HADMÉRNÖK

XIII. Évfolyam „KÖFOP" szám – 2018. január

KIBERBIZTONSÁGI CÉLOK, JÖVŐKÉPEK, SZABÁLYOZÓK AZ EU-BAN ÉS KAPCSOLATRENDSZERÜK AZ INTEROPERABILITÁSSAL

CYBERSECURITY GOALS, VISIONS, REGULATIONS IN EU, AND RELATIONSHIPS WITH INTEROPERABILITY

MUNK Sándor

(ORCID: 0000-0001-8576-308X)

munk.sandor@uni-nke.hu

Absztrakt

Az informatikai szolgáltatások, rendszerek, eszközök, alkalmazások egyre jelentősebb mértékben járulnak hozzá az állami működés hatékonyságának, a vállalkozások eredményességének és versenyképességének, valamint az állampolgárok életminőségének javításához.
A kiberbiztonság és az interoperabilitás ma vitathatatlanul az informatikai szakterület legfontosabb, legaktuálisabb kérdései közé tartoznak. A két kérdéskör egymással részben szembenálló stratégiai célkitűzéseket, nézőpontot, követelményeket képvisel.
Jelen publikáció célja annak feltárása, hogy a kiberbiztonsággal kapcsolatos EU dokumentumokban, célokban, feladatokban megjelennek-e, és ha igen, milyen interoperabilitási kérdések.
A publikáció a KÖFOP-2.1.2-VEKOP-15-2016-00001 'A jó kormányzást megalapozó közszolgálat-fejlesztés' projekt támogatásával, a Kiberbiztonsági Ludovika Kiemelt Kutatóműhely keretében készült.

Kulcsszavak: *Európai Unió, interoperabilitás, kiberbiztonság*

Abstract

IT services, systems, devices, and applications are increasingly contributing to the efficiency of state operations, the efficiency and competitiveness of businesses and the improvement of citizens' quality of life.
Today cybersecurity and interoperability are indisputably one of the most important, most current issues in the IT field. The two issues have in some respect opposing strategic objectives, viewpoints, and requirements.
The aim of the recent publication is to explore whether interoperability issues are included in EU cybersecurity documents, objectives, and tasks, and if so, what are these issues.
The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in the Cyber Security Ludovika Workshop.

Keywords: *European Union, interoperability, cybersecurity*

A kézirat benyújtásának dátuma (Date of the submission): 2017. 07.15.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.10.05.

BEVEZETÉS

Az informatikai szolgáltatások, rendszerek, eszközök, alkalmazások[1] egyre jelentősebb mértékben járulnak hozzá az állami működés hatékonyságának, a vállalkozások eredményességének és versenyképességének, valamint az állampolgárok életminőségének javításához. Az informatikai (infokommunikációs) szolgáltatások fejlesztési és alkalmazási feladatainak stratégiai szintű tervezése a múlt század vége, az információs társadalom célkitűzésének megfogalmazása óta nemzetközi, nemzeti, és szervezeti szinten is kiemelt jelentőségű.

A kiberbiztonsági kutatások több szakterületét összefogó Ludovika Kiberbiztonsági Kiemelt Kutatóműhely kutatási tervének egyik pillérét, kutatási fejezetét képezik a kiberstratégiai kutatások. Ezen kutatások célja hozzájárulni ahhoz, hogy a különböző szintű – nemzetközi és nemzeti – stratégiai dokumentumok megfelelő választ tudjanak adni a társadalmi folyamatok stratégiai szintű tervezéséhez szükséges, az információtechnológia gyors fejlődéséből következő kérdésekre.

A kiberbiztonság és az interoperabilitás mind a felhasználói kör, mind a biztonsági és interoperabilitási feltételeket, képességeket megteremtő és fenntartó szakmai szereplők számára két eltérő, és ha nem is gyökeresen ellentétes, de mégis egymással sok tekintetben szembenálló nézőpontot, szempontrendszert jelent. Mindkettő meghatározott felhasználói igények kielégítését, megvalósítást szolgálja.

Előzetesen csak hipotézisként, de megfogalmazható, hogy általánosságban a biztonság magasabb szintje (legalábbis sok esetben) a használhatóságot korlátozza, míg a széleskörű interoperabilitásra épülő használat a biztonsági kockázatokat növeli. Ebből következően a két nézőpont, követelményrendszer csak a konkrét felhasználói igények mérlegelésével, azoknak megfelelően súlyozva érvényesíthető.

Jelen publikáció egy olyan szélesebb körű kutatás eredménye, amelynek célja a hatékony információmegosztást, együttműködést biztosító interoperabilitás, illetve a biztonság, mint egymással részben szembenálló stratégiai célkitűzések összefüggéseinek vizsgálata, megoldási lehetőségeinek elemzése. Egy korábbi publikáció [1] elemezte az az EU interoperabilitási dokumentumait és a kiberbiztonság kérdéseinek megjelenését azokban.

Jelen publikáció a kiberbiztonság és az interoperabilitás kapcsolatrendszerét a kiberbiztonság oldaláról vizsgálja. Alapvető kutatási célja annak feltárása, hogy a kiberbiztonsággal kapcsolatos alapvető EU dokumentumokban, célokban, feladatokban megjelennek-e, és ha igen, milyen formában az interoperabilitás kérdései, illetve meghatározzuk, hogy hol, milyen interoperabilitási kérdések szerepeltetése lenne célszerű

Ennek érdekében a következőkben:

- összegezzük a kiberbiztonság és az interoperabilitás alkalmazott fogalmi alapjait;
- bemutatjuk a kiberbiztonsági kérdéseket tartalmazó legfontosabb EU dokumentumokat;
- összegezzük, értékeljük az EU kiberbiztonsági célkitűzéseit;
- végül meghatározzuk az interoperabilitási kérdések aktuális és lehetséges megjelenését.

