EURÓPAI SZÁMVEVŐSZÉK

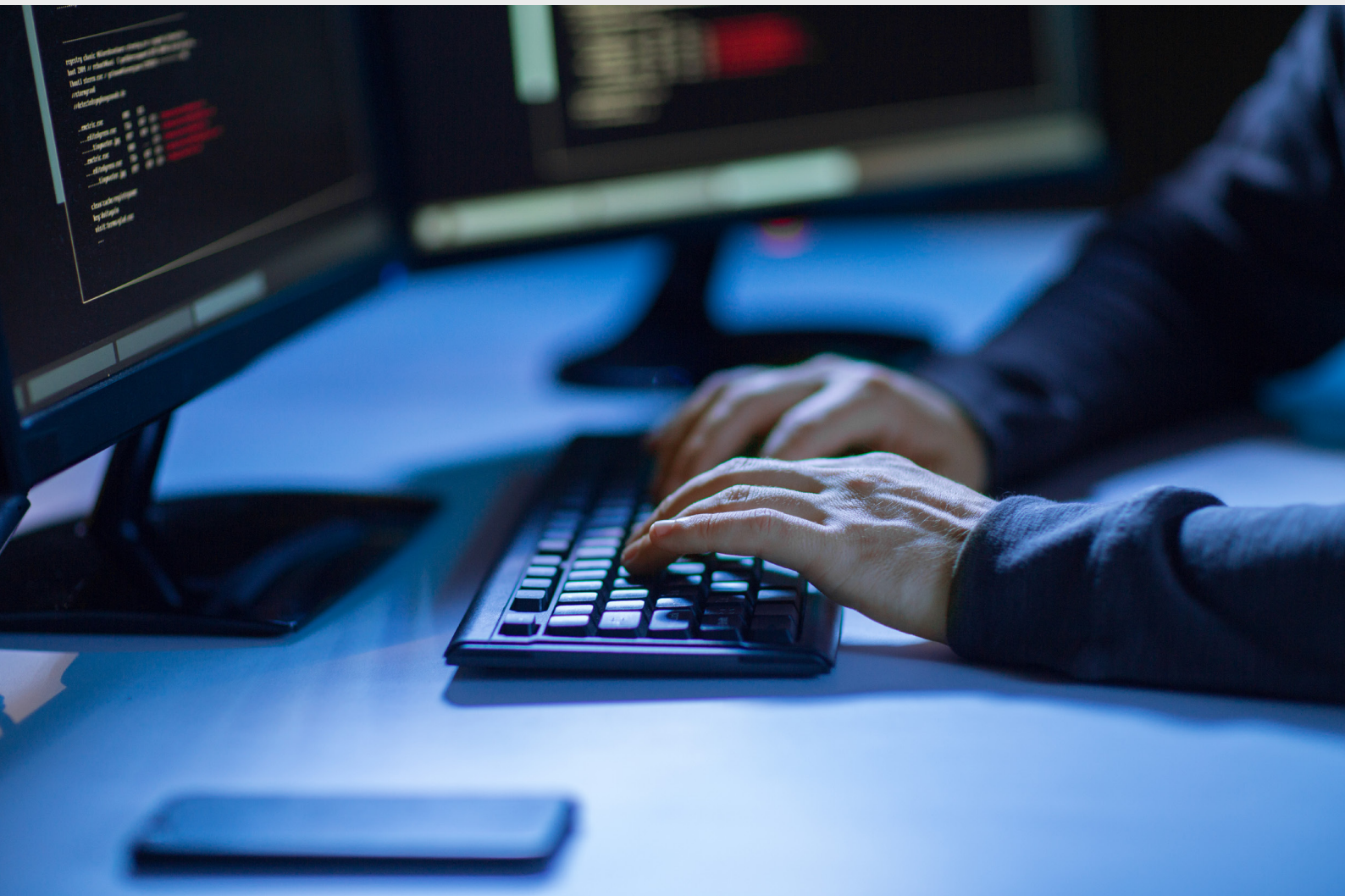
HU

2019

Az eredményes uniós kiberbiztonsági politika előtt álló kihívások

Tájékoztató

2019. március



A tájékoztatóról:

Ez a tájékoztató, amely nem ellenőrzési jelentés, áttekintést kíván nyújtani az Unió komplex kiberbiztonsági politikai hátteréről, és kísérletet tesz rá, hogy feltárja az eredményes szakpolitikai megvalósítás előtt álló fő kihívásokat. Tárgyalja többek között a hálózat- és információbiztonság, a kiberbűnözés, a kibervédelem és a félretájékoztatás témáját. Megállapításait a területre irányuló későbbi ellenőrzési munka során is fel fogjuk használni.

Elemzésünk a hivatalos dokumentumokban, állásfoglalásokban és harmadik felek által készített tanulmányokban nyilvánosan elérhető információk dokumentumalapú ellenőrzésén alapul. A helyszíni munkát 2018. április és szeptember között végeztük el, de egészen a 2018 decemberéig bekövetkezett fejleményeket figyelembe vettük. Munkánk kiegészítéseképpen felmérést végeztünk a tagállamok nemzeti számvevőszékei körében, valamint interjúkat készítettünk az uniós intézmények fő érdekeltjeivel és a magánszektor képviselőivel.

Az azonosított kihívásokat a következő négy nagy csoportba soroltuk: i. szakpolitikai keret; ii. finanszírozás és kiadások; iii. a kiberreziliencia kiépítése; iv. a kiberbiztonsági incidensekre való eredményes reagálás. A kiberbiztonság szintjének növelése megkerülhetetlen feladatot jelent az Európai Unió számára. Ezért minden fejezet végén felvetünk egy sor átgondolandó kérdést a szakpolitikusok, a jogalkotók és a gyakorlati szakemberek számára.

Végül köszönetet szeretnénk mondani a bizottsági szolgálatoktól, az Európai Külügyi Szolgálattól, az Európai Unió Tanácsától, az ENISA-tól, az Europoltól, az Európai Kiberbiztonsági Szervezettől és a tagállamok nemzeti számvevőszékeitől kapott konstruktív visszajelzésekért.

Tartalomjegyzék

Bekezdés

Összefoglaló I-XIII

Bevezetés 01-24

Mi a kiberbiztonság? 02-06

Mennyire súlyos a probléma? 07-10

Mit tesz az Unió a kiberbiztonságért? 11-24

Szakpolitika 13-18

Jogszabályok 19-24

A szakpolitikai és jogszabályi keret kialakítása 25-39

Első kihívás: Érdemi értékelés és elszámoltathatóság 26-32

Második kihívás: Az uniós jog hézagainak és egyenetlen átültetésének problémája 33-39

Finanszírozás és kiadások 40-64

Harmadik kihívás: A beruházási szintek összehangolása a célokkal 41-46

A beruházások mértékének növelése 41-44

A hatás növelése 45-46

Negyedik kihívás: Az uniós költségvetési kiadások világos áttekintése 47-60

Azonosítható kiberbiztonsági kiadások 50-56

Egyéb kiberbiztonsági kiadások 57-58

Előretekintés 59-60

Ötödik kihívás: Megfelelő erőforrások biztosítása az uniós ügynökségek számára 61-64

A kibertámadásoknak ellenálló társadalom kiépítése 65-100

Hatodik kihívás: Az irányítás és az előírások megerősítése 66-81

Információbiztonsági irányítás 66-75

Fenyegetés- és kockázatértékelés 76-78

Ösztönzők 79-81

Hetedik kihívás: Készségfejlesztés és figyelemfelhívás 82-90

Képzés, készségfejlesztés és kapacitásnövelés 84-87

Figyelemfelhívás 88-90

Nyolcadik kihívás: Az információcsere és a koordináció javítása 91-100

Az uniós intézmények egymás közötti és a tagállamokkal folytatott koordinációja 92-96

Együttműködés és információcsere a magánszférával 97-100

Sikeres reagálás kiberbiztonsági események esetén 101-117

Kilencedik kihívás: Eredményes észlelés és reagálás 102-111

Észlelés és értesítés 102-105

Összehangolt reagálás 106-111

Tizedik kihívás: A kritikus infrastruktúrák és a társadalmi funkciók védelme 112-117

Az infrastruktúrák védelme 112-115

Az önállóság növelése 116-117

Záró gondolatok 118-121

I. melléklet — Összetett, többrétegű kép számos szereplővel

II. melléklet — Az Unió kiberbiztonsággal kapcsolatos kiadásai 2014 óta

III. melléklet — Az uniós tagállamok számvevőszékeinek jelentései

Betűszók és rövidítések

Glosszárium

A számvevőszéki munkacsoport

Összefoglaló

I A technológia rengeteg új lehetőséget nyit meg, és az új termékek és szolgáltatások mindennapi életünk szerves részévé válnak. Ugyanakkor egyre nő az esély arra, hogy kiberbűnözés vagy kibertámadás áldozatává váljunk, amelyek egyre nagyobb hatást gyakorolnak társadalmunkra és gazdaságunkra. Ezért igencsak időszerű volt, amikor 2017-ben az Európai Unió elkezdte felgyorsítani a kiberbiztonság és a digitális autonómia megerősítésére irányuló erőfeszítéseit.

II Ez a nyilvánosan elérhető információkon alapuló tájékoztató – amely nem ellenőrzési jelentés – áttekintést kíván nyújtani erről az összetett és egyenetlen szakpolitikai háttérről, és kísérletet tesz rá, hogy feltárja az eredményes szakpolitikai megvalósítás előtt álló fő kihívásokat. A dokumentum hatóköre az Unió kiberbiztonsági politikájára, a kiberbűnözésre és a kibervédelemre, valamint a félretájékoztatás elleni küzdelemre terjed ki. Az azonosított kihívásokat a következő négy nagy csoportba soroltuk: i. szakpolitikai és jogszabályi keret; ii. finanszírozás és kiadások; iii. a kiberreziliencia kiépítése; iv. a kiberbiztonsági incidensekre való eredményes reagálás. Minden fejezet tartalmaz néhány átgondolandó kérdést is a bemutatott kihívásokkal kapcsolatban.

Szakpolitikai és jogszabályi keret

III Mérhető célkitűzések hiányában és kevés megbízható adat birtokában nehézséget jelent olyan fellépéseket kidolgozni, amelyek révén az Unió – kiberbiztonsági stratégiája átfogó céljainak megfelelően – a világ legbiztonságosabb digitális környezetévé válhat. Ritkán mérik fel a végeredményeket, és mindeddig kevés szakpolitikai területről készült értékelés. A legfontosabb kihívás ezért **az érdemi elszámoltathatóság és értékelés biztosítása**, amire az értékelési gyakorlatokon alapuló teljesítménykultúra felé való elmozdulás révén nyílhat lehetőség.

IV A jogi keret továbbra is hiányos. **Az uniós jog hiányosságai és következetlen átültetése** megnehezíthetik a jogszabályok hatásának maximális érvényesítését.

Finanszírozás és kiadások

V **A beruházási szintek és a célok összehangolása** kihívást jelent, ugyanis ahhoz nem csupán a kiberbiztonságba történő beruházások átfogó szintjének emelésére van szükség, amely az Unióban eleddig alacsony és fragmentált volt, de a hatást is növelni kell, különösen a kutatási kiadások jobb hasznosítása, valamint az induló vállalkozások megfelelő célorientáltságának és finanszírozásának biztosítása révén.

VI **Az uniós kiadásokra való világos rálátás** nélkülözhetetlen ahhoz, hogy az Unió és tagállamai tisztában legyenek azzal, milyen hiányosságokat kell felszámolniuk kitűzött céljaik eléréséhez. Mivel a kiberbiztonsági stratégia finanszírozására nem áll rendelkezésre célzott uniós költségvetés, nincs egyértelmű kép arról, hogy mire mekkora összeget költenek.

VII A fokozottan biztonságorientált politikai prioritások idején megakadályozhatja az Unió ambícióinak valóra váltását, ha **a kibervédelemhez kapcsolódó tevékenységet folytató uniós ügynökségek nem rendelkeznek a szükséges erőforrásokkal**. Ez a probléma pedig csak úgy kezelhető, ha módot találnak a tehetségek bevonzására és megtartására.

A kiberreziliencia kiépítése

VIII Mind az Unióban, mind nemzetközi szinten számos hiányosság tapasztalható a kiberbiztonsági irányítás terén a köz- és a magánszférában egyaránt. Ez akadályozza a nemzetközi közösséget abban, hogy megfelelően reagáljon a számítógépes támadásokra és megfékezze azokat, valamint ellehetetleníti a koherens, uniós szintű megközelítést. Ezért szintén kihívást jelent a **kiberbiztonsági irányítás megerősítése**.

IX **A készségek fejlesztése és a tudatosság növelése** minden ágazatban és a társadalom minden szintjén elengedhetetlen, tekintettel arra, hogy egyre nagyobb hiány mutatkozik a globális kiberbiztonsági készségek terén. Jelenleg a képzésre, a tanúsításra vagy a kiberbiztonsági kockázatértékelésre vonatkozóan csak csekély mértékben léteznek uniós szintű szabványok.

X A kibertámadásokkal szembeni átfogó reziliencia megerősítéséhez nélkülözhetetlen a bizalom. Maga a Bizottság is arra a megállapításra jutott, hogy a koordináció általában még mindig nem elégséges. Továbbra is nehézséget jelent a köz- és a magánszféra közötti **információcsere és koordináció javítása**.

A kiberbiztonsági incidensekre való eredményes reagálás

XI A digitális rendszerek olyan összetetté váltak, hogy lehetetlen minden támadást kivédeni. Ezért a **gyors észlelés és reagálás** jelenti a legjobb megoldást. A kiberbiztonságot azonban még nem integrálták maradéktalanul a meglévő uniós szintű válságkezelési koordinációs mechanizmusokba, ami korlátozza az Uniót abban, hogy megfelelően reagáljon a nagyszabású, határokon átnyúló kiberbiztonsági eseményekre.

XII Kulcsfontosságú **a kritikus infrastruktúrák és a társadalmi funkciók védelme**. A választási folyamatokba való beavatkozás lehetősége és a félretájékoztatási kampányok kritikus kihívást jelentenek.

XIII Az Unióval szembeni kiberfenyegetések és a tágabb értelemben vett globális környezet által jelentett kihívások folyamatos elkötelezettséget igényelnek és elengedhetetlenné teszik az Unió alapvető értékeihez való feltétlen ragaszkodást.

Bevezetés

01 A technológiai fejlődés rengeteg új lehetőséget nyit meg előttünk. Egyre több új termék és szolgáltatás épül be szervesen mindennapi életünkbe. Eközben azonban egyre inkább függővé válunk a technológiától, és ezzel párhuzamosan nő a kiberbiztonság jelentősége is. Minél több személyes adatot töltünk fel az internetre, minél több szálon kapcsolódunk a virtuális világhoz, annál nagyobb valószínűséggel válhatunk valamiféle kiberbűncselekmény vagy kibertámadás áldozatává.

Mi a kiberbiztonság?

02 A kiberbiztonságnak nincsen standard, egyetemesen elfogadott definíciója[1]. Gyakorlatilag mindazokat az adatok bizalmas kezelésének, sértetlenségének és rendelkezésre állásának biztosítására irányuló biztosítékokat és intézkedéseket értjük alatta, amelyek az információs rendszereknek és azok felhasználóinak az adatokhoz való jogosulatlan hozzáféréssel, támadásokkal és károkozással szembeni védelmére szolgálnak.

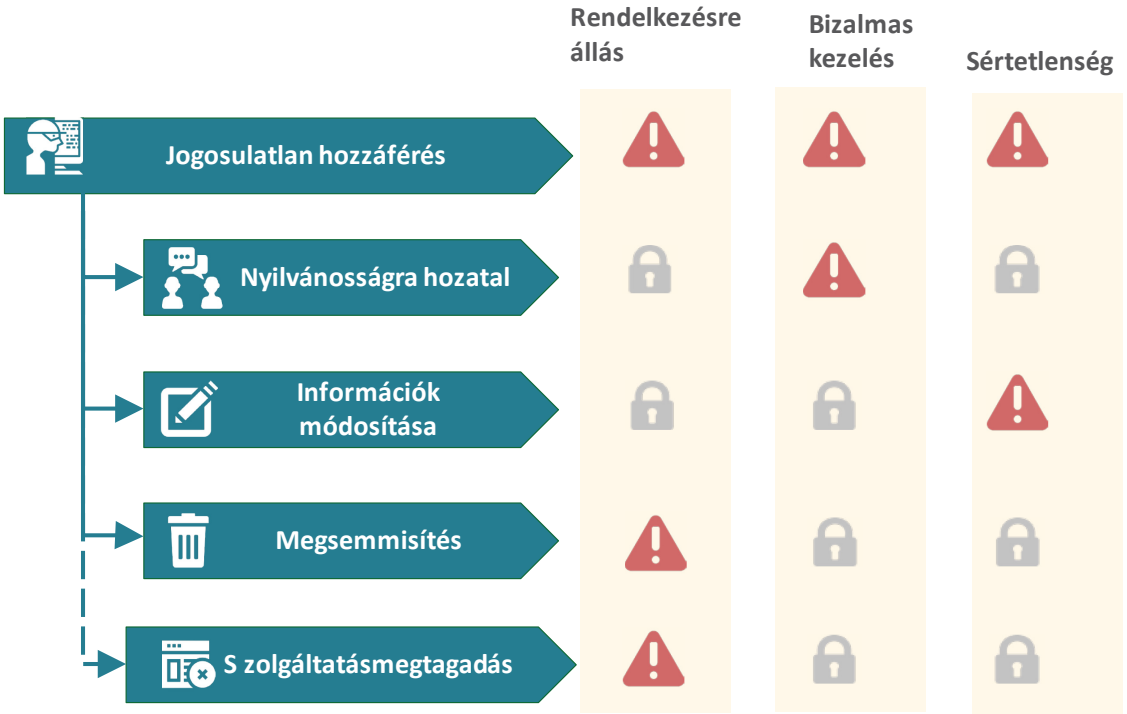
03 A kiberbiztonság csakúgy magában foglalja a kiberbiztonsági események megelőzését és felderítését, mint az azokra való reagálást és a következményeik elhárítását. Ezek az események szándékosan vagy véletlenül is bekövetkezhetnek: az információk véletlen nyilvánosságra hozatala ugyanúgy a fogalom körébe tartozik, mint a vállalkozások és kritikus infrastruktúrák elleni támadások, a személyes adatok eltulajdonítása, vagy akár a demokratikus folyamatokba való beavatkozás. Ezek mindegyike számos káros következménnyel járhat az egyénekre, a szervezetekre és a közösségekre nézve.

04 Az uniós szakpolitikai szóhasználatban a kiberbiztonság fogalma nem korlátozódik a hálózat- és információbiztonságra, hanem a kibertérben digitális technológiák alkalmazásával elkövetett valamennyi jogellenes tevékenységre kiterjed. Így a kiberbűnözés fogalomköre olyan tetteket is magában foglalhat, mint a számítógépes vírusokat terjesztő támadások vagy a készpénz-helyettesítő fizetési eszközökkel való visszaélések, és átfoghatja a rendszerek és tartalom közötti szakadékot, például a gyermekpornográf anyagok online terjesztése esetében. Emellett a kiberbiztonság hatókörébe tartozhatnak az online viták és adott esetben a választások befolyásolását célzó félretájékoztatási kampányok. Az Europol ráadásul párhuzamokat vél felfedezni a kiberbűnözés és a terrorizmus között is[2].

05 Különböző érdekeltek – köztük államok, bűnözői csoportok és hacktivisták – különféle szándékokkal bujtanak fel kiberbiztonsági események elkövetésére, amelyek hatása nemcsak tagállami, hanem uniós és globális szinten is érzékelhető. Mivel azonban az internet jellegénél fogva megfoghatatlan és nem ismer határokat, bizonyos eszközök és taktikák alkalmazása igencsak megnehezíti a támadások elkövetőinek azonosítását (ez az úgynevezett attribúciós probléma).

06 A sokféle kiberbiztonsági fenyegetést jellemzően aszerint csoportosítják, hogy mi történik az adatokkal (nyilvánosságra hozatal, módosítás, megsemmisítés vagy jogosulatlan hozzáférés), illetve hogy milyen információbiztonsági alapelvet sértenek meg (lásd: ***1. ábra***). A támadástípusokra az ***1. háttérmagyarázat*** hoz fel néhány példát. Ahogy egyre kifinomultabbá válnak az információs rendszerek elleni támadások, úgy csökken a védekezési mechanizmusaink eredményessége[3].

1. ábra. Fenyegetéstípusok és az általuk veszélyeztetett biztonsági elvek



Forrás: Európai Számvevőszék, egy európai parlamenti tanulmány[4] nyomán. Lakat = nincs hatás a biztonságra; felkiáltójel = biztonsági kockázat.

1. háttérmagyarázat

A kibertámadások típusai

Valahányszor egy-egy új eszköz csatlakozik fel az internetre vagy kapcsolódik össze más eszközökkel, nő az úgynevezett kiberbiztonsági „támadási felület”. A dolgok internetének, a számítási felhőnek, a nagy adathalmazoknak és az ipar digitalizációjának exponenciális növekedése együtt jár a sebezhetőség növekedésével, lehetővé téve a rosszindulatú szereplők számára, hogy egyre több áldozatot célozzanak meg. A támadástípusok sokfélesége és egyre kifinomultabb megtervezésük miatt csak herkulesi erőfeszítések árán lehet velük tartani a lépést[5].

A **rosszindulatú szoftverek** („malicious software”, röviden „malware”) az eszközök vagy hálózatok károsítására szolgálnak. Ilyen szoftverek többek között a vírusok, a trójai programok (trojan), a zsarolóprogramok (ransomware), a férgek (worm), a reklámprogramok (adware) és a kémprogramok (spyware). A **zsarolóprogramok** titkosítják az adatokat, így a felhasználók csak akkor juthatnak hozzá fájljaikhoz, ha váltságdíjat fizetnek (rendszerint kriptopénzben) vagy ha megteszik, amit a zsaroló kér tőlük. Az Europol szerint az elmúlt néhány évben robbanásszerűen megsokszorozódtak a zsarolóprogramok típusai, és jelenleg ezek jelentik a leggyakoribb problémát. Az **elosztott szolgáltatásmegtagadással járó támadás** (Distributed Denial of Service, DDoS, másik magyar nevén elosztott túlterheléses támadás) elérhetetlenné tesz bizonyos szolgáltatásokat vagy erőforrásokat azáltal, hogy kezelhetetlen mennyiségű kéréssel árasztja el őket. E támadástípus gyakorisága szintén egyre nő, 2017-ben a szervezetek egyharmada szembesült ilyen típusú támadással[6].

A felhasználók bizonyos manipulációk útján csalárd módon rávehetők egy cselekvés végrehajtására vagy bizalmas információk nyilvánosságra hozatalára. Ez a **„pszichológiai manipuláció”** néven ismert trükk adatlopásra vagy kiberkémkedésre adhat alkalmat. Több módszer is létezik erre, a leggyakoribbak egyike az **adathalászat**, ahol látszólag megbízható forrásból érkező e-mailek révén veszik rá a felhasználókat adataik felfedésére vagy arra, hogy olyan hiperhivatkozásokra (linkekre) kattintsanak rá, amelyek rosszindulatú szoftvereket töltenek le és azokkal megfertőzik a készülékeket. A tagállamok több mint fele számolt be hálózati támadásokra irányuló vizsgálatokról[7].

A fenyegetéstípusok közül talán a legkártékonyabb a **fejlett tartós fenyegetés** (advanced persistent threat, APT). Az ezek hátterében álló kifinomult támadók hosszú távon figyelik és lopják az adatokat, emellett néha destruktív célt is szolgálnak. Ezek a fenyegetések szintén arra törekszenek, hogy a lehető leghosszabb ideig észrevétlenek maradjanak. Az APT-k gyakran kötődnek különböző államokhoz, és előszeretettel célozzák meg a különösen érzékeny ágazatokat, például a technológiát, a védelmet és a kritikus infrastruktúrát. A kiberkémkedés az adatok szerint az összes kiberbiztonsági esemény legalább egynegyedét és a költségek döntő részét teszi ki[8].

Mennyire súlyos a probléma?

07 A megbízható adatok hiánya miatt nehéz megállapítani, hogy mekkora hatással jár a kibertámadásokra való felkészültség elégtelensége. A kiberbűnözés gazdasági hatása 2013 és 2017 között ötszörösére emelkedett[9], és a kormányzatokat csakúgy sújtotta, mint a kis- és nagyvállalatokat. Ezt a tendenciát tükrözi, hogy a kiberbiztosítási díjak a 2018. évi 3 milliárd euróról 2020-ra várhatóan 8,9 milliárd euróra emelkednek.

08 Miközben a kibertámadások pénzügyi hatása egyre nő, riasztó aránytalanság mutatkozik egyfelől a támadás megindításának költsége, másfelől a megelőzés, a kivizsgálás és a jóvátétel költsége között. Egy DDoS támadás például akár havi 15 euróból is kivitelezhető, ugyanakkor a megcélzott vállalkozás veszteségei – beleértve a hírnevet érintő károkat is – jóval magasabbak ennél[10].

09 Bár 2016-ban az uniós vállalkozások 80%-a tapasztalt legalább egy kiberbiztonsági incidenst[11], a kockázatok felismerése még mindig riasztóan elégtelen. Az uniós vállalkozások 69%-a egyáltalán nem tud vagy csak alapvető ismeretekkel rendelkezik a kiberfenyegetésekkel szembeni kitettségéről[12], és 60%-uk soha nem becsülte fel a lehetséges pénzügyi veszteségeket[13]. Ezenfelül egy globális felmérés szerint a szervezetek egyharmada inkább megfizetné a hackerek által kért váltságdíjat, mintsem beruházzon az információbiztonságba[14].

10 A *WannaCry* zsarolóvírus és a *NotPetya* törlőprogram (wiper) segítségével 2017-ben elkövetett rosszindulatú globális számítógépes támadások összesen több mint 320 000 áldozatot érintettek mintegy 150 országban[15]. Ezek az incidensek az egész világot ráébresztették a kibertámadások veszélyének fontosságára, és új lendülettel kezdtek törekedni arra, hogy a kiberbiztonság helyet kapjon az általános szakpolitikai szempontok között. Ráadásul az uniós polgárok 86%-a véli úgy, hogy egyre nagyobb a veszélye annak, hogy kiberbűnözés áldozatává váljanak[16].

