az érdekelt felek számára.

16.4. Az Európai Unió szerepvállalása a kiberbiztonság terén

Az Európai Unió 2004-ben hozott döntést arról, hogy szakmai szervezetet állít fel az információbiztonság területen végzendő technikai és tudományos feladatok koordinálására. A szervezetet formálisan az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az Európai Hálózat- és Infromációbiztonsági Ügynökség létrehozásáról című jogi aktus hívta életre, amelyet 2008-as és 2011-es módosítását követően 2013-ban helyezett hatályon kívül az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA). A rendelet kiadását követően az ENISA végül 2005 szeptemberében Krétán kezdte meg működését azzal a célkitűzéssel, hogy az EU-tagállamok és az üzleti szféra képességeit erősítsék a hálózat- és információbiztonság területén, elsősorban a problémák megelőzése, kezelése és a rájuk történő reagálás kapcsán. Az ENISA egyúttal a Bizottság mellett működő tanácsadó testületként is funkcionál, továbbá felkérés esetén részt vesz a jogszabályok korszerűsítését és kidolgozását megelőző technikai előkészítő munkában. A biztonság megfelelő szintjének elérése érdekében az ügynökség segíti a tagállamokat, és igyekszik fokozni az együttműködést az állami és a magánszektor szereplői között. Feladatai közé tartozik többek között a kockázatok elemzéséhez szükséges információk gyűjtése, tájékoztatás nyújtása a tagállamok és a Bizottság számára, a biztonsági problémák megelőzésére szolgáló közös módszerek kidolgozása, hozzájárulás a tudatosság növeléséhez, a biztonsági szabványok kialakításának követése, valamint a saját kutatásokból fakadó

következtetéseinek és iránymutatásainak megfogalmazása. A több mint 10 éves múlttal rendelkező szervezet számos dokumentumot (iránymutatást, ajánlást, útmutatót és kézikönyvet) adott ki, amelyekből a kiberbiztonság fogalmának meghatározásánál egyre már utaltunk is.

Az Európai Unió életében a következő mérföldkőnek tekinthető momentum a 2013 februárjában elfogadott uniós szintű kiberbiztonsági stratégia és a hozzá társuló Hálózat- és Információbiztonsági Irányelv (NIS). Az Európai Parlamentnek, a Tanácsnak, Az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának közös közleménye „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér" címmel jelent meg. A bevezető részben leírtak alapján három fő motivációs elem mentén jött létre a stratégia. A stratégia megszületését egyrészt gazdasági okok vezérelték, mivel az EU növekedése egyre jelentősebb mértékben függ az információs és kommunikációs rendszerektől, másrészt az EU kiberbiztonsági képességeinek fejlesztésére irányuló politikai célok is szerepet játszottak. A harmadik meghatározó tényező a stratégia kiadásában az EU azon szándéka volt, hogy a kibertérben is megvédje az alapvető jogokat, a demokráciát és a jogi normákat. Bár az említett motivációs faktorok nem egyedülállók, a tagországok eltérő kiberbiztonsági képességei miatt szükség van a magas szintű harmonizációra és koordinációra. A stratégia megvalósítása érdekében a stratégia öt alapvető prioritást és intézkedést fogalmaz meg:

- kibertámadásokkal szembeni ellenálló képesség elérése;
- a számítástechnikai bűnözés drasztikus csökkentése;
- kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (CSDP) tekintetében;
- kiberbiztonsági ipari és technológiai erőforrások kifejlesztése;
- összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, és az Európai Unió alapértékeinek támogatása.

A stratégia külön kiemeli annak jelentőségét, hogy az ipari és más nemzetközi szereplőkkel történő együttműködést jelentősen fokozni kell az ellenálló képesség és a kibervédelem növelése, valamint a kiberbűnözés csökkentése érdekében.