[1] Jelen publikációban az informatikai jelzőt tág értelemben, az 'információs tevékenységek technikai eszközökkel történő támogatása' értelmezésben, a más szakértők által információtechnológiai (IT), vagy infokommunikációs (information and communication technologies, ICT) kifejezések szinonimájaként használom.

A KIBERBIZTONSÁG ÉS AZ INTEROPERABILITÁS ALAPJAI, ÉRTELMEZÉSE

A ***kiberbiztonság*** (cybersecurity) kifejezés a kibertér fogalmához kapcsolódóan szerepel, annak keretei között, attól függően értelmezhető. A kibertér (cyberspace) kifejezés a számítógép-hálózatok által létrehozott virtuális világ megnevezésére jelent meg a fantasztikus iroda-lomban, majd vált a szakmai-tudományos élet vizsgálati tárgyává. Viszonyát más szakterületi fogalmakkal (információs környezet, információs színtér, számítógép-hálózatok, infokommunikációs rendszerek, stb.) a különböző alkalmazási területek, szakmai közösségek eltérően értelmezik.

A kiberbiztonság leegyszerűsítve a kibertér biztonsága, biztonság a kibertérben. Ez a megközelítés maga után vonja, hogy a kibertér tartalmának eltérő értelmezései módosítják, befolyásolják a kiberbiztonság értelmezését is. Az értelmezés során el kell különíteni a biztonságot, mint elérendő állapotot, és a biztonságot, mint ezen állapot kialakításának, fenntartásának, helyreállításának feladatrendszerét is. Jelen tanulmány nem tekinti tárgyának a különböző kibertér, kiberbiztonság értelmezések részletes vizsgálatát, értékelését (erről lásd például [2]).

A kiberbiztonsághoz kapcsolódó legfontosabb megállapítások, amelyek nagyrészt Haig Zsolt, Kovács László, és kollégáik munkáira [3, 4, 5], illetve napjaink új eredményeire [6, 7] épülnek, a következők:

- a kibertér az információk, az információs folyamatok, valamint az információkat továbbító, tároló, kezelő informatikai eszközök által alkotott képzeletbeli, virtuális tér;
- a kibertér egyes összetevői (az informatikai eszközök, az információhordozók, a kommunikációs összeköttetések) egyben a valós, fizikai tér összetevői is;
- a kibertér jellege változás alatt áll, fokozatosan bővül a nem információs rendeltetésű, de információs képességekkel is rendelkező kiberfizikai (cyber-physical) rendszerekkel, eszközökkel;
- a kiberbiztonság az az állapot, amelyben a kibertér összetevői (az információk, és az azokat kezelő informatikai eszközök) elegendően védettek a károsodástól, illetéktelen hozzáféréstől, módosítástól, vagy kihasználástól;
- a kibertér és a kiberbiztonság (kibervédelem) értelmezése a katonai alkalmazásban napjainkban eltérő, jóval tágabb a civil terminológiánál.

Az ***interoperabilitás*** kifejezés szélesebb körben a hatékony és eredményes együttműködéshez szükséges képességek alapvető összetevőjeként jelent meg az 1990-es években a katonai alkalmazásban. A kezdetben elsősorban technikai jellegű, mindenekelőtt az informatikai rendszerek közötti együttműködést megjelenítő fogalom értelmezése fokozatosan terjedt ki a szervezetekre, csoportosításokra, erőkre.

Az interoperabilitáshoz kapcsolódó legfontosabb megállapítások, amelyek alapvetően korábbi eredményeimre épülnek [8, 9, 10], a következők:

- az interoperabilitás általános értelemben két, vagy több objektum között fennálló viszony, az együttműködést támogató, eredményes és hatékony együttes működést biztosító kölcsönös képesség;
- az interoperabilitás alanyai aktív objektumok, amelyek lehetnek tudatosan tevékenykedő, szervezett embercsoportok, vagy célirányosan, meghatározott rendeltetéssel működő technikai rendszerek; ennek megfelelően megkülönböztethetünk szervezeti (működési, műveleti), illetve technikai interoperabilitást;
- a szervezetek közötti eredményes és hatékony együttműködés alapvető feltétele az érin-tettek közötti megfelelő szintű információcsere, az együttműködéshez szükséges információk megosztása, összehangolt felhasználása, az erre való képesség az információs interoperabilitás;
- az információs interoperabilitás különböző szereplők kölcsönös képessége információk közös értelmezésen alapuló, a hatékony együttműködéshez szükséges cseréjére,

amelynek szintjei a fizikai hordozók szintjén megnyilvánuló technikai, az információ reprezentációk (adatformátumok) szintjén megnyilvánuló szintaktikai, és a jelentés szintjén megnyilvánuló szemantikai interoperabilitás;
- az interoperabilitás problémája akkor merül fel, amikor az együttműködő szereplők között eltérések (heterogenitás) vannak az információcsere fizikai, adatformátum, vagy értelmezési szintjén;
- az informatikai interoperabilitás informatikai rendszerek, eszközök, alkalmazások kölcsönös képessége az általuk kezelt adatok – esetleges átalakítások közbeiktatásával történő – átvételére, cseréjére az elsődleges alkalmazói kör által meghatározott, ezen adatokhoz rendelt jelentés megőrzésével.

Az interoperabilitás fogalmát az európai közszolgáltatások vonatkozásában az Európai Interoperabilitási Keretrendszer határozza meg, mint különböző szervezetek együttműködési képességét kölcsönösen előnyös, egyeztetett közös célok megvalósítására, ami magában foglalja a szervezeti munkafolyamatok keretében történő, informatikai rendszereik közötti adatcserére épülő információcserét, megosztást. [11, 2. o.]

