Az Európai Gazdasági és Szociális Bizottság véleménye – Javaslat európai parlamenti és tanácsi rendeletre az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály”)

[COM(2017) 477 final/2 2017/0225 (COD)]

(2018/C 227/13)

Előadó: **Alberto MAZZOLA**

Társelőadó: **Antonio LONGO**

Felkérés:	Európai Parlament, 2017.10.23.
	az Európai Unió Tanácsa, 2017.10.25.
Jogalap:	az Európai Unió működéséről szóló szerződés 114. cikke
Illetékes szekció:	„Közlekedés, energia, infrastruktúra és információs társadalom” szekció
Elfogadás a szekcióülésen:	2018.2.5.
Elfogadás a plenáris ülésen:	2018.2.14.
Plenáris ülés száma: xx.	532.
A szavazás eredménye:	206/1/2
(mellette/ellene/tartózkodott):	

1. **Következtetés és ajánlások**

1.1. Az EGSZB úgy véli, hogy az ENISA Európai Bizottság által javasolt új állandó megbízatása jelentősen hozzá fog járulni az európai rendszerek ellenálló képességének növeléséhez. Előfordulhat azonban, hogy az ENISA számára előirányzott, kapcsolódó ideiglenes költségvetés és erőforrások nem elegendőek ahhoz, hogy az ügynökség eleget tudjon tenni megbízatásának.

1.2. Az EGSZB valamennyi tagállamnak azt javasolja, hogy hozza létre az ENISA egyértelmű és egyenértékű partnerszervezetét, ezt ugyanis a legtöbben még nem tették meg.

1.3. Az EGSZB emellett úgy érzi, hogy az ENISA-nak a kapacitásépítést illetően az e-kormányzatot támogató intézkedések számára kell elsőbbséget biztosítania ([1]). Kulcsfontosságú a személyek, szervezetek és tárgyak uniós/globális digitális azonosítója, és prioritásként kell kezelni a személyazonosság-lopás és az internetes csalás megelőzését és az ezek elleni küzdelmet.

1.4. Az EGSZB azt javasolja, hogy az ENISA rendszeres jelentéseket készítsen a tagállamok kiberfelkészültségéről, elsősorban a kiberbiztonsági irányelv II. mellékletében azonosított ágazatokra összpontosítva. Egy éves európai kibergyakorlat keretében értékelni kell a tagállamok felkészültségét és az európai kiberbiztonsági válságreagálási mechanizmus eredményességét, valamint ajánlásokat kell megfogalmazni.

1.5. Az EGSZB támogatja a kiberbiztonsági kompetenciahálózat létrehozására irányuló javaslatot. E hálózatot egy Európai Kiberbiztonsági Kutató- és Kompetenciaközpont (CRCC) tartaná fenn. E hálózat a legfontosabb technológiai kapacitások versenyképes európai ipari bázisának a szerződéses köz-magán társulás (cPPP) által elvégzett munkán alapuló kialakításával támogathatná az európai digitális önrendelkezést; e társulásnak háromoldalú közös vállalkozássá kell átalakulnia.

1.6. A kiberbalesetek legfontosabb okainak egyike az emberi tényező. Az EGSZB szerint erős kiberkészségbázist kell kialakítani, és tudatosságnövelő kampányokkal is javítani kell a kiberhigiéniát az egyének és a vállalkozások körében. Az EGSZB támogatja egy uniós tanúsítvánnyal rendelkező tanterv létrehozását a középiskolák és a szakemberek számára.

([1]) Digitális egységes piac – félidős értékelés.

1.7. Az EGSZB úgy gondolja, hogy az európai digitális egységes piac megköveteli a kiberbiztonságra vonatkozó szabályok egységes értelmezését, ideértve a tagállamok közötti kölcsönös elismerést is, továbbá hogy egy tanúsítási keretrendszer és a különböző ágazatokra vonatkozó tanúsítási programok biztosíthatnák a közös kiindulópontot. A különböző ágazatok számára azonban működési módjukból adódóan különböző megközelítéseket kell biztosítani. Az EGSZB ezért úgy gondolja, hogy a folyamatba be kell vonni az ágazati uniós ügynökségeket (EASA, ERA, EMA stb.), és egyes esetekben – az ENISA beleegyezésével – a koherencia biztosítása érdekében ezekre kell bízni a kiberbiztonsági rendszerek elkészítését. A CEN/CENELC/ETSI-vel együttműködésben az IT-biztonságra vonatkozó európai minimum-szabványokat kell elfogadni.

1.8. A tervbe vett európai kiberbiztonsági tanúsítási csoportnak, amelyet az ENISA támogat majd, az átfogó tanúsítási rendszerek kidolgozásának biztosítása érdekében a nemzeti tanúsításfelügyeleti szervekből, a magánszektor érdekelt feleiből, ezen belül a különböző alkalmazási területeken működő szereplőkből, valamint a tudomány és a civil társadalom képviselőiből kell állnia.

1.9. Az EGSZB álláspontja szerint az ügynökségnek vizsgálatok és ellenőrzések révén nyomon kell követnie az Európai Bizottság nevében a nemzeti tanúsításfelügyeleti hatóságok teljesítményét és döntéshozatalát, a felelősségi köröket és a szabályok be nem tartásáért kivetett szankciókat pedig a rendeletben kell meghatározni.

1.10. Az EGSZB úgy véli, hogy a tanúsítási rendszerek nem zárhatják ki a megfelelő címkézési rendszert, amelyet a fogyasztók bizalmának megerősítése érdekében az importtermékekre is alkalmazni kell.