A stratégiához szorosan kapcsolódó, nagy jelentőséggel bíró uniós dokumentum az EU 2016/1148 irányelve (2016. július 19.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről címet viseli, a szakemberek pedig NIS-irányelvként hivatkoznak rá. A NIS-irányelv az első olyan közösségi szintű szabályozás információbiztonsági területen, amely kötelezően és geopolitikai alapon határoz meg szabályokat és kötelező együttműködést az érintett intézmények számára. Az elsődleges célja a harmonizáció minimális szintjének elérése. Bár az irányelv megjelenése előtt is megfigyelhető volt a tagállamok információbiztonsággal foglalkozó szervezetei közötti együttműködés, jobbára csak önkéntességen, illetve kölcsönös bizalmon alapult. Ugyanakkor az irányelv előírja a tagállamok számára a minimális nemzeti kiberbiztonsági kapacitások kiépítését és fenntartását, így például nemzeti szintű kiberbiztonsági stratégiák elkészítését, kiberbiztonsági hatóságok felállítását, illetve a kiberbiztonsági incidensekre reagálni képes szervezetek (Computer Emergency Response Team – CERT) létrehozását.

CERT/CSIRT

A számítógépes vészhelyzeti reagáló csapatok olyan szakértőkből álló szervezeti egységek, amelyek képesek kezelni a számítógépes rendszerekben fellépő biztonsági incidenseket. Alternatív névként találkozhatunk a számítógépes biztonsági incidens reagáló csapat (CSIRT) elnevezéssel is. Jellemzően nemzetközi szervezetek, államok, illetve nagy kitettséggel bíró iparágak, esetleg nagyvállalatok tartanak fenn ilyen gyorsreagálású csapatokat.

A létrehozott szervezeteknek egyfelől monitorozniuk kell a különböző szolgáltatókat (például: kritikus infrastruktúra vagy digitális szolgáltatók) és együttműködni a más tagországok által létrehozott hasonló szervezetekkel, másrészt az ENISA-val és az annak keretein belül működő CERT-EU-val. Utóbbit egyéves próbaidőszakot követően 2012 szeptemberében hozták létre. Állománya alapvetően a legfontosabb európai uniós intézmények információbiztonsági szakértőiből áll, és szoros együttműködést folytat a tagállami CERT-ekkel, illetve a kiberbiztonság területén működő vállalatokkal.

Az Európai Unió kiberbiztonság terén tett intézkedései kapcsán fontos megemlíteni egy további szervezetet, amelyet az Európai Unió rendőri szervének (Europol) keretein belül 2013-ban hoztak létre. Az európai kiberbűnözés elleni központ (European Cybercrime Centre – EC3) elsődleges feladata a szervezett formában elkövetett kiberbűnözés elleni fellépés, a kritikus információs infrastruktúrákat célzó, valamint a kiemelkedő károkkal járó támadások megelőzése és elhárítása. A feladatok végrehajtása három úgynevezett fókuszpont mentén zajlik:

- *Terminal:* nemzetközi pénzügyi csalások vizsgálata együttműködésben az Európai Központi Bankkal és a tagállamok nemzeti bankjaival, valós idejű hozzáférést biztosítva a központ adatbázisaihoz és kriminológiai elemzéseihez.
- *Cyborg:* a kritikus infrastruktúrák elleni high-tech bűnözéssel szembeni fellépés érdekében a rosszindulatú szoftvereket elemző rendszer (Europol Malware Analysis System – EMAS) fenntartásával támogatja a kriminológiai vizsgálatokat, valamint az egyesített nyomozati csoportok (Joint Investigation Team – JIT) munkáját a transznacionális fenyegetésekkel szemben.
- *Twins:* a gyermekek szexuális kizsákmányolása elleni tevékenységeket koordináló elem.