Több más megfogalmazáshoz hasonlóan az interoperabilitás az EU értelmezés szerint is kölcsönös szervezeti képesség az együttműködésre, amely informatizálódó világunkban az információk közös értelmezésen alapuló, hatékony együttműködéshez szükséges cseréjére épül. Az interoperabilitás tehát nem tisztán informatikai (technikai) jellegű, hanem kiterjed a szervezeti, és jogi kérdésekre, együttműködésre, feltételekre, képességekre.

KIBERBIZTONSÁG AZ EU DOKUMENTUMOKBAN, EU KIBERBIZTONSÁGHOZ KAPCSOLÓDÓ DOKUMENTUMOK

A kiberbiztonság kérdései az Európai Unió lisszaboni, illetve Európa 2020 stratégiájában konkrét formában nem jelennek meg. Az utóbbiban szereplő egyetlen kapcsolódó gondolat a határokon átnyúló információáramlás, az egységes digitális piac online szolgáltatásai iránti bizalom megteremtésének célkitűzése, amely értelemszerűen a biztonság magas szintjét igényli.

A kiberbiztonsághoz kapcsolódó kérdések az EU dokumentumokban a 2010-es évek elejéig a hálózat- és informatikai biztonság keretei között jelentek meg. A tágabb értelmezésű kiberbiztonság, más európai biztonsági kezdeményezésekkel együtt a 2010-es évek közepén került előtérbe. Ennek megfelelően vizsgálatainkat a következőkben e két területre összpontosítjuk, bemutatjuk a témánk szempontjából releváns dokumentumokat és alapvető tartalmukat.

A ***hálózat- és informatikai biztonság az EU-ban*** legmagasabb szinten elsőként egy 2001-es dokumentumban jelent meg. A *Javaslat egy európai hálózat- és informatikai biztonsági politikára* a témakör átfogó megközelítésére épült, amely abból indult ki, hogy a hálózatok, és informatikai rendszerek széles körben alkalmazott támogató infrastruktúrákká, a gazdasági és társadalmi fejlődés kulcstényezőivé váltak, így biztonságuk alapvető prioritás. A dokumentum szerint a hálózat- és informatikai biztonság egy hálózat, vagy egy informatikai rendszer képessége, hogy egy adott megbízhatósági szinten ellenálljon a tárolt és továbbított adatok, valamint a hálózat, rendszer által nyújtott, vagy rajta keresztül elérhető kapcsolódó szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét, és bizalmasságát fenyegető véletlen eseményeknek, vagy rosszindulatú cselekményeknek. A dokumentum áttekintette a biztonsági fenyegetéseket, károkozásukat, és a lehetséges megoldásokat. Megállapította, hogy a különböző érvényben lévő (telekommunikációs, személyes adatvédelmi, kiberbűnözés elleni) EU szabályozások nem kellően összehangoltak, nem terjednek ki minden kérdésre. [12, 9., 19. o.]

Az *elektronikus hírközlő hálózatokra és szolgáltatásokra vonatkozó biztonsági kérdések* a 2002 márciusában kiadott szabályozó csomagban jelentek meg. A közös keretszabályozásról szóló dokumentumban szerepelt a kicserélt információk bizalmassága megőrzésének, a szemé-

lyes adatok és a magánélet biztonságának, valamint a nyilvános hírközlő hálózatok sértetlenségének és biztonságának követelménye [13, 4. 3, 8. (4) c. és f.]. Az engedélyezésről szóló dokumentumban pedig a hálózatokhoz történő jogosulatlan hozzáférés elleni védelem követelménye fogalmazódott meg. [14, Annex, A 16.] A fenti követelményeket a júliusban kiadott elektronikus hírközlési adatvédelmi dokumentum egészítette ki a személyes adatok védelmének részletes követelményeivel. Ebben a dokumentumban már megjelent a hálózati biztonság kifejezés. [15]

A fenti követelmények megvalósításában történő részvételre került létrehozásra 2004-ben az *Európai Uniós Hálózat- és Informatikai Biztonsági Ügynökség*. Az alapító dokumentumban [16] foglaltak szerint az ügynökség rendeltetése a hálózat- és informatikai biztonsági problémák megelőzésére, kezelésére, és megválaszolására irányuló képességek fejlesztése, tanácsadás, szakmai képesség kifejlesztése, és jogszabály előkészítés. Az ügynökség mandátuma lényegében azonos rendeltetéssel 2013-ban lett meghosszabbítva újabb hét évre. [17] A dokumentumban már megjelennek a kibertéri fenyegetések, a kiberbűnözés, és a személyes kiberbiztonság. Napjainkban az ügynökség jellegének leírására már a 'kiberbiztonsági' jelzőt használja.

A 2005-ben megjelent *i2010 európai információs társadalom stratégia* az egységes európai információs tér negyedik fő kihívásaként tartalmazta a biztonságot, mint az internet biztonságának növelését a csalókkal, a káros tartalommal és a technológiai meghibásodásokkal szemben, a befektetők és a fogyasztók bizalmának erősítése érdekében. [18, 5. o.] A megbízható, biztonságos és kiszámítható informatika a digitális szolgáltatások kritikus feltételeként szerepelt.

A *Biztonságos információs társadalom stratégia* [19] a 2001-es hálózat- és informatikai biztonsági politika frissítése, amely áttekinti az információs társadalom biztonságára leselkedő veszélyek aktuális helyzetét, és meghatározza a biztonság növelése érdekében megvalósítandó feladatokat. A stratégia alapgondolata a dinamikus és integrált megközelítés, a nyitott és minden érdekeltre kiterjedő párbeszéden, partnerségen, felhatalmazáson, és felelősségvállaláson alapuló tevékenység.