Mit tesz az Unió a kiberbiztonságért?

11 Az Unió 2001-ben megfigyelői szervezeti státuszt kapott az Európa Tanács számítástechnikai bűnözésről szóló egyezményének (Budapesti Egyezmény) bizottságában[17]. Azóta az Unió szakpolitikák, jogszabályok és pénzügyi források biztosítása révén törekszik a kibertámadásokkal szembeni rezilienciájának javítására. Amint a ***2. ábra*** mutatja, a növekvő számú jelentős kibertámadások és események következtében 2013 óta felgyorsult ez a tevékenység. Ezzel párhuzamosan a

tagállamok elfogadták (néhány esetben már aktualizálták is) első nemzeti kiberbiztonsági stratégiájukat.

12 A kiberbiztonsággal kapcsolatos feladatokban részt vevő főbb uniós szervekről a ***2. háttérmagyarázat*** és az ***I. melléklet*** nyújt áttekintést.

2. háttérmagyarázat

Kik vesznek részt a védekezésben?

Az **Európai Bizottság** törekszik arra, hogy növelje a kiberbiztonsági kapacitásokat és együttműködést, megerősítse az Unió szerepét a kiberbiztonság biztosításában, és a többi uniós szakpolitikába is beépítse a kiberbiztonság szempontját. A kiberbiztonsági politikáért a főigazgatóságok közül elsősorban a digitális egységes piacért felelős **DG CNECT** (kiberbiztonság), valamint a biztonsági unióért felelős **DG HOME** (kiberbűnözés) viseli a felelősséget. A **DG DIGIT** a Bizottság saját rendszereinek informatikai biztonságáért felelős.

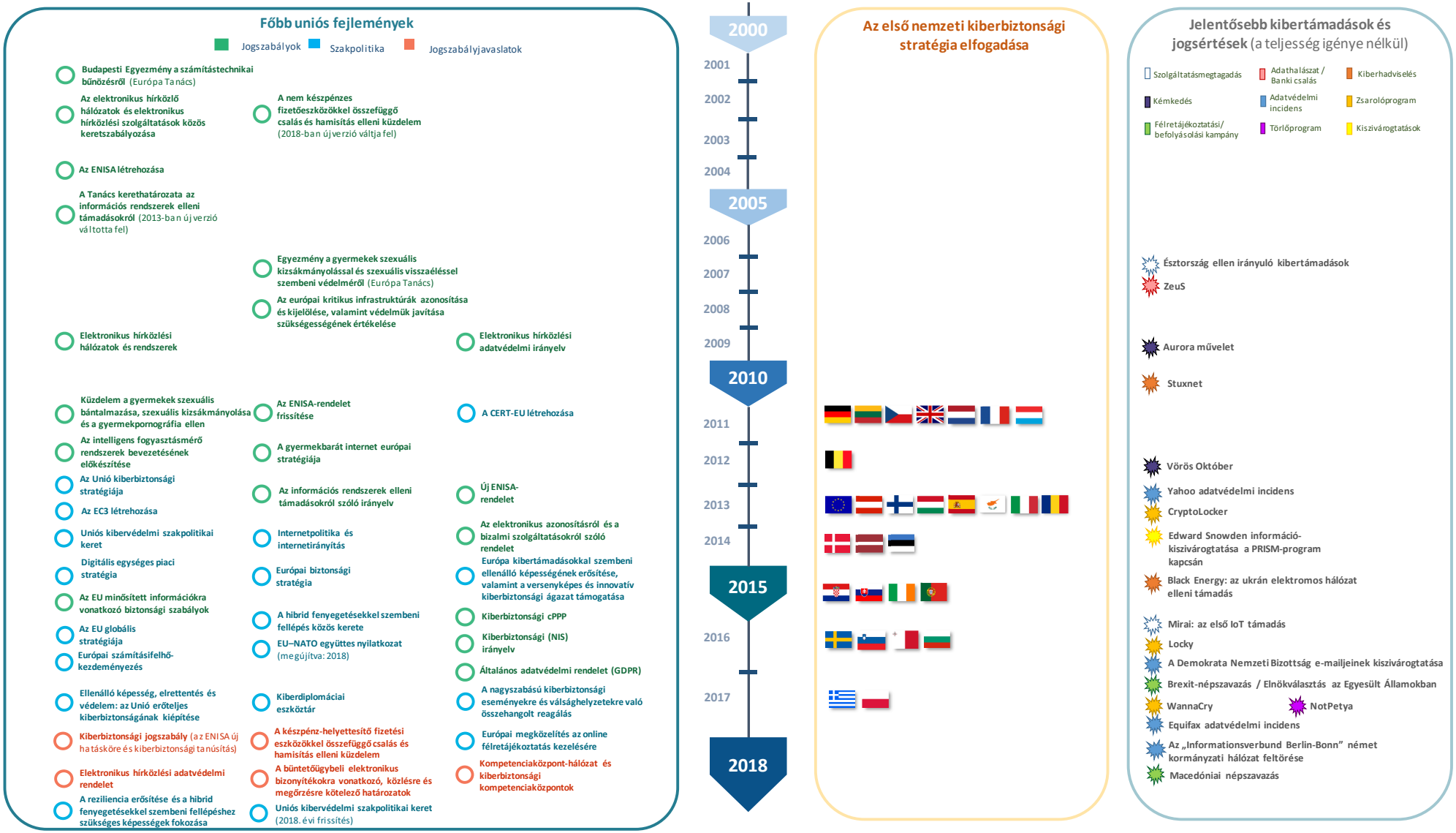
A Bizottság munkáját emellett számos uniós ügynökség is támogatja, köztük az **ENISA** (Európai Uniós Hálózat- és Információbiztonsági Ügynökség), az Unió kiberbiztonsági ügynöksége: ez a főként tanácsadó funkciót ellátó szerv a szakpolitikák kidolgozását, a kapacitásépítést és a figyelemfelkeltést támogatja. Az Europolon belül működő Számítástechnikai Bűnözés Elleni Európai Központot (**EC3**) azzal a céllal hozták létre, hogy eredményesebbé tegye a kiberbűncselekmények nyomán hozott uniós bűnüldözési válaszintézkedéseket. A Bizottság biztosít működési keretet az uniós intézmények, szervek és ügynökségek számítógépes vészhelyzeteket elhárító csoportjának (**CERT-EU**).

Az **Európai Külügyi Szolgálat** (EKSZ) irányítja a kibervédelmet, a kiberdiplomáciát és a stratégiai kommunikációt, továbbá hírszerzési és elemzőközpontoknak ad otthont. Az **Európai Védelmi Ügynökség** (EDA) célja a kibervédelmi kapacitások fejlesztése.

Saját kiberbiztonságukért a **tagállamok** viselik az elsődleges felelősséget, ezenfelül uniós szinten a **Tanács** révén fejthetnek ki tevékenységet, amely számos koordinációs és információmegosztási szervezettel (köztük a kiberpolitikai kérdésekkel foglalkozó horizontális munkacsoporttal) rendelkezik. Az **Európai Parlament** társjogalkotóként jár el.

A **magánszektorbeli szervezetek**, köztük az ipar, az internetirányítási szervek és a tudományos körök partnerként és közreműködőként – többek között egy szerződéses köz-magán társulás (**cPPP**) révén – vesznek részt a szakpolitikák kidolgozásában és végrehajtásában.

2. ábra. A szakpolitikák és jogszabályok kidolgozásának felgyorsulása (2018. december 31-i állapot)



Forrás: Európai Számvevőszék.

Szakpolitika

13 Az Unió összetett és többrétegű kiberbiztonsági ökoszisztémája számos belpolitikai területen átível, így felöleli többek között a bel- és igazságügy, a digitális egységes piac és a kutatási politika területét is. A külpolitikában a kiberbiztonság szervesen beépül a diplomáciába, és egyre fontosabb részét képezi az Unió kialakulóban lévő védelmi politikájának.

14 Az Unió szakpolitikájának sarokköve a **2013. évi kiberbiztonsági stratégia**[18], amelynek célja, hogy az Unió digitális környezete világszinten a legbiztonságosabbá váljon, megóvva ugyanakkor az alapvető értékeket és szabadságokat. A stratégia öt fő célkitűzése i. a kibertámadásokkal szembeni reziliencia fokozása, ii. a kiberbűnözés visszaszorítása, iii. kibervédelmi politikák és kapacitások kialakítása, iv. az ipari és technológiai kiberbiztonsági erőforrások fejlesztése, valamint v. az alapvető uniós értékekkel összehangolt nemzetközi kibertér-politika kialakítása.

15 A kiberbiztonsági stratégia három később elfogadott stratégiával kapcsolódik össze:

— Az **európai biztonsági stratégia** (2015) célja a kiberbűncselekmények üldözésének és igazságügyi kezelésének javítása elsősorban a meglévő politikák és jogszabályok megújítása és frissítése révén[19]. Célja továbbá a kiberbűnözéssel kapcsolatos nyomozásokat hátráltató akadályok feltárása és a kiberkapacitások kiépítésének felgyorsítása.

— A **digitális egységes piaci stratégia**[20] (2015) célja, hogy jobb hozzáférést biztosítson a digitális árukhoz és szolgáltatásokhoz azáltal, hogy megfelelő feltételeket teremt a digitális gazdaság növekedési potenciáljának maximalizálásához. Ehhez elengedhetetlen az online biztonság, bizalom és befogadás erősítése.

— A 2016. évi **globális stratégia**[21] célja, hogy megerősítse az Unió szerepét a világban. A kiberbiztonság ennek alappillérét képezi a kiberbiztonsági kérdések iránti megújított elkötelezettség, a fő partnerekkel való együttműködés, valamint a kiberbiztonsági kérdések valamennyi szakpolitikai területen átívelő megoldása iránti eltökéltség révén, beleértve a félretájékoztatás stratégiai kommunikáció révén történő megcáfolását is.

16 Az elmúlt években olyannyira fokozódott a kibertér militarizálása[22] és fegyverként való felhasználása[23], hogy egyesek már az ötödik hadszíntérként tekintenek rá[24]. A

kibervédelem óvja a kibertér rendszereit, hálózatait és kritikus infrastruktúráját a katonai és egyéb eszközök támadásai ellen. 2014-ben elfogadták, majd 2018-ban aktualizálták a **kibervédelmi szakpolitikai keretet**[25]. A 2018-as verzió hat prioritást jelöl meg, köztük a kibervédelmi kapacitás fejlesztését, valamint az Unió közös biztonság- és védelempolitikai (KBVP) kommunikációs és információs hálózatainak védelmét. A kibervédelem az állandó strukturált együttműködés (PESCO) és az EU–NATO együttműködésnek is részét képezi.

17 A **hibrid fenyegetésekkel szembeni fellépés közös uniós kerete** (2016) mind a kritikus infrastruktúrákat, mind a magánfelhasználókat fenyegető kiberfenyegetésekkel foglalkozik, kiemelve, hogy kibertámadások a közösségi médiában folytatott félretájékoztatási kampányok révén is végrehajthatók[26]. Megállapítja továbbá, hogy javítani kell a tudatosságot és fokozni kell az EU és a NATO közötti, a 2016. és 2018. évi EU–NATO együttes nyilatkozatban lefektetett együttműködést[27].

18 A Bizottság 2017-ben új kiberbiztonsági csomagot terjesztett elő, amely tükrözi a digitális védelem egyre sürgetőbb szükségességét. A csomag magában foglalt egy új bizottsági közleményt a 2013. évi kiberbiztonsági stratégia naprakésszé tételéről[28], egy esetleges nagyszabású támadásra irányuló gyors és összehangolt reagálási tervet, valamint a hálózati és információs rendszerek biztonságáról szóló irányelv (kiberbiztonsági vagy NIS-irányelv) gyors végrehajtását célzó intézkedések tervezetét[29]. Emellett a csomag több jogalkotási javaslatot is tartalmazott (lásd: ***22.*** bekezdés).

Jogszabályok

19 2002 óta több, a kiberbiztonság szempontjából különböző mértékben releváns jogszabály elfogadására került sor.

20 A 2013. évi kiberbiztonsági stratégia fő pilléreként a jogszabályi rendszer alapkövét az első uniós szintű kiberbiztonsági jogszabály, a 2016. évi **hálózat- és információbiztonsági (NIS) irányelv**[30] jelenti. Az irányelv célja (amelyet egyébként 2018 májusáig kellett átültetni) a kapacitások bizonyos szintű összehangolása azáltal, hogy nemzeti hálózat- és információbiztonsági stratégiák elfogadására, valamint integrált kapcsolattartó pontok és számítógép-biztonsági eseményekre reagáló csoportok (CSIRT)[31] létrehozására kötelezi a tagállamokat. Az irányelv ezenfelül biztonsági és bejelentési követelményeket állapít meg a kritikus ágazatokban alapvető szolgáltatásokat nyújtó szereplők és a digitális szolgáltatók számára.

21 Ezzel párhuzamosan 2016-ban hatályba lépett az **általános adatvédelmi rendelet**[32] (GDPR), amelynek alkalmazása 2018 májusában kezdődött meg. E rendelet azáltal kívánja biztosítani az európai polgárok személyes adatainak védelmét, hogy előírja az azok feldolgozására és terjesztésére irányadó szabályokat. Bizonyos jogokat biztosít az érintettek számára, valamint kötelezettségeket ró az adatkezelőkre (digitális szolgáltatók) az információk felhasználása és átadása tekintetében. A rendelet jogsértés esetére értesítési kötelezettséget, illetve egyes esetekben bírságokat is előír. A ***3. ábra*** bemutatja, hogyan egészíti ki egymást a kiberbiztonsági irányelv és az általános adatvédelmi rendelet a kiberbiztonság megerősítése és az adatvédelem biztosítása terén.

22 A jelenleg megvitatás alatt álló jogszabálytervezetek között van a kiberbiztonsági jogszabályra irányuló javaslat, amelynek célja az ENISA megerősítése és egy uniós szintű akkreditációs mechanizmus létrehozása[33], az elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező határozatokról szóló rendeletjavaslat[34], valamint az elektronikus bizonyítékokról szóló irányelvjavaslat[35]. Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozására (a továbbiakban: kiberbiztonsági és kutatási kompetenciaközpontok hálózata) irányuló 2018-as javaslat szintén a 2017. évi kiberbiztonsági csomag részét képezi[36].

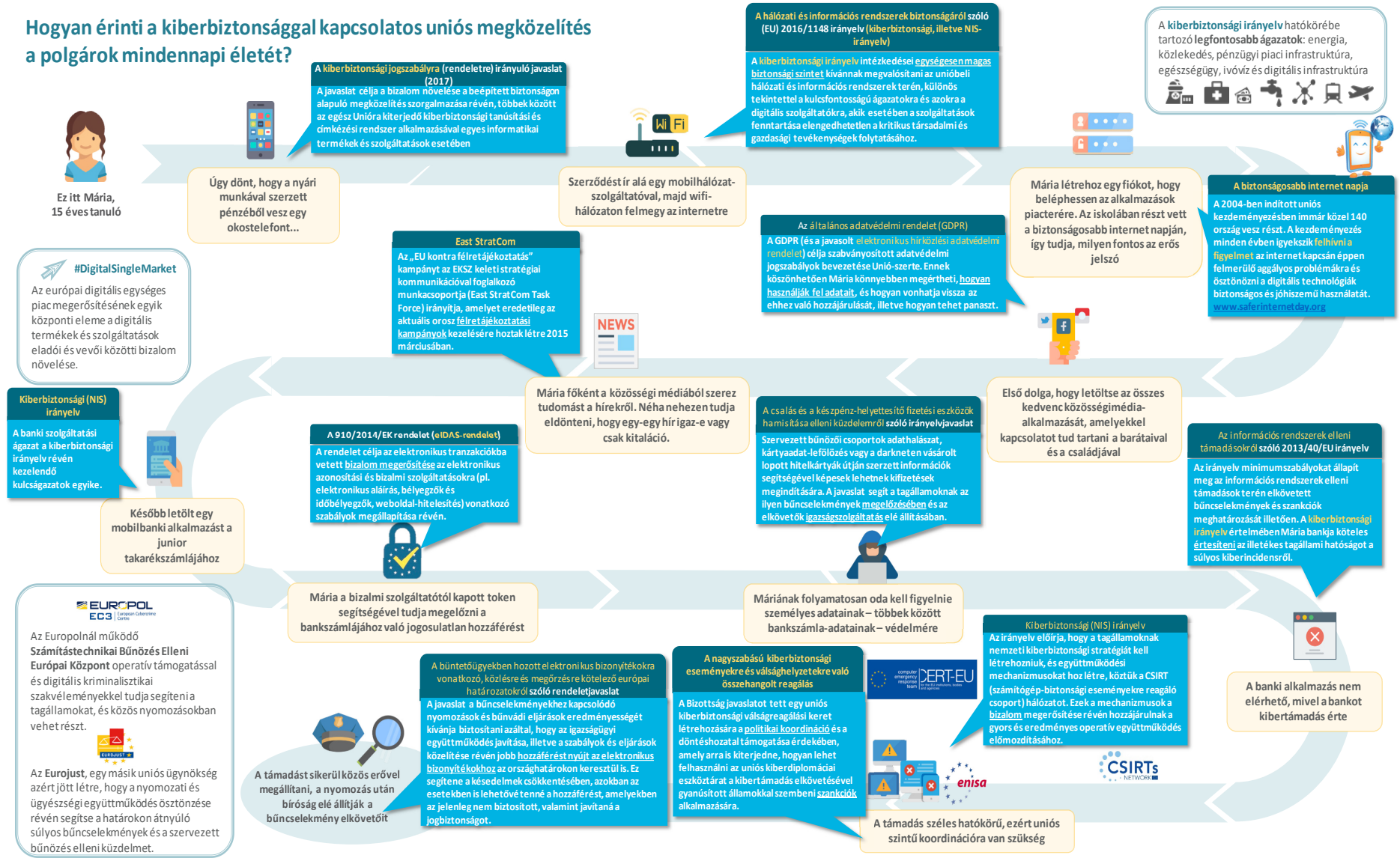
23 Nehéz lehet átlátni a kiberbiztonságra vonatkozó szakpolitikai és jogalkotási keret nagyságrendjét és azt, hogy az hogyan befolyásolja mindennapi életünket.

24 A ***4. ábra*** annak szemléltetésére tesz kísérletet, milyen módokon érintik a különböző jogalkotási aktusok és más tevékenységek egy képzeletbeli európai polgár életét.

3. ábra. Hogyan egészíti ki egymást az általános adatvédelmi rendelet és a kiberbiztonsági irányelv?

Forrás: Európai Számvevőszék.

4. ábra. Hogyan érinti a kiberbiztonsággal kapcsolatos uniós megközelítés a polgárok mindennapi életét?



Forrás: Európai Számvevőszék.

A szakpolitikai és jogszabályi keret kialakítása

25 Az Unió összetett és többrétegű kiberbiztonsági ökoszisztémájában számos érdekelt fél vesz részt (lásd: ***I. melléklet***) . Komoly kihívást jelent a rendszer különböző elemeinek integrálása. 2013 óta határozott erőfeszítések történtek az Unió kiberbiztonsági területének összehangolására[37].

Első kihívás: Érdemi értékelés és elszámoltathatóság

26 A Bizottság megjegyezte, hogy nehezen állapítható meg ok-okozati összefüggés a 2013. évi stratégia és a tapasztalt esetleges változások között. A 2013. évi stratégia célkitűzéseit igen általános jelleggel fogalmazták meg, így azok „inkább jövőképet, mintsem mérhető célt fogalmaznak meg”[38]. Márpedig mérhető célkitűzések hiányában nehézségekbe ütközik az ilyen általános ívű célokhoz illeszkedő intézkedések kidolgozása. Az aktualizált kibervédelmi szakpolitikai keret (2018) törekedni fog a kiberbiztonság és az elérendő bizalom minimális szintjét meghatározó célkitűzések kidolgozására. Ez ugyanakkor a kibervédelemre korlátozódik: az Unió egésze tekintetében a reziliencia kívánt mértékére nézve nem határoztak meg célkitűzéseket.

27 Ritkán mérik fel a végeredményeket, és mindeddig kevés szakpolitikai területről készült értékelés[39]. Ez részben annak tudható be, hogy számos – jogalkotási és egyéb – intézkedés végrehajtására csak a közelmúltban került sor, így nem lehet teljes körűen értékelni azok hatását. A kihívást olyan érdemi értékelési kritériumok meghatározása jelenti, amelyek segíthetnek a hatás mérésében. Ráadásul a szigorú értékelés még nem vált általános gyakorlattá a kiberbiztonság tekintetében. Ezért el kellene mozdulni egy értékelési gyakorlatokon és szabványosított beszámoláson alapuló teljesítménykultúra felé. Az ENISA jelenlegi megbízatása nem terjed ki az uniós kiberbiztonság és készültség értékelésére és nyomon követésére.

28 A tényalapú szakpolitikai döntéshozatalhoz nélkülözhetetlen, hogy elegendő megbízható adat és statisztika álljon rendelkezésre a tendenciák és a szükségletek nyomon követéséhez és elemzéséhez. Kötelező és közös monitoringrendszer hiányában nehéz elegendő megbízható adatot szerezni. A mutatók gyakran nem állnak közvetlenül rendelkezésre és meghatározásuk is problémás lehet[40]. Néhány területen – például az uniós szakpolitikai ciklus kapcsán – ugyanakkor specifikus mérőszámokat dolgoztak ki a súlyos bűncselekmények és a szervezett bűnözés elleni küzdelem céljára.

29 Kevés tagállam gyűjt rendszeresen hivatalos adatokat a kiberbiztonsági kérdésekről, ami akadályozza az összehasonlíthatóságot. Az Unió eddig nemigen tett említést arról, hogy szükség lenne a statisztikák európai szintű konszolidálására[41]. Ezenkívül kevés olyan független elemzés áll rendelkezésre, amely az Unió egészére nézve vizsgálná a főbb témákat[42], azaz a kiberbiztonság ökonómiáját, beleértve a magatartási szempontokat (az ösztönzők összehangolatlansága, információs aszimmetriák), a kiberkudarcok és a kiberbűnözés hatásának megértését, a kibertrendekre és a várható kihívásokra vonatkozó makrostatisztikákat, valamint a fenyegetések legjobb kezelési módjait.

30 Konkrét célkitűzések, illetve kellő mennyiségű megbízható adat és jól meghatározott mutató hiányában a stratégia eredményeiről eleddig javarészt csak kvalitatív értékelés készült. Az előrehaladási jelentések gyakran az eredmények alapos felmérése nélkül írják le az elvégzett tevékenységeket és az elért mérföldköveket. Ezenkívül még nem határozták meg a rendszerek rezilienciájának értékelésére szolgáló referenciaértékeket. Emellett a kiberbűnözés kodifikált meghatározásának hiányában szinte lehetetlen olyan releváns uniós szintű mutatókat találni, amelyek segítenék a nyomon követést és az értékelést.

31 Tagállamonként eltérő a kiberbiztonsági politika végrehajtásának független felügyelete. E terület ellenőrzését illetően felmérést végeztünk a tagállami számvevőszékek körében. A válaszadók fele[43] soha nem végzett ellenőrzést ezen a területen. Akik igen, azok az ellenőrzés során elsősorban a következőkre összpontosítottak: információkezelés; a kritikus infrastruktúra védelme; a legfőbb érdekelt felek közötti információcsere és koordináció; a váratlan eseményekre való felkészülés, értesítés és reagálás. A válaszadók kevesebb figyelmet fordítottak a tudatosság növelésére és a digitális készségek hiányára. Ezen ellenőrzések és értékelések eredményeit nemzetbiztonsági okokból nem mindig hozzák nyilvánosságra. A ***III. melléklet*** tartalmazza a tagállami számvevőszékek által közzétett ellenőrzési jelentések jegyzékét.

32 A válaszadók megítélése szerint a kibervédelemhez kapcsolódó készségek korlátozott volta (lásd még: ***82–90.*** bekezdés) és a kiberbiztonság terén elért előrehaladás értékelésének nehézsége jelentette a legnagyobb problémát az e téren végrehajtott kormányzati intézkedések ellenőrzése kapcsán.

Második kihívás: Az uniós jog hézagainak és egyenetlen átültetésének problémája

33 Az új technológiák és fenyegetések sebessége jócskán felülmúlja az uniós jogszabályok kidolgozásának és végrehajtásának ütemét. Az Unió eljárásait nem a digitális korszak szem előtt tartásával alakították ki, ezért döntő fontosságú prioritást jelent, hogy innovatív és rugalmas eljárások kidolgozása révén olyan szakpolitikai és jogi keretet kell létrehozni, amely alkalmas[44] a jövő jobb előrejelzésére és alakítására[45].

34 Bár történtek erőfeszítések a koherencia fokozására, a kiberbiztonság jogi kerete továbbra sem teljes (példákért lásd: ***1. táblázat***). A széttöredezettség és a hiányosságok hátráltatják az átfogó politikai célkitűzések elérését és csökkentik a hatékonyságot. Stratégiai értékelése során a Bizottság többek között a dolgok internete, a digitális termékek felhasználói és szolgáltatói közötti felelősségmegosztás egyensúlya, valamint bizonyos, a kiberbiztonsági irányelv által nem kezelt szempontok kapcsán tárt fel hiányosságokat. A javasolt kiberbiztonsági jogszabály ezt részben az úgynevezett beépített biztonság előmozdítása révén kívánja orvosolni, amelyet egy uniós szintű tanúsítási rendszer tenne lehetővé. Néhány érdekelt fél úgy véli, hogy még mindig feltűnő a világosan meghatározott ágazati kiberpolitika és a kiberkémkedésre irányuló közös stratégia hiánya[46].