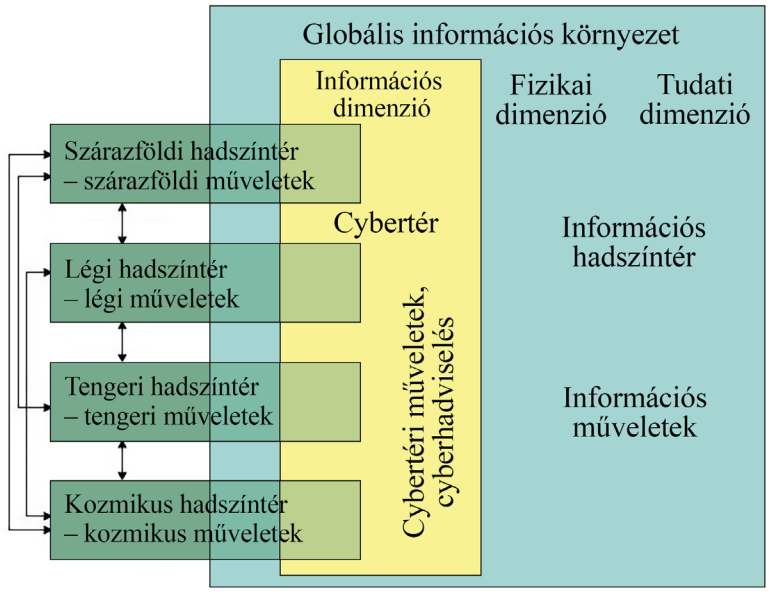
Az EC3 műveleteiben meghatározó szerepe van a hírszerző képességnek, amelynek keretében egy elemzőközpont kapcsolja össze a rendvédelmi szerveket, CERT-eket, illetve ipari és akadémiai közösségeket. Amennyiben intézkedés válik szükségessé, az erre létrehozott akciócsoport (Joint Cybercrime Action Taskforce – J-CAT) speciális szakértők bevonásával nemzetközi szintű választ képes adni a növekvő fenyegetésekre. Műveleti szinten fontos megemlíteni az EC3 keretei között kiépített uniós szintű digitális kriminológiai labort, amely a legmodernebb eszközeivel világszínvonalú nyomozati támogatást képes biztosítani, egyúttal független technológiai kutatást és fejlesztést folytat. Az EC3 stratégiai szerepkört is betölt, amelynek keretében politikai döntéshozók számára stratégiai elemzéseket készít, továbbá képzést biztosít a rendvédelmi szerveknek az EU-n belül és kívül egyaránt. Szintén a szervezet stratégiai szintű tevékenységeihez tartozik az általános tudatosság növelése, illetve a partneri kapcsolatok kialakítása nemzetközi szinten.

16.5. A NATO kiberbiztonsági tevékenysége

Az Észak-atlanti Szerződés Szervezetében – mint minden más területen is – a kiberbiztonsági kérdésekben a csúcstalálkozók a legfontosabb politikai szintű döntéshozatali fórumok. Bár a NATO mindig is védte saját kommunikációs és információs rendszereit, a kibervédelem kérdése 2002-ben került először napirendre a prágai csúcstalálkozón, majd négy évvel később a szövetség vezetői tovább szorgalmazták az információs rendszerek védelmének megerősítését. Egy évvel később az Észtországot ért kibertámadások hatására a NATO védelmi miniszterei úgy döntöttek, hogy sürgős intézkedéseket kell hozni ezen a téren, aminek eredményeként végül 2008 januárjában kiadták a NATO első jóváhagyott stratégiai szintű kibervédelmi dokumentumát (NATO Policy on Cyber Defence). A 2008-as grúz–orosz konfliktus során tapasztalt kibertámadások tovább ösztönözték a NATO döntéshozóit a szövetség kibervédelemhez kapcsolódó tevékenységének fokozására. Ennek nyomán 2010-ben Lisszabonban fogadták el azt a stratégiai koncepciót, amely konkrét lépéseket fogalmazott meg nemcsak egy, az akkor érvényben levőnél részletesebb kiberbiztonsági stratégiai dokumentum kidolgozására, de a végrehajtást szolgáló akcióterv elkészítésére is. A 2011-es második stratégiai kiberbiztonsági dokumentum kiadását követően a kibervédelem bekerült a NATO védelmi tervezési folyamatába, és létrehozták a szövetség Kommunikációs és Információs Ügynökségét (NATO Communications and Information Agency – NCIA). 2014 óta dedikált szervezet foglalkozik a kibervédelem szövetségi szintű stratégiai irányításával és a kapcsolódó védelmi tervezési feladatokal Kibervédelmi Tanács (Cyber Defence Committee – CDC) néven. Ugyanebben az évben érte el teljes műveleti képességét a NATO saját incidens reagáló képessége (NATO Computer Incident Response Capability – NCIRC), és ősszel elindulhatott a szövetség privát szektorral történő együttműködését célzó kezdeményezés (NATO Industry Cyber Partnership – NICP) is.