A *hálózat- és informatikai biztonság egységesen magas szintjének eléréséhez szükséges intézkedésekről szóló javaslat* 2013-as megjelenésének oka az informatikai rendszereket ért fenyegetések számának megnövekedése, a korábbi önkéntes megközelítés elégtelensége, valamint a tagállamok eltérő képességei és felkészültsége voltak. Alapvető célja a tagállami illetékes hatóságok és hálózatbiztonsági veszélyhelyzeteket elhárító csoportok[2] létrehozása, európai hálózatba kapcsolása, nemzeti hálózat- és informatikai biztonsági stratégiák elfogadása, egy kockázatkezelési kultúra kialakítása, valamint a köz- és magánszféra közötti információ-megosztás. [20, 2-4. o.]

A javaslatra épülő, napjainkban is érvényes *Hálózat- és informatikai biztonsági irányelv* [21] 2016-ban jelent meg. Az irányelv a tagállamok számára előírja hálózat- és informatikai biztonsági nemzeti stratégiák elfogadását, illetékes hatóságok, és számítógép-biztonsági eseményekre reagáló csoportok[3] kijelölését és uniós hálózatba szervezését, az alapvető szolgáltatásokat nyújtó szereplők azonosítását, valamint meghatározza a biztonsági kockázatkezelésre, és a biztonsági események bejelentésére vonatkozó követelményeket.

A ***kiberbiztonság az Európai Unióban*** a 2000-es évek elején több kérdéskörhöz kapcsolódóan is megjelent. Ezek közé tartozott a terrorizmus és a szervezett bűnözés elleni harc, a kritikus infrastruktúrák védelme, az elektronikus hírközlési szolgáltatások – és ennek feltételeként kiemelten az Internet – biztonsága. A kiberbűnözés, kibertámadások, kibertér kifejezések

[2] Computer Emergency Response Team (CERT).
[3] Computer Security Incident Response Team (CSIRT).

fokozatosan, és egyre növekvő mértékben nyertek tért az EU dokumentumokban, míg az első stratégia megszületett e tárgyban.

Az *EU kiberbiztonsági stratégiája*, 'A nyílt, megbízható és biztonságos kibertér' 2013-ban jelent meg. A dokumentum az Internet, és tágabb értelemben a kibertér nyitottságának és szabadságának megőrzését, a biztonsági eseményektől, a rosszindulatú tevékenységektől, és visszaélésektől történő megóvását tűzte ki célul. A stratégia öt prioritása a következő:

- a kibertámadásokkal szembeni ellenálló képesség elérése;
- a kiberbűnözés drasztikus csökkentése;
- kibervédelmi politika és képességek kifejlesztése;
- kiberbiztonsági ipari és technológiai erőforrások kifejlesztése;
- egy összehangolt EU szakpolitika kidolgozása a kibertérre vonatkozóan.

A stratégia lényeges eleme annak megfogalmazása, hogy a kiberbiztonság átfogó módon történő kezeléséhez a tevékenységeket három, különböző jogi keretekben működő fő pillérre, a hálózat- és informatikai biztonságra, a bűnüldözésre és a védelemre kell építeni. [22, 4-5. o., 17. o.]

2014-ben az Európai Bizottság elfogadta az *EU kibervédelmi politika keretei* című dokumentumot [23], amely rögzítette a kiberbiztonságnak az EU közös biztonság- és védelempolitikájához kapcsolódó kérdéseit, feladatait, ezen belül többek között:

- a közös biztonság- és védelempolitikai célú kibervédelmi képességek fejlesztését;
- a közös biztonság- és védelempolitikai hálózatok védelmét;
- valamint a civil-katonai, illetve védelmi-ipari-kutatási együttműködés elősegítését.

EURÓPAI UNIÓS KIBERBIZTONSÁGI IGÉNYEK, CÉLKITŰZÉSEK

Az interoperabilitási kérdéseknek az Európai Unió kiberbiztonsági dokumentumaiban, céljaiban, feladataiban történő megjelenési lehetőségeit, szerepét kutatva elsőként fel kell tárjuk az alapokat képező EU hálózat- és informatikai, majd kiberbiztonsági célokat, feladatokat. Ennek keretében a következőkben összegezzük, elemezzük az EU kapcsolódó biztonsági igényeit, majd a kiberbiztonsághoz kapcsolódó célkitűzéseket, feladatokat.

A ***kiberbiztonság***[4] ***iránti igények*** az Európai Unióban stratégiai szinten – az interoperabilitáshoz hasonlóan – már a Bangemann jelentésben [24] megjelentek. A dokumentum a felvázolt nyílt, versenyképes, és egységes piacra épülő globális információs társadalom kiépítéséhez közös szabályozást javasolt a szellemi tulajdonjogok, a személyes adatok, valamint az információk elektronikus és jogi védelme terén. Az EU lisszaboni, és Europe 2020 tízéves stratégiáiban viszont – mint azt már korábban jeleztük – ezek a biztonsági kérdések nem jelennek meg.

A 2001-es *javaslat a hálózat- és informatikai biztonsági politikára* a biztonság kérdéseinek fontosságát azzal indokolta, hogy a kommunikációs szolgáltatásokat a korábban jellemzően állami távközlési szolgáltatók helyett versengő magán szolgáltatók nyújtják, nemzeti helyett európai, és globális szinten. A távközlési hálózatok összekapcsolódnak, dedikált hálózatok helyébe konvergált hálózatok lépnek. A biztonság ezen a területen is áruvá válik, a szolgáltatások kellő biztonságát a piaci folyamatok nem biztosítják. A biztonság az elektronikus hírközlési szolgáltatások biztonságát jelentette, amelynek megoldását célozták az EU 2002-es elektronikus hírközlési szabályozásai, így a biztonság az EU jogalkotás és a távközlési szolgáltatók problémáját, feladatát képezte.

[4] Kezdetben hálózat- és informatikai biztonsági kérdések.