1.11. Európának a különböző uniós alapok, nemzeti alapok és magánszektorbeli beruházások összehangolásával, a köz- és a magánszféra közötti szoros együttműködésben a jelenlegi és jövőbeli kutatási keretprogramban fokoznia kell a stratégiai célkitűzések elérésére irányuló beruházásokat, többek között egy uniós Innovációs és Kutatási-Fejlesztési Kiberbiztonsági Alap létrehozása révén. Ezen túlmenően Európának alapot kellene létrehoznia a kiberbiztonság megvalósítása céljából, új ablakot nyitva a jelenlegi és jövőbeli Európai Hálózatfinanszírozási Eszközön és a következő ESBA 3.0-n belül.

1.12. Az EGSZB úgy véli, hogy az „emberek internetének” (IoP) részét alkotó „szokásos” eszközökhöz szükség van egy minimális biztonsági szintre. Ebben az esetben a tanúsítás a magasabb szintű biztonság biztosításának kulcsfontosságú módszere. A dolgok internetének (IoT) biztonságát prioritásként kell kezelni.

2. **A kiberbiztonság jelenlegi kerete**

2.1. A kiberbiztonság a jólét és a nemzetbiztonság, valamint a demokrácia működése, a szabadságjogok és az értékek szempontjából egyaránt kritikus fontosságú. „A kiberbiztonság olyan ökoszisztéma, mely akkor a legeredményesebb, ha a jogszabályok, a szervezetek, a készségek, az együttműködés és a technikai végrehajtás összhangja jellemzi” – állapítja meg az ENSZ globális kiberbiztonsági indexe, és még hozzáteszi, hogy a kiberbiztonság „egyre fontosabbá válik az országok döntéshozóinak szemében”.

2.2. Az internet forradalma miatt egyre inkább kritikussá válik a biztonságos ökoszisztéma iránti igény. Ez a forradalom nemcsak a fogyasztói (B2C) ágazatokat definiálta újra, így például a médiát, a kiskereskedelmet és a pénzügyi szolgáltatásokat, hanem átalakítja a feldolgozóipart, az energiaágazatot, a mezőgazdaságot, a közlekedést és a gazdaság más ágazatait is – amelyek együttesen a globális bruttó hazai termék közel kétharmadát teszik ki –, valamint a közművek infrastruktúráit és az emberek közigazgatással való érintkezését is.

2.3. A digitális egységes piac középpontjában az árukhoz, a szolgáltatásokhoz és a tartalmakhoz való hozzáférés javítása áll, mégpedig a digitális hálózatok és szolgáltatások megfelelő jogi keretének megteremtése, valamint az adatalapú gazdaság hasznainak learatása révén. A becslések szerint a stratégia évi 415 milliárd euróval járulhatna hozzá az uniós gazdasághoz. Ami a magánszektorban dolgozó szakembereket illeti, 2022-re 350 000 kiberbiztonsági ismeretekkel rendelkező szakember hiányát jelzik előre Európában ([2]).

([2]) HL JOIN(2017) 450 final.

2.4. Egy 2014-es tanulmány becslése szerint 2013-ban az Unióban a kiberbűnözés gazdasági hatása az uniós GDP 0,41 %-ának felelt meg (azaz mintegy 55 milliárd eurónak) ([3]).

2.5. Az Eurobarométer „Az európaiak hozzáállása a kiberbiztonsághoz" (*Europeans' attitudes towards cyber security*) című, 464a. számú tematikus felmérése szerint az internethasználók 73 %-a aggódik amiatt, hogy a webhelyek nem tárolják biztonságosan online személyes információit, 65 %-uk pedig amiatt aggódik, hogy a hatóságok nem tárolják biztonságosan ezeket az adatokat. A legtöbb válaszadó aggódik amiatt, hogy különböző kiberbűncselekmények áldozatává válhat, mindenekelőtt az eszközeire kerülő rosszindulatú szoftverek (69 %), a személyazonosság-lopás (69 %), valamint a bankkártyacsalás és az internetes banki csalás (66 %) miatt ([4]).

2.6. Eddig semelyik jogszabályi keret nem volt képes lépést tartani a digitális innováció ütemével, bár több jogszabályi szöveg járul hozzá elemenként a megfelelő keret létrehozásához: a hírközlési kódex felülvizsgálata, az általános adatvédelmi rendelet, a hálózati és információs rendszerek biztonságáról szóló irányelv (kiberbiztonsági irányelv), a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló rendelet (e-IDAS rendelet), az EU-USA adatvédelmi pajzs, a készpénz-helyettesítő fizetési eszközökkel elkövetett csalásról szóló irányelv és így tovább.

2.7. Az ENISA (az EU kiberbiztonsági ügynöksége) mellett sok más szervezet foglalkozik kiberbiztonsági kérdésekkel: az Europol; a Cert-EU (az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportja); az EU Helyzetelemző Központja (EU INTCEN); a Szabadságon, a Biztonságon és a Jog Érvényesülésén Alapuló Térség Nagyméretű IT-rendszereinek Üzemeltetési Igazgatását Végző Európai Ügynökség (eu-LISA); az információmegosztó és -elemző központok (ISAC-ok), az Európai Kiberbiztonsági Szervezet (ECSO), az Európai Védelmi Ügynökség (EDA); a NATO Kibervédelmi Kiválósági Együttműködési Központja; valamint a nemzetközi biztonsággal összefüggésben az információk és távközlés területén végbemenő fejleményekkel foglalkozó ENSZ kormányzati szakértői csoport (UN GGE).