A kiberbiztonság terén az egyik legfontosabb mérföldkő a szövetség nevéhez kötődik, miután 2016. június 14-én a NATO védelmi miniszterei között egyetértés született arról, hogy a következő hónapban megrendezésre kerülő varsói csúcstalálkozón a kiberteret a hadviselés ötödik dimenziójaként ismerik el. Az elismerés önmagában nem változtatott a NATO korábbi hozzáállásán, amely szerint a szövetség tevékenysége védelmi jellegű. 2017 elején frissítették a kibervédelmi akciótervet, amelyben a legnagyobb hangsúlyt a képességfejlesztés és az információmegosztás kapta. 2017 végén újabb szervezeti egység felállításáról döntöttek a szövetség védelmi miniszterei, és létrehozták a Kiberműveleti Központot (Cyber Operations Centre) a Szövetséges Erők Európai Főparancsnokságának (SHAPE) alárendeltségében.

Az Észak-atlanti Szerződés Szervezetében a kiberbiztonsági kihívásokkal összefüggő tevékenységek egyik legmeghatározóbb szereplője a szervezet által akkreditált kibervédelmi központ, amelynek terveit Észtország terjesztette elő, közvetlenül 2004-es csatlakozását követően. A NATO Kooperatív Kibervédelmi Kiválósági Központ (NATO Cooperative Cyber Defence Centre of Excellence – NATO CCDCOE) alapítására vonatkozó elképzeléseket 2006-ban hagyta jóvá a Szövetséges Erők Transzformációs Főparancsnoka, és 2007-ben indultak meg a potenciális szponzornemzetek közötti egyeztetések. Észtország, Németország, Olaszország, Lettország, Litvánia, Szlovákia és Spanyolország 2008 májusában írta alá az alapításról szóló egyetértési megállapodást.



16.2. ábra

A hadviselés dimenziói és a kibertér viszonya Haig Zsolt és Várhegyi István ábrázolásában

Forrás: HAIG–VÁRHEGYI 2008, 3.

A központ a kiberbiztonság területén oktatással, konzultációval, tanulságok gyűjtésével, kutatással és fejlesztéssel foglalkozik, amihez 2008. október 28-án szerezte meg a teljes akkreditációt az Észak-atlanti Tanácstól. Számos online és nyomtatott formában is elérhető kiadvány köthető a központhoz, amelyek főként a kiberkonfliktusok és kiberhadviselés etikai, illetve jogi kérdéseivel, a megfelelő kibervédelem kialakításával, technológiai kérdésekkel, továbbá a kiberbiztonsági stratégiák kialakításával és fejlesztésével foglalkoznak. A központ egyik legfontosabb kiadványa a *Tallinni kézikönyv* (Tallinn Manual), amelynek első, 2013-as kiadása után négy évvel már a második változat is megjelent, és a világon elsőként ad jogi kereteket a kiberhadviseléshez. A dokumentum egyik legfontosabb megállapítása, hogy a kibertérben vívott háború is háborúnak tekintendő, még akkor is, ha a valódi fegyverek bevetése elmarad. Ennek következtében pedig egy országnak jogában áll egy kibertámadásra hagyományos fegyverekkel válaszolni, ha a kibertámadásból fakadó károk megközelítik vagy meghaladják egy hagyományos fegyveres támadás veszteségeit. A kézikönyv további jelentős iránymutatásai közé tartozik, hogy a kibertámadásban részt vevő civilek ellen is fel lehet lépni, mivel a támadásban való részvétel által elveszítik a civilekre vonatkozó védelmet. Fontos megjegyezni, hogy a kiberbiztonság terén kritikusnak számító bizonyíthatósággal kapcsolatban is állást foglal a kiadvány. Ez alapján akár egy állam által koordinált kibertámadásról, akár hacktivizmusról van szó, nem jelent elegendő bizonyítékot egy adott ország részvételére, hogy az incidens a területén található számítógépekről vagy a kormányzati rendszerekből érkezik.

A szövetség műveleti és technikai szintű kezdeményezései kapcsán említést érdemel a közös képességfejlesztési kezdeményezés (Smart Defence Initiative) keretein belül megvalósuló információmegosztó platform (Malware Information Sharing Platform – MISP), a multinacionális kibervédelmi képességfejlesztési projekt (Multinational Cyber Defence Capability Development – MN CD2), valamint a multinacionális kibervédelmi oktatási és kiképző projekt (Multinational Cyber Defence Education and Training – MN CD E&T). Képzési területen több szervezet is aktív a szövetségi struktúrában, egyrészt a már említett CCD COE is részt vesz az oktatásban és kiképzésben, valamint a Kommunikációs és Információs Rendszerek Iskola (NATO Communications and Information Systems School – NCISS) mellett további nagy múltú intézmények is szerepet vállalnak, így az Oberammergauban található NATO-iskola, vagy a NATO Védelmi Főiskolája Rómában.