1. táblázat. A jogszabályi keret hézagai és egyenetlen átültetése (nem teljes körű áttekintés)

Szakpolitikai terület	Példák
Digitális egységes piac	o A fogyasztási cikkek adásvételéről szóló jelenlegi irányelv nem terjed ki a kiberbiztonságra. A digitális tartalmakról[47], illetve az áruk internetes értékesítéséről[48] szóló irányelvjavaslatok célja e hiányosság orvoslása. o Az uniós tagállamokban korlátozott és eltérő jogi keretek vannak érvényben a gondossági kötelezettségekre nézve, ami jogbizonytalansághoz vezet, és megnehezíti a jogorvoslati lehetőségek érvényesítését[49]. o A tagállamok nem egyforma gyorsasággal dolgozzák ki a szoftverek feltárt sebezhetőségeivel kapcsolatos tájékoztatásra irányuló intézkedéseiket, és uniós szinten nincs olyan átfogó jogi keret, amely biztosíthatná a koordinált megközelítést[50].
A hálózat- és információbiztonság megerősítése	o A tagállamok a kiberbiztonsági irányelvből kimaradt ágazatokat is szabadon bevonhatják a vonatkozó szakpolitikáik hatálya alá[51]. Ilyen például a lakáságazat, amely nem tartozik a hatálya alá, de más bűncselekmények, köztük az ember- és kábítószercsempészet és az illegális bevándorlás kapujaként szolgálhat[52].
A kiberbűnözés elleni küzdelem	o Számos tagállam jogszabályai még nem tartalmaznak az e-bizonyítékokra vonatkozó rendelkezéseket[53] (lásd még: ***22. bekezdés***). o A készpénz-helyettesítő fizetési eszközökkel összefüggő csalásokról szóló jelenlegi kerethatározat nem említi kifejezetten a nem fizikai fizetési eszközöket, mint például a virtuális fizetőeszközöket, az elektronikus pénzt és a mobilpénzt, és nem terjed ki az adathalászatra, a kártyaadat-lefölözésre, valamint a fizetői adatok birtoklására és megosztására[54]. o Az információs rendszerek elleni támadásokról szóló irányelv nem foglalkozik közvetlenül a belülről történő illegális adatszerzéssel (pl. kiberkémkedés), ami kihívást jelent a bűnüldözés számára[55]. o Az Európai Unió Bíróságának az adatmegőrzésről szóló ítélete[56] nyomán a jogi keret tagállamok általi eltérő alkalmazása akadályozta a bűnüldözést, ami adott esetben egyes nyomozati szálak elvesztéséhez vezethet és akadályozhatja az online bűnözői tevékenység eredményes üldözését[57].

Forrás: Európai Számvevőszék.

35 A jogszabályok egyes elemeinek alkalmazása továbbra is önkéntes mind a nemzeti hatóságok, mind a magánszolgáltatók számára. Az együttműködési csoport keretében például önkéntes alapon értékelik a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiákat és a CSIRT csoportok eredményességét. A kiberbiztonsági jogszabály által javasolt tanúsítási rendszer szerint az informatikai termékekre és szolgáltatásokra vonatkozó tanúsítás alkalmazása is önkéntes alapon történne.

36 Az Unióban a kiberbiztonság a tagállamok hatáskörébe tartozik, ugyanakkor az Uniónak jelentős szerepe van a tagállamok kapacitásfejlesztési feltételeinek megteremtésében, valamint a tagállamok közötti együttműködés és bizalom megteremtésében. Ennek ellenére a tagállamok között akkora eltérések mutatkoznak a kapacitás és a szerepvállalás tekintetében[58], hogy az érzékeny (nemzetbiztonsági) információk szolgáltatása továbbra is önkéntes marad.

37 Az uniós jog következetlen tagállami átültetése ellentmondásos jogi és operatív környezetet eredményezhet, és megakadályozhatja, hogy a jogszabályok kifejtsék teljes potenciáljukat. A tagállamok például eltérő módon értelmezik a kettős felhasználású termékek kivitelére vonatkozó ellenőrzéseket[59], emiatt pedig egyes uniós székhelyű vállalatok olyan technológiákat és szolgáltatásokat exportálhatnak, amelyek alkalmasak lehetnek a kibertér felügyeletére és – cenzúra vagy lehallgatás révén – az emberi jogok megsértésére. Az Európai Parlament aggodalmát fejezte ki ezzel kapcsolatban[60].

38 Ezenfelül a magánélet védelme és a véleménynyilvánítás szabadságának garantálása testre szabott jogalkotási választ igényel, hogy meg lehessen találni a szükséges egyensúlyt az alapvető értékek védelme és az Unió biztonsági szempontjai között. Hogyan biztosíthatjuk például a végpontok közötti titkosítást a bűnüldözés ellehetetlenítése nélkül? Milyen hatással van az általános adatvédelmi rendelet a domain-nevek és IP-címtartományok jogosultjaival kapcsolatban nyilvánosan hozzáférhető információkra és hogyan valósíthatók meg a rendelet céljai? És milyen kedvezőtlen hatásokat gyakorolhat mindez a bűncselekményekkel kapcsolatos nyomozásra[61]?

39 A jogszabályok önmagukban nem garantálnak megfelelő rezilienciát. Bár a kiberbiztonsági irányelv célja az, hogy Unió-szerte magas szintű biztonságot teremtsen, kifejezetten minimális, nem pedig maximális szintű harmonizáció megvalósítására összpontosít[62]. Ahogy egyre alakul a kibertér, úgy kerülnek a felszínre újabb és újabb szabályozási rések.

A szakpolitikai keret kapcsán átgondolandó kérdések

- Milyen kritikus lépéseket kell tenni annak érdekében, hogy a szakpolitikai döntéshozók és a jogalkotók egyaránt az erőteljesebb teljesítménykultúra felé mozduljanak el a kiberbiztonság kapcsán, beleértve az általános reziliencia meghatározását is?

- Hogyan járulhat hozzá jobban a kutatás az érdemi értékeléshez szükséges adatok és statisztikák előállításához?

- Hogyan lehetne az Unió jogalkotási folyamatait oly módon kiigazítani, hogy azok rugalmasabbak legyenek, és jobban figyelembe vegyék a technológiai fejlődésben és az azzal járó fenyegetésekben bekövetkező fejlemények sebességét?

- Hogyan lehetne az uniós szakpolitikai ciklusban használt mérőszámok (mutatók, célértékek) kidolgozási folyamatát kiigazítani és intenzívebbé tenni, illetve a mérőszámokat úgy átalakítani, hogy azok a kiberbiztonság más területein is alkalmazhatók legyenek?

- Mit tanulhatnak a nemzeti számvevőszékek egymástól a kiberbiztonsági politikák és intézkedések ellenőrzésével kapcsolatos megközelítéseket illetően?

- Melyek azok a következetlenségek az uniós jogi keret átültetése és végrehajtása terén, amelyek akadályozzák a kiberbiztonsági résekre és a kiberbűnözésre való eredményesebb reagálást, és ezt a tagállamok és az uniós intézmények hogyan tudnák a leghatékonyabban kezelni?

- Mennyire eredményesen előzi meg a kiberáruk és -szolgáltatások exportjának uniós ellenőrzése az emberi jogok megsértését az Unión kívül?

Finanszírozás és kiadások

40 Az Unió törekvése az, hogy a világ legbiztonságosabb online környezetévé váljon. Ennek eléréséhez jelentős munkára van szükség minden érintett részéről; többek között nélkülözhetetlen a stabil, biztos kézzel irányított pénzügyi háttér biztosítása.

Harmadik kihívás: A beruházási szintek összehangolása a célokkal

A beruházások mértékének növelése

41 A becslések szerint az összes globális kiberbiztonsági kiadás a GDP körülbelül 0,1% százalékát teszi ki. Az Egyesült Államokban[63] ez a szám eléri a 0,35%-ot (a magánszektort is beleértve). A GDP százalékában az Egyesült Államok szövetségi kormányzati kiadásai 0,1% körül alakulnak, ami 2019-ben mintegy 21 milliárd dolláros költségvetési előirányzatnak felel meg[64].

42 Az Unióban ehhez képest alacsony volt a kiadások szintje, ezenfelül a kiadások szétaprózottak voltak és gyakran nem támaszkodtak összehangolt, a kormányzat által irányított programokra. Nehéz számadatokat szerezni, de a kiberbiztonsággal kapcsolatos uniós közkiadások becslések szerint évente 1–2 milliárd eurót tesznek ki[65]. Néhány tagállam vonatkozó kiadásai a GDP százalékában kifejezve az USA szintjének egytizedét sem érik el[66]. Az Uniónak és tagállamainak tudniuk kell, hogy mennyit ruháznak be együttesen ebbe a területbe, hogy megállapíthassák, milyen réseket kell még áthidalniuk.

43 Nehéz átfogó képet kialakítani, mivel a kiberbiztonság horizontális jellege miatt nem állnak rendelkezésre egyértelmű adatok, és a kiberbiztonsági kiadásokat gyakran nem lehet megkülönböztetni az általános informatikai kiadásoktól[67]. Felmérésünk megerősítette, hogy mind a köz-, mind a magánszektor kiadásairól nehéz megbízható statisztikákat gyűjteni. A nemzeti számvevőszékek háromnegyede arról számolt be, hogy nem rendelkezik központi rálátással a kormányzati kiberbiztonsági kiadásokra, és egyetlen tagállam sem kötelezte a közintézményeket arra, hogy pénzügyi tervükben külön szerepeltessék a kiberbiztonsági kiadásokat.

44 Különösen nagy kihívást jelent az európai kiberbiztonsági vállalkozásokra irányuló állami és magánberuházások növelése. A kezdeti szakaszban még gyakran áll rendelkezésre állami tőke, a növekedési és terjeszkedési szakaszban azonban már

kevésbé[68]. Számos uniós finanszírozási kezdeményezés létezik, de azokat nagyrészt a bürokrácia miatt nem használják ki[69]. Az uniós kiberbiztonsági cégek nemzetközi társaikhoz képest összességében alulteljesítenek: nemcsak számuk kevesebb, hanem átlagosan jóval kevesebb finanszírozást is tudnak mobilizálni[70]. Az Unió digitális politikai célkitűzéseinek eléréséhez ezért kulcsfontosságú az induló vállalkozások megfelelő célorientáltságának és finanszírozásának biztosítása.

A hatás növelése

45 A kiberberuházási szakadék megszüntetésének hasznos eredményekhez kell vezetnie. Például az Unió kutatási és innovációs ágazatának ereje ellenére az eredményeket nem szabadalmazzák, hozzák kereskedelmi forgalomba és sokszorosítják kellő mértékben ahhoz, hogy segíthessenek a reziliencia, a versenyképesség és a digitális autonómia megerősítésében[71]. Ez különösen igaz az Unió globális versenytársaival való összehasonlításban. A megfelelően hasznosított eredmények elégtelen aránya számos tényezőre vezethető vissza[72], többek között az alábbiakra:

- nem áll rendelkezésre olyan következetes transznacionális stratégia, amely lehetővé tenné, hogy a megközelítést olyan nagyságrendben is megvalósíthassák, amely kielégítené a versenyképesség és az autonómia növelése iránti szélesebb körű uniós digitális igényeket;
- az értéklánc hossza miatt az eszközök hamar elavulttá válnak;
- nem biztosított a fenntarthatóság, mivel a projektek (beleértve a frissítéseket és a patch-kibocsátást) általában a projektcsoport feloszlatásával és a támogatás megszüntetésével véget érnek.

46 A Bizottság kiberbiztonsági kompetenciaközpontok és kutatási kompetenciaközpontok hálózatának létrehozására irányuló javaslata kísérletet tesz a kiberbiztonsági kutatási terület széttagoltságának megszüntetésére és a nagyléptékű beruházások ösztönzésére[73]. Unió-szerte összesen mintegy 665 szakértői központ működik.

Negyedik kihívás: Az uniós költségvetési kiadások világos áttekintése

47 A kiadások központi áttekintése fontos az átláthatóság és a jobb koordináció szempontjából. Enélkül a szakpolitikusok nehezen látják át, hogy a kiadások hogyan igazodnak a kiemelt célok elérésével kapcsolatos szükségletekhez.

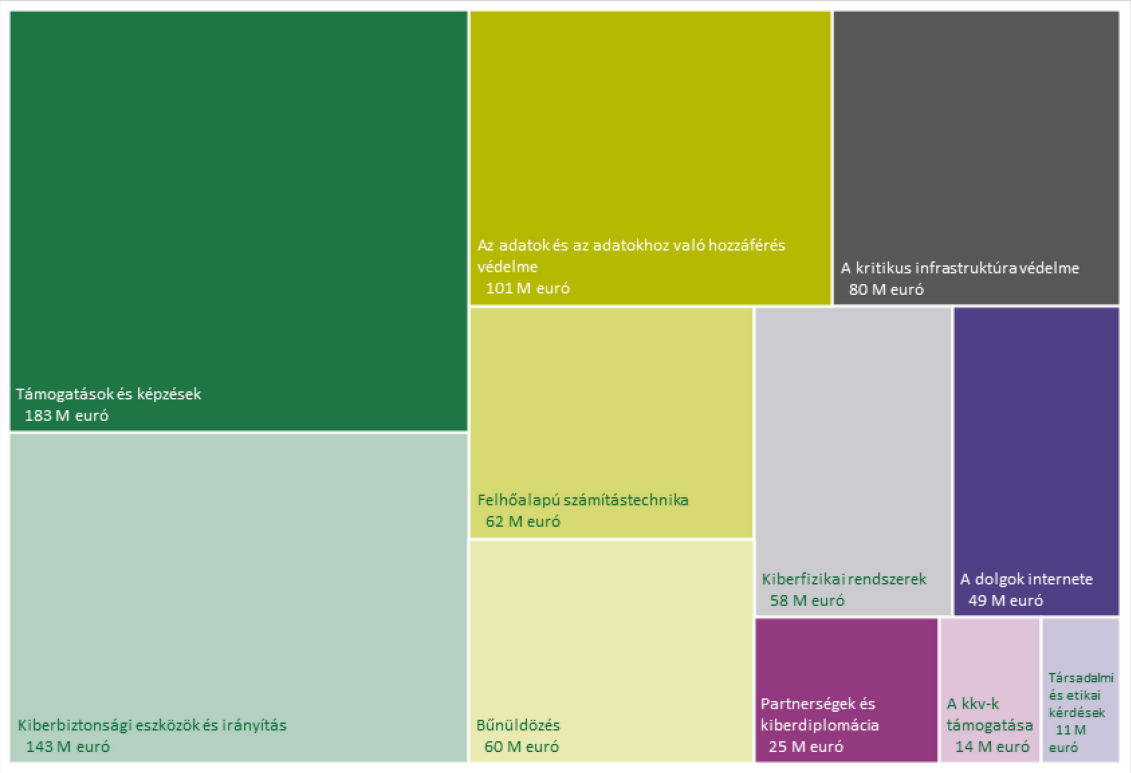
48 A kiberbiztonsági stratégia finanszírozására nem áll rendelkezésre elkülönített költségvetés. Uniós szinten a kiberbiztonsággal kapcsolatos kiadások az Unió általános költségvetéséből és tagállami társfinanszírozásból származnak. Elemzésünk szerint az uniós általános költségvetésben egy legalább tíz különböző eszközből álló komplex rendszer finanszírozza ezt a területet, ugyanakkor nem világos, hogy mire mekkora összeget költenek (lásd: ***II. melléklet***).

49 Ezért komoly kihívást jelent a kiadások számos szakpolitikai területet átfogó, egyértelmű áttekintésének kialakítása. A kiadási programokat a Bizottság különböző részlegei kezelik, amelyek mindegyike saját célokkal, szabályokkal és ütemtervekkel rendelkezik. Tovább bonyolítja a helyzetet az esetleges tagállami társfinanszírozás, akárcsak a Belső Biztonsági Alap rendőrségi együttműködést támogató eszköze esetében[74].

Azonosítható kiberbiztonsági kiadások

50 A 2014–2018-as időszakban a Bizottság legalább 1,4 milliárd eurót költött a stratégia végrehajtására[75], és ennek legnagyobb részét a Horizont 2020 program[76] számára irányozta elő. A Horizont 2020 finanszírozása elsősorban a „Biztonságos társadalmak” kihívás és a „Vezető szerep az alap- és az ipari technológiák területén” célkitűzés projektjei keretében jut célba[77]. A 2018 szeptemberéig tartó időszakra nézve 279 olyan kiberbiztonsággal kapcsolatos projektet azonosítottunk, összesen 786 millió euró uniós finanszírozással, amely eljutott a szerződéskötési szakaszig[78]. Az ***5. ábra*** e projektek tipológiáját mutatja be elemzésünk alapján.

5. ábra. Szerződésbe állított Horizont 2020 kiberbiztonsági kutatási projektek (millió euró)



Forrás: Európai Számvevőszék.

51 Az európai kiberbiztonsági ágazat ösztönzése érdekében 2016-ban létrejött egy szerződéses köz-magán partnerség (cPPP). Ezzel a cél az volt, hogy a Horizont 2020 programból 450 millió eurót a cPPP-be átcsoportosítva 2020-ig további 1,8 milliárd eurót vonzzanak be a magánszektorból. A 2017. december 31-ig tartó 18 hónapos időszakban 67,5 millió euró került át a Horizont 2020-ból a cPPP-be, a magánszektor pedig 1 milliárd eurónyi beruházást teljesített[79].

52 A kiberbűnözés elleni küzdelmet a Belső Biztonsági Alap rendőrségi együttműködést támogató eszköze (ISF-P) is segíti. Az ISF-P tanulmányokat, szakértői találkozókat és kommunikációs tevékenységeket támogat; ezek összege 2014 és 2017 között közel 62 millió eurót tett ki. A tagállamok továbbá támogatást kaphatnak a megosztott irányítás keretében vásárolt felszerelésekhez, illetve végrehajtott képzéshez, kutatáshoz és adatgyűjtéshez. Ilyen támogatást tizenkilenc tagállam vett igénybe 42 millió euró értékben.

53 Igazságügyi együttműködésre és a kölcsönös jogsegélyről szóló szerződések működésére – különös tekintettel az elektronikus adatok és a pénzügyi információk

cseréjére – 9 millió eurót fordítottak a Jogérvényesülési Főigazgatóság által kezelt Jogérvényesülés program keretében.

54 A kiberbiztonsági irányelv kifejezetten előírja, hogy a CSIRT-ek számára megfelelő erőforrásokat kell biztosítani feladataik eredményes ellátásához[80]. 2016 és 2018 között évi 13 millió euró állt rendelkezésre az Európai Hálózatfinanszírozási Eszközből, amelyből a tagállamok támogatást kérhettek az irányelv követelményeinek végrehajtásához. Nem készült olyan tanulmány, amely meghatározná az ahhoz szükséges források tényleges összegét, hogy a CSIRT-hálózat és az együttműködési csoport tevékenysége érezhető hatást gyakorolhasson.

55 Az ügynökségek több működési költsége kifejezetten kiberbiztonsági vagy a számítástechnikai bűnözéssel kapcsolatos tevékenységekre irányult. Ugyanakkor a nyilvánosan rendelkezésre álló információk alapján nehéz pontosan meghatározni a kapcsolódó számadatokat.

56 A Budapesti Egyezmény (lásd: ***11.*** bekezdés) alkotja az Unió külső kiberbiztonsági kiadásainak gerincét. Az Unió a 2014–2018-as időszakban mintegy 50 millió eurót költött a kiberbiztonságnak a saját külső határain túli megerősítésére. Ennek közel fele a stabilitás és a béke elősegítését szolgáló eszköz révén valósult meg; a fő projekt – a 13,5 millió eurós GLACY+ projekt – célja a kiberbűnözésre vonatkozó jogszabályok kidolgozására és végrehajtására, valamint a nemzetközi együttműködés fokozására irányuló kapacitások megerősítése volt világszerte[81]. Egyebekben a más uniós pénzügyi eszközök kiadásainak fókuszában nagyrészt a Nyugat-Balkán[82], valamint az európai szomszédság állt: a keleti partnerség országaival folytatott Cybercrime@EaP projekt célja például a kiberbűnözéssel és az e-bizonyítékokkal kapcsolatos nemzetközi együttműködés javítása.

Egyéb kiberbiztonsági kiadások

57 Az uniós programokon belül nem mindig lehetséges a kifejezetten kiberbiztonsági jellegű kiadások azonosítása:

- a Horizont 2020-ból a Kiváló Európai Elektronikai Alkatrészek és Rendszerek (ECSEL) Közös Vállalkozás révén is irányítottak át támogatást kiberfizikai rendszerek számára. Nem tudtuk azonban meghatározni, hogy a 2015 és 2016 között összesen 437 millió euró értékben végrehajtott 27 projekt tartalmából mi kapcsolódott konkrétan a kiberbiztonsághoz.

- Az európai strukturális és beruházási alapok keretében legfeljebb 400 millió euró áll rendelkezésre a kiberbiztonsággal és a bizalmi szolgáltatásokkal kapcsolatos kiadások fedezésére. Ez a digitális infrastruktúra, az elektronikus azonosítás, valamint a magánélet védelmét szolgáló és bizalmi szolgáltatások átjárhatóságának és összekapcsolódásának fokozását célzó biztonsági és adatvédelmi beruházásokat foglal magában.

58 2018. évi műveleti tervében az Európai Beruházási Bank bejelentette azon szándékát, hogy egy hároméves időszak alatt akár 6 milliárd euróra növeli a kettős felhasználású technológiák, a kiberbiztonság és a polgári biztonság finanszírozását[83].

Előretekintés

59 A javasolt új Digitális Európa program[84] (DEP) 2021–2027-es időszakra vonatkozó 2 milliárd eurós kiberbiztonsági összetevőjének célja az uniós kiberbiztonsági ágazat és a társadalomnak nyújtott átfogó védelem megerősítése, többek között a kiberbiztonsági irányelv végrehajtásának támogatása révén. A DEP keretében eszközölt uniós kiadások fő végrehajtási mechanizmusát várhatóan a kiberbiztonsági kompetenciaközpontok javasolt hálózata és egy kutatási kompetenciaközpont alkotja majd, ami a tervek szerint egyszerűbb megközelítést eredményez.

60 Az uniós költségvetés védelmi kiadásai a közelmúltban növekedtek az európai védelmi ipari fejlesztési program révén, amelyre 2019-re és 2020-ra 500 millió eurót irányoznak elő[85]. A program célja, hogy a közös fejlesztés ösztönzése révén javítsa a tagállamok védelmi kiadásainak koordinációját és hatékonyságát. A program a tervek szerint összesen 13 milliárd euró értékű védelmi kapacitási beruházást generál majd 2020 után az Európai Védelmi Alapon keresztül, és ez a beruházás részben a kibervédelemre fog irányulni[86].

Ötödik kihívás: Megfelelő erőforrások biztosítása az uniós ügynökségek számára

61 Az Unió kiberbiztonsági politikájának középpontjában álló három fő szerv – az ENISA, az Europol EC3 és a CERT-EU (lásd: ***2. háttérmagyarázat***) – a fokozottan biztonságorientált politikai prioritások idején erőforrásproblémákkal küzd. Az uniós ügynökségeknek a jelenlegi emberi és pénzügyi erőforrások mellett továbbra is nehézséget okoz az elvárások teljesítése[87].

62 Az ügynökségeknek a növekvő kereslet kielégítéséhez szükséges többletforrásokra irányuló kéréseit nem sikerült teljes mértékben kielégíteni, ami veszélyeztetheti a szakpolitikai célkitűzések (időben történő) teljesítését. Néhány példa:

- 2017-ben az ENISA részben a korlátozott erőforrások miatt nem érte el teljes mértékben a célkitűzéseit[88]. A 2017. évi csomag az erőforrások növelését javasolta az ENISA megbízatásának bővülésére tekintettel.

- Az Europol EC3 IKT-kapacitásánál foglalkoztatott elemzők létszáma és az IKT-kapacitásba történő beruházás tekintetében a kínálat nem tartott lépést a kereslettel[89]. Az Europol EC-nél működő Számítástechnikai Bűnözés Elleni Közös Akció Munkacsoportba (J-CAT) a tagállamok és harmadik országok delegálnak szakértőket a hírszerzésen alapuló nyomozások támogatására. A költségeket azonban nagyrészt a küldő államok viselik, ami nem ösztönzi őket nagyobb számú szakértő kiküldésére. Ezért bevezetésre került az Europol által vagy valamely uniós szakpolitikai ciklus keretében finanszírozott ideiglenes, eseti kiküldetések intézménye, ami több ország számára teszi lehetővé a részvételt.

63 Bizonyos korlátok oka magukban az intézményekben keresendő. A CERT-EU és az ENISA számos munkatársa szerződéses alkalmazott, és esetükben a munkaerő-felvételi eljárások jellemzően lassúak. Más problémák – például a tehetségek vonzásával és megtartásával kapcsolatos nehézségek – hátterében az áll, hogy az ügynökségek nem tudják felvenni a versenyt a magánszférabeli bérekkel, illetve hogy nem kedvezőek a szakmai előmeneteli lehetőségek. Az ENISA emiatt 2014 és 2016 között munkájának nagy részét kiszervezte[90].

64 Az alkalmazotti létszám és a szükséges eszközök elégtelensége jelentős kockázatokkal járhat, különösen a fenyegetésekre vonatkozó hírszerzés tekintetében. A nyílt és zárt forrásokból származó adatok mennyisége továbbra is rohamosan nő, és az elemzőknek lassan nem lesz elég kapacitásuk ahhoz, hogy megfelelő fenyegetéselemzéseket végezzenek. Az ilyen adatok sikeres integrálásához és összekapcsolásához szükséges megfelelő kapacitások és eszközök nélkül nem lesz lehetséges azok alapján az Unió egész területén megosztható és elemezhető, hasznosítható információkat leképezni a fenyegetéseket illetően[91].

Átgondolandó kérdések – Finanszírozás és kiadások

- Hogyan egyszerűsíthetnék a Bizottság és a jogalkotók az uniós kiberbiztonsági kiadásokat, és hogyan rendelhetnék hozzá azokat kifejezettebben bizonyos egyértelműen meghatározott célokhoz?
- Hogyan lehetne átfogó megoldást találni az uniós ügynökségek erőforrásproblémáira, figyelembe véve az Unió szükségleteit és céljait?
- Uniós és tagállami szinten milyen intézkedéseket határoznak meg a tevékenységük bővítéséhez beruházási tőkét igénylő kkv-k előtt álló akadályok csökkentése érdekében?
- Milyen konkrét és tartós eredmények születnek a Horizont 2020 forrásainak felhasználásával a kiberbiztonsági megoldások előállítása terén?
- Hogyan erősíti meg az uniós kapacitásépítés az Unió határain kívüli kapacitásokat az uniós értékekkel összhangban?