2.8. A beépített biztonság kulcsfontosságú a jó minőségű áruk és szolgáltatások biztosításához: az intelligens eszközök nem annyira intelligensek, ha nincs megoldva a biztonságuk, és ugyanez igaz az intelligens autókra, az intelligens városokra és az intelligens kórházakra – az ide tartozó eszközök, rendszerek, architektúrák és szolgáltatások mind megkövetelik a beépített biztonságot.

2.9. Az Európai Tanács 2017. október 19–20-án a javasolt reformcsomag után az uniós kiberbiztonság közös megközelítésének elfogadására szólított fel: eszerint szükség van egy „közös megközelítésre a kiberbiztonságra vonatkozóan: a digitális világban bizalom szükséges, és ez csak úgy biztosítható, ha gondoskodunk arról, hogy az összes digitális szakpolitika esetében eleve szempont legyen a biztonság garantálása, valamint ha megfelelő biztonsági tanúsítvánnyal látjuk el a termékeket és a szolgáltatásokat, továbbá ha növeljük a kibertámadások megelőzésére, megakadályozására, felderítésére és elhárítására szolgáló kapacitásainkat" ([5]).

2.10. Az Európai Parlament 2017. május 17-i állásfoglalásában „hangsúlyozza a végpontok közötti adatbiztonság fontosságát a teljes pénzügyi szolgáltatási értékláncban; felhívja a figyelmet a pénzpiaci infrastruktúráinkat, a dolgok internetét, a valutáinkat és az adatainkat célzó kibertámadások jelentette nagy és kiterjedt kockázatokra; […] sürgeti az európai felügyeleti hatóságokat, hogy […] rendszeresen vizsgálják felül a pénzintézetek IKT-val kapcsolatos kockázataira vonatkozó hatályos működési előírásokat; szorgalmazza továbbá […] az európai felügyeleti hatóság által kidolgozott, e kockázatok felülvizsgálatára vonatkozó iránymutatások létrehozását; hangsúlyozza annak fontosságát, hogy az európai felügyeleti hatóságok rendelkezzenek […] technológiai know-how-val" ([6]).

2.11. Az EGSZB-nek korábban több alkalma volt arra, hogy számot vessen a kérdéssel ([7]) – például a tallinni csúcstalálkozón, az e-kormányzat jövőbeli fejlődéséről szóló konferencián ([8]) –, és a digitális menetrenddel foglalkozó állandó tanulmányozócsoportot hozott létre.

([3]) Európai bizottsági szolgálati munkadokumentum – Az európai parlamenti és tanácsi rendeletre irányuló javaslatot kísérő hatásvizsgálat, 1/6. rész, 21. o., Brüsszel, 2017. 09. 13.

([4]) Az Eurobarométer 464a. tematikus felmérése, EB87.4: Az európaiak hozzáállása a kiberbiztonsághoz (*Europeans' attitudes towards cyber security*), 2017. szeptember.

([5]) Az Európai Tanács következtetései, 2017. október 19., csütörtök.

([6]) Az Európai Parlament 2017. május 17-i állásfoglalása (A8-0176/2017).

([7]) Digitális egységes piac – félidős értékelés. HL C 75., 2017.3.10., 124. o., HL C 246., 2017.7.28., 8. o., HL C 345., 2017.10.13., 52. o., HL C 288., 2017.8.31., 62. o., HL C 271., 2013.9.19., 133. o.

([8]) Az EGSZB 31/2017. sz. sajtóközleménye (angol nyelven): „Civil Society debates E-government and cybersecurity with incoming Estonian Presidency": https://www.eesc.europa.eu/en/news-media/press-releases/civil-society-debates-e-government-and-cybersecurity-incoming-estonian-presidency

3. **Az Európai Bizottság javaslatai**

3.1. A kiberbiztonsági csomag része egy közös közlemény, amely felülvizsgálja a korábbi európai kiberbiztonsági stratégiát (2013), valamint egy kiberbiztonsági jogszabály, amely elsősorban az ENISA új megbízatásával és a javasolt tanúsítási keretrendszerrel foglalkozik.

3.2. A stratégia három fő részre tagolódik: ezek az ellenálló képesség, az elrettentés és a nemzetközi együttműködés. Az elrettentéssel foglalkozó rész főként a kiberbűnözésre, így többek között a Budapesti Egyezményre összpontosít, a nemzetközi együttműködéssel foglalkozó rész pedig a kibervédelmet, a kiberdiplomáciát és a NATO-val való együttműködést vizsgálja.

3.3. A javaslat többek között a következő új kezdeményezéseket határozza meg:

— a kiberbiztonsággal foglalkozó uniós ügynökség megerősítése;

— uniós kiberbiztonsági tanúsítási rendszer bevezetése;

— a kiberbiztonsági irányelv mielőbbi végrehajtása.

3.4. Az ellenálló képességgel foglalkozó rész a kiberbiztonsággal kapcsolatos intézkedésekre tesz javaslatot, amelyek különösen a következőket érintik: piaci kérdések, a kiberbiztonsági irányelv, gyors vészhelyzeti reagálás, az uniós kompetencia fejlesztése, oktatás, képzés (a kiberkészségek és a kiberhigiénia terén), valamint tudatosságnövelés.

3.5. A kiberbiztonsági jogszabály ezzel párhuzamosan egy ikt-termékek és -szolgáltatások kiberbiztonsági tanúsítására szolgáló keretrendszer létrehozására tesz javaslatot.