16.6. Az EBESZ kiberbiztonsági törekvései

Az 57 tagállamot tömörítő Európai Biztonsági és Együttműködési Szervezet (Organization for Security and Co-operation in Europe) jelenleg a világ legnagyobb biztonsági szervezete, amelynek gyökerei egészen az 1970-es évekig nyúlnak vissza, és a kiberbiztonság terén hasonló szerepet próbál betölteni, mint a fegyverzetkorlátozás és -csökkentés terén. A szervezet a nukleáris és hagyományos fegyverek terén alkalmazott bizalom- és biztonságerősítő intézkedések mintájára igyekszik válaszokat adni a kibertérből érkező kihívásokra, azonban szakértői körökben ezek alkalmazhatósága és hatékonysága vitatott. Az EBESZ kiberbiztonság terén folytatott szerepvállalása elsősorban a kiberbűnüldözés és a terrorizmus elleni küzdelemre fókuszál. A Miniszterek Tanácsa (Ministerial Council) elsőként 2004-ben, illetve 2006-ban döntött arról, hogy nemzetközi együttműködés keretében kívánnak fellépni az internet terrorista célú felhasználásával szemben. 2008-ban a szervezet Parlamenti Közgyűlése (Parlamentary Assembly) felszólította a tagállamokat az aktív szerepvállalásra és együttműködésre a kiberbűnözés ellen, illetve a kiberbiztonság növelése érdekében folytatott tevékenységek kapcsán. A szervezet kiberbiztonság terén tett kezdeti lépéseit követően öt évre volt szükség ahhoz, hogy a tagállamok külügyminiszterei elfogadják az információs és kommunikációs technológia használatához köthető konfliktusok kialakulásának megelőzését célzó első bizalomerősítő (Confidence Building Measures – BCM) intézkedéscsomagot. A 2013 decemberében Kijevben elfogadott intézkedések (Decision No. 1106, 975th Plenary Meeting, PC Journal No. 975, Agenda item 1) főként a kibertérből érkező fenyegetésekkel kapcsolatos információmegosztásra, az információs és kommunikációs technológia használatára és biztonságára, valamint a nemzeti szintű szervezetekre, stratégiákra és az alkalmazott terminológiára fókuszáltak. Az intézkedéscsomagnak további fontos részét képezik a feszültségek csökkentését és a félreértések tisztázását célzó kockázatcsökkentő konzultációk, a megtett intézkedésekkel kapcsolatos információmegosztás a nyílt és biztonságos internet szavatolása érdekében, illetve a kapcsolattartók kijelölése és az EBESZ platformként történő alkalmazása a kiberbiztonság terén folytatott párbeszédek során. A 2013-ban elfogadott 11 bizalomerősítő intézkedést 2016-ban egy második csomag követte, amely 5 újabb ponttal egészítette ki az EBESZ intézkedéseit. Ezek főként az együttműködés és megelőzés gyakorlati aspektusaira fókuszálnak a védett kommuniká-

ciós csatornák kialakítása, a magánszektor bevonása, a kritikus infrastruktúrák védelmének fokozása, valamint a sérülékenységek megosztása révén.

Az EBESZ saját értelmezésében az egyik legalkalmasabb fórum arra, hogy a tagországok kölcsönös bizalmat alakítsanak ki a kibertérben, és a szervezetben felhalmozott jó gyakorlatok egyszerűen átültethetők a kibertérre is. Azonban korábban is utaltunk rá, hogy szakmai körökben nem mindenki ért egyet azzal, hogy a hidegháború során a nukleáris fegyverzetcsökkentést és leszerelést szolgáló intézkedések hatékonyan alkalmazhatók a kibertérből érkező fenyegetések csökkentésére, a kiberfegyverek proliferációjának megakadályozására és a kiberkonfliktusok kialakulásának megelőzésére. A bizalomerősítés hatékonyságát megkérdőjelező szakértők egyik alapvető érve, hogy a stratégiai kiberfegyverek és a nukleáris fegyverek karakterisztikája nem azonos az elrettentőerő tekintetében (egyetlen fegyver pusztítóereje, a biztos pusztítás, széles körű vita a fegyverek alkalmazásáról). (Cirenza 2016) Az amerikai légierő egyetemének kiadványa az alábbi hat szempont szerint hasonlítja össze a kiberháborút és a nukleáris elrettentést (Cimbala 2014):