A kibertámadásoknak ellenálló társadalom kiépítése

65 A kiberbiztonsági irányítás a fenyegetések és kockázatok kezelésével, a kapacitások és a tudatosság megerősítésével, valamint a bizalmon alapuló koordinációval és információcserével foglalkozik.

Hatodik kihívás: Az irányítás és az előírások megerősítése

Információbiztonsági irányítás

66 Az információbiztonsági irányítás lényege az adatok bizalmas kezelésének, integritásának és rendelkezésre állásának biztosítására szolgáló struktúrák és intézkedések bevezetése. Nem pusztán technikai kérdésről van szó: előfeltétel az eredményes irányítás, a megbízható folyamatok és a szervezeti célkitűzésekkel összehangolt stratégiák[92]. Ennek egy részhalmaza a kiberbiztonsági irányítás, amely a kiberfenyegetések minden típusával foglalkozik, a célzott, kifinomult támadásoktól a jogsértéseken át a nehezen felderíthető vagy kezelhető eseményekig.

67 A kiberbiztonsági irányítási modellek tagállamonként eltérőek, és a kiberbiztonsággal kapcsolatos felelősség gyakran több szervezet között oszlik meg. Ezek a különbségek még nemzeti szinten is akadályozhatják a nagyszabású, határokon átnyúló eseményekre való reagáláshoz és a fenyegetésekkel kapcsolatos értesülések cseréjéhez szükséges együttműködést, és ez még inkább igaz az Unió szintjén. A nemzeti számvevőszékekről készített felmérésünk feltárta, hogy a legnagyobb kockázatként a hatóságok irányítási rendszerének és a kockázatkezelésének hiányosságait észlelték.

68 A kiberbiztonsági irányítás terén annak ellenére számos hiányosság tapasztalható, hogy azok súlyos következményekkel járhatnak a magánszektorbeli szervezetekre nézve. Tíz szervezet közül csaknem kilenc úgy nyilatkozott, hogy kiberbiztonsági funkciója nem elégíti ki teljes mértékben a szükségleteit[93], és a kiberbiztonsági tisztviselők gyakran legalább két szinttel el az igazgatótanács alatt helyezkednek el a hierarchiában[94].

69 Az uniós társasági jogi irányelvek nem írnak elő konkrét követelményeket a kiberkockázatok nyilvánosságra hozatalára vonatkozóan. Az Egyesült Államokban az

Értékpapír- és Tőzsdebizottság (Securities and Exchange Commission) nemrégiben nem kötelező erejű iránymutatást bocsátott ki, hogy segítséget nyújtson az állami vállalatoknak a kiberbiztonsági kockázatokra és eseményekre vonatkozó közzétételek előkészítésében[95]. Az európai felügyeleti hatóságok vegyes bizottsága[96] figyelmeztetett a kiberkockázatok növekvő veszélyeire, javasolta a pénzügyi intézményeknek, hogy erősítsék meg sérülékeny informatikai rendszereiket, és tárják fel az információbiztonsággal, az összekapcsoltsággal és a kiszervezéssel szervesen együtt járó kockázatokat[97].

70 A kkv-k információbiztonsági irányításának megerősítése azért is különösen nehéz, mert az esetek többségében nem képesek a megfelelő rendszerek megvalósítására. A kkv-k nem rendelkeznek megfelelő iránymutatásokkal az információbiztonsági és adatvédelmi követelmények alkalmazását és a technológiai kockázatok csökkentését illetően[98]. Ezért kulcsfontosságú kihívást jelent, hogy a politikai döntéshozók jobban megértsék a kkv-k szükségleteit és biztosítsák nekik a szükséges ösztönzőket és támogatást.

71 A koherens, nemzetközi kiberbiztonsági irányítási keret hiánya akadályozza a nemzetközi közösséget abban, hogy megfelelően reagáljon a számítógépes támadásokra és megfékezze azokat. Ezért fontos, hogy konszenzus alakuljon ki egy olyan irányítási keretről, amely a legjobban tükrözi az Unió érdekeit és értékeit[99]. A nemzetközi kibertérre vonatkozó kötelező erejű normák bevezetésére irányuló törekvéseket egyre több bizonytalanság övezi: példa erre, hogy 2017-ben az ENSZ kormányzati szakértői csoportján belül nem sikerült konszenzusra jutni azt illetően, miként kell alkalmazni a nemzetközi jogot az eseményekre adott állami reagálásra.

72 A kibertér irányítására vonatkozó menetrendjének megerősítése érdekében az Unió hivatalos formában is létrehozott hat kiberpartnerséget, hogy rendszeres szakpolitikai párbeszédet alakítson ki a bizalom megteremtése és az együttműködési területek azonosítása érdekében[100]. Az eredmények vegyesek: az Unió – bár javított a pozícióján – összességében még nem tekinthető „jelentős kiberbiztonsági szereplőnek” a nemzetközi színtéren[101].

Információbiztonság az uniós intézményeknél

73 Minden uniós intézmény saját információbiztonsági irányítási szabályokkal rendelkezik. Intézményközi megállapodás rendelkezik arról, hogy az információbiztonság terén a Bizottság segítséget nyújt a többi intézmény és ügynökség számára. Az uniós intézmények és szervek felismerték, hogy koherens módon kell fejleszteniük kiberkapacitásaikat és a kockázatkezelési megközelítéseiket. A Bizottság,

a Tanács és az EKSZ 2020-ben jelentést nyújt be a kiberkérdésekkel foglalkozó horizontális munkacsoport számára az uniós intézmények és ügynökségek kiberbiztonsági irányításának pontosítása és harmonizálása terén elért eredményekről[102].

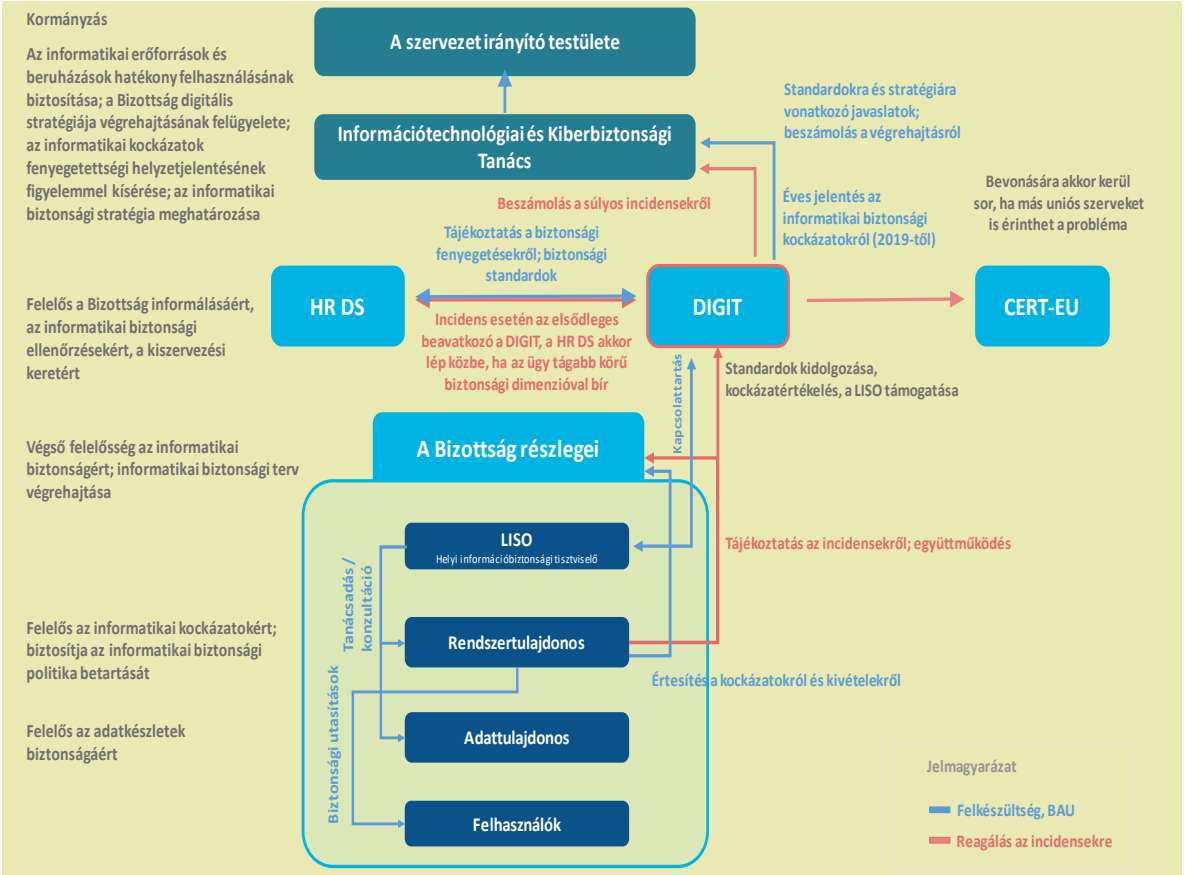
74 A Bizottságon belül az Informatikai Főigazgatóság (DIGIT) felelős az informatikai infrastruktúra és szolgáltatások biztonságáért (lásd: ***3. háttérmagyarázat***). A Bizottság digitális stratégiájának fő informatikai biztonsági célkitűzései az informatikai biztonság beépítése az irányítási folyamatokba, (költség)hatékony infrastruktúra és reziliencia biztosítása, az eseményfelderítés és a reagálás hatókörének kiszélesítése, valamint az informatikai és a biztonsági irányítás integrálása[103]. A Bizottság – szolgáltatói szerződése alapján – biztosítja szinte minden szoftver aktív karbantartását és gondoskodik arról, hogy csak a kereskedők által támogatott szoftvereket használjanak[104].

75 Az intézmények védelmének fontossága az Unió globális KBVP-misszióira és szervezeteire is kiterjed. Az Unió kibervédelmi politikai keretének (2018. évi aktualizált változat) egyik prioritása az uniós szervezetek által a KBVP keretében használt kommunikációs és információs rendszerek védelmének erősítése. Létrehozták az EKSZ kiberirányítási testületét, amely 2017 júniusában tartotta meg első ülését[105].

3. háttérmagyarázat

A Bizottság információs rendszereinek védelme

A Bizottság mintegy 1300 rendszere és 50 000 eszköze folyamatosan kibertámadások célpontja. Az informatikai felelősség decentralizált, amint az alábbi ábra mutatja. Az információs és informatikai biztonság az Informatikai Főigazgatóság által meghatározott közös informatikai biztonsági terven alapul. Az Információtechnológiai és Kiberbiztonsági Tanács a Bizottság de facto információbiztonsági főtisztviselőjeként jár el, és az informatikai biztonság műveleti oldalát összekapcsolja a Bizottság felső vezetésével, amelyet a Szervezetirányító Tanács képvisel.



Forrás: Európai Számvevőszék, a Bizottság határozatai alapján[106].

A Humánerőforrásügyi és Biztonsági Főigazgatóság (DG HR DS) fő feladata a Bizottság alkalmazottainak, információinak és eszközeinek védelme. Ennek kapcsán olyan események tekintetében is folytat biztonsági vizsgálatokat, amelyek biztonsági dimenziója túlmutat az információtechnológián, ezáltal munkájával a kémelhárítási és terrorizmusellenes tevékenységeket is segíti.

A DIGIT felelős az informatikai biztonságért és biztosítja a CERT-EU (hálózatbiztonsági vészhelyzeteket elhárító csoport) működési keretét. A 2011-ben létrehozott CERT-EU mintegy 2,5 millió euró éves költségvetéssel és körülbelül 30 fős személyi állománnyal rendelkezik. Ez a csoport az elsődleges reagáló szerv a több intézményt érintő információbiztonsági események esetében, ugyanakkor még nem működik megszakítás nélkül. A CERT-EU információmegosztó platformmal is rendelkezik. 2018-ban a csoport nem kötelező erejű egyetértési megállapodást írt alá az ENISA-val, az EC3-mal és az Európai Védelmi Ügynökséggel az együttműködés és a koordináció megerősítése érdekében. Ezenkívül technikai megállapodást írt alá NATO kiberbiztonsági eseményeket kezelő képességével (NCIRC).

Fenyegetés- és kockázatértékelés

76 A stabil alapokon nyugvó és folyamatos fenyegetés- és kockázatértékelések fontos eszközt jelentenek az állami és magánszervezetek számára egyaránt. Nem

létezik azonban szabványos megközelítés a kiberfenyegetések osztályozására és feltérképezésére vagy a kockázatok értékelésére, ezért az értékelések tartalma jelentősen eltér, ami megnehezíti a kiberbiztonság koherens uniós szintű megközelítését[107]. Ezen túlmenően a szervezetek gyakran azonos forrásra vagy akár már elkészített fenyegetésértékelésekre támaszkodnak, így ugyanazok a megállapítások újra és újra előtérbe kerülnek[108], ami azzal a kockázattal jár, hogy eközben nem fordítanak kellő figyelmet más veszélyekre. A helyzetet tovább súlyosbítja, hogy a szervezetek továbbra sem szívesen osztják meg másokkal az információkat, és nem jelentenek be minden eseményt.

77 Az EKSZ-nél működő, hibrid fenyegetésekkel foglalkozó információs és elemzőcsoportot (Hibrid Fusion Cell)[109] azzal a céllal hozták létre, hogy az elemzések megosztása révén javítsa a helyzetismeretet és támogassa a döntéshozatalt, ugyanakkor bővíteni kell szakértelmét, többek között a kiberbiztonság terén is. Ezzel párhuzamosan a CERT-EU jelentéseket és tájékoztatókat készít az uniós intézmények, szervek és ügynökségek számára az azokra irányuló kiberfenyegetésekről.

78 Az ENISA a múltban megállapította, hogy számos tagállam rendelkezik kvalitatív ismeretekkel a fenyegetésekkel kapcsolatban, de több kiberfenyegetés-modellezésre lenne szükség[110]. A stratégiai elemzési kapacitások nyomon követése is segíti az általános megértést. A fenyegetésértékelés azonban nemcsak a technológiai veszélyekre terjedhet ki, hanem az átfogóbb kép érdekében a társadalmi-politikai és gazdasági fenyegetésekre, valamint a fenyegetések mozgatórugóira és a szereplők indítékaira is.

Ösztönzők

79 Még mindig túl kevés jogi és gazdasági ösztönző létezik annak előmozdítására, hogy a szervezetek tájékoztatást és információkat osszanak meg az eseményekről. A hírnévromlás kockázata miatt számos szervezet továbbra is szívesebben kezeli diszkréten a kibertámadásokat, vagy fizeti ki az elkövetőket. Csak a jövőben fog kiderülni, hogy a kiberbiztonsági irányelv milyen eredményesen növeli majd az értesítések szintjét. A Bizottság arra számít, hogy elsősorban nemzeti szinten következik be fejlődés, de a kiberbiztonsági jogszabály az egész Unióra kiterjedő dimenzióval egészíti ki ezt a síkot[111].

80 A közigazgatási szervek azáltal, hogy bizonyos szabványokat beépítenek a közbeszerzésbe, közbeszerzési eljárás keretében digitális termékek és szolgáltatások vásárlóiként, valamint a kutatás és a programok finanszírozása révén jelentős hatást

gyakorolhatnak a szolgáltatókra, például azáltal, hogy előírják bizonyos technikai standardok – például az IPv6 internetprotokoll – alkalmazását a kiberbűnözés elleni küzdelem segítése érdekében. Jelenleg azonban nem létezik a kiberbiztonsági infrastruktúrára vonatkozó közös közbeszerzési keret[112]. A Bizottság sokat tehet ezen a téren. A következő többéves pénzügyi keret kapcsán javasolt DEP azt a problémát próbálja meg orvosolni, hogy a közszektor mindeddig csak korlátozott mértékben ruházott be a legfrissebb kiberbiztonsági technológiák beszerzésébe.

81 Szabályozói minőségében a Bizottság biztosíthatja, hogy a biztonság növelése érdekében a megfelelő normákat fejlesszék ki széles körű alkalmazásra. A Bizottság és az Europol együttműködik különböző internetirányító szervekkel, például az ICANN-nal (lásd: ***38.*** bekezdés) és a RIPE-NCC-vel[113], ami kulcsfontosságú ahhoz, hogy a legmegfelelőbb kiberbűnözési architektúrát vezessék be a bűnüldöző és igazságügyi hatóságok támogatására.

Hetedik kihívás: Készségfejlesztés és figyelemfelhívás

82 Az ENISA rámutatott arra, hogy a felhasználók kritikus szerepet játszanak a kibertámadások elleni küzdelemben, és hogy a készségek, az oktatás és a tudatosság fejlesztése elengedhetetlen a kibertámadásokkal szemben ellenállóképes társadalom kialakításához[114]. Akik gyakorlottak a figyelmeztető jelek észrevételében és rendelkeznek a megfelelő technikákkal, a munkahelyen és otthon egyaránt lelassíthatják vagy megelőzhetik a támadásokat.

83 Különös aggodalomra ad okot, hogy egyre kevésbé állnak arányban egymással a kiberbűncselekmények elkövetéséhez vagy a kibertámadások elindításához szükséges szaktudás, valamint az ellenük való védekezéshez szükséges készségek. A kiberbűncselekmény-szolgáltatási modell csökkentette a kiberbűnözési piacra való belépés korlátait: ma már olyanok is bérelhetnek botneteket, kártevőterjesztő készleteket és zsarolóprogram-csomagokat, akik nem rendelkeznek a szükséges műszaki ismeretekkel azok megépítéséhez.

Képzés, készségfejlesztés és kapacitásnövelés

84 A világ növekvő hiánnyal szembesül a kiberbiztonsági készségek terén: 2015 óta 20%-kal nőtt a munkaerőhiány[115]. A hagyományos toborzási csatornákon keresztül nem sikerül kielégíteni a keresletet, még a vezetői és az interdiszciplináris pozíciókban sem[116]. Globális szinten a kiberbiztonsági alkalmazottak közel 90%-a férfi: a nemek közötti megoszlás tartós egyoldalúsága még inkább leszűkíti a toborzási

lehetőségeket[117]. A kiberbűnözéshez kapcsolódó tárgyak az egyetemeken sem kapnak elég súlyt a nem technikai jellegű programokban.

85 Széles körű képzésre és oktatásra lenne szükség a köztisztviselők, a bűnüldöző szervek tagjai, az igazságügyi hatóságok, a fegyveres erők és a nevelők körében. A bíróságoknak például képesnek kell lenniük a kiberbűnözés és áldozatai gyorsan változó technikai sajátosságainak kezelésére[118], azonban jelenleg nincsenek uniós szintű szabványok a képzésre és a tanúsításra vonatkozóan[119]. Az uniós intézményekben fontos a megfelelő készségkombináció kialakítása. Enélkül az intézmények nem tudják megfelelően meghatározni az intézkedések hatókörét és azonosítani a megfelelő partnereket és biztonsági igényeket, sőt akár a programok irányítására is képtelenné válhatnak. Ez pedig csökkentheti az uniós programok és szakpolitikai fejlesztés eredményességét.

86 Bár az uniós szintű oktatáspolitikáért a tagállamok felelősek, már jelenleg is számos képzési tevékenység (lásd: ***2. táblázat***) és gyakorlat (lásd: ***4. háttérmagyarázat***) van folyamatban. Az Unió segíthet abban, hogy az uniós szintű szabványok bekerüljenek az összes érintett tudományág tantervébe[120]. A digitális kriminalisztika területén például közös képzési szabványokra van szükség ahhoz, hogy elő lehessen segíteni a digitális bizonyítékok elfogadhatóságát a tagállamokban. A kiberbűnözés határokon átnyúló jellege miatt több joghatóság is érintett lehet egy-egy eseményben, ami uniós szintű képzést igényel. Mindezek ellenére a CEPOL – az Unió bűnüldözési képzési ügynöksége – megállapította, hogy a tagállamok több mint kétharmada nem biztosít rendszeres kiberképzést a bűnüldöző szervek tagjai számára[121]. Az Uniónak ezenfelül lehetősége nyílhat arra is, hogy azonosítsa a polgári és a katonai szférában nyújtott oktatás és a képzés közötti szinergiák kihasználásának módjait[122]. Mindemellett az ENISA megállapította, hogy bár a kritikus ágazatokban jelenleg is kiterjedt képzési lehetőségek állnak rendelkezésre, azok nem foglalkoznak elég célirányosan a kritikus infrastruktúrák rezilienciájával[123].

2. táblázat. Néhány uniós kiberbiztonsági képzési kezdeményezés

Az Európai Védelmi Ügynökség projektjei, pl. a magánszektor gyakorlatainak támogatása és a „Cyber Ranges” projekt	Az Európai Biztonsági és Védelmi Főiskola hálózat (polgári-katonai képzés), beleértve a kibervédelmi oktatási, képzési és értékelési platformot	Az ENISA képzései: a kereskedelmi kínálatból hiányzó képzési programok nyújtása
Europol, CEPOL, ECTEG[124] képzési programok, beleértve a képzésirányítási modellt és a képzési kompetenciakeretet (tanúsítással)	Kompetenciaközpont-hálózat és Kutatási Kompetenciaközpont (javasolt)	A Biztonsági Unió 11. eredményjelentésében javasolt titkosítási intézkedések
Az EU és a NATO közötti együttműködés a kibervédelmi képzés és oktatás terén	Katonai Erasmus program	Európai Igazságügyi Képzési Hálózat

Forrás: Európai Számvevőszék.

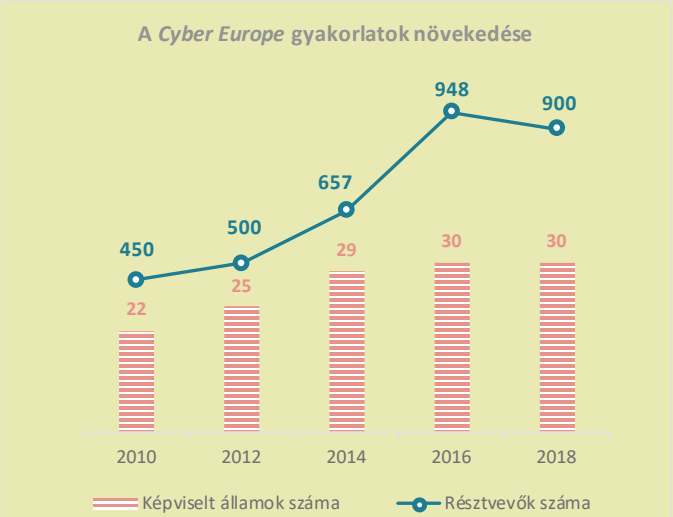
87 Az Unió 17 külképviseletéhez helyezett ki terrorellenes és biztonsági szakértőket az Unió belső és külső biztonsága közötti kapcsolat megerősítése érdekében[125]. Az erőforrások szűkössége ellenére a mélyrehatóbb kiberbiztonsági ismeretek segíthetnék a megfelelő projektek megvalósítását, valamint szinergiákat teremthetnének más programokkal vagy finanszírozási forrásokkal[126]. Hozzájárulhatnának továbbá a kiberbiztonság által a politikai párbeszéd során elfoglalt pozíció javításához, bár e területnek sok más prioritással – például a migrációval, a szervezett bűnözéssel és a külföldi harcosok visszatérésével – kell versenyeznie.

4. háttérmagyarázat

Gyakorlatok

A gyakorlatok a kiberoktatás és -képzés fontos elemei, amelyek a kapacitások tesztelése, a való életben előforduló helyzetekre való reagálás és munkakapcsolatok kiépítése révén kiváló lehetőségeket kínálnak a felkészültség növelésére. 2010 óta jóval gyakrabban szerveznek ilyen gyakorlatokat.

A résztvevők a helyszínen vagy távoli eléréssel oldják meg a feladatokat. A tanulságok levonása érdekében utólagos értékeléseket végeznek, bár ezek nem feltétlenül fogják át teljes mértékben a stratégiai/politikai, a működési és a technikai szintek mindegyikét[127].



Forrás: Európai Számvevőszék, az ENISA dokumentumai alapján.

Az EU és a NATO kiemelt gyakorlatai – a kétévente megrendezésre kerülő „Cyber Europe” (operatív) és az évente megrendezett „Locked Shields” (technikai) gyakorlat – több mint ezer résztvevőt vonzanak mintegy 30 részt vevő országából. Mindkét gyakorlat a kritikus infrastruktúra szimulált támadásokkal szembeni védelmére és fenntartására összpontosít. A gyakorlatok hatóköre is jelentősen megnőtt: a gyakorló szakemberek helyzetismeretének javítása érdekében immár a médiára, illetve a jogi és pénzügypolitikai elemekre is kiterjed. A párhuzamos és összehangolt (stratégiai) PACE gyakorlatok az EU és a NATO közötti interakciót vizsgálják hibrid válságforgatókönyvek esetében.

Ezek mellett ugyanakkor más nemzetközi gyakorlatok megrendezésére is sor kerül. Az ENISA évente szervez kiberbiztonsági versenyt, amely keretében a csapatok olyan, biztonsággal kapcsolatos kihívások megoldásán versenyeznek egymással, mint az internet- és mobilbiztonság, kriptofeladványok, visszafejtés, valamint etikai és a kriminalisztikai feladatok. Az első miniszteri szintű gyakorlat, a 2017 szeptemberében megrendezett EU CYBRID a stratégiai döntéshozatalra összpontosított. 2018-ban elindították a NATO-hoz kapcsolódó „Crossed Swords” gyakorlatot azzal a céllal, hogy javítsák a „Locked Shields” gyakorlat támadó elemeit. A NATO a szervezője a „Cyber Coalition” gyakorlatoknak is.

Mindezek során kulcsfontosságú feladatot jelent az összes fontos érdekelt fél aktív részvételének biztosítása, a gyakorlatok összehangolása, a párhuzamosságok elkerülése és a levont tanulságok hatékony megosztása.