3.6. A kiberbiztonsági jogszabály emellett kiemelt szerepet javasol az ENISA mint a kiberbiztonságért felelős uniós ügynökség számára, és állandó megbízatást ad az ügynökségnek. Jelenlegi feladatain túlmenően az ENISA-tól új támogatási és koordinációs feladatok ellátását várják, a következőkkel kapcsolatban: a kiberbiztonsági irányelv végrehajtásához nyújtott támogatás, az uniós kiberbiztonsági stratégia, a kiberbiztonsági tervezet, kapacitásépítés, tudás- és információmegosztás, tudatosságnövelés, piaci feladatok, úgymint a szabványosításhoz és a tanúsításhoz nyújtott támogatás, kutatás és innováció, pán-európai kiberbiztonsági gyakorlatok és titkársági feladatok ellátása a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT) hálózata számára.

4. **Általános észrevételek – Áttekintés**

4.1. ***Kontextus: reziliencia***

4.1.1. *Egységes kiberbiztonsági piac*

Gondossági kötelezettség: A közös közleményben említett „gondossági kötelezettség” javasolt elvének kidolgozása a biztonságos fejlesztési életciklus-folyamatok alkalmazása tekintetében figyelemreméltó, az uniós ágazattal kidolgozandó koncepció, amely az uniós jogszabályi megfelelés átfogó megközelítéséhez vezethetne. Alapértelmezés szerint a biztonságot minden jövőbeli fejlesztés esetében figyelembe kell venni.

Felelősség: Vita esetén a tanúsítás meg fogja könnyíteni a felelősség meghatározását.

4.1.2. Kiberbiztonsági irányelv: energia, közlekedés, banki/pénzügyi tevékenységek, egészségügy, ivóvízellátás, digitális infrastruktúra, e-kereskedelem.

Az EGSZB alapvetőnek tartja a kiberbiztonsági irányelv teljeskörű és hatékony végrehajtását a kritikus fontosságú nemzeti ágazatok ellenálló képességének biztosítása érdekében.

Az EGSZB úgy gondolja, hogy a közszféra és a magánszféra szereplői közötti információcserét ágazati információmegosztó- és -elemző központok (ISAC-ok) révén meg kell erősíteni. A jelenleg használt mechanizmus értékelése/elemzése alapján a bizalmas információk ISAC-okon belüli és a CSIRT-ek és ISAC-ok közötti biztonságos megosztására szolgáló megfelelő mechanizmust kell kialakítani.

4.1.3. *Gyors vészhelyzeti reagálás*

A „Tervezet” megközelítése biztosítaná a nagyszabású eseményekre való, uniós és tagállami szintű operatív reagálás hatékony folyamatát. Az EGSZB hangsúlyozza, hogy be kell vonni a magánszektort; az operatív reagálási mechanizmusban figyelembe kell venni az alapvető szolgáltatások működtetőit is, mivel a fenyegetésekre vonatkozó értékes információkkal szolgálhatnak, és/vagy támogathatják a fenyegetések és nagyszabású válságok felderítését és az azokra való reagálást.

A közös közlemény javasolja, hogy a kiberbiztonsági incidenseket illesszék be az uniós szintű válságkezelési mechanizmusokba. Jóllehet az EGSZB megérti, hogy támadás esetén közös reagálásra és szolidaritásra van szükség, jobban meg kell érteni, hogy ezt hogyan lehetne alkalmazni, mivel a kiberfenyegetések rendszerint több országra átterjednek. Helyi igény esetén a nemzeti vészhelyzetek során használt eszközöket csak részben lehetne megosztani.

4.1.4. *Az uniós kompetencia fejlesztése*

Ahhoz, hogy az EU valóban versenyképes legyen a globális színtéren, továbbá a megbízható technológia bázis felépítéséhez elengedhetetlen egy koherens, hosszú távú keret megteremtése, amely a kiberbiztonsági értéklánc valamennyi szakaszát magába foglalja. Ezzel kapcsolatban az európai kiberbiztonsági értéklánc kialakításához kulcsfontosságú az európai regionális ökoszisztémák közötti együttműködés elősegítése. Az EGSZB üdvözli a kiberbiztonsági kompetenciahálózat létrehozására irányuló javaslatot.

E hálózat egy versenyképes európai ipari bázis létrehozásával és a fő technológiai kapacitások tekintetében az EU-n kívül kifejlesztett know-how-tól való függőség csökkentésével támogathatná az európai digitális önrendelkezést, technikai gyakorlatokat, munkaértekezleteket, sőt, akár alapvető kiberhigiéniai képzést biztosíthatna szakemberek és nem szakemberek számára, valamint egy európai piac kibontakozása érdekében – a cPPP által elvégzett munka alapján – elősegíthetné egy nemzeti köz-magán szervezetekből álló hálózat létrejöttét. „A kiberbiztonsági szerződéses köz-magán társulás (cPPP) fejlesztése minden bizonnyal elvezet annak optimalizálásához, kiigazításához vagy bővítéséhez” (az észt–bolgár–osztrák elnökségi trió kiberbiztonsági munkaprogramja); e fejlesztés egy háromoldalú (Európai Bizottság, tagállamok, vállalkozások) közös vállalkozás révén valósulhat meg.

Ahhoz, hogy e hálózat eredményes legyen, és európai szinten elérje javasolt célkitűzéseit, jól meghatározott irányítási rendszerre kell támaszkodnia.

E hálózatot egy Európai Kiberbiztonsági Kutató- és Kompetenciaközpont (CRCC) támogatná európai szinten, amely Unió-szerte összekapcsolná a meglévő nemzeti kompetenciaközpontokat. A CRCC nemcsak koordinálná és irányítaná a kutatást, mint más közös vállalkozások esetében, hanem lehetővé tenné egy európai kiberbiztonsági ökoszisztéma eredményes kialakítását is, amely támogatná az uniós innováció bevezetését és elterjesztését.