16.1. táblázat

A kiberháború és a nukleáris elrettentés viszonya

Kiberháború	**Nukleáris elrettentés**
A támadás eredete bizonytalan, adott a lehetőség harmadik fél számára, hogy más szereplőnek álcázza magát.	Állami támadás esetén nagy biztossággal azonosítható a támadó, de a nem állami támadók kezén levő nukleáris anyagok és eszközök is követhetők.
Kár elsősorban az információs rendszereket és hálózatokat éri, amelyeknek azonban hatása lehet a katonai harctéri rendszerek működésére, illetve a gazdasági és szociális infrastruktúrákra.	Az elrettentés hibája katasztrofális károkat okozhat még korlátozott nukleáris háború esetén is.
A támadás megfelelően robusztus védelem, illetve a sérülékenységek gyors javításával meghiúsítható.	A támadás elhárítása kevésbé valószínű, mint a biztos megtorlás lehetősége.
A kibertámadások célja jellemzően a megzavarás, és nem a megsemmisítés.	A nukleáris elrettentés alapja a fizikai javak és a népesség azonnali és tömeges pusztításának realitása.
A kiberháború és a kibertámadások hosszabb ideig is eltarthatnak anélkül, hogy detektálnák, vagy egyértelmű károkat okoznának, illetve bizonyos támadásokat a detektálást követően sem jelentenek.	A teszteket leszámítva a nukleáris fegyver bevetése egy ország vagy egy nem állami szereplő által, a robbanás méretétől és az azonnali következményektől függetlenül gyökeres változást idézne elő a világpolitikában.
A kiberháborús képességek esetén a bekerülési költségek relatíve alacsonyak, és az állami szereplőktől az egyéni hackerekig bárki hadviselő féllé válhat.	Második csapásra képes nukleáris elrettentés kiépítéséhez és fenntartásához állami infrastruktúra, számottevő tudományos és technikai szakértelem, valamint hosszú távú finanszírozás szükséges.

Forrás: Cimbala 2014, 91.

Ha valaki soha nem foglalkozott a nukleáris elrettentéssel és a kibertérből érkező kihívásokkal, a fenti táblázat hasznos áttekintést nyújt a kiberfegyverekről, illetve kiberháborúról, valamint a nukleáris fegyverek, illetve elrettentés jellemzőiről, amelyekből kirajzolódnak az alapvető eltérések. A különböző jellemzők ellenére a bizalomépítés terén az EBESZ transznacionális fenyegetésekkel foglalkozó részlege aktív segítséget nyújt a tagországok számára elsősorban a kiberbiztonsági tisztviselő révén, aki közreműködik a bizalomerősítő intézkedések nemzeti szintű implementálásában, iránymutatást és tanácsokat fogalmaz meg, és koordinátori szerepkört lát el.

16.7. Kiberbiztonsági kitekintés

A kibertérben zajló folyamatok kapcsán a fenyegetések dinamikus növekedéséről már esett szó, és a jelenlegi előrejelzések alapján a digitalizáció terjedése, a tudástranszfer és a kiberbiztonsági tudatosság alacsony foka miatt a közeli jövőben biztosan nem várható, hogy a kitettségünk mértéke, illetve a támadások száma, mérete csökkenne. Időszakos változások és kilengések természetesen előfordulnak a kiberbiztonság terén is, de általánosságban egyre súlyosabb támadásokra kell felkészülnünk. Ebben a folyamatban jelentős szerephez jutnak az olyan előremutató technológiák, mint a mesterséges intelligencia, a gépi tanulás vagy éppen az úgynevezett dolgok internete (Internet of Things – IoT).