Figyelemfelhívás

88 A polgárok gyakran válnak támadások és félretájékoztatás áldozatává, mivel tudtukon kívül nagyobb valószínűséggel vannak kitéve az olcsó és széles körben forgalmazott eszközök és szoftverek sebezhetőségének, illetve pszichológiai manipulációnak. A tudatosság növelése ezért alapvető fontosságú a kibertámadásokkal szembeni reziliencia megerősítéséhez, ez ugyanakkor semmiképpen sem könnyű feladat, mivel a szakértelemmel nem rendelkezők nehezen látják át a kiberbiztonság összetettségét és a kapcsolódó kockázatokat.

89 Többek között az éves európai kiberbiztonsági tudatossági hónap (ECSM) és a biztonságosabb internet napja nyújt alkalmat a tudatosság növelésére. Az ECSM-kezdeményezéshez immár hét nem uniós ország is csatlakozott[128]. Az Europol *„Mondj nemet!”* kampányának célja, hogy csökkentse a gyermekek szexuális erőszak és zsarolás áldozatává válásának kockázatát az interneten. A kockázat csökkentése azért fontos, mert jelenleg kevés áldozat jelenti be az ilyen bűncselekményeket a rendőrségnek[129].A Bizottság elismeri, hogy a kiberbiztonsági stratégia eddig csak „részben volt eredményes” a polgárok és a vállalkozások tudatosságának növelése terén[130]. Ennek oka a feladat nagyságrendje, az erőforrások korlátozott volta, a tagállamok egyenlőtlen szerepvállalása, valamint a tudományos bizonyítékok hiánya a tudatosság növelésének és mérésének legjobb módját illetően.

90 A Bizottságra és az érintett ügynökségekre vár annak biztosítása, hogy a tudatosság növelésére irányuló intézkedések célirányosak és inkluzívak legyenek és széles közönséghez elérjenek, kövessék a fenyegetések időbeni alakulását és ne gyakoroljanak nem szándékolt hatásokat (pl. „biztonsági fásultság”[131]), valamint szintén az ő feladatuk, hogy értékelési módszereket és mérőszámokat dolgozzanak ki az intézkedések eredményességének értékelésére. Ez ugyanúgy érvényes magukra az uniós intézményekre is, ahol szintén fejlesztésre szorul a tudatossági kultúra[132].

Nyolcadik kihívás: Az információcsere és a koordináció javítása

91 A kiberbiztonsághoz kulcsfontosságú a köz- és a magánszféra közötti együttműködés, elsősorban az információk megosztása és a bevált gyakorlatok cseréje terén. Minden szinten elengedhetetlen a bizalom ahhoz, hogy megfelelő környezetet lehessen teremteni a bizalmas információk határokon átnyúló megosztásához. Az elégtelen koordináció széttagoltsághoz, párhuzamos erőfeszítésekhez és a szakértelem szétaprózódásához vezet. Hathatós koordinációval azonban kézzelfogható sikereket lehet elérni, mint történt például a dark webes piacok bezárása esetében[133]. A bizalom

– mind uniós szinten, mind egyes tagállamokban – az elmúlt években elért eredmények ellenére sem éri el a kívánatos szintet[134,135].

Az uniós intézmények egymás közötti és a tagállamokkal folytatott koordinációja

92 A kiberbiztonsági stratégia és a kiberbiztonsági irányelv által bevezetett együttműködési struktúrák egyik célja az érdekelt felek közötti bizalom erősítése volt. A stratégia értékelése szerint sikerült lefektetni az uniós szintű stratégiai és operatív együttműködés alapjait[136]. Ennek ellenére a koordináció általában „nem elégséges”[137]. A kihívást annak biztosítása jelenti, hogy az információcsere egyfelől érdemi legyen, másfelől teljes áttekintést adjon a helyzetről. E tekintetben fontos, hogy elfogadott terminológián alapuló közös értelmezést sikerüljön kialakítani (lásd: ***5. háttérmagyarázat***).

93 Az ENISA értékelése azonban megállapította, hogy a kiberbiztonsággal kapcsolatos uniós megközelítést nem hangolják össze megfelelően, és emiatt nem sikerül kihasználni az ENISA és más érdekelt felek tevékenységei közötti szinergiákat. Az együttműködési mechanizmusok még viszonylag kiforratlanok[138]: a kiberbiztonsági jogszabály ezt az ENISA koordinátori szerepének megerősítésével kívánja orvosolni. A 2018-ban az ENISA, az EDA, az Europol EC3 és a CERT-EU között aláírt egyetértési megállapodás mögött is az a törekvés állt, hogy szorosabbra fűzzék az együttműködést[139]. A Bizottság számára az elkövetkező években a szakpolitikai kezdeményezések, a szükségletek és a beruházási programok megfelelő összehangolása jelenti majd az egyik prioritást, a széttagoltság leküzdése és a szinergiák kialakítása érdekében[140].

94 A koordinációs funkciók különböző intézményi testületekbe vannak beágyazva. A Biztonsági Unióval foglalkozó munkacsoportot azért hozták létre, hogy központi szerepet töltsön be a Bizottság különböző főigazgatóságainak koordinálásában a Biztonsági Unió menetrendjének támogatása érdekében[141]. A munkacsoport kiberbiztonsággal foglalkozó almunkacsoportjának elnöki tisztét a DG CNECT tölti be.

95 A Tanácsban a kiberbiztonsági kérdéseken a kiberkérdésekkel foglalkozó horizontális munkacsoport (HWP) dolgozik, amely koordinálja a stratégiai és horizontális kiberkérdéseket, és segít a gyakorlatok előkészítésében és azok eredményeinek értékelésében. Szorosan együttműködik a Politikai és Biztonsági Bizottsággal, amely központi döntéshozatali szerepet tölt be a kibertérre vonatkozó diplomáciai intézkedésekkel kapcsolatban (lásd: következő fejezet, ***6. háttérmagyarázat***). Mivel a kiberbiztonság átfogó téma, nem egyszerű az összes

releváns érdek összehangolása: a közelmúltban nem kevesebb mint 24 munkacsoport és előkészítő testület foglalkozott a kiberfenyegetésekkel kapcsolatos kérdésekkel[142].

96 Az ENISA megerősítésére, illetve a kiberbiztonsági kompetenciaközpontok hálózatának és egy kutatási kompetenciaközpontnak a létrehozására irányuló két legutóbbi jogalkotási javaslat (2018) kifejezetten a széttagoltság és a párhuzamos erőfeszítések kezelésére irányul. A kiberbiztonsági kompetenciaközpontok hálózata és a kutatási kompetenciaközpont létrehozásának mozgatórugója a kiberbiztonsági irányelv együttműködési struktúrái mellett megmaradt rések kitöltése volt, hiszen e struktúrák még nem támogatják a legújabb technológiai megoldások kifejlesztését.

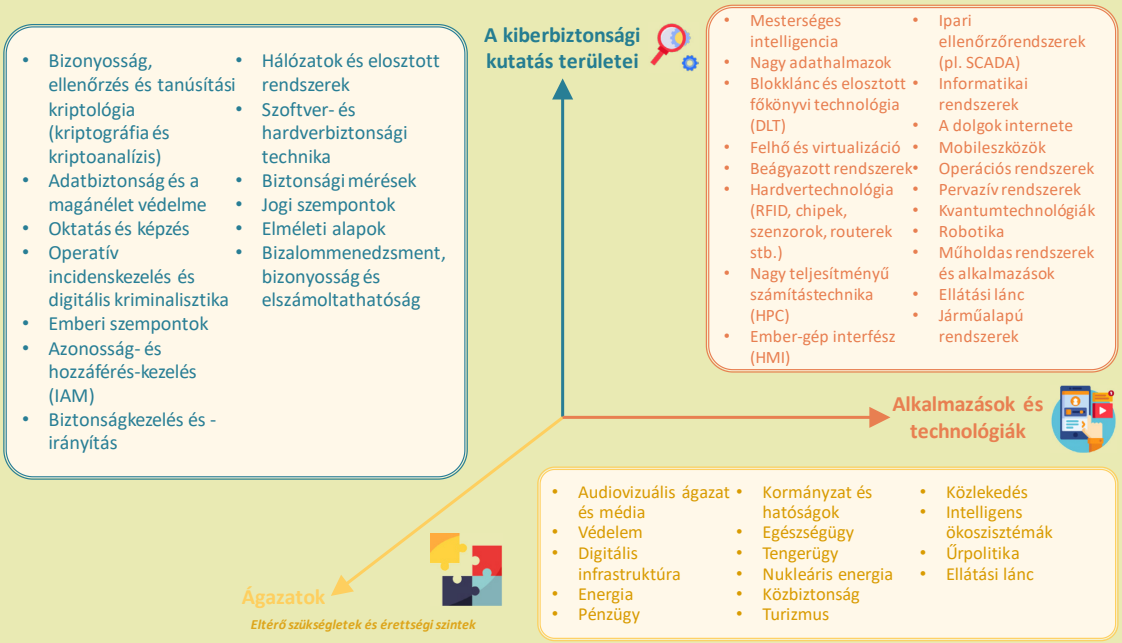
5. háttérmagyarázat

Értsünk szót kibernyelven: *technológiai koherencia*

Az egyértelmű terminológia javítja a helyzetismeretet és a koordinációt[143], és segít annak pontos megállapításában, hogy mi jelent veszélyt, illetve kockázatot.

A Bizottság Közös Kutatóközpontja (JRC) a közelmúltban felülvizsgált kutatási osztályozási rendszert dolgozott ki különböző nemzetközi szabványok alapján[144]. Célja ezzel az, hogy a kutatási egységek Európa-szerte referenciaindexként használhassák a rendszert.

Kiberbiztonsági osztályozási rendszer



Forrás: Európai Számvevőszék, az Európai Bizottság adatai alapján.

Az uniós intézmények és ügynökségek a közelmúltig nem használtak közös fogalommeghatározásokat. Ez változóban van. Az Együttműködési Csoport az általa kidolgozott tervezetben kidolgozott egy eseményosztályozási rendszert a határokon átnyúló hatékony együttműködés elősegítése érdekében.

Együttműködés és információcsere a magánszférával

97 A kiberbiztonság átfogó szintjének megerősítéséhez alapvető fontosságú a hatóságok és a magánszektor közötti együttműködés. Ennek ellenére a Bizottság a kiberbiztonsági stratégia 2017. évi értékelésében úgy találta, hogy a magánszereplők, illetve a köz- és a magánszektor közötti információcsere a megbízható beszámolási mechanizmusok és az információmegosztást elősegítő ösztönzők hiánya miatt „még nem optimális”[145], és ez hátráltatja a stratégiai célok elérését. A Bizottság azt is megállapította, hogy nem létezik olyan hatékony együttműködési mechanizmus, amelynek keretében a tagállamok együttműködhetnének a hosszú távú ágazati kapacitások nagyléptékű stratégiai javítása érdekében[146].

98 Az információmegosztó és -elemző központok (ISAC) egyrészt a köz- és a magánszféra közötti információmegosztást elősegítő platformok és erőforrások biztosítására, másrészt a kiberfenyegetésekkel kapcsolatos információk gyűjtésére létrehozott szervezetek. Céljuk a bizalom megerősítése a tapasztalatok, a tudás és az elemzés megosztása révén, különös tekintettel a kiváltó okokra, a váratlan eseményekre és a fenyegetésekre. Már számos tagállamban léteznek nemzeti és ágazati ISAC-ok, de európai szinten még mindig viszonylag korlátozott a számuk[147]. Ugyanakkor e központok működése számos nehézséggel jár (erőforrás-korlátok, az eredmények értékelésének nehézségei, a megfelelő struktúrák biztosítása a köz- és a magánszféra egyidejű bevonásához, a bűnüldöző hatóságok bevonása), amelyeket le kell küzdeni ahhoz, hogy hozzájárulhassanak a kiberbiztonsági irányelv végrehajtásához és az európai szintű biztonsági képességek kiépítéséhez[148].

99 A magánszektorral való szoros együttműködés különösen fontos az összetett kiberbűnözés elleni küzdelemben, hatékonysága azonban a bizalom szintjétől függ, így nem egyenletes a tagállamok körében[149]. Az Europol EC3 egy sor tanácsadó csoportot hozott létre a magánszektor szereplőivel, az uniós intézményekkel és ügynökségekkel, valamint más nemzetközi szervezetekkel a kooperáció, a hálózatépítés és a stratégiai információk megosztása révén megvalósuló együttműködés javítása érdekében. E csoportok az uniós szakpolitikai ciklus céljaival összehangolt tervek alapján végzik munkájukat[150]. A titkosítással való visszaélés szintén egy olyan problémás terület,

amely kapcsán szorosabb együttműködésre van szükség a magánszektorral. Az Europol EC3 jelenleg vizsgálja a lehetőségeket arra, hogy egyes esetek mentén, rövid távon szakértőket delegáljon a J-CAT-hoz a magánszférából és a tudományos körökből (lásd: ***62.*** bekezdés).

100 A hatékony együttműködési mechanizmusok hiánya káros a polgári és a védelmi közösségekre – az államiakra és a magánszférabeliekre egyaránt. A közös kihívást jelentő területek közé tartoznak a kriptográfia, a biztonságos beágyazott rendszerek, a rosszindulatú szoftverek felderítése, a szimulációs technikák, a hálózatok és rendszerek kommunikációvédelme és a hitelesítési technológiák. A polgári–katonai együttműködés előmozdítása, valamint a kutatás és a technológia támogatása (különösen a kkv-k támogatása révén) az aktualizált uniós kibervédelmi szakpolitikai keret (2018. évi frissítés) két prioritása.

Átgondolandó kérdések – A reziliencia fejlesztése

- Hogyan lehet uniós szinten megfelelő egyensúlyt teremteni egyfelől a kiberbiztonsági politika előtérbe helyezésének és egységesítésének szükségessége, másfelől a különböző szereplők közötti hatékony koordináció és a felelősségek megosztása között?
- Mennyire felkészültek az uniós intézmények és ügynökségek a közvetlenül ellenük indított következő nagyszabású támadásra?
- Hogyan tehetjük vonzóbbá a tehetséges munkavállalók számára az uniós kiberbiztonsági ügynökségeket?
- Milyen további lépésekre van szükség ahhoz, hogy az uniós intézmények és ügynökségek megfelelő kapacitással rendelkezzenek egy koherens kockázat- és veszélyértékelési keret alkalmazásához?
- Milyen módon kezelik az európai felügyeleti hatóságok (az Európai Bankfelügyeleti Hatóság, az Európai Értékpapír-piaci Felügyeleti Hatóság és az Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság) a pénzügyi ágazat szerves kiberbiztonsági sebezhetőségeit, és milyen tanulságokat vonhat le ebből a többi ágazat?
- A szakértelem általános hiánya mellett hogyan lehet a hatóságoknak nyújtott uniós technikai segítségnyújtást úgy felhasználni, hogy az a lehető legnagyobb átfogó hatást fejtse ki a kibertámadásokkal szembeni reziliencia javítása terén?
- Hogyan biztosítható az Unió és a tagállamok érdemi jelenléte a nemzetközi vitákban, hogy részt vehessenek a kibertér irányításának és normáinak alakításában és előmozdíthassák az uniós értékek érvényesülését?
- Melyik uniós és tagállami szintű tudatosságnövelő intézkedések (beleértve a megelőzést) képesek valódi változást előidézni, és mit tehet az Unió ezek szélesebb körű alkalmazása érdekében?
- Hogyan járulhat hozzá az Unió a nemek szerinti megoszlás kiegyensúlyozásához a kiberbiztonság területén?
- Hogyan erősíthetik meg az Unió és a tagállamok a kibervédelmi szakpolitikai kerettel (2018. évi frissítés) összhangban a polgári és a védelmi közösségek közötti szinergiákat?

Sikeres reagálás kiberbiztonsági események esetén

101 A kibertámadásokra való eredményes reagálás megtervezése alapvető fontosságú azok mielőbbi megállításához. Különösen fontos, hogy a kritikus ágazatok, a tagállamok és az uniós intézmények gyorsan és összehangoltan tudjanak reagálni. Ehhez elengedhetetlen a korai észlelés.

Kilencedik kihívás: Eredményes észlelés és reagálás

Észlelés és értesítés

102 Egyszerű észlelési eszközök segítségével a mindennapokban legyőzhető a támadások túlnyomó többsége[151]. A digitális rendszerek ugyanakkor olyan összetetté váltak, hogy lehetetlen minden támadást kivédeni. Kifinomultságuk miatt a támadások gyakran hosszú időn át észrevétlenek maradnak. A szakértők ezért azt tartják, hogy a gyors észlelésre és védelemre kell összpontosítani[152]. Egyes felderítési eszközöket — például az automatizálást, a gépi tanulást és a viselkedéselemzést, amelyek a kockázatok csökkentését, valamint a rendszerviselkedés elemzését és hasznosítását célozzák – a vállalkozásoknak csak kis része vezette be[153]. Ez részben annak tudható be, hogy gyakoriak a hamis pozitív eredmények, amelyek ártalmatlan tevékenységeket tévesen rosszindulatúnak tüntetnek fel.

103 A jogsértés észlelését és elemzését követően gyors bejelentésre és beszámolásra van szükség, hogy a többi köz- és magánszervezet megelőző intézkedéseket hozhasson, és az érintett hatóságok támogatni tudják az érintetteket. Sok szervezet vonakodik attól, hogy elismerje és bejelentse a kiberbiztonsági eseményeket[154]. Szintén alapvető fontosságú a bűnüldöző hatóságok korai bevonása a kiberbűncselekmény-gyanús esetekkel szembeni azonnali reagálásba, valamint a CSIRT-ekkel folytatott proaktív információcsere.

104 A biztonsági események bejelentésére vonatkozó közös uniós követelmények korábbi hiánya azzal a kockázattal járt, hogy késlelteti a jogsértések bejelentését és hátráltatja a reagálást; a kiberbiztonsági irányelv bevezetése orvosolni próbálta ezt a problémát (lásd: ***20.*** bekezdés). A 2017. évi WannaCry támadásokat követően a Bizottság arra a következtetésre jutott, hogy a CSIRT hálózati rendszer „még nem teljesen működőképes”[155]. Mivel az irányelv végrehajtása folytatódik, idővel ki fog

derülni, hogy az Együttműködési Csoport által kidolgozott iránymutatás sikeresnek bizonyul-e az események bejelentésével kapcsolatos ellenérzések leküzdésében[156].

105 Egyes ágazatokban az alapvető szolgáltatásokat nyújtó szereplőket a hatályos uniós rendeletek értelmében több bejelentési kötelezettség is terheli (többek közt a fogyasztók irányában), ami ronthatja a folyamat hatékonyságát. A pénzügyi és banki ágazat szereplőire például eltérő értesítési kritériumok, szabványok, küszöbértékek és időkeretek vonatkoznak az általános adatvédelmi rendelet, a kiberbiztonsági irányelv, a pénzforgalmi szolgáltatásokról szóló irányelv, az EKB/SSM, a 2. cél és az eIDAS-rendelet alapján[157]. Ezért fontos e kötelezettségek leegyszerűsítése, mivel azon túl, hogy felesleges adminisztratív terhet jelent, ez a heterogenitás szétaprózódott beszámoláshoz is vezethet.

Összehangolt reagálás

106 Még folyamatban van az európai kiberbiztonsági válságkezelési együttműködési keret kidolgozása. A kapcsolódó tervezetet[158] (lásd: ***18.*** bekezdés) azért vezették be, hogy beépítse a kiberperspektívát a politikai szintű integrált válságelhárítási mechanizmusba (IPCR), javítsa a helyzetismeretet és biztosítsa az egyéb uniós válságkezelési mechanizmusokkal való jobb integrációt[159]. A tervezet uniós intézmények, ügynökségek és tagállamok részvételéről rendelkezik. Mindezeknek a válságelhárítási mechanizmusoknak a zökkenőmentes integrálása komoly feladat[160]. Fontos hiányosság az is, hogy jelenleg nem áll rendelkezésre közös, biztonságos kommunikációs hálózat az uniós intézmények között[161].

107 Nagyléptékű, határokon átnyúló események esetén az Unió állítólag mind operatív, mind politikai szinten csak korlátozott mértékben képes a számítógépes támadásokra való reagálásra, részben azért, mert a kiberbiztonságot még nem integrálták a meglévő uniós szintű válságkezelési koordinációs mechanizmusokba[162]. A kiberbiztonsági irányelv nem foglalkozott ezzel a problémával.

108 A tagállamok nem támogatták az ENISA közelmúltban javasolt reformját, amely nagyobb operatív szerepet szánt az ügynökségnek a nagyszabású kiberbiztonsági események kezelésében; inkább azt a megoldást részesítették előnyben, hogy az ügynökség a saját operatív fellépéseiket támogassa és egészítse ki[163]. Tagállami szinten már számos CERT/CSIRT létezik, de ezek kapacitásai jelentős mértékben eltérnek egymástól. Ez akadályt gördít a nagyszabású események kezeléséhez szükséges eredményes nemzetközi együttműködés elé[164].

109 Megpróbáltuk feltérképezni a tervezetben meghatározott különböző szereplőkhöz rendelt szerepeket, de találtunk olyan hiányosságokat, amelyeket a végrehajtás során orvosolni kell. Az egyik kezdetben alulértékelt terület a bűnüldözés volt, bár azóta 2018 decemberében hatályba lépett az uniós bűnüldözési vészhelyzet-elhárítási protokoll[165]. A tervezet sikerének előfeltétele, hogy az gyakorlati jellegű legyen, és hogy minden fél pontosan tudja, mit kell tennie; ehhez a következő években széles körű tesztelésre lesz szükség.

110 Az eredményes reagálás többet jelent, mint a károk enyhítése; döntő fontosságú a támadások felelőseinek azonosítása is. Az anonimizálási eszközökkel, a kriptovalutákkal és a titkosítással kapcsolatos növekvő visszaélések különösen megnehezíthetik az elkövetők felkutatását és azonosítását, főként hibrid támadás esetén. Ez a jelenség „attribúciós probléma” néven ismert. Orvoslása nem csupán technikai kérdés, hanem a büntetőjog szempontjából is kihívást jelent. Az országok közötti jogi és eljárási különbségek akadályozhatják a bűnügyi nyomozásokat és a gyanúsítottak büntetőeljárás alá vonását. Az attribúciós probléma kezeléséhez egyértelműbb eljárások révén formalizáltabb operatív információcserére lesz szükség például az Europollal vagy az Eurojust Számítástechnikai Bűnözés Elleni Európai Igazságügyi Hálózatával.

111 Politikai szinten a kiberdiplomáciai eszköztárat (lásd: ***6. háttérmagyarázat***) a kibertérben zajló nemzetközi viták békés eszközökkel történő rendezésének támogatása érdekében dolgozták ki. A kiberbiztonsági gyorsreagáló csoportok létrehozása és a kiberbiztonság terén történő kölcsönös segítségnyújtásra irányuló kezdeményezés két olyan, a PESCO keretében fejlesztés alatt álló projekt, amely célja a fokozott információmegosztás elősegítése[166].

6. háttérmagyarázat

A kiberdiplomáciai eszköztár

A rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések[167], más néven a „kiberdiplomáciai eszköztár”, a kiberdiplomáciáról szóló 2015. évi tanácsi következtetések nyomán jöttek létre[168]. A kiberdiplomácia célja, hogy olyan közös és átfogó megközelítést dolgozzon ki és hajtson végre a kibertér tekintetében, amely az uniós értékeken, a jogállamiságon, kapacitásépítésen és partnerségeken, a többszereplős internetirányítási modell előmozdításán, valamint a kiberbiztonsági fenyegetések enyhítésén és a nemzetközi kapcsolatok stabilitásának növelésén alapulnak.

Az eszköztár lehetővé teszi az Unió és tagállamai számára, hogy közös diplomáciai válaszlépéseket tegyenek a rosszindulatú kibertevékenységekkel szemben, amelyek

teljes mértékben kihasználják a közös kül- és biztonságpolitika kínálta intézkedéseket. Lehetnek köztük megelőző (pl. figyelemfelkeltő vagy kapacitásépítési), együttműködési, stabilitási és korlátozó intézkedések (pl. utazási tilalmak, fegyverembargók, források befagyasztása), illetve támogathatják a tagállamok reagálását is[169]. Az alapgondolat az, hogy a fenyegetések csökkentésére irányuló további együttműködés és a közös reagálás valószínű következményeinek egyértelmű kommunikálása megelőzheti a (potenciálisan) agresszív magatartást.

A rossz szándékú kibertevékenységekre adott közös uniós válaszintézkedésnek minden esetben arányosnak kell lennie az adott kibertevékenység hatókörével, léptékével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásával.

Az eszköztár sikerességét alapvetően meghatározza majd, hogy mennyire jól illeszkedik a tervezethez és az IPCR-hez (lásd: ***106.*** bekezdés), hogy mennyire sikerül az információk gyors és folyamatos megosztása (többek között az attribúciós elemek)[170] révén támogatni a helyzetismeretet, és végül hogy mennyire lesz eredményes az együttműködés. Az eszköztár sikere szempontjából kulcsfontosságú továbbá az eredményes és összehangolt kommunikáció. Az eszköztárat eddig kétszer használták fel: az Egyesült Államokkal való párbeszéd megkezdésére a *WannaCry* támadás után[171], valamint az informatikai technológiák rosszindulatú felhasználását elítélő tanácsi következtetések kidolgozása során[172]. Az eszköztár üzembe helyezése folyamatban van; egyelőre nem tudható, hogy mennyire lesz eredményes célkitűzéseinek elérésében.

Tizedik kihívás: A kritikus infrastruktúrák és a társadalmi funkciók védelme

Az infrastruktúrák védelme

112 Az Unió kritikus infrastruktúrájának nagy részét ipari ellenőrzési rendszereken (ICS)[173] keresztül működtetik. Ezek közül sokat önálló rendszerként terveztek meg, amelyek csak korlátozottan kapcsolódnak a külvilághoz. Amikor e rendszerek egyedi alkotóelemeit elkezdték összekapcsolni az internettel, azok kiszolgáltatottabbá váltak a külső beavatkozással szemben. A meglévő rendszerek karbantartása és patchelése már gyakran nem lehetséges, a frissítés azonban nem gyors, és nem is olcsó. A kritikus infrastruktúra biztonságának fokozására irányuló erőfeszítéseknek ezért az ipari ellenőrző rendszerek fejlesztésére is ki kell terjedniük.