A *hálózat- és informatikai biztonság intézményes megjelenése* 2004-ben a biztonság kérdéseinek szükségességét már szélesebb alapra helyezte, a kritikus információs infrastruktúrák, az egységes piac hajtóerejét képező e-kereskedelembe vetett bizalom, a sok szolgáltató által működtetett hálózatok komplex biztonsága, a kockázatelemzésre alapozott biztonságpolitika, a biztonsági kérdések globális jellege oldaláról közelítette meg. A kérdéskör jelentőségét a hálózati infrastruktúrák, az Internet, és szolgáltatásaik gyors fejlődése eredményeként megjelenő kiberbűnözés tovább növelte. Ettől fogva a biztonságban érintett szereplők között megjelentek a különböző Európai Uniós, nemzeti (kormányzati), kritikus infrastruktúra üzemeltetői és más hálózati- és informatikai biztonsági eseménykezelő központok is.

A 2010-es *Digitális Menetrend Európa számára* [25] a biztonságot a megbízható szolgáltatásokba, a kiberbűnözés elleni védettségbe vetett felhasználói bizalomhoz kapcsolva jelenítette meg, de olyan társadalmi problémákat is hangsúlyozott, mint a szexuális kizsákmányolás, a gyermekpornográfia, valamint a személyiségi jogok, személyi adatok védelme. Lényegében ugyanezeket a kérdéseket fogalmazta meg a 2015-ös *Digitális Egységes Piac stratégia* is. [26]

A *hálózat- és informatikai biztonság kiberbiztonsággá bővülése* 2013-ben a biztonsági fenyegetések körének bővülésére, a kibervédelemnek a biztonság- és védelempolitika jelentős területévé válására, a biztonság komplex megközelítésének előtérbe kerülésére épült. A hálózatok és informatikai rendszerek helyett a kibertér biztonsága vált elsőrendű kérdéssé, amely többek között magában foglalja a szűkebb értelemben vett számítástechnikai eszközök körébe korábban nem sorolt ipari felügyeleti irányító és adatgyűjtő (Supervisory Control and Data Acquisition, SCADA) rendszereket, informatikai képességekkel felruházott 'okos' eszközöket, a kialakulóban lévő Dolgok Internetét. A biztonság szereplőinek köre tovább bővült, kiterjedt a védelmi szféra illetékes szervezeteire, és számos ágazat érintettjeire is.

A ***kiberbiztonsági célkitűzések*** tartalma a különböző EU dokumentumokban folyamatosan bővült, finomodott. Az első ilyen dokumentum, *a hálózat- és informatikai biztonsági politikára vonatkozó javaslat* (2001) hét célkitűzése a következő volt:

- figyelemfelhívás a biztonsági kérdésekre;
- európai figyelmeztető és információs rendszer (CERT hálózat) kiépítése;
- technológiai kutatás támogatása (az 5. keretprogram keretében);
- piacorientált szabványosítás és tanúsítás támogatása;
- szabályozási keretek biztosítása;
- e-kormányzati, e-beszerzési biztonsági megoldások megvalósítása;
- nemzetközi együttműködés erősítése.

A 2010-es *Európai Digitális Menetrend* bizalom és biztonság intézkedési területén két kulcsfontosságú, jogalkotás jellegű tevékenység szerepelt:

- az EU hálózat- és informatikai biztonsági politika megerősítése, ENISA modernizáció, EU intézményi CERT létrehozása;
- az informatikai rendszerek elleni kibertámadásokkal szembeni harc jogi kereteinek megteremtése.
- Emellett további EU cselekvések is célként szerepeltek:
- európai kiberbűnözési platform létrehozása;
- európai kiberbűnözési központ (EC3) feltételeinek vizsgálata;
- globális kockázatkezelés erősítése a kiber- és a fizikai térben;
- kiberbiztonsági gyakorlatok támogatása;
- személyes adatvédelmi szabályozás modernizációja.

A 2013-as *Kiberbiztonsági stratégia* öt stratégiai célkitűzést fogalmazott meg, amelyek a következők voltak:

- kibertámadásokkal szembeni ellenálló képesség elérése;

- a kiberbűnözés drasztikus csökkentése;
- a közös biztonság- és védelempolitikához szükséges kibervédelmi politika és képességek kifejlesztése;
- kiberbiztonsági ipari és technológiai erőforrások kifejlesztése;
- az Európai Unió céljait, alapértékeit támogató koherens nemzetközi kibertéri szakpolitika létrehozása.

A 2014-es *Kibervédelmi politikai keretdokumentum* öt prioritást fogalmaz meg:

- a közös biztonság- és védelempolitikához kapcsolódó tagállami kibervédelmi képességek fejlesztésének támogatása (benne a kibervédelemhez kapcsolódó, katonai műveleteket támogató erőforrások összevonását és megosztását segítő projektek: kriminalisztika, interoperabilitás fejlesztése, szabványosítás);
- közös biztonság- és védelempolitikai hálózatok védelmének fejlesztése;
- EU civil-katonai együttműködés támogatása;
- kutatás-fejlesztési együttműködés a magán- és egyetemi szektorral;
- felkészítési, képzési, és gyakorlatozási lehetőségek bővítése;
- együttműködés javítása az érintett nemzetközi partnerekkel.

INTEROPERABILITÁSHOZ KAPCSOLÓDÓ KÉRDÉSEK AZ EU KIBERBIZTONSÁGI DOKUMENTUMOKBAN

Az interoperabilitás kérdései a kiberbiztonsági területen elsősorban az együttműködéshez, az ehhez szükséges információcseréhez kapcsolódóan jelenhetnek meg. Mint azt a következőkben igazoljuk, nincs ez másként az EU kiberbiztonsági dokumentumok esetében sem. Elsőként áttekintjük az EU irányelveit, szabályozóit, majd feldolgozzuk az EU Hálózat- és Informatikai Biztonsági Ügynökség témánkhoz kapcsolódó, szakmai szempontból részletesebb dokumentumait.