4.2. ***Kontextus: elrettentés***

4.2.1. A kiberbűnözés elleni küzdelem nemzeti és európai szinten is kiemelt prioritás, amely határozott politikai elkötelezettséget igényel. Az elrettentést célzó tevékenységeket a köz- és a magánszektor közötti erőteljes partnerségre alapozva kell végrehajtani, nemzeti és európai szinten egyaránt hatékony információmegosztás és szakértelem létrehozásával. Előirányozható az Europol által végzett kiberkriminalisztikai és ellenőrzési tevékenységek bővítésének a lehetősége is.

4.3. ***Nemzetközi együttműködés***

4.3.1. A harmadik országokkal való megbízható együttműködés kiberdiplomácián és üzleti partnerségeken keresztüli kiépítése és fenntartása kulcsfontosságú ahhoz, hogy megerősödjenek Európa nagyszabású kibertámadások megelőzésére, megakadályozására és az azokra való reagálásra irányuló képességei. Európának elő kell mozdítania az USA-val, Kínával, Izraellel, Indiával és Japánnal való együttműködést. Az uniós exportszabályozás modernizálása hozzájárulhat az emberi jogok megsértésének vagy a technológiákkal az Unió saját biztonsága ellen való visszaéléseknek a megelőzéséhez, de célja annak biztosítása is, hogy ne hozzák hátrányosabb helyzetbe az uniós ipart a harmadik országokból származó kínálathoz képest. A csatlakozásra váró országok tekintetében eseti stratégiát kell előirányozni, hogy felkészülhessenek az érzékeny adatok határokon átnyúló cseréjére, beleértve az ENISA-országok egyes tevékenységeiben megfigyelőként történő részvételt – ezeket az országokat a kiberbiztonságért való küzdelemre irányuló hajlandóságuk alapján kell rangsorolni, és akár feketelista létrehozását is érdemes megfontolni.

4.3.2. Az EGSZB üdvözli a kibervédelem bevezetését a lehetséges jövőbeli uniós kiberbiztonsági kompetenciaközpont tervbe vett második szakaszában. Ebből adódóan Európa a köztes időszakban megvizsgálhatná a kettős felhasználású kompetenciák fejlesztését, építve például az Európai Védelmi Alapra és a kibervédelmi képzési és oktatási platform 2018-ra tervezett létrehozására. A kölcsönösen elismert potenciálra és fenyegetésekre való tekintettel az EGSZB szükségesnek tartja az EU–NATO együttműködés kialakítását, ezenkívül az európai iparnak is szorosan figyelemmel kell kísérnie a kiberbiztonsági szabványok nagyobb kölcsönös átjárhatóságával kapcsolatos EU–NATO együttműködés és az együttműködés más formáinak fejleményeit is a kibervédelem uniós megközelítésével összefüggésben.

4.4. ***Uniós tanúsítási keretrendszer***

4.4.1. Az EGSZB úgy véli, hogy Európának a szabályok egységes értelmezése révén szembe kell szállnia a kiberbiztonság terén megfigyelhető szétforgácsolódással, ideértve a tagállamok közötti, egységes keretben zajló kölcsönös elismerést is, amelynek célja a digitális egységes piac védelmének megkönnyítése. A tanúsítási keretrendszer egy közös alapot határozhatna meg (szükség esetén a magasabb szintekre vonatkozó konkrét szabályokkal), biztosítva a vertikális ágazatok közötti szinergiákat és csökkentve a jelenlegi felaprózottságot.

4.4.2. Az EGSZB üdvözli az uniós kiberbiztonsági tanúsítási keretrendszer és a különböző ágazatokra vonatkozó tanúsítási rendszerek létrehozását, amely megfelelő követelményeken alapul, és amelyre a fő érdekelt felekkel együttműködésben kerül sor. A piacra jutási idő és a tanúsítási költségek, valamint a minőség és a biztonság azonban olyan kulcsfontosságú elemek, amelyeket figyelembe kell venni. A biztonság fokozása érdekében tanúsítási rendszereket kell létrehozni a szükségletekkel és fenyegetésekkel kapcsolatos jelenlegi ismeretek alapján: a szükséges frissítések lehetővé tétele érdekében figyelembe kell venni e rendszerek rugalmasságát és fejlődőképességét. A különböző ágazatok számára a működési módjukból adódóan különböző megközelítéseket kell biztosítani. Az EGSZB ezért úgy gondolja, hogy a folyamatba be kell vonni az ágazati uniós ügynökségeket (EASA, EBH, ERA, EMA stb.), és egyes esetekben, az ENISA beleegyezésével – az átfedések és a koherencia hiányának elkerülése érdekében – ezekre kell bízni a kiberbiztonsági rendszerek kidolgozását.

4.4.3. Az EGSZB számára fontos, hogy a tanúsítási keretrendszer olyan közösen meghatározott európai kiberbiztonsági és IKT-szabványokon alapuljon, amelyek lehetőleg nemzetközileg elismertek. Tekintve az időkeretet és a nemzeti előjogokat, az IT-biztonságra vonatkozó európai minimumszabványokat a CEN/CENELC/ETSI-vel együttműködésben kell elfogadni. A szakmai szabványokat kedvezően kell értékelni, de ezek nem lehetnek jogilag kötelezők és nem hátráltathatják a versenyt.

4.4.4. Egyértelműen fontos, hogy a felelősségeket a fenyegetések hatása alapján társítsák a megbízhatóság különböző szintjeivel. A biztosítótársaságokkal való párbeszéd elindítása hasznos lehet az eredményes és az alkalmazó ágazattal összhangban levő kiberbiztonsági követelmények elfogadása szempontjából. Az EGSZB nézete szerint támogatni és ösztönözni kell azokat a vállalatokat, amelyek magas megbízhatósági szintre törekednek, különösen az életvédelem szempontjából kritikus berendezések és rendszerek esetében.