113 Ahogy az ipar folyamatosan digitalizálódik (közismert nevén „Ipar 4.0”), egy-egy ipari ágazatban bekövetkező nagyszabású esemény hatása más ágazatokra is

átterjedhet. Az ENISA hangsúlyozta, hogy fontos lenne feltérképezni a kritikus ágazatok kölcsönös függőségei által gyakorolt hatást[174]. Ez elengedhetetlen az események lehetséges terjedési útvonalainak felméréséhez és segíti a koordinált reagálást.

114 A kiberbiztonsági irányelv célja a kritikus infrastruktúrákért felelős kulcsfontosságú ágazatok felkészültségének megerősítése. Az irányelv hatóköre azonban nem terjed ki valamennyi ágazatra (lásd: ***1. táblázat***)[175], ami „csökkenti a stratégia eredményességét”[176]: e tekintetben különösen aggályos a választások demokratikus integritásának védelme a választási infrastruktúrába való beavatkozás és a félretájékoztatás ellen (lásd: ***7. háttérmagyarázat***). A meglévő jogszabályok felülvizsgálatán kívül ezért a fő kihívást az jelenti majd, hogyan lehet bevonni ezeket az ágazatokat a nagyszabású eseményekre való hatékony reagálásba.

115 A kritikus infrastruktúrák sebezhetősége nem áll meg Európa határainál. A Bizottság számára különös kihívást jelent, hogy arra ösztönözze a tagjelölt országokat, hogy a tagállamokkal azonos normákat fogadjanak el többek között a kibervédelemmel kapcsolatos jogszabályok vagy a kritikus infrastruktúrák védelme terén.

7. háttérmagyarázat

A kritikus társadalmi funkciók védelme: *küzdelem a választásokba való beavatkozás ellen*

2019 májusában mintegy 400 millió szavazó járul az urnákhoz az európai parlamenti választásokon, amelyekre most első alkalommal már az általános adatvédelmi rendelet alapján kerül sor. A közelmúltban több olyan botrányra került sor, amelyek középpontjában a személyes adatokkal való, politikai mikro-célirányosítással kapcsolatos visszaélések, illetve példátlan, összehangolt félretájékoztatási („fake news”, álhír-) kampányok álltak. A Bizottság figyelmeztetett arra, hogy a választásokba nagy valószínűséggel megpróbálnak majd kibereszközökkel beavatkozni[177]: ennek kivédésében a kormányzatok és a társadalom egészének részt kell vennie.

Választási infrastruktúra

A választások lebonyolítása összetett feladat, védelmük és feddhetetlenségük biztosítása a tagállamok felelőssége. A választásokba és a választási infrastruktúrába való beavatkozás célja a választói preferenciák, a részvételi arány vagy maga a választási folyamat befolyásolása lehet, ideértve a tényleges szavazást, a szavazatösszesítést és a kommunikációt. Az európai parlamenti választások során az úgynevezett „utolsó mérföld” (az eredmények nemzeti fővárosok általi kommunikálása Brüsszel felé) védelme különösen kritikus kihívást jelent, mivel ezzel

kapcsolatban nem alakítottak ki, illetve nem teszteltek közös biztonsági megközelítést[178].

A Bizottság közelmúltbeli választási csomagja a választási kiberbiztonság erősítésére irányuló intézkedéseket is tartalmazott, többek között nemzeti kapcsolattartó pontok kijelölését a választások előtti koordináció és információcsere céljából. Különösen fontos a bevált gyakorlatok és a levont tanulságok megosztása[179].

A választási rendszerek nem minősülnek a kritikus infrastruktúra részének[180], és nem tartoznak a kiberbiztonsági irányelv hatókörébe sem. Az Együttműködési Csoport ennek ellenére a hatóságok támogatása érdekében gyakorlati útmutatást dolgozott ki a választások technológiai biztonságáról. A nemzeti kapcsolattartó pontok várhatóan 2019 elején találkoznak[181]. A tagállamokat arra is ösztönzik, hogy végezzenek kockázatértékelést a választási folyamataikra irányuló kiberfenyegetésekkel kapcsolatban.

Félretájékoztatás

A félretájékoztatás a hibrid támadások egyre fontosabb eleme, amely kibertámadások és hálózatok feltörése révén fejti ki hatását. A félretájékoztatás a hibrid támadások egyre fontosabb eleme, amely kibertámadások és hálózatok feltörése révén fejti ki hatását. Az utóbbi időben olyannyira megnőtt léptékét, sebességét és hatókörét illetően is, hogy immár valódi biztonsági fenyegetést jelent az Unió számára.

Az Unió számos intézkedést hozott a félretájékoztatás kezelése érdekében. 2015-ben létrehozták az EKSZ-nél működő, keleti stratégiai kommunikációval foglalkozó munkacsoportot (East StratCom Task Force) az orosz félretájékoztatási kampányok ellen[182]. A szakértők dicsérik az uniós politikák előmozdítása, a szomszédsági országok független médiájának támogatása, valamint a félretájékoztatás előrejelzése, nyomon követése és kezelése terén végzett munkáját[183]. A félretájékoztatási kampányok nagyságrendjéhez és összetettségéhez képest azonban a munkacsoport forrásai korlátozottak[184]. Módszeresebb interakcióra lenne szükség a meglévő uniós struktúrákkal, és javítani kellene a stratégiai kommunikációs együttműködést[185]. Az Európai Tanács 2018 decemberében új cselekvési tervet[186] hagyott jóvá ezen a területen.

A közelmúltban a Bizottság az online félretájékoztatás kezeléséről szóló 2018. áprilisi közleménye[187] nyomán kidolgozott egy, a meglévő szakpolitikai eszközökön alapuló, önkéntes és önszabályozó gyakorlati kódexet[188], amelyhez online platformok és a reklámipar is csatlakoztak[189]. A fellépés többek között segíti a tartalom megbízhatóságának növelését, valamint támogatja a média- és hírműveltség növelésére irányuló erőfeszítéseket. Létrehoztak egy tényellenőrzéssel foglalkozó független európai hálózatot is.

A Bizottság kijelentette, hogy ha a magatartási kódexet nem tartják be, további szabályozási intézkedésekre kerülhet sor. Döntő fontosságú lesz az intézkedések

eredményességének megállapítása, különösen annak meghatározása, miként mérik a bizalom, az átláthatóság és az elszámoltathatóság terén elért javulást.

Szintén kihívást jelent majd megtalálni annak módját, hogyan lehetne javítani a félretájékoztatás felderítésén, elemzésén és kommunikálásán[190]. Szükség lesz a nyílt adatforrások aktív és stratégiai nyomon követésére és elemzésére is[191]. A fenyegetettségi környezet jobb átlátására irányuló erőfeszítések során figyelmet kell fordítani a kialakulóban lévő tendenciákra – például a „deepfake" videókra (mesterséges intelligencia és mélyreható gépi tanulás segítségével készített hamis videók) –, valamint az észlelésükhöz szükséges eszközökre is.

Az önállóság növelése

116 Az Unió nettó importőr a kiberbiztonsági termékek és szolgáltatások terén, ami növeli a nem uniós gazdasági szereplőkkel szembeni technológiai függőség és sebezhetőség kockázatát[192]. Ez a helyzet különösen kedvezőtlen az Unió kritikus infrastruktúrájának biztonsága szempontjából, amelyet összetett globális ellátási láncok is támogatnak. A kockázatot tovább súlyosbítja, amikor nem uniós gazdasági szereplők európai kiberbiztonsági vállalkozásokat vásárolnak fel. A közvetlen külföldi befektetések (FDI) átvilágításáért a tagállamok felelősek, uniós szintű átvilágítási mechanizmus jelenleg nem létezik[193].

117 A nagyobb stratégiai autonómia az EU globális stratégiájának célkitűzései közé tartozik, és ilyenként szerepel az *Ellenálló képesség, elrettentés, védelem* című 2017. évi közleményben[194] is. Az e jelentésben bemutatott számtalan kihívás megoldása segíteni fog a kívánt autonómia megvalósításában. Önmagában azonban egyetlen intézkedés sem képes erre.

Átgondolandó kérdések – Eredményes reagálás

- Hogyan javította a kiberbiztonsági irányelv a kiberbiztonsági eseményekkel kapcsolatos értesítéseket a kritikus ágazatokban és azokon túl?
- Mennyire eredményesen végzik az uniós intézmények a jelentős kiberbiztonsági eseményekkel kapcsolatos válságkezelési koordinációt?
- Hogyan játszhatna nagyobb szerepet a kiberdiplomácia az Unió külső fellépéseiben?
- A félretájékoztatás kezelésével foglalkozó jelenlegi uniós struktúrák és fellépések arányosak-e a probléma nagyságrendjével és összetettségével?

Záró gondolatok

118 Az elmúlt években az Unió és tagállamai az általános kibertámadásokkal szembeni reziliencia javítása érdekében előbbre sorolták napirendjükön a kiberbiztonság kérdését. Az uniós kiberbiztonság szintjének növelése ugyanakkor továbbra is monumentális feladatot jelent. E tájékoztatóban rá kívántunk mutatni néhányra azon főbb kihívások közül, amelyekkel az Uniónak szembe kell néznie, ha valóban a világ legbiztonságosabb digitális környezetévé akar válni.

119 Áttekintésünkből kiderül, hogy az érdemi **elszámoltathatóság és értékelés** biztosítása érdekében el kell mozdulni az értékelési gyakorlatokon alapuló teljesítménykultúra felé. Továbbra is vannak **rések a jogi keretben, és a tagállamok nem ültetik át következetesen a meglévő jogszabályokat**. Mindez megnehezítheti a jogszabályok hatásának maximális érvényesítését. Szintén kihívást jelent a **beruházási szintek és a stratégiai célok összehangolása**, ahhoz ugyanis növelni kell a kiberbiztonságba történő beruházások szintjét és hatását. Ez még nehezebb akkor, ha az Unió és tagállamai nem rendelkeznek **világos áttekintéssel az uniós kiberbiztonsági kiadások** felett. A megállapítások szerint **a kibervédelemhez kapcsolódó tevékenységet folytató uniós ügynökségek nem rendelkeznek a szükséges erőforrásokkal**, többek között nehézségekkel küzdenek a tehetséges munkaerő bevonzása és megtartása terén.

120 Egyes elérhető tanulmányok szerint **a kiberbiztonsági irányítás megerősítése** elősegíti, hogy a globális közösség jobban tudjon reagálni a kibertámadásokra és a váratlan eseményekre. Ugyanakkor lehetetlen megelőzni az összes támadást. Ezért kulcsfontosságú feladatot jelent a **gyors észlelés és reagálás**, a **kritikus infrastruktúrák és társadalmi funkciók védelme**, valamint a köz- és a magánszféra közötti **információcsere és koordináció** javítása. Végezetül a globális kiberbiztonsági készségek fokozódó elégtelenségére tekintettel létfontosságú **a készségek fejlesztése és a tudatosság növelése** is, minden ágazatban és a társadalom minden szintjén.

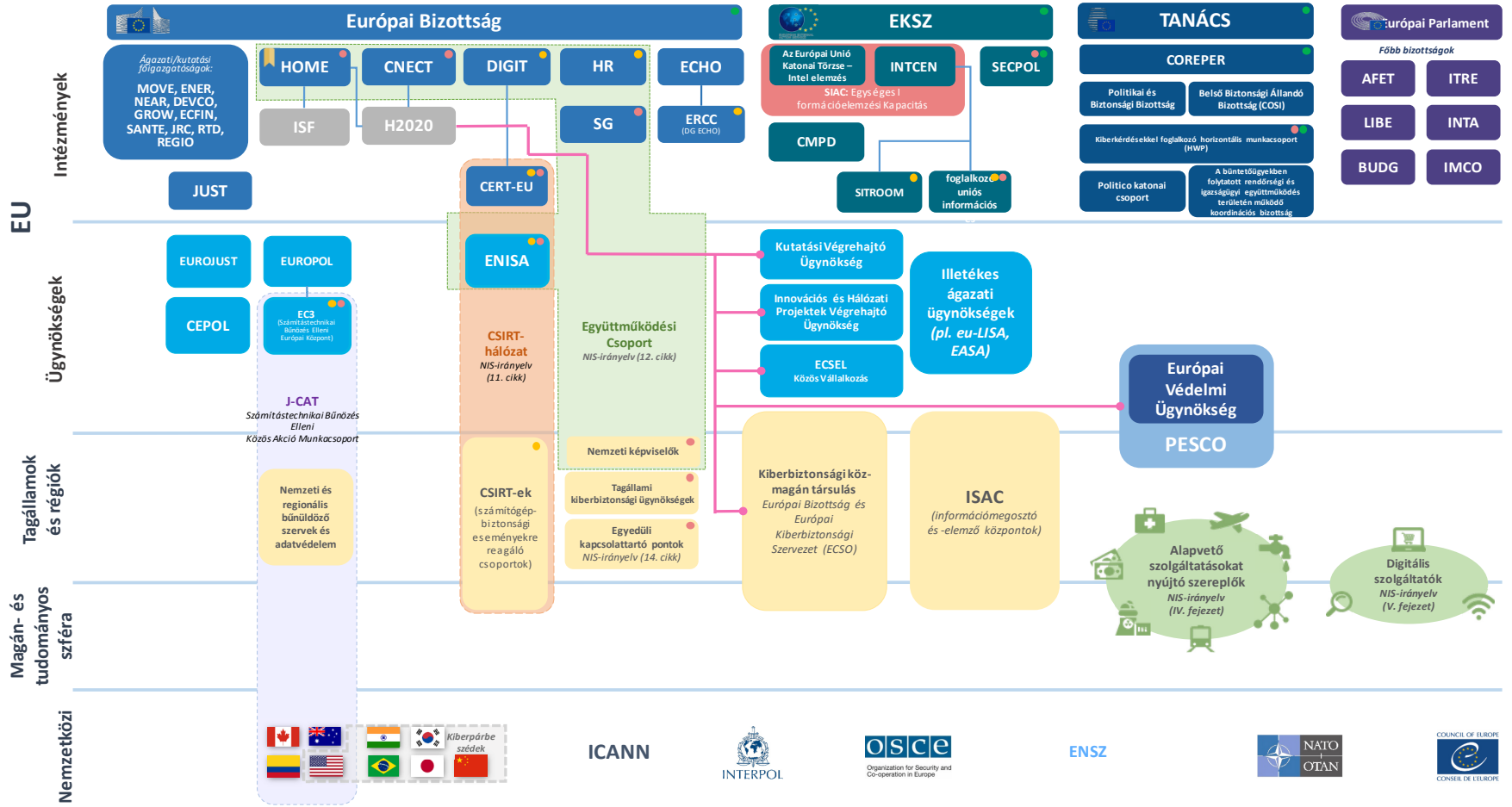
121 Mindezek az Unióval szembeni kiberfenyegetések és a tágabb értelemben vett globális környezet által jelentett kihívások folyamatos elkötelezettséget igényelnek és elengedhetetlenné teszik az Unió értékeihez való feltétlen ragaszkodást.

Ezt a tájékoztatót 2019. február 14-i ülésén fogadta el a III. Kamara.

a Számvevőszék nevében

Klaus-Heiner Lehne
elnök

I. melléklet — Összetett, többrétegű kép számos szereplővel



A 2017. évi uniós tervezet (***Blueprint***) szerinti együttműködési szintek a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálás érdekében; közös helyzetismeret és nyilvános kommunikáció

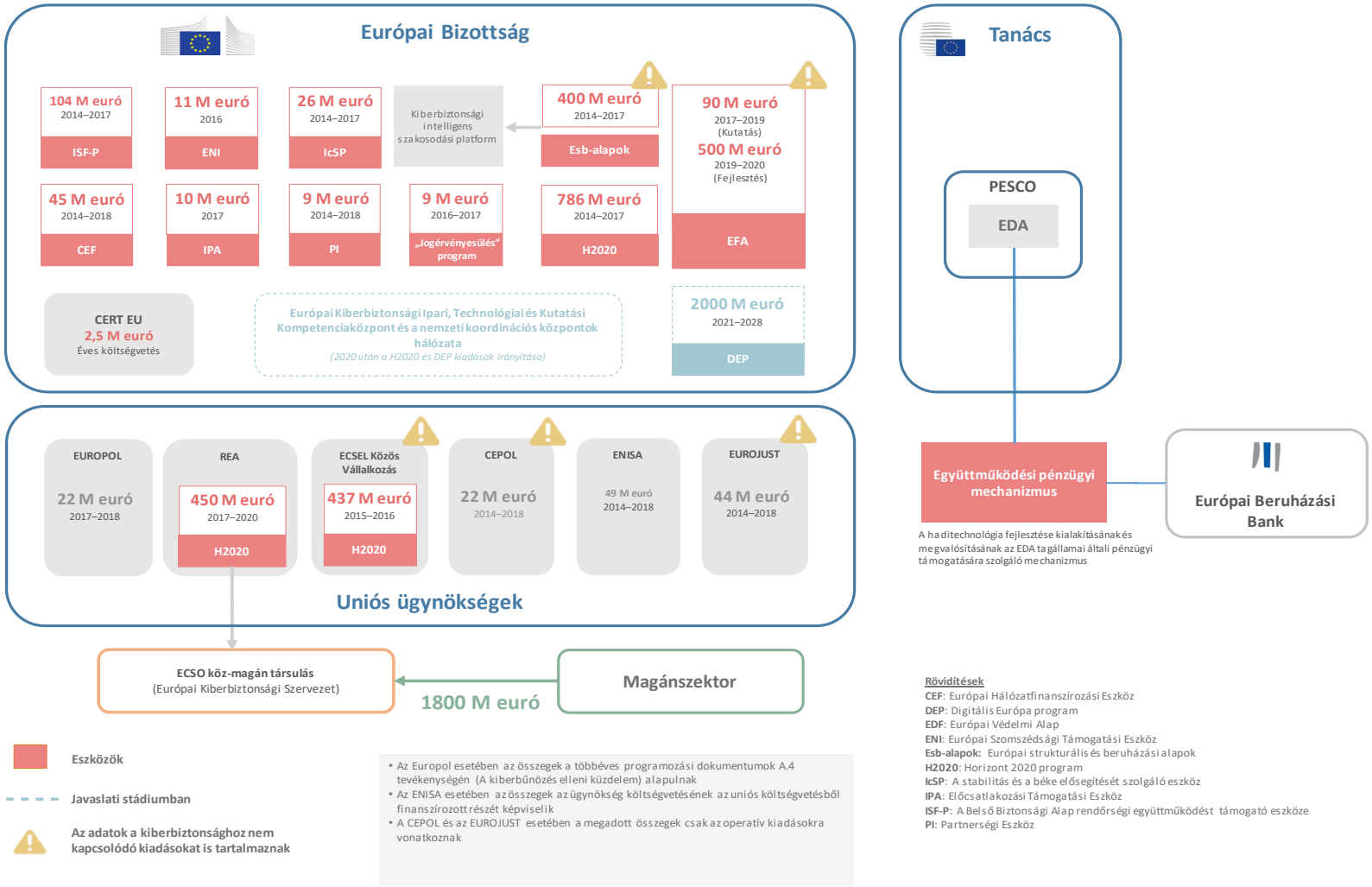
- **Technikai** — Válság alatti incidenskezelés; incidensek monitorozása és felügyelete, ezen belül folyamatos fenyegetés- és kockázatértékelés
- **Operatív** — A politikai szintű döntéshozatal előkészítése; a kiberbiztonsági válságirányítás koordinálása; az uniós szintű következmények és hatás értékelése
- **Politikai** — A válság kiberbiztonsági és nem kiberbiztonsági szempontjainak stratégiai és politikai irányítása, beleértve a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéhez (kiberdiplomáciai eszköztár) tartozó intézkedéseket

Elsődleges kiadások a H2020 programból
A DG HOME-nál működik a Biztonsági Unióval foglalkozó munkacsoport titkársága

Megjegyzés: A CERT-EU intézményközi megállapodás 11 uniós intézményre és szervre, valamint 37 uniós ügynökségre terjed ki

Forrás: Európai Számvevőszék.

II. melléklet — Az Unió kiberbiztonsággal kapcsolatos kiadásai 2014 óta



Forrás: Európai Számvevőszék, az Európai Bizottság és az uniós ügynökségek dokumentumai alapján.

III. melléklet — Az uniós tagállamok számvevőszékeinek jelentései

Típus	Cím (és hiperhivatkozás)	Év	Tagállam
Szabályszerűségi ellenőrzések	Belső ellenőrzési értékelési feljegyzés	2014	FR
	Az általános szociális biztonsági rendszer számláira vonatkozó tanúsítási jelentés (védelem,külügyek)	2016	FR
	Az állami beszámoló tanúsítása	2016	FR
	A kritikus jelentőségű észt nemzeti adatbázisok biztonságának és megőrzésének biztosítása	2018 vége / még nem jelent meg	EE
	A belső ellenőrzések eredményessége a nemzeti adatbázisokban tárolt személyes adatok védelme terén	2008	EE
Teljesítményellenőrzések/Értékarányossági ellenőrzések	Jelentés a számítógépes támadások visszaszorításáról	2013	DK
	RIR 2014:23 Információbiztonság a polgári közigazgatásban	2014	SE
	Jelentés a személyek és a vállalatok bizalmas adatainak a kormány általi feldolgozásáról	2014	DK
	Nemzeti kiberbiztonsági program	2014	UK
	Jelentés a Német Szövetségi Parlament Költségvetési Bizottságának a szövetségi költségvetési törvénykönyv (BHO) 88. §-ának 2. bekezdése alapján – informatikai konszolidáció, szövetségi kormány	2015	DE
	Jelentés a dán társadalom részére alapvető szolgáltatások nyújtását támogató informatikai rendszerekhez való hozzáférésről	2015	DK
	Plaine de France köztervezési hatóság	2015	FR
	Kiberbiztonsági környezet Litvániában litván nyelvű verzió angol nyelvű összefoglaló	2015	LT
	Az állami szervek teljesítménye a lengyelországi kiberbiztonsági feladatok ellátása terén (lengyel nyelven)	2015	PL
	RIR 2015:21 Kiberbűnözés – a rendőrség és az ügyészek hatékonysága növelhető	2015	SE
	A digitális készségek hiánya a kormánynál (felmérés)	2015	UK

Típus	Cím (és hiperhivatkozás)	Év	Tagállam
	Jelentés a Szövetségi Parlamentnek: Szövetségi pénzügyek: az örökösödési adó beszedése	2016	BE
	Jelentés a külső szolgáltatókhoz kiszervezett rendszerek informatikai biztonságának irányításáról	2016	DK
	Ellenőrzési jelentés az Állami Hitelintézet 2016. évi hiteltevékenységéről	2016	ES
	A Kormányzati Biztonsági Hálózat irányítása	2016	FI
	A közfeladatok ellátásához használt informatikai rendszerek biztonságának biztosítása	2016	PL
	A kiberzaklatás megelőzése és felszámolása a gyermekek és a fiatalok körében	2016	PL
	Kilenc ügynökség információbiztonsági tevékenysége – Egy további ellenőrzés az állami információbiztonságról. RiR 2016:8	2016	SE
	Az információk védelme a kormányzati szerveknél	2016	UK
	Jelentés az informatikai rendszerek és egészségügyi adatok védelméről három dán régióban	2017	DK
	Feljegyzés „A belső ellenőrzések eredményessége a nemzeti adatbázisokban tárolt személyes adatok védelme terén” című nemzetközi párhuzamos ellenőrzés eredményeiről	2017	EE
	Kibervédelmi intézkedések	2017	FI
	Az elektronikus szolgáltatások működési megbízhatóságának irányítása	2017	FI
	A mezőgazdasági kamarák hálózata (összefoglalás)	2017	FR
	A Vaucluse-i Kereskedelmi és Iparkamara (készítette: PACA régió, Regionális Könyvvizsgálói Kamara)	2017	FR
	A kritikus jelentőségű észt nemzeti adatbázisok biztonságának és megőrzésének biztosítása	2018 vége / még nem jelent meg	EE
	Az állami elektronikus hírközlési infrastruktúra fejlesztése litván nyelvű verzió angol nyelvű összefoglaló	2017	LT

Típus	Cím (és hiperhivatkozás)	Év	Tagállam
	Információtechnológiai ellenőrzés:Kiberbiztonság a kormányzati szerveknél	2017	MT
	A nemzeti nyilvántartási rendszer: biztonság, teljesítmény és használhatóság	2017	PL
	A WannaCry incidens	2017	UK
	Online csalás	2017	UK
	Jelentés a zsarolóprogram-támadások elleni védelemről	2018	DK
	Az Arpajon kórház (Île-de-France Régió Regionális Kamarája)	2018	FR
	A kritikus állami információs források kezelése	2018	LT
	Elektronikus bűncselekmények	2019	LT
	Információbiztonság Lengyelországban	2019	PL
Egyéb	Közintézmények adatbázisa	n.a.	BE
	Kérdőív a biztonsági és kockázatelemzési szakpolitikáról (folyamatban)	n.a.	BE

Betűszók és rövidítések

CERT-EU: a számítógépes vészhelyzeteket elhárító csoport

cPPP: szerződéses köz-magán társulás

CSIRT: számítógép-biztonsági eseményekre reagáló csoport

DDoS: elosztott szolgáltatásmegtagadással járó támadás (Distributed Denial of Service)

DEP: Digitális Európa program

DG CNECT: A Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága

DG DIGIT: Informatikai Főigazgatóság

DG HOME: Migrációügyi és Uniós Belügyi Főigazgatóság

DG JUST: Jogérvényesülési és Fogyasztópolitikai Főigazgatóság

EC3: az Europol Számítástechnikai Bűnözés Elleni Európai Központja

ECA: Európai Számvevőszék

ECSEL: Kiváló Európai Elektronikai Alkatrészek és Rendszerek

ECSM: a kiberbiztonság-tudatosság európai hónapja

ECSO: Európai Kiberbiztonsági Szervezet

EDA: Európai Védelmi Ügynökség

EKSZ: Európai Külügyi Szolgálat

ENISA: Európai Uniós Hálózat- és Információbiztonsági Ügynökség

ESA: európai felügyeleti hatóság

Esb-alapok: európai strukturális és beruházási alapok

EU: Európai Unió

FDI: közvetlen külföldi tőkebefektetés

GDPR: általános adatvédelmi rendelet

HWPCI: kiberkérdésekkel foglalkozó horizontális munkacsoport

ICS: Ipari kontrollrendszerek

ISF-P: a Belső Biztonsági Alap rendőrségi együttműködést támogató eszköze

ISSB: információbiztonsági irányítóbizottság

JRC: Közös Kutatóközpont

KBVP: közös biztonság- és védelempolitika

Kiberbiztonsági (NIS) irányelv: a hálózati és információs rendszerek biztonságáról szóló irányelv

Kkv: kis- és középvállalkozás

LISO: helyi információbiztonsági tisztviselő

NAO: nemzeti számvevőszék

NCIRC: a NATO kiberbiztonsági eseményeket kezelő képessége

PESCO: állandó strukturált együttműködési keret

Glosszárium

A kibertér által katalizált bűncselekmény: Hagyományos, azonban informatikai rendszerek felhasználása révén nagyobb léptékben elkövetett bűncselekmény.