Az ***interoperabilitás kérdései az EU kiberbiztonsági dokumentumokban*** már az első, *hálózat- és informatikai biztonsági politikára vonatkozó javaslatban* is megjelentek. A dokumentum számos helyen nevesítve is megfogalmazta a biztonsághoz kapcsolódó interoperabilitás szükségességét. A javasolt intézkedések között általánosságban szerepelt, hogy a tagállamoknak hatékony és interoperábilis biztonsági megoldásokat kell alkalmazniuk e-közigazgatási és e-beszerzési tevékenységeikben. [12, 4. o.] Az alapvető biztonsági megoldások interoperabilitása a 6. kutatási-fejlesztési keretprogram javasolt irányai között is megjelent. A dokumentum egyedileg is említette a titkosítási eszközök és szoftverek, hitelesítési, elektronikus aláírási, és nyilvános kulcsú infrastruktúra megoldások interoperabilitásának szükségességét. [12, 10., 15., 24 o.]

A 2006-os *Biztonságos információs társadalom stratégia* arra hívta fel a figyelmet, hogy a közös platformokra és alkalmazásokra épülő interoperabilitás amellett, hogy elősegíti az informatikai szolgáltatások elterjedését, biztonsági kockázatokat is jelent. A szabványos megoldások széles körű felhasználása felerősíti a bennük előforduló sérülékenységek hatását, következményeit. Így ezeket a kockázatokat az interoperabilitási megoldásokban kezelni kell. A dokumentum alapgondolata a biztonság (ezen belül a hálózat- és informatikai biztonság) dinamikus és integrált megközelítése, amely valamennyi érdekelt – a köz- és magánszféra párbeszédén, partnerségén és felelősségvállalásán alapul. Külön megfogalmazásra került a bűnüldöző szervezetek közötti, az Internethez kapcsolódó kiberbűnözés elleni együttműködés fejlesztése. [19, 5., 7. o.]

A 2013-as *EU kiberbiztonsági stratégia* az öt stratégiai prioritás közül négyben tartalmaz az interoperabilitáshoz kapcsolódó kérdéseket. Ennek központi gondolata, hogy a kibertámadásokkal szembeni ellenállási képesség fejlesztésének alapja a közigazgatás és a magánszektor képességeinek, erőforrásainak, és eljárásainak együttműködése, az illetékes kiberbiztonsági

szervezetek közötti információmegosztás, és kölcsönös segítségnyújtás. A Kiberbűnözés Elleni Európai Központ[5] feladataként említi a tagállamok illetékes hatóságai, a magánszektor és más érdekelt felek közötti információmegosztási csatornákat kiépítését. A közös biztonság- és védelempolitikához kapcsolódóan a képességfejlesztés katonai jellegű megközelítésének[6] részeként szerepel az interoperabilitás. Végül a kibervédelmi szakpolitika kidolgozásának egyik irányaként fogalmazta meg a nemzetközi kritikus információs infrastruktúra védelmi hálózatokra épülő információmegosztás javítását. [22, 5., 10., 16. o.]

A stratégiát követően kidolgozott *kibervédelmi politikai keretdokumentum* tartalmazza a katonai kiberbiztonsági szervezetek (CERT-ek) közötti önkéntes együttműködés fejlesztésének feladatát, valamint a közös biztonság- és védelempolitikai hálózatok védelmének javítása érdekében támogatja a kiberfenyegetésekre vonatkozó információk valós idejű megosztását, valamint az ehhez szükséges mechanizmusok kiépítését a tagállamok és az érintett EU szervezetek között. [23, 5., 7. o.]

Az előzőektől eltérő, de témánk szempontjából fontos, önálló kérdéskörhöz kapcsolódik az *elektronikus azonosítás és bizalmi szolgáltatások*[7] *EU 2014-es szabályozása* [27], amely meghatározza az elektronikus azonosítás, hitelesítés, aláírás, időbélyegző EU szintű alkalmazhatóságának, az ilyen szolgáltatások kölcsönös elismerésének követelményeit és feltételeit. A szabályozó interoperabilitási követelményt ír elő a nemzeti elektronikus azonosítási rendszerek, valamint a minősített tanúsítványok és az elektronikus aláírások határokon átnyúló interoperabilitása számára.

A kiberbiztonsághoz kapcsolódó ***interoperabilitási kérdések*** részletesebben ***az EU Hálózat- és Informatikai Biztonsági Ügynökség dokumentumaiban*** kereshetőek. A fellelhető megállapítások jellemzően nem használják az interoperabilitás fogalmát, helyette információcsere megoldásokkal, adatcsere formátumokkal, taxonómiákkal és ontológiákkal, valamint az információcserét biztosító rendszerekkel, eszközökkel találkozhatunk. Önálló témakört képeznek a bizalmi szolgáltatásokhoz kapcsolódó interoperabilitási kérdések.

Nem igényel különösebb bizonyítást, hogy *a kiberbiztonságban érintett szereplők*[8] *közötti hatékony információcsere* alapvető feltétele az együttműködő szervezetek (és egyre bővülő mértékben informatikai rendszereik) közötti technikai, formai (szintaktikai) és fogalmi (szemantikai) interoperabilitás. Az ENISA már egy 2004-es tanulmányában megfogalmazta a biztonsági események osztályozására, illetve az adatcsere formátumokra vonatkozó szabványok hiányát. [28, 49. o.] 2009-ben útmutatót adott ki a hálózati biztonsági információcsere bevált megoldásairól. [29] A riasztások, figyelmeztetések, közlemények kiadott útmutatója még 2013-ban is hiányosságként azonosítja a formatizált információcsere alacsony szintjét, a létező adatformátumok alkalmazásának hiányát, a kötetlen szövegre, megérzés alapú értékelésre alapozott megoldásokat. [30, 33. o.] Egy 2014-es tanulmány részletesen ismerteti a biztonsági információk cseréje során felhasználható – az interoperabilitáshoz kapcsolódó – szabványos adatformátumokat, protokollokat, keretrendszereket. [31]