4.4.5. Tekintettel a 85/374/EGK irányelv ([9]) elfogadása óta eltelt időre, és figyelembe véve a jelenlegi technológiai fejlesztéseket, az EGSZB arra kéri az Európai Bizottságot, hogy vizsgálja meg annak lehetőségét, hogy az irányelv hatályába beemelje az ebben a rendeletre irányuló javaslatban felvázolt egyes forgatókönyveket annak érdekében, hogy lehetővé tegye a fokozottabb védelmet nyújtó, biztonságosabb termékek kidolgozását.

4.4.6. Az EGSZB úgy véli, hogy a tervbe vett európai kiberbiztonsági tanúsítási csoportnak, amelyet az ENISA támogat majd, az átfogó tanúsítási rendszerek kidolgozásának biztosítása érdekében a nemzeti tanúsításfelügyeleti szervekből, a magánszektor érdekelt feleiből és a különböző alkalmazási területeken működő szereplőkből kell állnia. Ezen túlmenően együttműködést kell előirányozni e csoport és az EU/EGT ágazati érdekképviseleti szervezetei (pl. kiberbiztonsági szerződéses köz-magán társulás, bankszektor, közlekedés, energia, szövetségek stb.) között, szakértők kinevezése útján. E csoportnak képesnek kell lennie arra, hogy figyelembe vegye a tanúsítás terén elért európai eredményeket (főként a SO-GIS kölcsönös elismerési megállapodás [MRA], nemzeti rendszerek és tulajdonjogi védelem hatálya alá tartozó rendszerek alapján), és az európai versenyelőnyök megőrzésére kell törekednie.

([9]) HL L 210., 1985.8.7., 29. o.

4.4.7. Az EGSZB azt javasolja, hogy az érdekelt felek e csoportja legyen a felelős az Európai Bizottsággal közösen a tanúsítási rendszerek közös elkészítéséért. A közszféra és a magánszféra (felhasználók és szállítók) érdekelt felei közötti konszenzusos megállapodás útján ágazati követelményeket is meg kell határozni.

4.4.8. Ezenfelül a csoportnak rendszeresen felül kell vizsgálnia a tanúsítási rendszereket, figyelembe véve az egyes ágazatok követelményeit, és szükség esetén ki kell igazítania a rendszereket.

4.4.9. Az EGSZB támogatja a nemzeti tanúsítási rendszerek fokozatos megszüntetését, miután európai rendszert vezettek be, mint azt a rendelet 49. cikke javasolja. Az egységes piac nem működhet egymástól eltérő és egymással versengő nemzeti szabályokkal. Az EGSZB javasolja e célból, hogy vegyék számba az összes nemzeti rendszert.

4.4.10. Az EGSZB azt javasolja, hogy az Európai Bizottság kezdeményezzen egy olyan intézkedést, amelynek célja a kiberbiztonsági tanúsítás és tanúsítványok érvényesítése az EU-ban, valamint ezek elismerésének támogatása valamennyi nemzetközi kereskedelmi megállapodásban.

4.5. ***ENISA***

4.5.1. Az EGSZB úgy véli, hogy az ENISA Európai Bizottság által javasolt új állandó megbízatása jelentősen hozzá fog járulni az európai rendszerek ellenálló képességének növeléséhez. Előfordulhat azonban, hogy a megreformált ENISA számára előirányzott, kapcsolódó ideiglenes költségvetés és erőforrások nem elegendőek ahhoz, hogy az ügynökség eleget tudjon tenni megbízatásának.

4.5.2. Az EGSZB valamennyi tagállamot arra ösztönöz, hogy hozza létre az ENISA egyértelmű és ahhoz hasonló partnerszervezetét, ezt ugyanis a legtöbben még nem tették meg. Elő kell segíteni a nemzeti szakértők ENISA-hoz történő kirendelésére irányuló strukturált programot, amellyel támogatni lehet a bevált gyakorlatok cseréjét és a bizalom erősítését. Az EGSZB azt is javasolja, hogy az Európai Bizottság gondoskodjon a tagállamokban már működő helyes gyakorlatok és hatékony intézkedések összegyűjtéséről és megosztásáról.

4.5.3. Az EGSZB emellett úgy érzi, hogy az ENISA-nak a kapacitásépítést illetően az e-kormányzatot támogató intézkedések számára kell elsőbbséget biztosítania ([10]). Kulcsfontosságú a személyek, szervezetek, vállalatok és tárgyak uniós/globális digitális azonosítója, és prioritásként kell kezelni az azonosságlopás és az internetes csalás megelőzését és az ezek elleni küzdelmet, valamint a szellemi tulajdon ipari lopásával szembeni fellépést.

4.5.4. Az ENISA-nak emellett rendszeres jelentéseket kell készítenie a tagállamok kiberfelkészültségéről, elsősorban a kiberbiztonsági irányelv II. mellékletében azonosított ágazatokra összpontosítva. Egy évenkénti európai kibergyakorlat keretében értékelni kell a tagállamok felkészültségét és az európai kiberbiztonsági válságreagálási mechanizmus eredményességét, valamint ajánlásokat kell megfogalmazni.

4.5.5. Az EGSZB aggódik amiatt, hogy az operatív együttműködést tekintve túlságosan szűkösek az erőforrások, gondolva például a CSIRT-hálózatra.