IoT, MI, ML

IoT: a dolgok internete olyan különböző elektronikai eszközökből áll, amelyeket valamilyen információ felismerésére, illetve internetalapú hálózaton történő kommunikációra terveztek. Az eszközök többnyire félautonóm vagy autonóm módon működnek, divatos kifejezéssel intelligens vagy okoseszközök hálózatba kötött halmaza.
MI: mesterséges intelligenciának vagy más néven gépi intelligenciának nevezzük, amikor egy gép olyan kognitív funkciókat valósít meg, amelyeket alapvetően az emberi tudattal társítunk, mint például a tanulás vagy a problémamegoldás képessége.
ML: az informatikai tudomány egyik területe, amely statisztikai technikákat alkalmaz annak érdekében, hogy a számítógépes rendszereket explicit programozás nélkül az adatokból való tanulás képességével ruházzák fel.

A jövőben egyre szélesebb körben válik elterjedtté a támadások egyes lépéseinek automatizálása, illetve az elhárító mechanizmusok alapján a támadás során alkalmazott rosszindulatú szoftverek bizonyos mértékig képesek lesznek módosítani az alkalmazott támadási vektoron. Ugyanakkor megfelelő alkalmazás esetén a védelem oldalán is számos pozitív hozadéka lehet a mesterséges intelligencia vagy a gépi tanulás bevetésének. Az okos automatizáció révén csökkenhet a téves riasztások száma, a ma még ember által végzett elemzői tevékenységek pontossága növekedhet, és nagymértékben csökkenhet a válaszidő, amely a kiberbiztonság terén az egyik legkritikusabb mérőszám.

Ma még sokak számára tudományos fantasztikumnak tűnik, hogy egy ipari folyamatirányító rendszer vagy egy katonai eszköz felett illetéktelenek átvegyék az irányítást, vagy megbénítsák azt, azonban ez már ma is lehetséges, amit több megtörtént eset is alátámaszt.

Az említett rendszerek a legtöbb esetben kritikus jelentőséggel bírnak egy ország vagy egy szövetség életében, ezért a jövőben várhatóan fokozatosan növekszik azoknak a szervezeteknek a száma, amelyek a kiberbiztonság valamelyik szegmensével foglalkoznak, illetve a fejezetben említett szervezetek is egyre nagyobb hangsúlyt fektetnek a saját szempontjukból releváns kérdések mielőbbi megoldására.

Egyvalami azonban a közeli jövőben biztosan nem fog változni. A támadók mindig könnyebb helyzetben lesznek, hiszen míg nekik többnyire csak egyetlen ponton kell valamilyen kihasználható sérülékenységet találniuk, a védőknek a teljes rendszer biztonságáról kell gondoskodniuk. Ezt a helyzeti előnyt tovább súlyosbítja, hogy a támadókat semmilyen szabályozás vagy előírás nem köti, miközben a védelem oldaláról ez korántsem mondható el, ráadásul a támadók előszeretettel segítik egymást, és osztják meg egymással a bevált gyakorlataikat vagy akár kártékony programjaik kódját. Ez a szemléletmód a védelmi oldalon is ismert, azonban az alkalmazás jóval nehézkesebb, sokszor az egy-egy megállapodásban leírtakon vagy szóban elhangzott ígérteken túl a gyakorlatban egyáltalán nem vagy csak nagyon lassan és nehézkesen működik pont az említett előírások vagy éppen az üzleti érdekek miatt. Univerzális megoldás nincs, de a felelős információmegosztás gyakorlati alkalmazása a kiberbiztonság terén valószínűleg az egyik legfontosabb eleme lesz a kibertérből érkező kihívásokkal szembeni megfelelő felkészültség elérésének.

Felhasznált irodalom

Beláz Annamária – Berzsenyi Dániel (2017): *Kiberbiztonsági Stratégia 2.0 A kiberbiztonság stratégiai irányításának kérdései.* Budapest, Nemzeti Közszolgálati Egyetem. (SVKK Elemzések, 2017/3.) Elérhető: http://real.mtak.hu/67199/1/SVKK_Elemzesek_2017_3_Kiberbiztonsagi_Strategia_2.0_Belaz_A._Berzsenyi_D._u.pdf (A letöltés dátuma: 2017. 07. 05.)

Biztonságpiac (2010): Tudástár. *Biztonságpiac,* 2010. 02. 24. Elérhető: http://biztonsagpiac.hu/tudastar (A letöltés dátuma: 2018. 01. 20.)

schmitt, Michael N. (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press.