A jelentésmegőrző információcsere alapvető feltétele *az alkalmazott fogalmak közötti átalakíthatóság*, ideális esetben – de a gyakorlatban el nem érhetően – az azonosság. Ennek a szemantikai interoperabilitási problémának a megoldását többek között taxonómiák, ontológiák segíthetik. Az ENISA dokumentumaiban ez a témakör 2011-ben jelent meg [32], hangsúlyozva

[5] European Cybercrime Centre (EC3).
[6] Doktrína, vezetés, szervezet, személyi állomány, kiképzés, technológia, infrastruktúra, logisztika és interoperabilitás.
[7] Trust service.
[8] Elsősorban a biztonsági eseménykezelő központok, csoportok, de emellett bűnüldöző, belbiztonsági, kritikus infrastruktúravédelmi, nemzetbiztonsági szervezetek.

a közös terminológia hiányát, az alkalmazott fogalmak formális tisztázásának jelentőségét. A dokumentum konkrét formában is megnevezi az interoperabilitást. A kérdéskör több későbbi dokumentumban is megjelenik, pld. fenyegetés, biztonsági esemény osztályozási rendszerek [30, 33-36. o.] formájában, és két új dokumentum [33, 34] központi témakörét is képezi.

Az *elektronikus azonosítás és bizalmi szolgáltatások* kérdései ENISA dokumentumokban is feldolgozásra kerültek. Az ügynökség a vonatkozó EU szabályozó kiadása előtt egy jelentésben [35] dolgozta fel a bizalmi szolgáltatásokhoz kapcsolódó szabványokat, szolgáltatásokat, és részletesen értékelte ezek interoperabilitásának helyzetét, javaslatokat fogalmazott meg az határokon átnyúló interoperabilitás megvalósítására.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A hálózat- és informatikai biztonság legmagasabb szinten elsőként egy európai átfogó hálózat- és informatikai biztonsági politikára vonatkozó javaslatban (2001) jelent meg. Ezt az elektronikus hírközlő hálózatok és szolgáltatások biztonsági kérdéseinek szabályozása követte.

A hálózat- és biztonságpolitika, valamint az ennek feladatai megvalósítására 2004-ben létrehozott ENISA napjainkig folyamatos fejlesztés alatt állt (2006, 2013, 2016). A középpontban a minden érdekeltre kiterjedő partnerség, a biztonsági stratégiák kidolgozása, és az együttműködő eseménykezelő központok hálózatának kialakítása állt.

A kiberbiztonság tágabb tartalmú értelmezése fokozatosan, és egyre növekvő mértékben nyert tért az EU dokumentumokban. Az első stratégia e tárgyban 2013-ban jelent meg, majd 2014-ben kiadásra került az EU kibervédelmi politika kereteit rögzítő dokumentum. A kiberbiztonság az EU értelmezés szerint – bár hivatalos meghatározásával még nem találkozhatunk – a közös biztonság- és védelempolitika kereteibe illeszkedő, átfogó, három pillérre (a hálózat- és informatikai biztonságra, a bűnüldözésre és a védelmi szférára) épülő kérdéskör.

A kiberbiztonság (kezdetben hálózat- és informatikai biztonság) iránti igények már a Bangemann jelentésben megjelentek a szellemi tulajdonjogok, a személyes adatok, valamint az információk elektronikus és jogi védelme formájában. Ezt az elektronikus hírközlési szolgáltatások biztonságának igénye követte. A biztonság szükségessége később megfogalmazódott a kritikus információs infrastruktúrák, az e-kereskedelembe vetett bizalom, a sok szolgáltató által működtetett hálózatok komplex biztonsága, valamint a biztonsági kérdések globális jellege oldaláról is. A kiberbiztonsági célkitűzések köre folyamatosan bővült, finomodott, 2014-ben magában foglalta többek között a kibertámadásokkal szembeni ellenállóképesség növelését; a kiberbűnözés drasztikus csökkentését; valamint a kiberbiztonsági együttműködés feltételeinek megteremtését, az együttműködés megvalósítását.

Az interoperabilitás kérdései a kiberbiztonsági területen elsősorban az együttműködéshez, az ehhez szükséges információcseréhez kapcsolódóan jelenhetnek meg. Az európai kiberbiztonság alapja a közigazgatás és a magánszektor képességeinek, erőforrásainak, és eljárásainak együttműködése, az illetékes kiberbiztonsági szervezetek közötti információmegosztás, és kölcsönös segítségnyújtás. Ez pedig megköveteli az együttműködő szervezetek (és egyre bővülő mértékben informatikai rendszereik) közötti technikai, formai (szintaktikai) és fogalmi (szemantikai) interoperabilitást. Ehhez kapcsolódóan az ENISA már megalakulását követően, és azóta is folyamatosan hangsúlyozza a hálózati biztonsági információcsere interoperabilitási kérdéseit, tesz javaslatokat ezek megoldására.

Az interoperabilitás másik kapcsolódási pontja a kiberbiztonsághoz az alapvető biztonsági megoldások (elsősorban az elektronikus azonosítás és a bizalmi szolgáltatások) határokon átnyúló interoperabilitása. Ezek már a 2000-es évek elején felmerültek, a legfrissebb dokumentum e tárgyban 2014-es. A nemzeti, ágazati, közigazgatási, vállalati rendszerekben alkalmazott biztonsági megoldások interoperabilitása nélkül nincs egységes digitális piac, nincs egységes európai információs tér.