4.5.6. Ami a piaccal kapcsolatos feladatokat illeti, az EGSZB úgy véli, hogy a tagállamokkal való együttműködés megerősítése és a kiberbiztonsági ügynökségek formális hálózatának létrehozása segítene az érdekelt felek közötti együttműködés támogatásában ([11]). A piacra jutási idő nagyon rövid, és kritikus jelentőségű az uniós vállalatok számára, hogy versenyezni tudjanak e területen, és az ENISA-nak képesnek kell lennie arra, hogy ezzel összhangban reagáljon. Az EGSZB úgy véli, hogy az ENISA a jövőben más uniós ügynökségekhez hasonlóan egy díj- és illetékrendszert alkalmazhatna. Az EGSZB aggódik amiatt, hogy az uniós és a nemzeti ügynökségek között a kompetenciákért folytatott verseny – mint más területeken is előfordult már – késleltetheti az uniós szabályozási keret megfelelő létrehozását, és kárt okozhat az uniós egységes piacnak.

4.5.7. Az EGSZB megállapítja, hogy kutatáshoz és innovációhoz, valamint a nemzetközi együttműködéshez kapcsolódó feladatok jelenleg minimálisak.

([10]) Digitális egységes piac/félidős értékelés.
([11]) HL C 75., 2017.3.10., 124. o.

4.5.8. Az EGSZB úgy véli, hogy a bel- és igazságügyi ügynökségek együttes ülésein rendszeres napirendi pontként kell szerepelnie a kiberbiztonságnak, és hogy az ENISA-nak és az Europolnak rendszeresen együtt kell működnie.

4.5.9. Mivel a kibervilág nagyon innovatív, gondosan át kell gondolni a szabványokat, elkerülve az innováció hátráltatását, amihez dinamikus keretrendszerre van szükség; a polgárok és a vállalkozások beruházásainak védelme érdekében a lehető legnagyobb mértékben garantálni kell mind az előre irányuló, mind pedig a visszamenőleges kompatibilitást.

4.5.10. A nemzeti tanúsításfelügyeleti hatóságok jelentőségére tekintettel az EGSZB javasolja, hogy már ez a rendelet hozza létre a határokon átnyúló problémák ENISA támogatásával történő megoldására felhatalmazott hatóságok formális hálózatát. A hálózat egy későbbi szakaszban egységes ügynökséggé alakulhat át.

4.5.11. A bizalom alapvető, de az ENISA nem adhat ki sem határozatokat, sem ellenőrzési jelentéseket. Az EGSZB álláspontja szerint az ügynökségnek vizsgálatok és ellenőrzések révén nyomon kell követnie az Európai Bizottság nevében a nemzeti tanúsításfelügyeleti hatóságok teljesítményét és döntéshozatalát.

4.5.12. Az ENISA igazgatótanácsában való – megfigyelői – részvételt az ágazati és fogyasztói szervezetekre is ki kell terjeszteni.

4.6. ***Ipar, kkv-k, finanszírozás/beruházások és innovatív üzleti modellek***

4.6.1. *Ipar és beruházások*

Az ikt területén működő uniós vállalatok globális versenyképességének növelése érdekében az intézkedéseknek az ikt-ágazat, ezen belül a kkv-k növekedésének és versenyképességének jobb támogatására kell összpontosítaniuk.

Európának a különböző uniós alapok, nemzeti alapok és magánszektorbeli beruházások összehangolásával, a köz- és a magánszféra közötti szoros együttműködésben fokoznia kell a stratégiai célkitűzések elérésére irányuló beruházásokat. A kritikus területeken egy uniós Innovációs és Kutatási-Fejlesztési Kiberbiztonsági Alap létrehozásával kell növelni és támogatni a beruházások szintjét a jelenlegi és jövőbeli kutatási keretprogramban. Ezen túlmenően Európának alapot kellene létrehoznia a kiberbiztonság megvalósítása céljából, új ablakot nyitva a jelenlegi és jövőbeli Európai Hálózatfinanszírozási Eszközön és a következő ESBA 3.0-n belül.

Ösztönzőket kell létrehozni az uniós tagállamok számára, hogy lehetőleg európai megoldásokat vásároljanak, és ha rendelkezésre állnak, európai szállítókat válasszanak, különösen az érzékeny alkalmazások esetében. Európának támogatnia kell a sikeres európai kibervállalatok növekedését, amelyek a világpiacon is képesek felvenni a versenyt.

4.6.2. *KKV-K*

A piac felaprózottsága miatt a piac jobb megszólítása érdekében tisztább képet kell alkotni az ügyfelek igényeit illetően. Strukturált kereslet nélkül a kkv-k és induló vállalkozások nem tudnak gyors ütemben növekedni. Ebben az összefüggésben tanácsos lenne egy európai kiberbiztonsági kkv-központ létrehozása.

A kiberbiztonsági technológia gyorsan változik, és gyorsaságuknak köszönhetően a kkv-k képesek a versenyképesség megőrzéséhez szükséges élenjáró megoldásokat biztosítani. Szemben harmadik országokkal az EU még mindig keresi a kkv-k megfelelő üzleti modelljét.

Kifejezetten az induló vállalkozásokra és kkv-kre irányuló, a tanúsítással járó költségeket támogató programokat lehetne kidolgozni, hogy így ellensúlyozzák azokat a nehézségeket, amelyekkel e vállalkozások szembesülnek, amikor technológiai és kereskedelmi fejlesztéseikhez próbálnak forrásokat szerezni.