Chen, Thomas M. – Robert, Jean Marc (2014): *The evolution of Viruses and Worms.* DOI: https://doi.org/10.1201/9781420030884.ch16

Cimbala, Stephen J. (2014): Nuclear Deterrence and Cyber The Quest for Concept. *Air & Space Power Journal,* March–April 2014. 87–107. Elérhető: www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-28_Issue-2/V-Cimbala.pdf (A letöltés dátuma: 2017. 05. 17.)

Dimitriadis, Christos (2017): *Cybersecurity Snapshot.* ISACA. Elérhető: www.isaca.org/resources/news-and-trends/isaca-now-blog/2016/cybersecurity-snapshot-cyberthreats-regulations-workforce-issues-in-2016 (A letöltés dátuma: 2017. 01. 19.)

ENISA (2015): *Definition of Cybersecurity – Gaps and overlaps in standardisation.* Elérhető: www.enisa.europa.eu/publications/definition-of-cybersecurity (A letöltés dátuma: 2017. 10. 22.)

Haig Zsolt – Várhegyi István (2008): A cybertér és a cyberhadviselés értelmezése. *Hadtudomány,* 28. évf. 2. sz. 1–12. Elérhető: http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf (A letöltés dátuma: 2017. 09. 07.)

ISO/IEC (2012): *ISO/IEC 27032:2012 – Information technology – Guidelines for cybersecurity.* Elérhető: www.iso27001security.com/html/27032.html (A letöltés dátuma: 2018. 01. 20.)

KISSEL, Richard ed. (2013): *Glossary of Key Information Security Terms.* National Institute of Standards and Technology. DOI: http://dx.doi.org/10.6028/NIST.IR.7298r2

KORZAK, Elaine (2017): UN GGE on Cybersecurity: The End of an Era? *The Diplomat,* July 31, 2017. Elérhető: https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ (A letöltés dátuma: 2017. 12. 04.)

MAURER, Tim – MORGUS, Robert (2014): *Compilation of Existing Cybersecurity and Information Security Related Definitions.* Washington, D. C., New America. Elérhető: www.newamerica.org/cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and-information-security-related-definitions/ (A letöltés dátuma: 2018. 01. 20.)

Ajánlott irodalom

BERZSENYI Dániel (2014): Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése. *Nemzet és Biztonság – Biztonságpolitikai Szemle,* 7. évf. 6. sz. 110–136. Elérhető: http://nemzetesbiztonsag.hu/letoltes.php?letolt=649 (A letöltés dátuma: 2017. 05. 17.)

ENISA (2016): *ENISA Threat Taxonomy.* European Union Agency for Cybersecurity. Elérhető: https://data.europa.eu/euodp/en/data/dataset/enisa-threat-taxonomy-1 (A letöltés dátuma: 2017. 01. 22.)

Internet Governance Forum (é. n.). UN DESA. Elérhető: www.intgovforum.org/multilingual/ (A letöltés dátuma: 2017. 11. 10.)

ITU (é. n.): Global Cybersecurity Index. International Telecommunications Union. Elérhető: www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (A letöltés dátuma: 2017. 11. 10.)

UN (2017): Cybersecurity: A global issue demanding a global approach. Elérhető: www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html (A letöltés dátuma: 2017. 11. 10.)

LIBE (2015): *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses.* European Parliament Directorate-General for Internal Policies. Elérhető: www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf (A letöltés dátuma: 2017. 10. 22.)

NCA (2017): *Pathways Into Cyber Crime.* National Crime Agency (UK). Elérhető: /www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file 2017 (A letöltés dátuma: 2017. 05. 04.)

NKBS (2013): Magyarország Nemzeti Kiberbiztonsági Stratégiája. Nemzeti Jogszabálytár. Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845, 2017 (A letöltés dátuma: 2017. 07. 07.)

OSCE (2016): *Cyber/ICT Security.* OSCE Transnational Threats Department. Elérhető: www.osce.org/files/f/documents/c/c/256071.pdf, 2016 (A letöltés dátuma: 2017. 10. 22.)

UNIDIR (2017): *The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century.* UNIDIR. Elérhető: www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf (A letöltés dátuma: 2017. 10. 22.)