Adathalászat (phishing): Látszólag megbízható forrásból származó e-mailek küldése annak érdekében, hogy a címzettet csalárd módon rábírják arra, hogy rosszindulatú linkekre kattintson vagy megossza személyes adatait.

Bizalmi szolgáltatások: Az elektronikus tranzakciók jogi hitelességét javító szolgáltatások: például elektronikus aláírás, pecsétek, időbélyegzők, regisztrált kézbesítési és weboldal-hitelesítés.

Botnet (zombihálózat): Rosszindulatú szoftverekkel megfertőzött számítógépek hálózata, amelyet távoli vezérléssel, a felhasználók tudta nélkül levélszemét (spam) küldésére, információk ellopására vagy összehangolt kibertámadások indítására használnak fel.

Digitális tartalom: Minden olyan adat – például szöveg, hang, kép vagy videó –, amelyet digitális formában tárolnak.

Dolgok internete (Internet of Things): Az interneten keresztül történő kommunikációt és adatcserét lehetővé tevő elektronikával, szoftverrel és szenzorokkal ellátott mindennapi tárgyakból álló hálózat.

Elosztott szolgáltatásmegtagadással járó támadás (Distributed Denial of Service, DDoS): Olyan kibertámadás, amely bizonyos online szolgáltatásokat vagy erőforrásokat elérhetetlenné tesz a jogszerű felhasználók számára azáltal, hogy kezelhetetlen mennyiségű kéréssel árasztja el azokat.

Felhőalapú számítástechnika: IT-eszközök – például tárhely, számítási teljesítmény vagy adatmegosztási kapacitás — keresletalapú rendelkezésre bocsátása az interneten, távoli szervereken történő tárhelyszolgáltatás révén.

Félretájékoztatás: Olyan igazolhatóan hamis vagy félrevezető információ, amelyet gazdasági haszonszerzés vagy a nyilvánosság szándékos megtévesztése céljából hoznak létre, tesznek közzé és terjesztenek, és amely kárt okozhat a közérdeknek.

Fölözés (skimming): A hitel- vagy betéti kártya adatainak ellopása az online bevitel során.

Hacktivista: Olyan egyén vagy csoport, amely társadalmi vagy politikai célok elérése érdekében jogosulatlan hozzáférést nyer bizonyos információs rendszerekhez vagy hálózatokhoz.

Hálózatbiztonság: A kiberbiztonság egyazon hálózaton lévő eszközökön keresztül továbbított adatok védelmével foglalkozó része, amely célja annak biztosítása, hogy az információkat ne szerezhessék meg, illetve módosíthassák.

Hibrid fenyegetés: Ellenséges szándék kifejezése hagyományos és nem hagyományos hadviselési technikák (katonai, politikai, gazdasági és technológiai módszerek) célirányos keverékének alkalmazásával.

Hozzáférési adatok: A felhasználók szolgáltatásokba való be- és kijelentkezéseire vonatkozó információk, például időpont, dátum és IP-cím.

Információbiztonság: A fizikai és digitális adatok jogosulatlan hozzáféréstől, felhasználástól, közzétételtől, zavarástól, módosítástól, rögzítéstől és megsemmisítéstől való védelmét szolgáló folyamatok és eszközök összessége.

Kártevőterjesztő (exploit) készlet: A kiberbűnözők általi felhasználásra szánt eszközkészletek egy típusa, amely a hálózati és információs rendszerek sebezhetőségeit támadja rosszindulatú szoftverek terjesztése vagy egyéb rosszindulatú tevékenységek céljából.

Kiberbiztonság: Az informatikai rendszerek és adatok jogosulatlan hozzáféréssel, támadásokkal és károkozással szembeni védelme céljából, azok rendelkezésre állásának, bizalmas kezelésének és sértetlenségének biztosítása érdekében elfogadott biztosítékok és intézkedések összessége.

Kiberbiztonsági esemény: Olyan esemény, amely közvetlenül vagy közvetve károsítja vagy veszélyezteti egy informatikai rendszer, illetve az abban feldolgozott, tárolt vagy továbbított adatok ellenálló képességét és biztonságát.

Kiberbűncselekmény-szolgáltatás (Crime-as-a-Service, CAAS): A digitális feketegazdaság hajtóerejét jelentő, bűncselekménynek minősülő üzleti modell, amely kereskedelmi szolgáltatások és eszközök széles körét biztosítja a szükséges készségekkel nem rendelkező, kezdő kiberbűnözők számára kiberbűncselekmények elkövetéséhez.

Kiberbűnözés: Olyan bűncselekmények, amelyek elsődleges eszköze vagy elsődleges célja számítógépekhez és informatikai rendszerekhez kapcsolódik. Ezek lehetnek hagyományos bűncselekmények (pl. csalás, hamisítás és személyazonosság-lopás), tartalommal kapcsolatos bűncselekmények (pl. gyermekpornográfia online terjesztése

vagy fajgyűlöletre uszítás), vagy kifejezetten a számítógépekkel és információs rendszerekkel kapcsolatos bűncselekmények (pl. információs rendszerek elleni támadások, szolgáltatásmegtagadással járó támadások vagy rosszindulatú szoftverek).

Kiber-ökoszisztéma: Egymással kapcsolatban álló eszközök, adatok, hálózatok, emberek, folyamatok és szervezetek, valamint az ezeket a kölcsönhatásokat befolyásoló és támogató folyamatok és technológiák összetett közössége.

Kibertámadás: Adatok vagy számítógépes rendszerek bizalmas jellegének, sértetlenségének és rendelkezésre állásának a kibertéren keresztüli gyengítésére vagy megsemmisítésére irányuló kísérlet.

Kibertámadásokkal szembeni reziliencia: A kibertámadások és a váratlan események megelőzésére és elhárítására, az azokra való felkészülésre, illetve hatásaik felszámolására való képesség.

Kibertér: Az immateriális globális környezet, amelyben számítógépes hálózatokon és technológiai eszközökön keresztül online kommunikáció folyik emberek, szoftverek és szolgáltatások között.

Kibertér-specifikus bűncselekmény: Olyan bűncselekmény, amelyet csak informatikai eszközökkel lehet elkövetni.

Kibervédelem: A kiberbiztonság egy alkategóriája, amelynek célja a kibertér katonai és egyéb megfelelő eszközökkel történő védelme katonai-stratégiai célok elérése érdekében.

Kriptovaluta: Olyan digitális eszköz, amelyet titkosítási technikák alkalmazásával, a központi bankoktól függetlenül bocsátanak ki és cserélnek, és amelyet egy-egy virtuális közösség tagjai egymás közötti fizetési módként elfogadnak.

Kritikus infrastruktúra: Olyan fizikai erőforrások, szolgáltatások és létesítmények, amelyek megzavarása vagy megsemmisítése súlyos következményekkel járna a gazdaság és a társadalom működésére nézve.

Örökölt rendszer (legacy system): Elavult vagy már nem korszerű számítógépes rendszer, alkalmazás vagy programozási nyelv, amely még használatban van, de amelyhez már nem elérhető frissítés és beszállítói (többek között biztonsági) támogatás.

Patch-szolgáltatás: Egy szoftver kapcsán végrehajtott módosítássorozat, amelynek célja annak frissítése, megjavítása vagy fejlesztése, így többek között a biztonsági sebezhetőségek orvoslása.

Pszichológiai manipuláció (social engineering): Az információbiztonság területén a kifejezés arra utal, amikor a sértettet megtévesztés révén ráveszik bizonyos cselekvések végrehajtására vagy bizalmas információk felfedésére.

Reklámprogram (adware): Rosszindulatú szoftver, amely az áldozatok online magatartását követő kódot tartalmazó reklámtranszparenseket vagy felugró ajánlatokat jelenít meg.

Rendelkezésre állás: Az információk időbeni és megbízható hozzáférhetőségének és használhatóságának biztosítása.

Rosszindulatú szoftver (malware): Kártékony szoftver, azaz a számítógépekben, szerverekben vagy hálózatokban való károkozásra irányuló számítógépes program.

Sebezhetőség-kezelés: A számítógépes és hálózati biztonság szerves része, célja a rendszer- és szoftversebezhetőségek kihasználásának proaktív enyhítése vagy megelőzése azok azonosítása, osztályozása és helyreállítása révén.

Sértetlenség: Az információk jogosulatlan módosítás és megsemmisítés elleni védelme és valódiságának garantálása.

Személyes adatok: Egy azonosítható személlyel kapcsolatos információk.

Szövegvektorizálás: Szavak, mondatok és teljes dokumentumok numerikus vektorokká való átalakítása a gépi tanulási algoritmusok általi felhasználás lehetővé tétele érdekében.

Titkosítás: Olvasható információk nem olvasható kóddá alakítása azok védelme érdekében. Az információk megtekintéséhez a felhasználónak titkos kulccsal vagy jelszóval kell rendelkeznie.

Titoktartás: Az információk, adatok és eszközök jogosulatlan hozzáféréstől és nyilvánosságra hozataltól való védelme.

Törlőprogram (wiper): Rosszindulatú számítógépes program, amely törli a megfertőzött számítógép merevlemezét.

Választási infrastruktúra: A kampányok informatikai rendszerei és adatbázisai, a jelöltekre vonatkozó érzékeny információk, a választók nyilvántartásba vétele és irányítási rendszerek.

Zsarolóprogram (ransomware): Rosszindulatú szoftver, amelyek megtagadja a sértettől a számítógépes rendszerhez való hozzáférést, vagy olvashatatlanná teszi

(általában titkosítja) a fájlokat. A támadó ezután rendszerint megzsarolja a sértettet azáltal, hogy váltságdíjhoz köti a hozzáférés visszaállítását.

[1] Az uniós kiberbiztonsági jogszabálytervezet meghatározása szerint a kiberbiztonság „mindazon tevékenységek [halmazát jelenti], amelyek a hálózati és információs rendszereknek, azok felhasználóinak és az érintett személyeknek a kiberfenyegetésekkel szembeni védelméhez szükségesek.” A jogszabályt várhatóan 2019 elején fogadja el az Európai Parlament és a Tanács.

[2] Europol: *Internet Organised Crime Threat Assessment 2017* (Az internetes szervezett bűnözés általi fenyegetettség értékelése, 2017).

[3] Európai Kiberbiztonsági Szervezet (ECSO): *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership* (Az európai kiberbiztonsági ágazat javaslata egy szerződéses köz-magán társulás létrehozására), 2016. június.

[4] Európai Parlament: *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses* (Kiberbiztonság az Európai Unióban és azon túl: Fenyegetések és szakpolitikai megoldások). Tanulmány a LIBE bizottság számára, 2015. szeptember.

[5] ENISA: *ENISA Threat Landscape Report 2017* (Az ENISA fenyegetettségi helyzetjelentése, 2017), 2018. január 18.

[6] Europol: *Internet Organised Crime Threat Assessment 2018* (Az internetes szervezett bűnözés általi fenyegetettség értékelése, 2018).

[7] Europol: *uo.*, 2018.

[8] European Centre for Political Economy: *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?* (Gondolatlenyúlás: Visszatarthatja-e Európát a kiberkémkedés az ipari versenyképességért folyó globális versenyben?), 2/18. sz. eseti kiadvány, 2018. február.

[9] Európai Bizottság: Az Elnök 2017. évi értékelő beszéde az Unió helyzetéről.

[10] Europol: *World’s Biggest Marketplace selling internet paralysing DDoS attacks taken down* (Leszerelték a világ legnagyobb internetbénító DDoS támadásokat forgalmazó piacterét), sajtóközlemény, 2018. április 25.

[11] Europol: *Internet Organised Crime Threat Assessment 2017* (Az internetes szervezett bűnözés általi fenyegetettség értékelése, 2017).

[12] Európai Bizottság: Tájékoztató a kiberbiztonságról, 2017. szeptember.

[13] Ilyen költség lehet többek között a bevételkiesés, a károsodott rendszerek helyreállítási költségei, az ellopott eszközökért vagy információkért való esetleges felelősség, az ügyfelek megtartását célzó ösztönzők, a magasabb biztosítási díjak, a védelmi költségek növekedése (új rendszerek, alkalmazottak, képzések), valamint az esetleges jogszabályi megfelelési és perköltségek.

[14] NTT Security: *Risk:Value 2018 Report* (Kockázat/érték, 2018. évi jelentés).

[15] A *WannaCry* zsarolóprogram a Microsoft Windows protokoll hiányosságait kihasználva tette lehetővé a számítógépek kontrolljának távoli átvételét. A Microsoft a sebezhetőség felfedezését követően javítócsomagot (patch) adott ki annak orvoslására. Több százezer számítógépen azonban nem végezték el a frissítést, és ezek közül sok megfertőződött. Forrás: A. Greenberg: *Hold North Korea Accountable For WannaCry—and the NSA, too* (WannaCry: a felelős Észak-Korea – és az NSA), WIRED, 2017. december 19.

[16] Európai Bizottság: *Europeans' attitudes towards cybersecurity* (Az európaiak hozzáállása a kiberbiztonsághoz), Eurobarométer 464a. különkiadás, 2017. szeptember. 2019 elején várhatóan nyomonkövetési jelentés közzétételére kerül sor.

[17] A Budapesti Egyezmény kötelező erejű nemzetközi iránymutatás a kiberbűnözés elleni jogszabályokat kidolgozó országok számára, amely keretet biztosít az állami felek közötti nemzetközi együttműködés számára. Az Európai Uniót jelenleg a Bizottság, az Európai Unió Tanácsa, az Europol, az ENISA és az Eurojust képviseli.

[18] Európai Bizottság: *Az Európai Unió kiberbiztonsági stratégiája: nyílt, megbízható és biztonságos kibertér*. JOIN(2013) 1 final, 2013. február 7.

[19] Európai Bizottság: *Az európai biztonsági stratégia*. COM(2015) 185 final, 2015. április 28.

[20] Európai Bizottság: *Európai digitális egységes piaci stratégia*. COM(2015) 192 final, 2015. május 6.

[21] EKSZ: *Közös jövőkép, közös fellépés: Erősebb Európa – Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan*, 2016. június.

[22] Európai Politikai Tanulmányok Központja: *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force* (Az EU kibervédelmi kapacitásának megerősítése – A CEPS munkacsoport jelentése), November 2018.

[23] Az Egyesült Államok, az Egyesült Királyság és Ausztrália által Észak-Koreának tulajdonított WannaCry zsarolóprogram-támadás mögötti rosszindulatú szoftvert eredetileg az Egyesült Államok Nemzetbiztonsági Ügynöksége fejlesztette ki saját célra a Windows sebezhetőségeinek kihasználása érdekében. Forrás: A. Greenberg: uo., WIRED, 2017. december 19. A támadások után a Microsoft elítélte azt a gyakorlatot, hogy egyes kormányok megtartják maguknak a szoftversebezhetőségekhez kapcsolódó információkat, és megismételte a Digitális Genfi Egyezmény létrehozására irányuló felhívását, amelynek szükségességét ezúton is hangsúlyozta.

[24] A másik négy a szárazföld, a tenger, a levegő és az űr.

[25] Uniós kibervédelmi szakpolitikai keret (2018. évi frissített változat), 14413/18, 2018. november 19.

[26] Európai Bizottság/Európai Külügyi Szolgálat: *A hibrid fenyegetésekkel szembeni fellépés közös kerete – európai uniós válasz*. JOIN(2016) 18 final, 2016. április 6.

[27] Az Európai Tanács elnökének, az Európai Bizottság elnökének és az Észak-atlanti Szerződés Szervezete főtitkárának közös nyilatkozata, 2016. július 8. és 2018. július 10.

[28] Európai Bizottság/Európai Külügyi Szolgálat: *Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése*. JOIN(2017) 450 final, 2017. szeptember 13.

[29] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19, 1. o.).

[30] Az Európai Parlament és a Tanács 2016. július 6-i (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

[31] Ezek a csoportok az irányelv által létrehozott együttműködési struktúrákba – a CSIRT-hálózatba (az uniós tagállamok által kinevezett CSIRT csoportokból és a CERT-EU-ból álló hálózat, amely titkárságának az ENISA ad otthont) és az együttműködési csoportba (a tagállamok közötti stratégiai együttműködést és információcserét támogató és elősegítő csoport, amely titkárságának a Bizottság ad otthont) – illeszkednek.

[32] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

[33] Az Európai Bizottság javaslata: Az Európai Parlament és a Tanács rendelete 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, 2017. szeptember 13.

[34] Az Európai Bizottság javaslata: Az Európai Parlament és a Tanács rendelete a büntetőügyekben hozott elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról. COM (2018) 225 final, 2018. április 17.

[35] Az Európai Bizottság javaslata: Az Európai Parlament és a Tanács irányelve a jogi képviselőknek a büntetőeljárásban bizonyítékok összegyűjtése céljából történő kinevezéséről szóló harmonizált szabályok meghatározásáról. COM (2018) 226 final, 2018. április 17.

[36] Az Európai Bizottság javaslata: Az Európai Parlament és a Tanács rendelete az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról. COM(2018) 630 final, 2018. szeptember 12.

[37] H. Carrapico, A. Barrinha: *The EU as a Coherent (Cyber)Security Actor?* (Az EU mint koherens (kiber)biztonsági szereplő?), Journal of Common Market Studies, Vol. 55, No. 6, 2017.

[38] Európai Bizottság: uo., SWD(2017) 295 final, 2017. szeptember 13.

[39] Az Európai Parlament Kutatószolgálata: *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects* (Transzatlanti kiberbizonytalanság és kiberbűnözés. Gazdasági hatás és kilátások), PE 603.948, 2017. december.

[40] ENISA: *An evaluation framework for Cyber Security Strategies* (A kiberbiztonsági stratégiák értékelési kerete), 2014. november 27.

[41] Ez alól kivételt jelent az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról szóló, 2013. augusztus 12-i 2013/40/EU európai parlamenti és tanácsi irányelv 14. cikke („Nyomon követés és statisztika”).

[42] Európai Gazdasági és Szociális Bizottság: *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks* (Kiberbiztonság: a magánszektor fokozódó kiberkockázatokkal szembeni tudatosságának és rezilienciájának biztosítása Európa-szerte), 2018. március. CEPS-ECRI Task Force: Cybersecurity in Finance: Getting the policy mix right! (Kiberbiztonság a pénzügy területén: A helyes szakpolitikai kombináció kialakítása), 2018. június.

[43] 28-ból 24 tagállami számvevőszék válaszolt a felmérésünkre.

[44] Vagyis elvalapú és minél technológiasemlegesebb.

[45] Az Európai Bizottság tudományos tanácsadási mechanizmusának 2/2017. számú tudományos véleménye, 2017. március 24.

[46] L. Rebuffi: *EU Digital Autonomy: A possible approach* (Az EU digitális autonómiája: egy lehetséges megközelítés), Digma Zeitschrift für Datenrecht und Informationssicherheit, 2018. szeptember. European Centre for Political Economy: uo., 2/18. sz. alkalmi kiadvány, 2018. február.

[47] Az Európai Bizottság javaslata: *Az Európai Parlament és a Tanács irányelve a digitálistartalom-szolgáltatásra irányuló szerződések egyes vonatkozásairól*. COM(2015) 634 final, 2015. december 9.

[48] Az Európai Bizottság javaslata: *Az Európai Parlament és a Tanács irányelve az áruk internetes és egyéb távértékesítésére irányuló szerződések egyes vonatkozásairól*. COM(2017) 635 final, 2015. december 9.

[49] Dutch Cyber Security Council: *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care* (Holland kiberbiztonsági tanács: Európai Elővigyázatossági Kiberbiztonsági Találkozó, 2016: A köz-magán tudományos szervezetek ajánlásai az Európai Bizottságnak a dolgok internetéről és a gondossági kötelezettségek összehangolásáról), 2016.

[50] Európai Politikai Tanulmányok Központja: *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force* (A szoftversebezhetőségek nyilvánosságra hozatala Európában: Technológia, politikák és jogi kihívások – a CEPS munkacsoport jelentése), 2018. június.

[51] Európai Bizottság: *A kiberbiztonsági irányelv maximális kihasználása – a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 1148/2016/EU irányelv hatékony végrehajtása felé*. COM(2017) 476 final/2, 2017. október 4.

[52] Europol: uo., 2017.

[53] Az Európai Unió Tanácsa: *Zárójelentés a kölcsönös értékelések hetedik fordulójáról: „A számítástechnikai bűnözés megelőzését és az ellene folytatott küzdelmet érintő európai szakpolitikák gyakorlati végrehajtása és működése*, 12711/1/17 REV 1, 2017. október 9.

[54] Európai Bizottság: *Impact assessment accompanying the document Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment* (A készpénz-helyettesítő fizetési eszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló irányelvre irányuló javaslatot kísérő hatásvizsgálat), SWD(2017) 298 final, 2017. szeptember 13. 2018 decemberében politikai megállapodás született az új jogszabályról, amelyet várhatóan 2019 elején fogadnak el.

[55] Europol: uo., 2017.

[56] C-362/14: Maximillian Schrems kontra Data Protection Commissioner (Írország), 2015. október 6.

[57] Europol/Eurojust: *Common challenges in combating cybercrime* (Közös kihívások a kiberbűnözés elleni küzdelemben), 7021/17, 2017. március 13.

[58] Európai Bizottság: *Assessment of the EU 2013 Cybersecurity Strategy* (Az Európai Unió 2013. évi kiberbiztonsági stratégiájának értékelése), SWD (2017) 295 final, 2017. szeptember 13.

[59] Az Európai Parlament Kutatószolgálata: *Briefing: EU Legislation in Progress – Review of dual-use export controls* (Rövid tájékoztató: Folyamatban lévő uniós jogszabályok – A kettős felhasználású termékek exportellenőrzésének felülvizsgálata , PE589.832), PE589.832.

[60] Az Európai Parlament állásfoglalása: *Az emberi jogok és a technológia: megfigyelési rendszerek és hálózati behatoló rendszerek hatása az emberi jogokra a harmadik országokban* (2014/2232(INI)), 2015. szeptember 8. A kettős felhasználású termékek és szolgáltatások (köztük szoftverek és technológiák) polgári és katonai alkalmazásúak is lehetnek.

[61] A nyilvánosan elérhető információkat az ICANN (Bejegyzett Nevek és Számok Internetszervezete) által kezelt WHOIS adatbázisban tárolják. Az ICANN tartja fenn a domainnév-rendszert. A domainnevekkel való visszaélés megkönnyíti a kiberbűnözést.

[62] A kiberbiztonsági irányelv (uo.) 3. cikke.

[63] Atlantic Council, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures* (Kockázati nexus: Legyőznek a kiberkockázatok? Az alternatív kiberjövők gazdasági haszna és költségei) 2015. szeptember 10.

[64] The White House, *Cybersecurity spending fiscal year 2019* (Fehér Ház: Kiberbiztonsági kiadások a 2019. évi pénzügyi évben).

[65] Európai Bizottság: *Hatásvizsgálat, amely a következő dokumentumot kíséri: „Javaslat európai parlamenti és tanácsi rendeletre a Digitális Európa program 2021–2027 közötti időszakra történő létrehozásáról”*, SWD(2018) 305 final, 2018. június 6.

[66] The Hague Centre for Strategic Studies: *Dutch investments in ICT and cybersecurity: putting it in perspective* (Hágai Stratégiai Tanulmányi Központ: A holland IKT-beruházások és a kiberbiztonság: perspektíva), 2016. december.

[67] Európai Bizottság: uo., COM(2018) 630 final, 2018. szeptember 12.

[68] Az Európai Parlamenti Kutatási Szolgálat Jövőkutatási Osztálya: *Achieving a sovereign and trustworthy ICT industry in the EU* (Önálló és megbízható IKT-ágazat megvalósítása az Unióban), 2017. december.

[69] European Digital SME Alliance, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem* (Állásfoglalás az európai kiberbiztonsági stratégiáról: A kkv-k ökoszisztémájának megerősítése), 2017. július 31.

[70] Az Európai Parlament Kutatószolgálatának Jövőkutatási Osztálya: uo., 2017. december.

[71] Uo.

[72] European Commission, *Impact assessment on the proposed research competence centre and network of national coordination centres* (Hatásvizsgálat a javasolt kutatási kompetenciaközpontról és a nemzeti koordinációs központok hálózatáról), SWD(2018) 403 final (1/4. rész), 2018. szeptember 12.

[73] Európai Bizottság: uo., COM(2018) 630 final, 2018. szeptember 12.

[74] A Számvevőszék 13/2018. sz. különjelentése: A terrorizmushoz vezető radikalizáció kezelése.

[75] Az ebben a részben említett számadatok nyilvánosan elérhető bizottsági dokumentumokból származnak, az ***51. bekezdésben*** említett 42 millió eurós adat kivételével, amelyet közvetlenül a Bizottság bocsátott rendelkezésünkre.

[76] A Horizont 2020 az Unió 80 milliárd eurós kutatási és innovációs programja, amelynek célja az Unió globális versenyképességének biztosítását célzó Innovatív Unió támogatása.

[77] Horizont 2020 keretprogram, 7. társadalmi kihívás: „Biztonságos és innovatív társadalmak: Európa és polgárai szabadságának és biztonságának védelme”.

[78] A Horizont 2020-projekteket a CORDIS adatkészlet segítségével elemeztük. A JRC kiberbiztonsági osztályozási rendszerének felhasználásával elvégeztük az egyes projektek leírásainak szövegvektorizálását (lásd: ***5. háttérmagyarázat*** a következő fejezetben) azon projektek azonosítása céljából, amelyek valószínűsíthetően a kiberbiztonsághoz kapcsolódnak. Ezt követően manuálisan ellenőriztük és elemeztük az eredményeket.