4.7. ***Az emberi tényező: tájékoztatás és védelem***

4.7.1. Az EGSZB megjegyzi, hogy az Európai Bizottság javaslata nem veszi kellőképpen figyelembe az embert mint a digitális folyamatok motorját, akár a fő informatikai események kedvezményezettjeként, akár kiváltó okaként.

4.7.2. Erős kiberkészségbázist kell kialakítani, javítani kell a kiberhigiéniát, és növelni kell a tudatosságot az egyének és a vállalkozások körében. Ennek az eredménynek az eléréséhez célzott beruházásokat kell fontolóra venni, mérlegelni kell a magas szintű oktatók képzéséhez szükséges időt és eredményes tudatosságnövelő kampányok elindítását. E három cselekvési irányvonal végrehajtása megköveteli a(z eredményes oktatási programok létrehozásáért és az ezekbe való befektetésért felelős) nemzeti és regionális hatóságok, valamint a vállalkozások és kkv-k kollektív megközelítés keretében való bevonását.

4.7.3. Elő kell irányozni egy uniós tanúsítvánnyal rendelkező lehetséges tanterv létrehozását a középiskolák és a szakemberek számára, az ENISA és nemzeti partnereinek aktív részvételével. Ezenfelül a kiberbiztonság területén a foglalkoztatás szintjének javítását célzó oktatási programok kidolgozásakor a nemek közötti egyenlőséget is figyelembe kell venni.

4.7.4. AZ EGSZB szerint a tanúsítási tevékenységnek magában kell foglalnia egy, a hardverre és szoftverre egyaránt vonatkozó, megfelelő címkézési rendszert, ahogyan az számos más termék esetében is megvalósul (pl. energetikai termékek). Ez az eszköz háromszoros előnyt nyújtana: csökkentené a vállalatok költségeit, megszüntetné a nemzeti szinten már elfogadott tanúsítási rendszerek különbözőségéből fakadó piaci széttagoltságot, és egyszerűbbé tenné a fogyasztók számára a megvásárolt termék minőségének és jellemzőinek értelmezését. Ennek kapcsán fontos, hogy ugyanezek a tanúsítási és címkézési mechanizmusok a harmadik országokból behozott termékekre is vonatkozzanak. Végül az EGSZB úgy véli, hogy célszerű lenne megalkotni egy erre a célra szolgáló logót, amely azonnal tájékoztatást adna a fogyasztóknak és a felhasználóknak a megvásárolt termékek, illetve azon weboldalak megbízhatóságával kapcsolatban, amelyeken adásvételre kerül sor, vagy amelyek érzékeny adatokat továbbítanak.

4.7.5. Az Európai Uniós Hálózat- és Információbiztonsági Ügynökségnek (ENISA) alapvető tájékoztatási és többszintű érzékenyítési tevékenységet kellene folytatnia, hogy tudatosabbá tegye a polgárokat a digitális térben való „biztonságos" viselkedéssel kapcsolatban, és növelje a felhasználók internet iránti bizalmát. Ebből a célból be kell vonni a vállalkozói szövetségeket, a fogyasztói szövetségeket, és más, a digitális szolgáltatások terén tevékenykedő szervezeteket.

4.7.6. Az EGSZB – ahogy azt már az INT/828. sz. véleményében is javasolta – a kiberbiztonsági jogszabály kiegészítése érdekében kulcsfontosságúnak tartja, hogy mielőbb elinduljon a digitális oktatásra és képzésre irányuló nagyszabású európai program, amely minden polgár számára garantálja az ahhoz szükséges eszközöket, hogy minél jobban szembe tudjanak nézni az átállással. Bár az EGSZB tudatában van az e téren meglévő tagállami hatásköröknek, üdvözölné, ha egy ilyen program az iskolákból indulna el, növelné a tanárok ismereteit, hozzáigazítaná a tanulmányi és módszertani programokat a digitális technológiákhoz (beleértve az e-tanulást is), és valamennyi tanuló számára jó minőségű oktatást biztosítana. Egy ilyen program természetszerűleg kiterjedne az egész életen át tartó tanulás lehetőségeinek biztosítására is, amelynek célja valamennyi munkavállaló készségeinek kiigazítása és aktualizálása ([12]).

5. **Részletes megjegyzések**

5.1. ***Újonnan megjelenő technológiák és megoldások: a dolgok internetének esete***

Az internethez csatlakoztatott eszközök száma állandóan nő, és az alkatrészek, rendszerek és megoldások digitalizálása, valamint az internetkapcsolat terjedése miatt várhatóan a Földön élő emberek számának többszörösét is el fogja érni. E trend új lehetőségeket teremt a kiberbűnözők számára, különösen mivel a dolgok internetének eszközei gyakran nem rendelkeznek olyan jó védelemmel, mint a hagyományos eszközök.

A dolgok internetének eszközeit használó különböző iparágakban az európai biztonsági szabványok használata csökkentheti a fejlesztési erőfeszítést, időt és költségvetést az internethez csatlakoztatott termékek értékláncában részt vevő valamennyi ipari szereplő javára.

Az „emberek internetébe" (IoP) tartozó „szokásos" eszközök esetében valószínűleg szükséges bizonyos formájú minimális biztonsági szint az IDAM (Identity & Access Management – azonosság és hozzáférés kezelése), a javítások és az eszközök kezelése révén. Mivel a tanúsítás a magasabb szintű biztonság biztosításának kulcsfontosságú módszere, az új uniós tanúsítási megközelítésben nagyobb hangsúlyt kell kapnia a dolgok internete biztonságának.

Kelt Brüsszelben, 2018. február 14-én.

az Európai Gazdasági és Szociális Bizottság
elnöke
Georges DASSIS

([12]) Digitális egységes piac / félidős értékelés.