Az interoperabilitási kérdések szerepe a kiberbiztonságban egyelőre kisebb, mivel a kiberbiztonsági eseménykezelő központok együttműködése napjainkban még alapvetően a hagyományos, vagy nem strukturált információcserére épül. Az Európai Unió e téren, tekintettel lehetőségeire, elsősorban az együttműködés ösztönzésére, a szabályozási kérdésekre összpontosít, a kérdéskör feladatai megvalósításának alapvető felelőse az ENISA.

Mindezek alapján levonható a következtetés, hogy a kiberbiztonság területén az eseménykezelő központok által alkalmazott informatikai rendszerek bővülésével, fejlődésével, már a közeljövőben előtérbe fognak kerülni a központok közötti, illetve a más érintett szervezetekkel folytatott információcsere interoperabilitási, elsősorban szemantikai interoperabilitási problémái. Ezen belül kiemelt szerepet fognak játszani a terminológiai kérdések, az alkalmazott fogalomrendszerek közötti átjárhatóság, vagy akár a biztonsági megoldásokban felhasználható adatok (rosszindulatú szoftver minták, támadási mintázatok, stb.) interoperábilis cseréje.

FELHASZNÁLT IRODALOM

[1] MUNK S.: *Interoperabilitási célok, jövőképek, és szabályozók az EU-ban és kapcsolatrendszerük a kiberbiztonsággal*; Hadmérnök, 2017 (Hadmérnök, 2017/K2 (149-162. o.).

[2] *Definition of Cybersecurity. Gaps and overlaps in standardisation; V1.0* European Union Agency for Network and Information Security, Heraklion, 2015

[3] HAIG Zs.: *Információ – társadalom – biztonság;* Nemzeti Közszolgálati Egyetem, Budapest, 2015.

[4] HAIG Zs.-VÁRHEGYI I.: *A cybertér és a cyberhadviselés értelmezése*; Hadtudomány, 2008 (XVIII.)/elektronikus szám (1-12. o.)

[5] HAIG Zs.-KOVÁCS L.-VÁNYA L.: *Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata*; Felderítő Szemle, 2011 (X.)/1-2. (183-209. o.)

[6] LEE, E. E.: *The Past, Present and Future of Cyber-Physical Systems: A Focus on Models;* Sensors, 2015 (15)/3. (4837-4869. o.)

[7] HORVÁTH I.-GERRITSEN, B. H. M.: *Cyber-physical Sytems: Concepts, Technologies and Implementation Principles;* In. HORVÁTH I.-RUSÁK, Z.-ALBERS, A.-BEHRENDT, M. (Eds): *Proceedings of TMCE 2012, May 7–11,* Karlsruhe, 2012. (19-36. o.)

[8] MUNK S.: *An analysis of basic interoperability related terms, system of interoperability types.* Academic and Applied Research in Military Science, 2002 (I.)/1. (117-132.o.)

[9] MUNK S.: *Katonai informatika a XXI. század elején;* Zrínyi Kiadó, Budapest, 2007 (264 o.)

[10] MUNK S.: *Katonai informatikai rendszerek interoperabilitásának aktuális hadtudományi kérdései;* MTA doktori értekezés. Magyar Tudományos Akadémia, Budapest, 2007.

[11] *Annex 2 to COM(2010) 744, European Interoperability Framework (EIF) for European Public Services;* European Commission, Brussels, 2010.

[12] *COM(2001) 298, Network and Information Security: Proposal for a European Policy Approach;* Commission of the European Communities, Brussels, 2001. június 6.

[13] *Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive);* European Parliament and the Council, 2002. március 7.

[14] *Directive 2002/20/EC on the authorization of electronic communications networks and services (Authorization Directive);* European Parliament and the Council, 2002. március 7.

[15] *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications);* European Parliament and the Council, 2002. július 12.

[16] *Regulation 460/2004 establishing the European Network and Information Security Agency;* European Parliament and the Council, 2004. március 10.

[17] *Regulation 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation 460/2004;* European Parliament and the Council, 2013. május 21.

[18] *COM(2005) 229, i2010 – A European Information Society for growth and employment;* Commission of the European Communities, Brussels, 2005. június 1.

[19] *COM(2006) 251, A strategy for a Secure Information Society – "Dialogue, partnership and empowerment";* Commission of the European Communities, Brussels, 2006. május 31.

[20] *COM(2013) 48, Proposal for a directive concerning measures to ensure a high common level of network and information security across the Union;* European Commission, Brussels, 2013. február 7.

[21] *Directive 2016/1148 concerning the processing measures for a high common level of security of network and information systems across the Union;* European Parliament and the Council, 2016. július 6.

[22] *JOIN(2013) 1, Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace;* European Commission, Brussels, 2013.

[23] *EU Cyber Defence Policy Framework;* Council of the European Union, Brussels, 2014. November 18.

[24] *Europe and the Global Information Society. Bangemann report recommendations to the European Council;* 1994.

[25] *COM(2010) 245, A Digital Agenda for Europe;* European Commission, Brussels, 2010. augusztus 26.

[26] *COM(2015) 192, A Digital Single Market Strategy for Europe;* European Commission, Brussels, 2015. május 6.

[27] *Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation);* European Parliament and the Council, 2014. július 23.

[28] *CERT cooperation and its further facilitation by relevant stakeholders;* ENISA, 2006.

[29] *Good Practice Guide Network Security Information Exchanges;* ENISA, 2009.

[30] *Alerts, Warnings and Announcements. Best Practices Guide;* ENISA, 2013. november.

[31] *Standards and tools for exchange and processing of actionable information;* ENISA, 2014. november.

[32] *Ontology and taxonomies of resilience;* ENISA, 2011 december.

[33] *Information sharing and common taxonomies between CSIRTs and Law Enforcement;* ENISA, 2015. december.

[34] *A good practice guide of using taxonomies in incident prevention and detection;* ENISA 2016. december.

[35] *Trusted e-ID Infrastructures and services in EU TSP services, standards and risk analysis report;* ENISA, 2013. december.