[79] Európai Kiberbiztonsági Szervezet: *ECS cPPP Progress Monitoring Report 2016-2017* (ECS cPPP előrehaladási monitoringjelentés, 2016–2017), 2018. október 29.

[80] A kiberbiztonsági irányelv (uo.) 9. cikkének (2) bekezdése.

[81] A GLACY+ („a számítástechnikai bűnözés elleni globális fellépés plusz”) az Európa Tanáccsal közös projekt. Tizenkét afrikai, ázsiai és csendes-óceáni, valamint latin-amerikai és karibi országot támogat, amelyek ennek köszönhetően maguk is csomópontként szolgálhatnak és megoszthatják tapasztalataikat a saját régiójukban.

[82] Az Európai Politikai Stratégiai Központ (EPSC), a Bizottság agytrösztje felhívta a figyelmet arra, hogy „digitális holttér” keletkezhet, ha tovább nő az Unió és a nyugat-balkáni szomszédos országok közötti szakadék. Több ország (így Kína és Oroszország) jelentős összegeket fektet be a régióban, ami azzal a kockázattal jár, hogy az Unió mint kiberbiztonsági szereplő háttérbe szorul a térségben. Forrás: EPSC: *Engaging with the Western Balkans: an investment in Europe’s security*(Összefogás a Nyugat-Balkánnal: Beruházás Európa biztonságába), 2018. május 17.

[83] Európai Beruházási Bank: *The EIB Group Operating Framework and Operational Plan 2018* (Az EBB-csoport működési kerete és működési terve, 2018), 2017. december 12. Tájékoztatónk szerkesztésének időpontjában nem állt rendelkezésre több információ.

[84] Európai Bizottság: *Javaslat: Az Európai Parlament és a Tanács rendelete a Digitális Európa programnak a 2021–2027 közötti időszakra történő létrehozásáról*. COM(2018) 434 final, 2018. június 6.

[85] Európai Bizottság: *Az Európai Parlament és a Tanács (EU) 2018/1092 rendelete (2018. július 18.) az Unió védelmi iparának versenyképességét és innovációs képességét támogató európai védelmi ipari fejlesztési program létrehozásáról* (HL L 200., 2018.8.7., 30. o.). Emellett 2017-ben napvilágot látott egy védelmi kutatásra irányuló előkészítő intézkedés, amelyre a Horizont 2020 költségvetéséből összesen 90 millió eurót irányoztak elő a 2017–2019-es időszakra. Nem egyértelmű, hogy ez kibervédelemmel kapcsolatos kiadásokat is magában foglal-e.

[86] A Számvevőszék 2019-ben külön tájékoztatót tervez közzétenni az Unió védelméről.

[87] Az Europol EC3, az ENISA, az EKSZ, az Európai Védelmi Ügynökség és a CERT-EU személyi állománya összesen 159 fő. Ez nem tartalmazza az Európai Bizottság és a tagállamok kiberbiztonsági feladatokat végző alkalmazottait. Forrás: Európai Politikai Tanulmányok Központja: uo., 2018. november.

[88] *ENISA evaluation* (Az ENISA értékelése), 2017.

[89] Az Europol a 2018–2020-as időszakra vonatkozó többéves tervében 70 ideiglenes alkalmazottnyi éves létszámnövelést kért, azonban 2018-ra még csak 26 főt hagytak jóvá. A 2019–2021-es időszakra vonatkozó többéves tervének tervezetében az Europol csak szerény mértékű növelést irányzott elő, „feltételezve, hogy nagyobb erőforrásigény úgysem elégíthető ki.” Forrás: Konzultáció a 2019–2021-es időszakra vonatkozó többéves programozás tervezetéről (A 000834, 2018. február 1.). A dokumentumot a közös parlamenti ellenőrző csoportnak nyújtották be.

[90] *ENISA evaluation* (Az ENISA értékelése), 2017. 2014 és 2016 között az ENISA operatív költségvetésének mintegy 80%-át fordították tanulmányok készíttetésére.

[91] ENISA: *Exploring the opportunities and limitations of current Threat Intelligence Platforms* (Az aktuális fenyegetés-felderítési platformok lehetőségeinek és korlátainak feltárása), 2017. december.

[92] ISACA (korábbi nevén: Information Systems Audit and Control Association): *Information Security Governance: Guidance for Boards of Directors and Executive Management* (Információbiztonsági irányítás: Az igazgatótanácsokra és a vezetőségre vonatkozó iránymutatás), 2. kiadás, 2006.

[93] EY: *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017* (A kiberbiztonság helyreállítása: Felkészülés a kibertámadásokra. Huszadik globális információbiztonsági felmérés, 2017), 16. o.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy és H. Lung): *Hit or myth? Understanding the true costs and impact of cybersecurity programs* (Megússzuk? A kiberbiztonsági programok valós költségei és hatása), 2017. július.

[95] Securities and Exchange Commission: *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures* (Értékpapír- és Tőzsdebizottság: Nyilatkozat és értelmezési segédlet a közvállalatok kiberbiztonsági közzétételeihez), 2018. február 21.

[96] Az Európai Bankhatóság, az Európai Értékpapír-piaci Hatóság és az Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság közötti együttműködési fórum.

[97] Európai Értékpapírpiaci Hatóság: *Joint Committee report on risks and vulnerabilities in the EU financial system* (A közös bizottság jelentése az uniós pénzügyi rendszer kockázatairól és gyenge pontjairól), 2018. április.

[98] ENISA: *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs* (Információbiztonsági és adatvédelmi normák a kkv-k számára: Ajánlások a kkv-k által elfogadott információbiztonsági és adatvédelmi normák javítására), 2015. december.

[99] Az uniós tagállamokra utalva a Bizottság tudományos tanácsadási mechanizmusa említést tett „az alapvető elvekről és értékekről való megállapodás jelentős és egyedülálló szintjéről, valamint a hatékony uniós kiberbiztonsági irányítás sarokkövét képező közös stratégiai érdek fennállásáról". Forrás: 2/2017 sz. tudományos vélemény, 2017. március 24.

[100] Egyesült Államok, Kína, Japán, Dél-Korea, India és Brazília.

[101] European Security and Defence College (T. Renard és A. Barrinha): *Handbook on cyber security, Chapter 3.4: The EU as a partner in cyber diplomacy and defence* (Kézikönyv a kiberbiztonságról, 3.4. fejezet: Az Unió mint kiberdiplomáciai és kibervédelmi partner), 2018. november 23.

[102] Az Európai Unió Tanácsa: *Cselekvési terv az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése" című, az Európai Parlamenthez és a Tanácshoz intézett közös közleményről szóló tanácsi következtetések végrehajtására*, 15748/17, 2017. december 12.

[103] Európai Bizottság: *European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission* (Az Európai Bizottság digitális stratégiája: Digitálissá alakított, felhasználó- és adatközpontú Bizottság), C(2018) 7118 final, 2018. november 21.

[104] Mariya Gabriel biztos írásbeli válasza az E-004294–17. sz. írásbeli parlamenti kérdésre, 2017. június 28.

[105] Az Európai Unió Tanácsa: *Annual Report on the Implementation of the Cyber Defence Policy Framework* (Éves jelentés a kibervédelmi politikai keret végrehajtásáról), 15870/17, 2017. december 19.

[106] Az (EU) 2015/443, 2015/444 és 2017/46 határozatok a Bizottság kommunikációs és információs rendszereinek biztonságát szabályozzák. A 2018. november 21-i C(2018) 7706 bizottsági határozat, amely a korábbi Informatikai Tanács és Információsrendszer-biztonsági Irányítótestület összevonásával létrehozza az Információtechnológiai és Kiberbiztonsági Tanácsot.

[107] Európai Gazdasági és Szociális Bizottság: uo., 2018. március.

[108] Európai Parlament: uo., 2015. szeptember.

[109] A hibrid fenyegetésekkel foglalkozó információs és elemzőcsoportot 2016-ban hozták létre az Európai Unió Helyzetelemző Központján belül az EKSZ-nél. A csoport hibrid fenyegetésekkel kapcsolatos, minősített és nyílt forrásból származó információkat kap a különböző érdekelt felektől és elemzi azokat.

[110] ENISA: *National-level Risk Assessments: An Analysis Report* (Nemzeti szintű kockázatértékelések: Elemzési jelentés), 2013. november.

[111] Európai Bizottság: *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act* (Hatásvizsgálat az Európai Uniós Kiberbiztonsági Ügynökségről és a kiberbiztonsági jogszabályról), SWD(2017) 500 final (1/6. rész), 2017. szeptember 13.

[112] Európai Bizottság: uo., SWD(2018) 403 final, 2018. szeptember 12.

[113] „Réseaux IP Européens Network Coordination Centre", Európa regionális internetnyilvántartása, amely az internetszámkészletek kiosztását és nyilvántartását felügyeli.

[114] ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs* (Az EISAS együttműködésen alapuló nagyszabású kísérleti figyelemfelhívó kampány uniós polgárok és kkv-k számára), 2012. november.

[115] Centre for Cyber Safety and Education (Kiberbiztonsági és Oktatási Központ), Booz Allen Hamilton, Alta Associates és Frost & Sullivan: *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk* (Globális alkalmazotti információbiztonsági tanulmány 2017 – A munkaerő kiberkockázatokkal kapcsolatos kapacitásának és reagálásának értékelése).

[116] Európai Gazdasági és Szociális Bizottság: uo., 2018. március.

[117] House of Lords: *House of Commons Joint Committee on the National Security Strategy, Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017–19*(Az Alsóház nemzetbiztonsági stratégiai közös bizottsága: Kiberbiztonsági készségek és az Egyesült Királyság kritikus nemzeti infrastruktúrája. A 2017–19. ülésszak második jelentése), 2018. július 16.

[118] Europol/Eurojust: *Common challenges in combating cybercrime* (Közös kihívások a kiberbűnözés elleni küzdelemben), 7021/17, 2017. március 13.

[119] Europol/Eurojust: uo., 7021/17, 2017. március 13.

[120] Európai Bizottság: uo., SWD(2018) 403 final, 2018. szeptember 12.

[121] CEPOL: *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022* (Az Igazgatótanács 33/2018/MB határozata a CEPOL 2020–2022-es időszakra vonatkozó egységes programozási dokumentumáról), 2018. november 20.

[122] Például az EKSZ, a tagállamok, valamint különféle ügynökségek és szervek (pl. CEPOL, ECTEG vagy EDSC) közötti együttműködés.

[123] ENISA: *Stock-taking of information security training needs in critical sectors* (A kritikus ágazatok információbiztonsági képzési szükségleteinek felmérése), 2017. december.

[124] Számítástechnikai Bűnözés Elleni Európai Képzési és Oktatási Csoport.

[125] Európai Bizottság: Tizenharmadik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról. COM(2018) 46 final, 2018. január 24.

[126] A 14/2018 sz. különjelentés megállapításai alapján, uo.

[127] Az Európai Parlament 2018. június 13-i állásfoglalása a kibervédelemről (2018/2004(INI)). Az Európai Unió Tanácsa: uo., 15870/17, 2017. december 19.

[128] Svájc, Macedónia Volt Jugoszláv Köztársaság, Ukrajna, Bosznia-Hercegovina, Koszovó (ez a megnevezés nem érinti a jogállással kapcsolatos álláspontokat, továbbá összhangban van az 1244/1999. sz. ENSZ BT-határozattal és a Nemzetközi Bíróságnak a koszovói függetlenségi nyilatkozatról szóló véleményével), Törökország és az Egyesült Államok.

[129] Europol: *Internet Organised Crime Threat Assessment 2018* (Az internetes szervezett bűnözés általi fenyegetettség értékelése, 2018).

[130] Európai Bizottság: uo., SWD(2017) 295 final, 2017. szeptember 13.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman és S. Furman: *Security Fatigue* (Biztonsági fásultság), "IT Professional", 18. kötet, 5. szám, 2016, 26–32. o. Lásd még: NIST.

[132] Európai Bizottság/Európai Külügyi Szolgálat: *A reziliencia és a hibrid fenyegetések kezelésére szolgáló képességek megerősítése*, JOIN(2018) 16 final, 2018. június 13.

[133] Például az AlphaBay és a Hansa bezárása az FBI és a holland nemzeti rendőrség által vezetett, az Europol támogatásával végrehajtott közös műveletek eredményeképpen. Ezek voltak a tiltott áruk – többek között kábítószerek, lőfegyverek és kiberbűnözési eszközök, például rosszindulatú szoftverek – kereskedelmének két legnagyobb piactere. Forrás: Europol: *Crime on the Dark Web: Law Enforcement coordination is the only cure* (Bűnözés a dark weben: A koordinált bűnüldözés az egyetlen gyógyszer), sajtóközlemény, 2018. május 29.

[134] Európai Bizottság: uo., SWD(2018) 403 final, 2018. szeptember 12.

[135] Az Európai Unió Tanácsa: uo., 12711/1/17 REV 1, 2017. október 9.

[136] Európai Bizottság: uo., SWD(2017) 295 final, 2017. szeptember 13.

[137] Európai Bizottság/Európai Külügyi Szolgálat: uo., JOIN (2018) 16, 2018. június 13.

[138] Európai Bizottság: SWD(2017) 500 final, 2017. szeptember 13.

[139] *Az ENISA, az EDA, az Europol EC3 és a CERT-EU közötti egyetértési megállapodás*, 2018. május 23.

[140] Az Európai Bizottság ajánlati felhívása: *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap* (A Kiberbiztonsági Kompetenciahálózatra irányuló kísérleti projekt létrehozása és működtetése egy közös kiberbiztonsági kutatási és innovációs ütemterv kidolgozása és végrehajtása céljából), 2017. október 27.

[141] Jean-Claude Juncker: Mission letter for the Commissioner for the Security Union (A Biztonsági Unióért felelős biztos megbízólevele), 2016. augusztus 2. A védelem területe nem tartozik a munkacsoport hatáskörébe.

[142] Az Európai Unió Tanácsa: *EU cybersecurity roadmap* (Az Unió kiberbiztonsági menetrendje), 8901/17, 2017. május 11.

[143] Friends of Europe: *Debating Security Plus: Crowdsourcing solutions to the world's security issues*, (Vita a biztonságról plusz: Közösségi ötletbörze a világ biztonsági kérdéseinek megoldásáról), 5. kiadás, 2017. november.

[144] A JRC technikai jelentései: *European Cybersecurity Centres of Expertise Map: Definitions and Taxonomy* (Az európai kiberbiztonsági szakértői térkép: Fogalommeghatározások és osztályozás). Impact assessment on the proposed research competence centre and network of national coordination centres (Hatásvizsgálat a javasolt kutatási kompetenciaközpontról és a nemzeti koordinációs központok hálózatáról), SWD(2018) 403 final, 2018. szeptember 12.

[145] Európai Bizottság: uo., SWD(2017) 295 final, 2017. szeptember 13.

[146] Európai Bizottság: uo., SWD(2018) 403 final, 2018. szeptember 12.

[147] Például az Európai Pénzügyi Intézetek információmegosztó és -elemző központjának tagjai között vannak a pénzügyi szektor képviselői, nemzeti CERT-ek, bűnüldöző szervek, az ENISA, az Europol, az Európai Központi Bank, az Európai Pénzforgalmi Tanács és az Európai Bizottság.

[148] ENISA: *Information Sharing and Analysis Centres (ISACs) Cooperative models* (Információmegosztó és -elemző központok (ISAC): Együttműködésen alapuló modellek), 2018. február 14.

[149] Az Európai Unió Tanácsa: uo., 12711/1/17 REV 1, 2017. október 9.

[150] https://www.europol.europa.eu/empact.

[151] Az Accenture 2018-ban 15 ország közreműködésével végzett tanulmánya megállapította, hogy a célzott kibertámadások 87% -át megakadályozzák: *2018 State of Cyber Resilience* (A kibertámadásokkal szembeni reziliencia helyzete, 2018), 2018. április 10.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy* (A kiberbiztonság a stratégiai autonómia átgondolására kényszerít), Oxford University Politics Blog, 2018. szeptember 14.

[153] Caroline Preece: *Three reasons why cyber threat detection is still ineffective* (Három ok, amiért még mindig nem eredményes a kiberfenyegetések felderítése), IT Pro, 2017. július 14.

[154] Európai Gazdasági és Szociális Bizottság: *uo.*, 2018. március.

[155] Európai Bizottság: *Nyolcadik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról*. COM(2017) 354 final, 2017. június 29.

[156] Lásd: a Kiberbiztonsági Együttműködési Csoport különböző kiadványai.

[157] PSD2: a pénzforgalmi szolgáltatásokról szóló második irányelv; EKB/SSM: Európai Központi Bank/egységes felügyeleti mechanizmus; 2. cél: a transzeurópai automatizált valós idejű bruttó elszámolású rendszer (második generáció), a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU rendelet. Forrás: CEPS-ECRI munkacsoport, uo., 2018. június.

[158] Európai Bizottság: *Ajánlás a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról*, C(2017) 6100 final, 2017. szeptember 13.

[159] Európai Bizottság: uo., SWD(2017) 295 final, 2017. szeptember 13. Számos válságkezelési mechanizmus létezik, többek között a politikai szintű integrált válságelhárítási mechanizmus (IPCR), az Argus (a Bizottság válságreagálási mechanizmusa), az EKSZ válságreagálási mechanizmusa, az uniós polgári védelmi mechanizmus és az uniós bűnüldözési vészhelyzet-elhárítási protokoll.

[160] Emellett ez az Európai Unióról szóló szerződés 42. cikkének (7) bekezdésében (kölcsönös segítségnyújtási záradék) vagy az Európai Unió működéséről szóló szerződés 222. cikkében (szolidaritási záradék) foglalt rendelkezések aktiválását is eredményezheti.

[161] Európai Bizottság/Európai Külügyi Szolgálat: uo., JOIN(2018) 16, 2018. június 13. 2018 decemberében a média az EKSZ diplomáciai kommunikációs hálózatának (COREU) állítólagos feltöréséről számolt be (forrás: *New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran* (New York Times: A meghackelt uniós csatornák szerint nagy az aggodalom Trumppal, Oroszországgal és Iránnal kapcsolatban), 2018. december 18. Az ügy vizsgálata folyamatban van.

[162] A korai figyelmeztetésekre és a kölcsönös segítségnyújtásra irányuló együttműködés is további fejlesztésre szorul: *Council Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises* (A Tanács következtetései a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálásról), 10085/18, 2018. június 26.

[163] Az Európai Parlament Kutatószolgálata: *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act* (Tájékoztató a folyamatban lévő uniós jogszabályokról: Az ENISA és az új kiberbiztonsági jogszabály), PE 614.643, 2018. szeptember.

[164] Európai Gazdasági és Szociális Bizottság: uo., 2018. március.

[165] Az Európai Unió Tanácsa: *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks* (Az uniós bűnüldözési vészhelyzet-elhárítási protokoll (LE ERP) jelentősebb határokon átnyúló kibertámadások esetére), 14893/18, 2018. december.

[166] Kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok és kölcsönös segítségnyújtás a kiberbiztonság területén; a kiberfenyegetésekkel és az eseményekre való reagálással kapcsolatos információk megosztási platformja. Forrás: Az Európai Unió Tanácsa: *Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview* (Állandó strukturált együttműködés (PESCO): a PESCO-projektek aktualizált listája – Áttekintés), 2018. november 19.

[167] Az Európai Unió Tanácsa: Következtetések a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről, 9916/17, 2017. június 7.

[168] Az Európai Unió Tanácsa: *A Tanács következtetései a kiberdiplomáciáról*, 6122/55 , 2015. február 11.

[169] Az Európai Unió Tanácsa: *A rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretére irányuló végrehajtási iránymutatások tervezete*, 13007/17.

[170] Egy-egy biztonsági esemény kapcsán a felelősség megállapítása továbbra is a tagállamok szuverén politikai döntése marad, és az eszköztárban szereplő intézkedések között vannak olyanok is, amelyek esetében nincs szükség attribúcióra.

[171] Az eszköztár nem eredményezett közös fellépést; az egyes tagállamok elfogadták az USA álláspontját.

[172] Az Európai Unió Tanácsa: *Következtetések a rossz szándékú kibertevékenységekről*, 7925/18, 2018. április 16.

[173] A különböző iparágakban – például a közműveknél, a vegyipari és ipari gyártásban, az élelmiszer-feldolgozásban, a szállítási rendszerekben és csomópontokon, valamint a logisztikai szolgáltatásoknál – az alkalmazott folyamatok ellenőrzésére használt számítógépes rendszerek.

[174] ENISA: uo., 2017. december.

[175] Például a közigazgatás, a vegyipar és az atomenergia-ipar, a feldolgozóipar, az élelmiszer-feldolgozás, az idegenforgalom, a logisztika és a polgári védelem.

[176] Európai Bizottság: uo., SWD(2017) 295 final, 2017. szeptember 13.

[177] Věra Jourová biztos beszéde az Európai Parlament plenáris ülésén: *Increasing EU resilience against the influence of foreign actors on the upcoming EP election campaign* (A közelgő európai parlamenti választási kampány külföldi szereplők általi befolyásolása elleni uniós reziliencia növelése), 2018. november 14.

[178] Carnegie Endowment for International Peace, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks* (Orosz beavatkozás a választásokba: Európa küzdelme az álhírek és a kibertámadások ellen), 2018. május 23.

[179] European Political and Strategy Centre (L. Past): *Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses* (A választási technológiák kiberbiztonsága: Elkerülhetetlen támadások, sokféle válaszlehetőség), in: *Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts* (Választási interferencia a digitális korban – Reziliencia a kibereszközökkel végrehajtandó fenyegetésekkel szemben: 35 vezető gyakorló szakember és szakértő gondolatébresztő írásainak gyűjteménye), 2018.

[180] Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK tanácsi irányelv szerint.

[181] Az Európai Bizottság ajánlása az európai parlamenti választásokkal összefüggésben a választási együttműködési hálózatokról, az online átláthatóságról, a kiberbiztonsági eseményekkel szembeni védelemről és a félretájékoztatási kampányok elleni küzdelemről. C(2018) 5949, 2018. szeptember 12.

[182] Az Európai Tanács 2015. március 20-i következtetései (EUCO 11/15). Azóta két további munkacsoport hozzáadására került sor a Nyugat-Balkán és a déli szomszédság vonatkozásában.

[183] Az Atlanti Tanács egy jelentésében felszólította az Uniót, hogy valamennyi tagállamot kötelezze arra, hogy küldjenek nemzeti szakértőket a munkacsoportba. Lásd: D. Fried és A. Polyakova: *Democratic Defense Against Disinformation* (Demokratikus védekezés a félretájékoztatás ellen), 2018. március 5.

[184] Eredetileg nem volt saját költségvetése; 2018-ban 1,1 millió eurót kapott az Európai Parlamenttől egy „StratCom Plus" előkészítő intézkedésre.

[185] Carnegie Endowment for International Peace (E. Brattberg, T. Maurer): uo., 2018. május 23.

[186] Európai Bizottság, az Unió külügyi és biztonságpolitikai főképviselője: *Cselekvési terv a félretájékoztatással szemben*, JOIN (2018) 36 final. A terv az uniós intézményeknek a félretájékoztatás felderítésére, elemzésére és nyilvánosság elé tárására irányuló képességei javítására, az összehangolt és közös reagálás megerősítésére, a magánszektor mozgósítására, valamint a tudatosság növelésére és a társadalmi reziliencia javítására összpontosít.

[187] Európai Bizottság: *Európai megközelítés az online félretájékoztatás kezelésére*, COM(2018) 236 final, 2018. április 26.

[188] Nem tévesztendő össze a jogellenes online gyűlöletbeszéd elleni magatartási kódexszel.

[189] JRC: *The digital transformation of news media and the rise of disinformation and fake news* (A hírmédia digitális átalakítása, a félretájékoztatás és az álhírek virágzása), JRC Technical Reports, JRC Digital Economy Working Paper 2018-02, 2018. április.

[190] ENISA: *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")* (A hálózat- és információbiztonság megerősítése, védelem az online félretájékoztatással („fake news", álhírek) szemben, 2018. április.

[191] European Political and Strategy Centre (C. Frutos López): *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats* (A választási szervezetek támogatása a kiberfenyegetések előrejelzésében és kivédésében), in: uo., 2018.

[192] Európai Bizottság: uo., SWD(2018) 403 final, 2018. szeptember 12.

[193] A közvetlen külföldi befektetések átvilágításáról szóló, 2017 szeptemberében benyújtott rendeletjavaslat (COM(2017) 487 final, 2018. szeptember 13.) jelenleg halad át a jogalkotási folyamaton. A rendeletjavaslat kifejezetten foglalkozik a kritikus technológiákkal, köztük a mesterséges intelligenciával, a kiberbiztonsággal és a kettős felhasználású alkalmazásokkal.

[194] Európai Bizottság/Európai Külügyi Szolgálat: uo., JOIN(2017) 450 final, 2017. szeptember 13.

A számvevőszéki munkacsoport

Az eredményes uniós kiberbiztonsági politika előtt álló kihívások című tájékoztatót a külső fellépések, biztonságpolitika és jogérvényesülés kiadási területeiért felelős, Bettina Jakobsen számvevőszéki tag elnökölte III. Kamara fogadta el. A feladat végrehajtását Baudilio Tomé Muguruza számvevőszéki tag vezette Daniel Costa de Magalhaes kabinetfőnök és Ignacio Garcia de Parada kabinetattasé, Alejandro Ballester-Gallardo ügyvezető, Michiel Sweerts feladatfelelős, valamint Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone, Silvia Monteiro Da Cunha számvevők és Johannes Bolkart gyakornok támogatásával. A nyelvi támogatást Hannah Critoph biztosította.

Balról jobbra: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes.

EURÓPAI SZÁMVEVŐSZÉK

Kiadóhivatal

EURÓPAI SZÁMVEVŐSZÉK
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Telefon: +352 4398-1

Megkeresés: eca.europa.eu/hu/Pages/ContactForm.aspx
Weboldal: eca.europa.eu
Twitter: @EUAuditors